Block-Chain Question Bank

**1-Explain permission blockchain in detail.**

**What Is a Permissioned Blockchain?**

A permissioned blockchain is a distributed ledger that is not publicly accessible. It can only be accessed by users with permissions. The users can only perform specific actions granted to them by the ledger administrators and are required to identify themselves through certificates or other digital means.

You might consider the addition of permissioned users as an extra blockchain security system. Administrators maintain an access control layer to allow certain actions to be performed only by certain identifiable participants. Records are kept within the blockchain of who is involved in the transactions. This makes permissioned blockchains different from public blockchains.

## Understanding Permissioned Blockchains

A [blockchain](https://www.investopedia.com/terms/b/blockchain.asp) can be built and accessed in multiple ways. Some blockchains need special permissions to read, access, and write information. Others only require that you have the ability to connect and can conduct work for the network. The intrinsic configuration of each blockchain controls the participants' transactions and defines their roles in which each participant can access and contribute to the blockchain.

It may also include maintaining the identity of each blockchain participant on the network. Such blockchains are called permissioned blockchains.

## Difference Between Permissionless and Permissioned Blockchains

Permissioned blockchains are similar to permissionless blockchains because they use the same technologies. However, permissioned blockchains do not allow users to access the blockchain without identification.

For example, a bank may be running a permissioned blockchain operated through a designated number of nodes internal to the bank to track money transfers. You cannot access this blockchain because you don't have the permissions required. In contrast, you could join a permissionless blockchain like a cryptocurrency mining network once you have established a semi-anonymous account in that network.

### **Benefits of Permissioned Blockchains**

There are many benefits of permissioned blockchains which makes it most preferable to use when compared with the permissionless blockchains. Let’s understand the beneficial features of permissioned blockchains with its benefits.

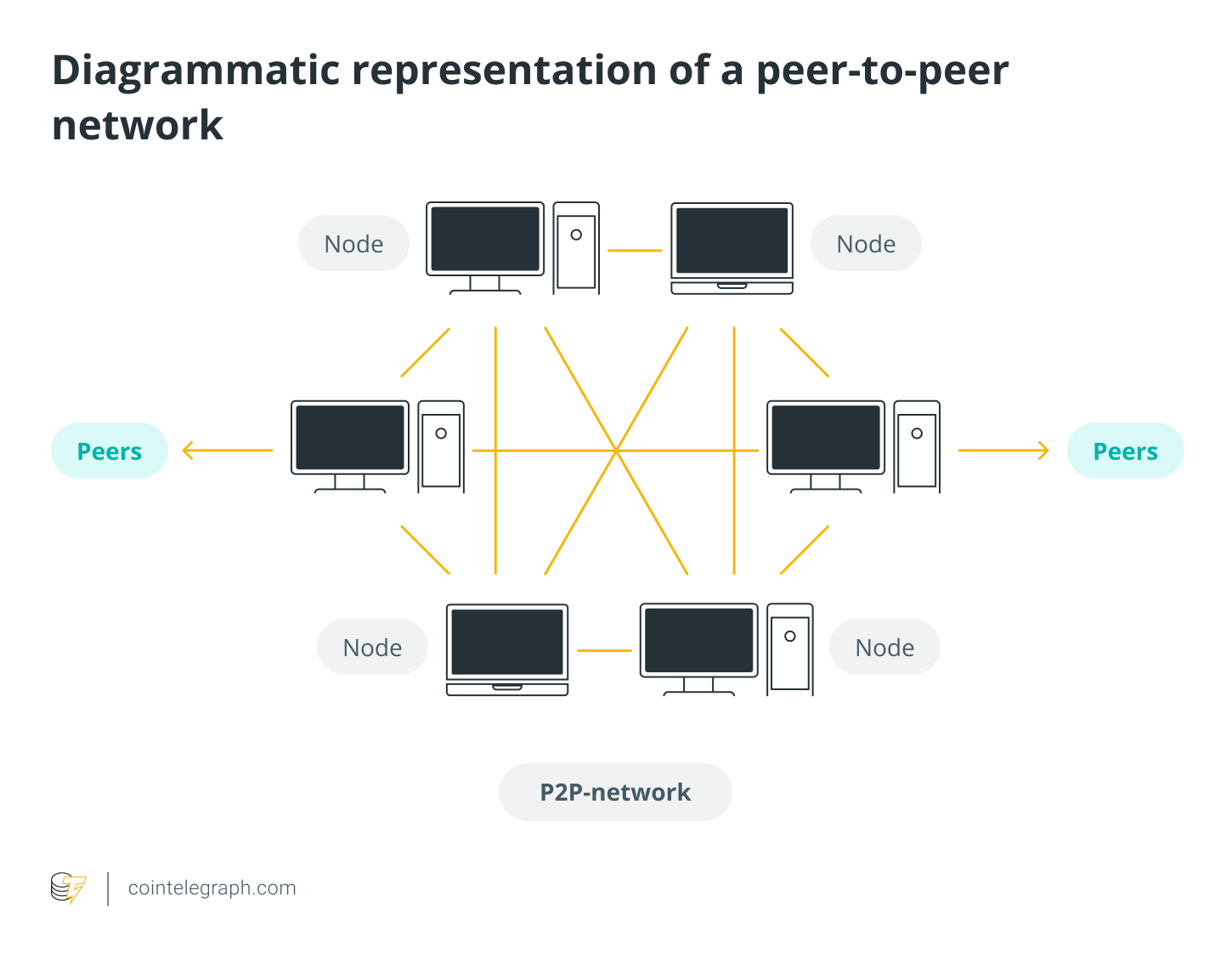
* **Efficient performance:** When we compared permissioned blockchains to permissionless blockchains, they offer better performance. The core reason behind this is the limited number of nodes on the platform. This removes the unnecessary computations required to reach consensus on the network, improving the overall performance. On top of that, permissioned networks have their own pre-determined nodes for validating a transaction.
* **Proper governance structure:** Permissioned networks do come with an appropriate structure of governance. This means that they are organized. Administrators also require less time to update the rules over the network, which is considerably faster when compared to public blockchains. The public blockchain network suffers from the consensus problem as not all nodes work together to get the new update implemented. These nodes might place their self-interest above the needs of the blockchain, which, in return, means slower updates to the whole network. In comparison, permissioned blockchain doesn’t have the problem, as the nodes work together to move the updates faster.
* **Decentralized storage:** Permissioned networks also make proper use of blockchain, including utilizing its decentralized nature for data storage.
* **Cost-Effective:** There is no doubt that permissioned blockchains are more cost-effective when compared with the permissionless blockchains.

**2-Explain decentralized and peer to peer blockchain system.**

Peer-to-Peer (P2P) technology is based on the decentralization concept, which lets network participants conduct transactions without needing any middle-man, intermediaries or central server. Peer-to-peer technology is how Bitcoin ([BTC](https://cointelegraph.com/bitcoin-price)) operates; no administrator is required to maintain track of user transactions on the network. Instead, the peers in the network cooperate to handle deals and manage the BTC.

## How do P2P networks work?

As mentioned, there are no central in peer-to-peer blockchain networks. Instead, all nodes (peers) are connected to one another. A mesh network with a “flat” topology connects the network nodes and there is no hierarchy. In a peer-to-peer network, nodes simultaneously give and consume services with reciprocity serving as the motivation for participation, making P2P networks open, decentralized and robust by nature.



Each node on the network must serve as both a client and a server to other nodes in a P2P network, making it distinct from a traditional client-server setup. There is always a central server in a client-server configuration from which the client downloads files.

On the contrary, in a decentralized setup, each node acts as a server that can download files and share them with other nodes. A node may perform both the sharing and receiving functions concurrently, which accounts for the P2P network’s speed, security and efficiency. The measures listed below can help to ensure the security of your P2P networking systems:

Furthermore, in order for new peers joining the network to readily locate other peers to connect to, P2P architecture functions best when there are many active peers in a blockchain network. It is important to note that there are still enough peers left in the network to pick up the slack if a significant number of peers leave.

However, there are fewer resources accessible overall when there are few peers. For instance, with a P2P file-sharing application, a file might be downloaded more quickly if it is popular, which indicates that many peers are sharing it.

## What are the various types of peer-to-peers (P2P) networks?

A P2P architecture can be categorized into structured, unstructured and hybrid peer-to-peer networks, as explained below.

### **Structured peer-to-peer networks**

In this type of network, nodes interact based on an organized structure, enabling nodes to precisely search for files, even if the content is unavailable. However, due to an organized system, some sort of centralization exists in structured P2P networks. Unlike unstructured peer-to-peer networks, structured peer-to-peer networks are challenging to set up, although they provide simple data access.

### **Unstructured peer-to-peer networks**

There is no set structure for the nodes in this kind of network, allowing network participants to join or leave the network as they desire. Also, due to a lack of definite structure, participants converse with one another at random. However, unstructured P2P networks require all nodes to remain active to power a high number of transactions, mandating huge CPU power to ensure that the network runs properly.

### **Hybrid peer-to-peer networks**

This type of P2P network mixes some P2P design aspects with the traditional client-server approach. For example, it makes it possible to locate a node using the central server. A distributed network application framework called the client-server architecture assigns tasks to servers and clients in the same system that connect via a computer network or the Internet.

## Benefits of P2P blockchain networks

Peer-to-peer networks offer many benefits over the traditional client-server architecture as there is no single point of failure in a distributed network of computers. On the other hand, data may get erased if the server goes down in a client-server model. Moreover, P2P networks may withstand attacks reasonably well since they are decentralized and lack a centralized server. Unlike banks, blockchains using P2P architecture cannot restrict network participants from doing a transaction.

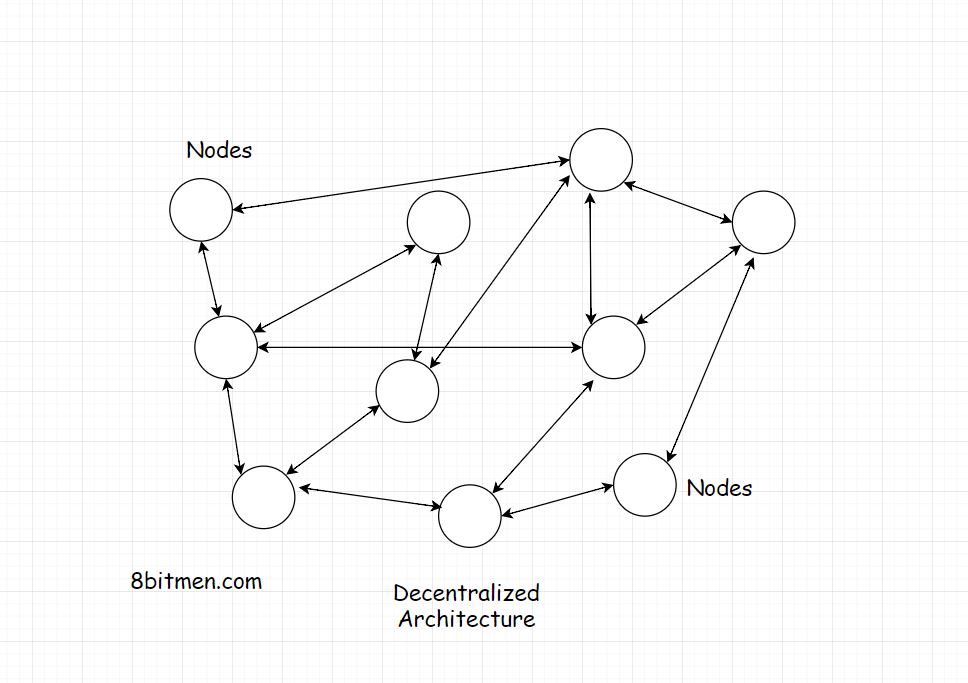
**Decentralized architecture in detail**

Decentralized simply means not centralized. The control, as opposed to with a single entity, lies with the end users. BitTorrent a [peer to peer network](https://scaleyourapp.com/p2p-peer-to-peer-networks-oversimplified-everything-you-should-know/) is an ideal example of this.  
Where the peers are responsible for the availability of content on the network. More peers seed the data, higher is the availability & download speed.

Decentralized systems just like the distributed architecture have no single points of failure. Even if several nodes go down, the network as a whole is still up.

There is no single entity control, so there is zero possibility of the network going down anytime unless all the nodes go down simultaneously which is a rare possibility when we have systems connected all over the globe.

This kind of architecture is almost infinitely scalable, unlike a centralized system in which scalability depends upon the resources of the organization in charge.



Another example of a decentralized system is blockchain. During a blockchain transaction. The participant nodes/miners decide which transactions will be preferred above the others & so on. Their computing powers decide the network throughput.

**3-Define a concept of blockchain.**

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

**Why blockchain is important:** Business runs on information. The faster it’s received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

### **Key elements of a blockchain**

#### Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.

#### Immutable records

No participant can change or tamper with a transaction after it’s been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

#### Smart contracts

To speed transactions, a set of rules — called a [smart contract](https://www.ibm.com/in-en/topics/smart-contracts) — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

### **How blockchain works**

#### As each transaction occurs, it is recorded as a “block” of data

Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.

#### Each block is connected to the ones before and after it

These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.

#### Transactions are blocked together in an irreversible chain: a blockchain

Each additional block strengthens the verification of the previous block and hence the entire blockchain. This renders the blockchain tamper-evident, delivering the key strength of immutability. This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.

## Benefits of blockchain

**What needs to change:** Operations often waste effort on duplicate record keeping and third-party validations. Record-keeping systems can be vulnerable to fraud and cyberattacks. Limited transparency can slow data verification. And with the arrival of IoT, transaction volumes have exploded. All of this slows business, drains the bottom line — and means we need a better way. Enter blockchain.

#### Greater trust

With blockchain, as a member of a members-only network, you can rest assured that you are receiving accurate and timely data, and that your confidential blockchain records will be shared only with network members to whom you have specifically granted access.

#### Greater security

Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.

#### More efficiencies

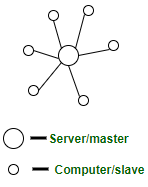
With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules — called a smart contract — can be stored on the blockchain and executed automatically.

**4-Differentiate between decentralized and centralized system**

### **CENTRALIZED SYSTEMS:**

We start with centralized systems because they are the most intuitive and easy to understand and define.

Centralized systems are systems that use client/server architecture where one or more client nodes are directly connected to a central server. This is the most commonly used type of system in many organizations where a client sends a request to a company server and receives the response.



**Example –**   
Wikipedia. Consider a massive server to which we send our requests and the server responds with the article that we requested. Suppose we enter the search term ‘junk food’ in the Wikipedia search bar. This search term is sent as a request to the Wikipedia servers (mostly located in Virginia, U.S.A) which then responds back with the articles based on relevance. In this situation, we are the client node, Wikipedia servers are the central server.

**Characteristics of Centralized System –**

* **Presence of a global clock:** As the entire system consists of a central node (a server/ a master) and many client nodes (a computer/ a slave), all client nodes sync up with the global clock (the clock of the central node).
* **One single central unit:** One single central unit which serves/coordinates all the other nodes in the system.
* **Dependent failure of components:** Central node failure causes the entire system to fail. This makes sense because when the server is down, no other entity is there to send/receive responses/requests.

**Scaling –**   
Only vertical scaling on the central server is possible. Horizontal scaling will contradict the single central unit characteristic of this system of a single central entity.

**Components of Centralized System –**   
Components of Centralized System are,

* Node (Computer, Mobile, etc.).
* Server.
* Communication link (Cables, Wi-Fi, etc.).

**Advantages of Centralized System –**

* Easy to physically secure. It is easy to secure and service the server and client nodes by virtue of their location
* Smooth and elegant personal experience – A client has a dedicated system which he uses (for example, a personal computer) and the company has a similar system which can be modified to suit custom needs
* Dedicated resources (memory, CPU cores, etc)
* More cost-efficient for small systems up to a certain limit – As the central systems take fewer funds to set up, they have an edge when small systems have to be built
* Quick updates are possible – Only one machine to update.
* Easy detachment of a node from the system. Just remove the connection of the client node from the server and voila! Node detached.

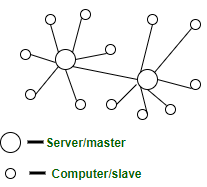
**Disadvantages of Centralized System –**

* Highly dependent on the network connectivity – The system can fail if the nodes lose connectivity as there is only one central node.
* No graceful degradation of the system – abrupt failure of the entire system
* Less possibility of data backup. If the server node fails and there is no backup, you lose the data straight away
* Difficult server maintenance – There is only one server node and due to availability reasons, it is inefficient and unprofessional to take the server down for maintenance. So, updates have to be done on-the-fly(hot updates) which is difficult and the system could break.

### **DECENTRALIZED SYSTEMS:**

These are other types of systems that have been gaining a lot of popularity, primarily because of the massive hype of Bitcoin. Now many organizations are trying to find the application of such systems.

In decentralized systems, every node makes its own decision. The final behavior of the system is the aggregate of the decisions of the individual nodes. Note that there is no single entity that receives and responds to the request.



**Example –**   
Bitcoin. Let’s take Bitcoin for example because it is the most popular use case of decentralized systems. No single entity/organization owns the bitcoin network. The network is a sum of all the nodes who talk to each other for maintaining the amount of bitcoin every account holder has.

**Characteristics of Decentralized System –**

* **Lack of a global clock:** Every node is independent of each other and hence, has different clocks that they run and follow.
* **Multiple central units (Computers/Nodes/Servers):** More than one central unit which can listen for connections from other nodes
* **Dependent failure of components:** one central node failure causes a part of the system to fail; not the whole system

**Scaling –**   
Vertical scaling is possible. Each node can add resources (hardware, software) to itself to increase the performance leading to an increase in the performance of the entire system.

**Components –**   
Components of Decentralized System are,

* Node (Computer, Mobile, etc.)
* Communication link (Cables, Wi-Fi, etc.)

**Advantages of Decentralized System –**

* Minimal problem of performance bottlenecks occurring – The entire load gets balanced on all the nodes; leading to minimal to no bottleneck situations
* High availability – Some nodes (computers, mobiles, servers) are always available/online for work, leading to high availability
* More autonomy and control over resources – As each node controls its own behaviour, it has better autonomy leading to more control over resources

**Disadvantages of Decentralized System –**

* Difficult to achieve global big tasks – No chain of command-to-command others to perform certain tasks
* No regulatory oversight
* Difficult to know which node failed – Each node must be pinged for availability checking and partitioning of work has to be done to actually find out which node failed by checking the expected output with what the node generated
* Difficult to know which node responded – When a request is served by a decentralized system, the request is actually served by one of the nodes in the system but it is actually difficult to find out which node indeed served the request.

**5-Elaborate various types of Block chain.**

## Types of Blockchains

There are primarily two types of blockchains; Private and Public blockchain. However, there are several variations too, like Consortium and Hybrid blockchains. Before we get into details of the different types of blockchains, let us first learn what similarities do they share. Every blockchain consists of a cluster of nodes functioning on a peer-to-peer (P2P) network system. Every node in a network has a copy of the shared ledger which gets updated timely. Each node can verify transactions, initiate or receive transactions and create blocks.

### **1. Public Blockchain**

A public blockchain is a non-restrictive, permission-less distributed ledger system. Anyone who has access to the internet can sign in on a blockchain platform to become an authorized node and be a part of the blockchain network. A node or user which is a part of the public blockchain is authorized to access current and past records, verify transactions or do proof-of-work for an incoming block, and do mining. The most basic use of public blockchains is for mining and exchanging cryptocurrencies. Thus, the most common public blockchains are **Bitcoin** and **Litecoin blockchains**. Public blockchains are mostly secure if the users strictly follow security rules and methods. However, it is only risky when the participants don’t follow the security protocols sincerely.

**Example:** Bitcoin, Ethereum, Litecoin

### **2. Private Blockchain**

A private blockchain is a restrictive or permission blockchain operative only in a closed network. Private blockchains are usually used within an organization or enterprises where only selected members are participants of a blockchain network. The level of security, authorizations, permissions, accessibility is in the hands of the controlling organization. Thus, private blockchains are similar in use as a public blockchain but have a small and restrictive network. Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc.

**Examples** of private blockchains are; Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.

**Must Learn –**[**Need of Hyperledger in Bitcoin**](https://data-flair.training/blogs/hyperledger-in-bitcoin/)

### **3. Consortium Blockchain**

A consortium blockchain is a semi-decentralized type where more than one organization manages a blockchain network. This is contrary to what we saw in a private blockchain, which is managed by only a single organization. More than one organization can act as a node in this type of blockchain and exchange information or do mining. Consortium blockchains are typically used by banks, government organizations, etc.

**Examples** of consortium blockchain are; Energy Web Foundation, R3, etc.

### **4. Hybrid Blockchain**

A hybrid blockchain is a combination of the private and public blockchain. It uses the features of both types of blockchains that is one can have a private permission-based system as well as a public permission-less system. With such a hybrid network, users can control who gets access to which data stored in the blockchain. Only a selected section of data or records from the blockchain can be allowed to go public keeping the rest as confidential in the private network. The hybrid system of blockchain is flexible so that users can easily join a private blockchain with multiple public blockchains. A transaction in a private network of a hybrid blockchain is usually verified within that network. But users can also release it in the public blockchain to get verified. The public blockchains increase the hashing and involve more nodes for verification. This enhances the security and transparency of the blockchain network.

**Example** of a hybrid blockchain is Dragonchain.

**6-Explain various component of Block chain system**

[Blockchain](https://www.geeksforgeeks.org/types-of-blockchain-and-chain-terminology/) is a distributed ledger where data can be stored securely such that any alteration in the data is not possible. In other words, we can also define it as a decentralized computation and information sharing platform that enables multiple authoritative domains, who coordinate in a rational decision-making process. Here, decentralized/ distributed term means that all nodes have equal priority, and they share their resources among themselves.

As per the name ‘[Blockchain](https://www.geeksforgeeks.org/features-of-blockchain/)‘, it itself suggests that information (i.e transactions) will be stored in the form of blocks. Every node can see the block, but they can’t tamper with them. If a block value is tampered the hash value associated with that block changes and that block will be disconnected from the network. On an average of 12.6 seconds, every node in the blockchain network gets the most updated blockchain. The technology behind Bitcoins is the **Blockchain Network**. Following are the components of a Blockchain network –

1. Node
2. Ledger
3. Wallet
4. Nonce
5. Hash

**1. Node –**  
It is of two types – Full Node and Partial Node.

* **Full Node** –   
  It maintains a full copy of all the transactions. It has the capacity to validate, accept and reject the transactions.
* **Partial Node** –   
  It is also called a Lightweight Node because it doesn’t maintain the whole copy of the blockchain ledger. It maintains only the hash value of the transaction. The whole transaction is accessed using this hash value only. These nodes have low storage and low computational power.

**2. Ledger –**   
It is a digital database of information.  Here, we have used the term ‘digital’ because the currency exchanged between different nodes is digital i.e. cryptocurrency. There are three types of ledger. They are –

1. **Public Ledger –**  
   It is open and transparent to all. Anyone in the blockchain network can read or write something.
2. **Distributed Ledger –**  
   In this ledger, all nodes have a local copy of the database. Here, a group of nodes collectively execute the job i.e verify transactions, add blocks in the blockchain.
3. **Decentralized Ledger –**  
   In this ledger, no one node or group of nodes has a central control. Every node participates in the execution of the job.

**3. Wallet –**  
It is a digital wallet that allows user to store their cryptocurrency. Every node in the blockchain network has a Wallet. Privacy of a wallet in a blockchain network is maintained using public and private key pairs. In a wallet, there is no need for currency conversion as the currency in the wallet is universally acceptable. Cryptocurrency wallets are mainly of two types –

1. **Hot Wallet –**  
   These wallets are used for online day-to-day transactions connected to the internet. Hackers can attack this wallet as it is connected to the internet. Hot wallets are further classified into two types –  
   **a. Online/ Web wallets –**  
   These wallets run on the cloud platform. Examples – MyEther Wallet, MetaMask Wallet.  
   **b. Software wallets –**  
   It consists of desktop wallets and mobile wallets. Desktop wallets can be downloaded on a desktop and the user has full control of the wallet. An example of a desktop wallet is Electrum.   
   **c. Mobile wallets –**  
   They are designed to operate on smartphone devices. Example – mycelium.
2. **Cold Wallet –**  
   These wallets are not connected to the internet. It is very safe and hackers cannot attack it. These wallets are purchased by the user. Example – Paper wallet, hardware wallet.   
   **a. Paper wallet –**  
   They are offline wallets in which a piece of paper is used that contains the crypto address. The private key is printed in QR code format. QR code is scanned for cryptocurrency transactions.  
   **b. Hardware wallet –**  
   It is a physical electronic device that uses a random number generator that is associated with the wallet.

The focus of wallets is on these three things –

1. Privacy
2. Transactions should be secure
3. Easy to use

Privacy of a wallet is maintained using public and private key pairs. Transactions are made secure as a private key is used both to send fund and to open the encrypted message.

**4. Nonce –**  
A nonce is an abbreviation for “number only used once,” which is a number added to a hashed or encrypted block in a blockchain. It is the 32-bit number generated randomly only one time that assists to create a new block or validate a transaction. It is used to make the transaction more secure.

It is hard to select the number which can be used as the nonce. It requires a vital amount of trial-and-error. First, a miner guesses a nonce. Then, it appends the guessed nonce to the hash of the current header. After that, it rehashes the value and compares this to the target hash. Now it checks that whether the resulting hash value meets the requirements or not. If all the conditions are met, it means that the miner has created an answer and is granted the block.

**5. Hash –**  
The data is mapped to a fixed size using hashing. It plays a very important role in cryptography. In a blockchain network hash value of one transaction is the input of another transaction. Properties of the hash function are as follows –

* Collision resistant
* Hiding
* Puzzle friendliness

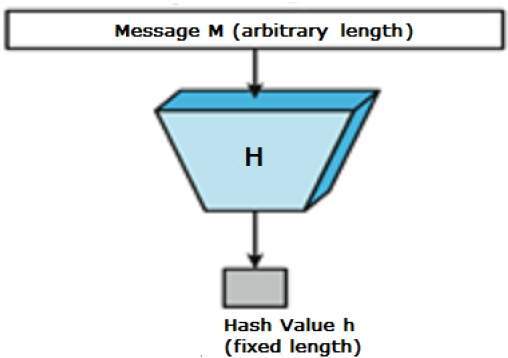
**Module 2 (15 Marks)**

**1-Explain various properties of cryptography hash Function**

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function −



## Properties of Hash Functions

In order to be an effective cryptographic tool, the hash function is desired to possess following properties −

* **Pre-Image Resistance**
  + This property means that it should be computationally hard to reverse a hash function.
  + In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
  + This property protects against an attacker who only has a hash value and is trying to find the input.
* **Second Pre-Image Resistance**
  + This property means given an input and its hash, it should be hard to find a different input with the same hash.
  + In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
  + This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.
* **Collision Resistance**
  + This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.
  + In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
  + Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.
  + This property makes it very difficult for an attacker to find two input values with the same hash.
  + Also, if a hash function is collision-resistant **then it is second pre-image resistant.**

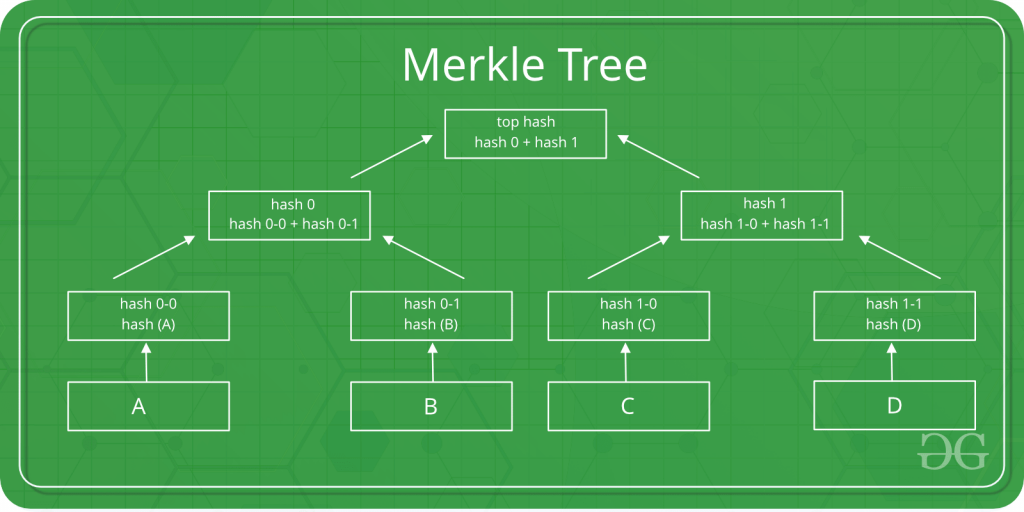
**2-Write short note on:**

**1-Merkle Tree**

Merkle tree also known as hash tree is a data structure used for data verification and synchronization.   
It is a tree data structure where each non-leaf node is a hash of its child nodes. All the leaf nodes are at the same depth and are as far left as possible.   
It maintains data integrity and uses hash functions for this purpose.

**Hash Functions:**

So before understanding how Merkle trees work, we need to understand how hash functions work.   
A hash function maps an input to a fixed output and this output is called hash. The output is unique for every input and this enables fingerprinting of data. So, huge amounts of data can be easily identified through their hash.



This is a **binary Merkel tree**, the top hash is a hash of the entire tree.

* This structure of the tree allows efficient mapping of huge data and small changes made to the data can be easily identified.
* If we want to know where data change has occurred then 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 the structure.
* The root hash is used as the fingerprint for the entire data.

**For a Binary Merkel tree**

|  |  |
| --- | --- |
| Operation | Complexity |
| Space | O(n) |
| Searching | O(logn) |
| Traversal | O(n) |
| Insertion | O(logn) |
| Deletion | O(logn) |
| Synchronization | O(logn) |

**Applications:**

* Merkle trees are useful in distributed systems where same data should exist in multiple places.
* Merkle trees can be used to check inconsistencies.
* Apache Cassandra uses Merkle trees to detect inconsistencies between replicas of entire databases.
* It is used in bitcoin and blockchain.

**2-Digital Signature**

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent.

In many countries, including the United States, digital signatures are [considered legally binding](https://www.techtarget.com/searchcontentmanagement/answer/Are-electronic-signatures-legally-binding) in the same way as traditional handwritten document signatures.

### How do digital signatures work?

Digital signatures are based on [public key](https://www.techtarget.com/searchsecurity/definition/public-key) cryptography, also known as [asymmetric cryptography](https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography). Using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), two keys are generated, creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through public key cryptography's two [mutually authenticating cryptographic keys](https://www.techtarget.com/searchsecurity/answer/Which-private-keys-and-public-keys-can-create-a-digital-signature). The individual who creates the digital signature uses a [private key](https://www.techtarget.com/searchsecurity/definition/private-key) to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key.

If the recipient can't open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated.

Digital signature technology requires all parties trust that the individual creating the signature has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder.

**3-Public key cryptography**

**Public-key cryptography**, or **asymmetric cryptography**, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a **public key** and a corresponding **private key**.[[1]](https://en.wikipedia.org/wiki/Public-key_cryptography#cite_note-rfc4949-1)[[2]](https://en.wikipedia.org/wiki/Public-key_cryptography#cite_note-2) Key pairs are generated with [cryptographic](https://en.wikipedia.org/wiki/Cryptographic) [algorithms](https://en.wikipedia.org/wiki/Algorithms) based on [mathematical](https://en.wikipedia.org/wiki/Mathematical) problems termed [one-way functions](https://en.wikipedia.org/wiki/One-way_function). Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security.[[3]](https://en.wikipedia.org/wiki/Public-key_cryptography#cite_note-3)

In a **public-key encryption** system, anyone with a public key can [encrypt](https://en.wikipedia.org/wiki/Encryption) a message, yielding a **ciphertext**, but only those who know the corresponding private key can decrypt the ciphertext to obtain the original message.[[4]](https://en.wikipedia.org/wiki/Public-key_cryptography#cite_note-hac-pke-4)

For example, a journalist can publish the public key of an encryption key pair on a web site so that sources can send secret messages to the news organization in ciphertext. Only the journalist who knows the corresponding private key can decrypt the ciphertexts to obtain the sources' messages—an eavesdropper reading email on its way to the journalist can't decrypt the ciphertexts. However, public-key encryption doesn't conceal [metadata](https://en.wikipedia.org/wiki/Metadata) like what computer a source used to send a message, when they sent it, or how long it is. Public-key encryption on its own also doesn't tell the recipient anything about who sent a message—it just conceals the content of a message in a ciphertext that can only be decrypted with the private key.

In a [**digital signature**](https://en.wikipedia.org/wiki/Digital_signature) system, a sender can use a private key together with a message to create a **signature**. Anyone with the corresponding public key can verify whether the signature matches the message, but a forger who doesn't know the private key can't find any message/signature pair that will pass verification with the public key.[[5]](https://en.wikipedia.org/wiki/Public-key_cryptography#cite_note-hac-digsig-5)[[6]](https://en.wikipedia.org/wiki/Public-key_cryptography#cite_note-djb-forgery-6)

For example, a software publisher can create a signature key pair and include the public key in software installed on computers. Later, the publisher can distribute an update to the software signed using the private key, and any computer receiving an update can confirm it is genuine by verifying the signature using the public key. As long as the software publisher keeps the private key secret, even if a forger can distribute malicious updates to computers, they can't convince the computers that any malicious updates are genuine.

**3-Elaborate use of hash function and digital signature of block chain**

Businesses today are in search of innovative ways to safeguard information. One way that businesses have found is blockchain. Blockchain technologies have not only transformed how data is stored and secured, but also how business is conducted.

Their decentralized and distributed nature has businesses adopt powerful protocols to secure data. The technology ensures the expulsion of all unwanted and undesired parties like governments, banks, and other intermediaries that pose several restrictions and difficulties in conducting business.

Blockchain technology makes use of cryptographic hashing and digital signature systems of information security. Cryptographic hashing and digital signature aren’t unique to blockchains. However, with the technology’s distributed ledger system, they boost the security systems.

## What is Hashing in Blockchain Technology?

In terms of security and privacy, hashing refers to the process of mapping arbitrary size of data and generating a specific digit mathematical value for it, known as a “hash value”, “message”, or simply “hash”. Even the slightest change in the data will modify the hash value.

This hash value is one-way and indeterministic meaning it is impossible to reverse-engineer the cryptographic hash function and reproduce the underlying original data.

The original data input could be of any size; however, the produced hash value will be of a specific digit. The hashing function is largely used in blockchain when adding new blocks to the blockchain. Every block on the network contains data and is secured via cryptographic hashes. The keys to these blocks are with the owner of the data.

However, once the data is stored in a block it becomes immutable meaning it cannot be changed or deleted and stays there forever.

There are various hashing procedures or protocols tailored for a variety of requirements of users. Hashes have several use cases and one of the most popular among them is digital fingerprinting. A digital fingerprint is quite similar to an actual fingerprint just that you hash the digital fingerprint for verifying them.

The hash value acts as confirmation concerning producing the output from the procedure. Moreover, it also confirms whether the output had been subject to any attempts of tampering.

## Digital Signatures in Blockchain

Let us now understand what digital signatures are in blockchain. Digital signatures enable trust and uprightness in a blockchain network. They are cryptographic proof systems and perform a major role in the verification process.

“Trust in the blockchain system could ensure proving that the message could originate from a particular source, thereby ruling out any concerns of hacking or other discrepancies. Digital signatures can be considered as the digital counterparts of stamped seals or handwritten signatures. “

Digital signatures have the power to offer better security levels by curbing the possibilities of identity breaches. Digital signatures applications are popularly found in use cases like digital use cases to send and receive money or digital assets like cryptocurrencies and NFTs.

They provide users with two keys, a public key and a private key, that have mathematical links to each other.

**4-Expalin various cryptography techniques**

Various cryptography techniques have been developed to provide data security to ensure that the data transferred between communication parties is confidential, not modified by an unauthorized party, to prevent hackers from accessing and using their information.  Caesar cipher, monoalphabetic cipher, homophonic substitution cipher, Polyalphabetic Cipher, Playfair cipher, rail fence, One-time pad, hill cipher are some of the examples of cryptography techniques.

### **Top 5 Cryptography Techniques**

Here are some very easy codes and more complex modern [encryption](https://www.educba.com/what-is-encryption/) technologies used on the Internet today.

#### 1) Simple Codes

* This category is any way of writing a message by side that it is difficult for anyone else to read. That involves writing stuff in another alphabet. Here we can see that Icelandic runes and IPA and another niche built alphabets such as the Deseret Alphabet.
* In this, we can use language to code. We have looked into the creation of created languages such as Elvish and Esperanto.
* Chester Naz and Judith Schiess Avila’s book Code Talker is a book that explains how the Navajo language had been used as a code in the Second World War and never was cracked into extremely intense conditions.
* If Navajo had no words for a particular notion, the code speakers chose a term instead. The Navajo word for ‘hummingbird, ‘for example, had become a fighter plane, and ‘iron hat ‘was Germany.

#### 2) Symmetric Encryption

* Symmetrical encryption is a type of encryption that is used for the [encryption and decryption](https://www.educba.com/encryption-vs-decryption/) of electronic data by just one key (a secret key). Substitution ciphers are symmetrical encryption techniques, but modern symmetric encryption can be much more complicated.
* Data are converted to a method that anyone cannot understand without a secret key to decrypt it using symmetrical encryption algorithms.
* Symmetric encryption is an old algorithm, but it is faster and efficient than asymmetric encryption. Because of great performance and fast speed of symmetric as compare to asymmetric encryption.
* Whereas Symmetric key cryptography involves the usage of the same key for encryption and decryption. At the same time, Asymmetric key cryptography involves using one key for encryption and another different key for decryption.
* Symmetric encryption is typical for big quantities of information, e.g. for database encryption, in bulk encryption. In the case of a database, the secret key can only be encrypted or decrypted by the database itself.

We can see the working of Symmetric encryption in the picture given below:

**Two kinds of symmetrical encryption algorithms are available:**

1. Block algorithm
2. Stream algorithm

**A) Block Algorithm**

The set of bits is encoded with a specific secret key in electronic data blocks. The system keeps the data in its memory while it is waiting to get complete blocks when the data are encrypted. Some important Block cipher algorithms are DES, Triple DES, [AES](https://www.educba.com/advanced-encryption-standard/), etc.

**B) Stream Cipher Algorithm**

In this, Plain text numbers or characters are combined with pseudorandom cipher digit stream. Some important Stream cipher algorithms are RC4, A5, BLOWFISH, etc. In [symmetric key encryption](https://www.educba.com/symmetric-key-encryption/), The encryption code can be cracked if someone finds out the symmetric key. But this problem can be overcome with the Diffie-Hellman algorithm. In the Diffie-Hellman key exchange or agreement algorithm, the sender and receiver must agree on a symmetric key using this technique. This key can then be used for encryption or decryption purpose.

#### 3) Asymmetric Encryption

* [Asymmetric encryption](https://www.educba.com/asymmetric-encryption/) is also called public-key cryptography. Asymmetric key encryption helps to resolve a key exchange problem of symmetric key Cryptography. In Asymmetric encryption, Two keys are used to encrypt plain text in asymmetrical encryption. Through the internet or big network, the secret keys are exchanged. It is necessary to notice that anyone with a secret key can decrypt the message, so asymmetric encryption uses two corresponding keys to increase safety.
* Anyone who wishes to send you a message will have a public key freely accessible, but the second private key is held the secret for you to understand you only. A message encrypted with a public key can be decoded with a private key. A message encrypted with a private key can also be decrypted with a public key.

We can see the working of Asymmetric encryption in the picture given below:

#### 4) Steganography

* Steganography is a technique that facilitates the hiring of a message that is to be kept secret inside other messages. Earlier, people used methods to hide messages such as invisible ink, minute variations, etc.
* But in an age of technology, [Steganography](https://www.educba.com/steganography-techniques/) is a technique to conceal data that can be the file, message, image, etc., inside other files, message or images.

#### 5) Hashing

* Hashing is the cryptographic technique that converts data that can be any form into a unique string. Regardless of size or type, any data can be hashed using a hashing algorithm. It takes data of random length and converts it into a fixed hashed value.
* Hashing is different from other encryption methods because, in hashing, encryption cannot be reversed; that is cannot be decrypted using keys. MD5, SHA1, SHA 256 is the widely used hashing algorithms.

**Module 3 (20 Marks)**

**1-Explain process of creation of coins in bitcoins**

**2-Explain the concession mechanism in bitcoin (pow,pos).**

A consensus mechanism is a fault-tolerant mechanism that is used in computer and [blockchain](https://www.investopedia.com/terms/b/blockchain.asp) systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with [cryptocurrencies](https://www.investopedia.com/terms/c/cryptocurrency.asp). It is useful in record-keeping, among other things.

On the [Bitcoin](https://www.investopedia.com/terms/b/bitcoin.asp) blockchain, for instance, the consensus mechanism is known as Proof-of-Work (PoW), which requires the exertion of computational power in order to solve a difficult but arbitrary puzzle in order to keep all nodes in the network honest.

## Consensus Mechanism Explained

In any centralized system, like a database holding key information about driving licenses in a country, a central administrator has the authority to maintain and update the database. The task of making any updates—like adding/deleting/updating names of people who qualified for certain licenses—is performed by a central authority who remains the sole in-charge of maintaining genuine records.

Public blockchains that operate as decentralized, self-regulating systems work on a global scale without any single authority. They involve contributions from hundreds of thousands of participants who work on verification and authentication of transactions occurring on the blockchain, and on the [block mining activities](https://www.investopedia.com/tech/how-does-bitcoin-mining-work/).

In such a dynamically changing status of the blockchain, these publicly shared ledgers need an efficient, fair, real-time, functional, reliable, and secure mechanism to ensure that all the transactions occurring on the network are genuine and all participants agree on a consensus on the status of the ledger. This all-important task is performed by the consensus mechanism, which is a set of rules that decides on the legitimacy of contributions made by the various participants (i.e., nodes or transactors) of the blockchain.

## Blockchain Consensus Mechanisms

There are different kinds of consensus mechanism algorithms, each of which works on different principles.

The [proof of work (PoW)](https://www.investopedia.com/terms/p/proof-work.asp) is a common consensus algorithm used by the most popular cryptocurrency networks like [bitcoin](https://www.investopedia.com/terms/b/bitcoin.asp) and [litecoin](https://www.investopedia.com/terms/l/litecoin.asp). It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain. However, this whole mining mechanism of bitcoin needs high energy consumption and a longer processing time.

The [proof of stake (PoS)](https://www.investopedia.com/terms/p/proof-stake-pos.asp) is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. It involves the allocation of responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it. However, this comes with the drawback that it incentivizes cryptocoin hoarding instead of spending.

While PoW and PoS are by far the most prevalent in the blockchain space, there are other consensus algorithms like [Proof of Capacity](https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp) (PoC) which allow sharing of memory space of the contributing nodes on the blockchain network. The more memory or hard disk space a node has, the more rights it is granted for maintaining the public ledger. [Proof of Activity](https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp) (PoA), used on the [Decred](https://www.investopedia.com/news/decred-cryptocurrency-combines-pow-pos/) blockchain, is a hybrid that makes use of aspects of both PoW and PoS. [Proof of Burn](https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp) (PoB) is another that requires transactors to send small amounts of cryptocurrency to inaccessible wallet addresses, in effect "burning" them out of existence.

Or

**Elaborate various objective of Concession Mechanism of Bitcoin / mining process**

**4-Write short note on**

**1-Double Spending**

Blockchain is a list of blocks. Each block comprises some information associated with some hash. Blockchain is used nowadays widely for transactions. It is an immutable, distributed, and decentralized ledger. The working of Blockchain is as follows.  Suppose a user wants to make a transaction. A block is created and sent to other users. Users validate the block and the transaction gets executed. The block is added and the users get incentives.

### Understanding Double Spending

Although Blockchain is secured, still it has some loopholes. Hackers or malicious users take advantage of these loopholes to perform their activities.

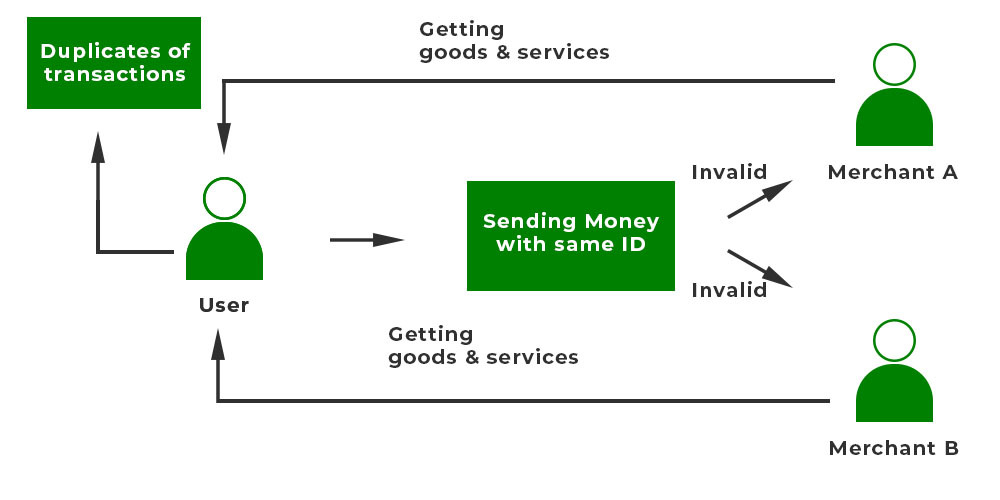
* [Double spending](https://www.geeksforgeeks.org/solutions-to-prevent-double-spending-of-bitcoins/) means the expenditure of the same digital currency twice or more to avail the multiple services. It is a technical flaw that allows users to duplicate money.
* Since digital currencies are nothing but files, a malicious user can create multiple copies of the same currency file and can use it in multiple places.
* This issue can also occur if there is an alteration in the network or copies of the currency are only used and not the original one.
* There are also double spends that allow hackers to reverse transactions so that transaction happens two times.
* By doing this, the user loses money two times one for the fake block created by the hacker and for the original block as well.
* The hacker gets incentives as well for the fake blocks that have been mined and confirmed.

### How Does Double Spending Happen?

Double spending can never arise physically. It can happen in online transactions. This mostly occurs when there is no authority to verify the transaction. It can also happen if the user’s wallet is not secured. Suppose a user wants to avail of services from Merchant ‘A’ and Merchant ‘B’.

* The user first made a digital transaction with Merchant ‘A’.
* The copy of the cryptocurrency is stored on the user’s computer.
* So, the user uses the same cryptocurrency to pay Merchant ‘B’
* Now both the merchants have the illusion that the money has been credited since the transactions were not confirmed by the miners.

This is the case of double spending.



**Example:**Suppose a user has 1 BTC. He/she wants to avail of services from merchant A and merchant B. The user creates multiple copies of the same BTC and stores it. The user first sends the original BTC to Merchant A and gets the service. Simultaneously, the user sends the copied version of 1 BTC to Merchant B. Since the second transaction was not confirmed by other miners, the merchant accepts the bitcoin and sends the service. But the cryptocurrency that was sent is invalid. This is the case of Double Spending.

**2-Bitcoin Script into FORTH**

**Module:4 (10/15 Marks)**

**1-Explain distributed concession mechanism in detail**

A procedure to reach a common agreement in a distributed or decentralized multi-agent platform. It is important for the message passing system.

**Example** –

A number of processes in a network decide to elect a leader. Each process begins with a bid for leadership. In traditional or conventional distributed systems, we apply consensus to ensure reliability and fault tolerance. It means, in a decentralized environment when you have multiple individual parties, and they can make their own decision, then it may happen that some node or some parties are working maliciously or working as a faulty individual.  So in those particular cases, it is important to come to a decision or common point of view. So having a common point of view in an environment where people can behave maliciously or people can crash the work in a faulty way, is the main difficulty. So under this kind of distributed environment, our objective is to ensure reliability which means to ensure correct operation in the presence of faulty individuals.

**Features:**

* It ensures reliability and fault tolerance in distributed systems.
* In the presence of faulty individuals, it is Ensure correct operations.

**Examples** –

Commit a transaction in a database, State machine replication, Clock synchronization.

**How to achieve distributed consensus:**

There are some conditions that need to be followed in order to achieve distributed consensus.

* **Termination –**  
  Every non-faulty process must eventually decide.
* **Agreement –**  
  The final decision of every non-faulty process must be identical.
* **Validity –**  
  Every non-faulty process must begin and ends with the same value.
* **Integrity –**  
  Every correct individual decides at most one value, and the decided value must be proposed by some individual.

Here is one validation criterion, so basically, we should reach a decision with a value that must be the initial value of some process because it is silly to reach an agreement when the agreed value reflects nobody’s initial choice.

**The correctness of Distributed Consensus Protocol:**

It can be described by the following two properties as follows.

* **Safety Property –**  
  It ensures that you will never converge to an incorrect value or correct individuals in a network will never converge to an incorrect value.
* **Liveness Property –**  
  It states that every correct value must be accepted eventually which means something good will eventually happen.

**Application of Distributed Consensus:**

* Leader election in a fault-tolerant environment for initiating some global action without introducing a single point of failure.
* Maintaining consistency in a distributed network. Suppose you have different nodes monitoring the same environment. If one of the nodes crashes, a consensus protocol ensures robustness against such faults.

**Or**

**Explain various faults in DC**

**2-Expalin the process of smart contracts**

## Smart contracts: contracts to formalise agreements in the digital age

The smart contract is written in virtual language and has the power to execute and enforce itself, autonomously and automatically, based on a series of programmed parameters. With blockchain technology, its main value lies in reinforcing security, transparency and trust between signatories, avoiding misunderstandings, falsifications or alterations and dispensing with intermediaries.

Smart contracts promise to strengthen trust, security and transparency between the parties.

When we buy a house, we have to sign a sales contract with the seller, but this is not a simple process: we need a bank, a notary, a land registry and a lot of paperwork. **Smart contracts,** which have emerged from [blockchain](https://www.iberdrola.com/innovation/blockchain-how-it-works-and-its-applications), technology, promise to simplify this type of process as much as possible.

### **WHAT IS A SMART CONTRACT?**

A smart contract is an agreement between two people or entities in the form of computer code programmed to execute automatically. The idea was proposed in the 1990s by **Nick Szabo,** a pioneer of modern computer science, who defined them as a set of virtual promises with associated protocols to enforce them. The Bitcoin protocol, which basically records the proof of a payment, can be seen as a primitive version of a smart contract.

Smart contracts are executed on blockchain, which means that the terms are stored in a distributed database and cannot be changed. Transactions are also processed on the blockchain, which automates payments and counterparties. Since the emergence of the digital currency **Ethereum,** the creation and execution of smart contracts has been simplified, as complex transactions can be programmed into the Ethereum protocol.

### **HOW DOES A SMART CONTRACT WORK?**

The operation of a smart contract is similar to other **blockchain** transfers. These are the necessary steps:

1. A user initiates a transaction from their **blockchain** wallet.

2. The transaction arrives at the distributed **database,** where the identity is confirmed.

3. The transaction, which may be a **transfer** of funds, is approved.

4. The transaction includes the **code** that defines what type of transaction is to be executed.

5. The transactions are added as a **block** within the blockchain.

6. Any change in **contract** status follows the same process to be updated.

### **SMART CONTRACT APPLICATIONS (EXAMPLES)**

Smart contracts have applications in all areas where traditional contracts are currently signed:

**Records**

Smart contracts will facilitate the storage and maintenance of records. For example, the millions of confidential patient records that need to be securely stored and updated.

**Trade**

Most commercial activities depend on the approval of their funding, which is a time-consuming and resource-intensive process. Thanks to smart contracts, this time can be dramatically reduced.

**Supply chains**

[Internet of Things](https://www.iberdrola.com/innovation/internet-of-things-iot) devices can be used throughout the supply chain to record every step of a product and improve its traceability. In this way, errors, theft and loss can be eliminated.

**Mortgages**

Mortgage transactions based on smart contracts will be cheaper, faster and safer. This will allow buyers to access the property earlier and update the records automatically.

**Property market**

Smart contracts can be used to register property ownership more efficiently. Moreover, their use can extend beyond flats, buildings or land and register all types of assets.

**Module:5 (20 Marks)**

**1-Expalin the structure of Block and transaction in Ethereum platform**

**2-Explain various features of hyper ledger and elaborate its transaction**

For each and every transaction in the fabric, the following steps are followed-

1. **Creation of the proposal:**Imagine a deal between a smartphone manufacturer company and a smartphone dealership. The transaction begins when a member organization proposes or invokes a transaction request with the help of the client application or portal. Then the client application sends the proposal to peers in each organization for endorsement.
2. **Endorsement of the transaction:**After the proposal reaches the endorser peers (peers in each organization for endorsement of a proposal) the peer checks the fabric certificate authority of the requesting member and other details that are needed no authenticate the transaction. Then it executes the chain code (a piece of code that is written in one of the supported languages such as Go or Java) and returns a response. This response indicates the approval or rejection of the following transaction. The response is carried out to the client.
3. **Submission to ordering service:**After receiving the endorsement output, the approved transactions are sent to the ordering service by the client-side application. The peer responsible for the ordering service includes the transaction into a specific block and sends it to the peer nodes of different members of the network.
4. **Updating the ledger:**After receiving this block the peer nodes of such organizations update their local ledger with this block. Hence the new transactions are now committed.

### **Benefits Of Hyperledger Fabric**

**1. Open Source:**Hyperledger fabric is an open-source blockchain framework hosted by the Linux foundation. It has an active community of developers The code is designed to be publicly accessible. Anyone in the community can see, modify, and distribute the code as they see fit. People across the world can come and help to develop the source code.

**2. Private and Confidential:**In a public blockchain network each and every node in the network is receiving a copy of the whole ledger. Thus keeping privacy becomes a much bigger concern as everything is open to everyone. In addition to this one, the identities of all the participating members are not known and authenticated. Anyone can participate as it is a public blockchain. But in the case of Hyperledger fabric, the identities of all participating members are authenticated. And the ledger is only exposed to the authenticated members. This benefit is the most useful in industry-level cases, like banking, insurance, etc where customer data should be kept private.

**3. Access  Control:**In the Hyperledger fabric, there is a virtual blockchain network on top of the physical blockchain network. It has its own access rules. It employs its own mechanism for transaction ordering and provides an additional layer of access control. It is especially useful when members want to limit the exposure of data and make it private. Such that it can be viewed by the related parties only. As an example when two competitors are on the same network. The fabric also offers private data collection and accessibility, where one competitor can control the access to its own data such that the data do not get exposed to the other competitor.

**4. Chaincode Functionality:**It includes a container technology to host smart contracts called chain code that defines the business rules of the system. And it’s designed to support various pluggable components and to accommodate the complexity that exists across the entire economy. This is useful for some of the specific types of transactions like asset ownership change.

**5. Performance:**As the Hyperledger fabric is a private blockchain network, There is no need to validate the transactions on this network so the transaction speed is faster, resulting in a better performance.

**3-Explain an architecture of Hyper Nature Fabric**

### **Modular Architecture**

The modular architecture of Hyperledger Fabric separates the transaction processing workflow into three different stages: [smart contracts](https://www.investopedia.com/terms/s/smart-contracts.asp) called chaincode that comprise the distributed logic processing and agreement of the system, transaction ordering, and transaction validation and commitment.67 This segregation offers multiple benefits:

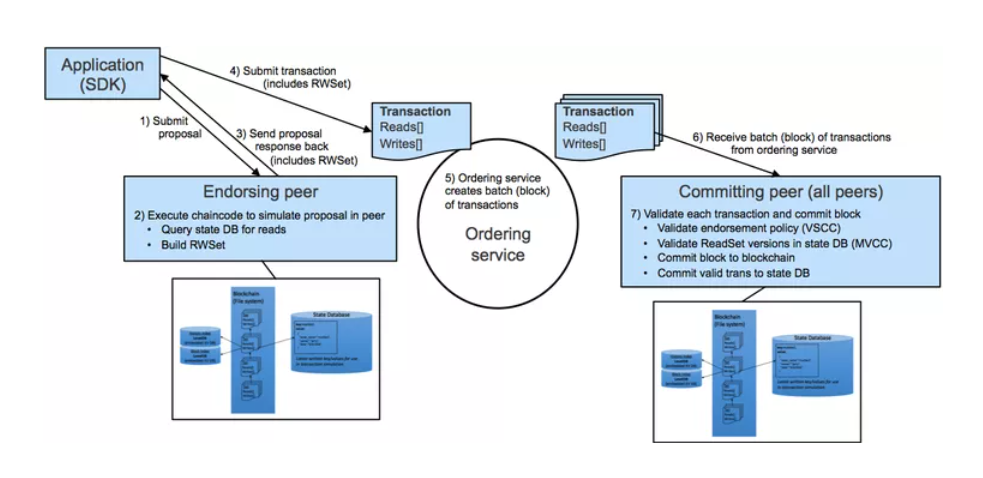
* A reduced number of trust levels and verification that keeps the network and processing clutter-free
* Improved network scalability
* Better overall performance

Additionally, Hyperledger Fabric’s support for plug-and-play of various components allows for easy reuse of existing features and ready-made integration of various modules. For instance, if a function already exists that verifies the participant’s identity, an enterprise-level network simply needs to plug and reuse this existing module instead of building the same function from scratch.

The participants on the network have three distinct roles:

* Endorser
* Committer
* Consenter

In a nutshell, the transaction proposal is submitted to the endorser peer according to the predefined endorsement policy about the number of endorsers required. After sufficient endorsements by the endorser(s), a batch or block of transactions is delivered to the committer(s). Committers validate that the endorsement policy was followed and that there are no conflicting transactions. Once both the checks are made, the transactions are committed to the ledger.



Since only confirming instructions—such as signatures and read/write set—are sent across the network, the scalability and performance of the network is enhanced. Only endorsers and committers have access to the transaction, and security is improved with a fewer number of participants having access to key data points.

**4-Write short note on**

**1-Membership and Identity management in hyper-ledger**

# Hyperledger Fabric Functionalities

Hyperledger Fabric is an implementation of distributed ledger technology (DLT) that delivers enterprise-ready network security, scalability, confidentiality and performance, in a modular blockchain architecture. Hyperledger Fabric delivers the following blockchain network functionalities:

## Identity management

To enable permissioned networks, Hyperledger Fabric provides a membership identity service that manages user IDs and authenticates all participants on the network. Access control lists can be used to provide additional layers of permission through authorization of specific network operations. For example, a specific user ID could be permitted to invoke a chaincode application, but blocked from deploying new chaincode.

**2-Gossip Protocols**

# Gossip Protocol

The term gossip protocol refers to a specific type of P2P (peer-to-peer) communication that takes place between computers and other digital devices. The coinage of the term was inspired by the conventional form of gossip that is common within social groups.

In the context of computer science, gossip protocol is related to a kind of communication that takes place when data is transmitted through different computer [nodes](https://academy.binance.com/en/articles/what-are-nodes), which are part of a distributed network. As the name suggests, a gossip protocol communication takes place when information is broadcasted from one computer to another until it is eventually spread all across the network. Currently, there are numerous variants of the Gossip protocol that can be applied to different scenarios depending on the needs of the user or organization.

there are [two](http://publicatio.bibl.u-szeged.hu/1529/1/gossip11.pdf) main types of Gossip manifestation: information dissemination and information aggregation. These two types are key elements of large-scale distributed systems.

On the one hand, gossip dissemination, also known as multicast, relates to the traditional way of data distribution (one network node at a time). On the other hand, the aggregating gossip protocols are the ones that process data, i.e., that first summarize information and then distribute it (this type of gossip communication may also be referred to as distributed data mining).

An interesting example of a distributed system that uses a gossip protocol is the Hashgraph created by Leemon Baird in 2016. It is a distributed ledger technology that employs an asynchronous [Byzantine Fault Tolerance](https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained) (aBFT) [consensus algorithm](https://academy.binance.com/en/articles/what-is-a-blockchain-consensus-algorithm). The nodes of a Hashgraph network gather and summarize information about transactions and other events and spread this data to other neighbor nodes that are chosen randomly. So instead of building a chain of blocks, the Hashgraph network builds a tree of events where all information is recorded (no data is ever discarded).

**Module:6 (10 Marks)**

**1-Application scope of Block chain in Gout**

# How blockchain can transform government sector: E-government, e-voting, e-identities and e-documents

The excitement around the applicability of blockchain in the public sector is building at a large scale. Government agencies have started testing blockchain technology’s potential to improve the public sector. However, the technology’s application in the public sector remains in the experimental stages.

Blockchain-based solutions could shift governments away from siloed and inherently insecure centralized systems. Public blockchains may transform the foundations upon which every government sector operates.

Blockchain technology could [accelerate key government functions](https://cointelegraph.com/news/blockchain-will-transform-government-services-and-that-s-just-the-beginning). Such functions entail identity verification and certifying transactions such for land-use registry and safekeeping of medical records.

Having realized the technology’s potential, governments worldwide are exploring ways to integrate blockchains into government functions.

This article discusses the benefits of applying blockchain in the government. But, before answering the question “What are the benefits of blockchain to society?” it’s best to examine the underpinnings of this novel technology first.

## Why should governments use blockchain technology?

States can gain many advantages from using blockchain technology in their governmental infrastructure. One fundamental role of governments is to store and manage sensitive information. States store details about their citizens, assets, organizations and activities.

Storing sensitive public data while maintaining data privacy can be complex and cost-intensive. Even first-world governments routinely fail to prevent data leaks.

Centralized government systems are inefficient and inherently costly and insecure. Governments everywhere have been actively seeking novel technologies to offer improved public services that are also cost effective.

A government relying on blockchain technology could simplify the management of trusted information. The state can do so while protecting against unauthorized access and data manipulation.

A blockchain-based system has several attributes that may be of great use in government. Several reasons why governments should use blockchain technology are outlined below.

**2-Explain an application of supply chain management in Block chain**

**The following examples are the applications of Blockchain in the supply chain**.

#### **Automotive Supplier Payments**

Blockchain allows the transfer of funds anywhere in the world without the need for traditional banking transactions, as transactions are made directly between payer and payee. It is also secure and rapid; taking minutes, compared to days for automated clearing house payments, for example.

Bitcoin transfers specifically also incur lower fees. Australian vehicle manufacturer Tomcar uses Bitcoin to pay some of its suppliers. Currently, three partners in Israel and Taiwan accept payment from Tomcar using Bitcoin.

Tomcar’s supplier agreements use standard terms. The advantage is in the cost savings. On the other hand, the firm is careful to avoid hanging onto too much Bitcoin. While Bitcoin is international by nature, some national governments see it as a way for companies to invest. Companies may therefore be subject to taxation on Bitcoin holdings.

#### **Meat Traceability**

Companies can use distributed ledger systems (blockchains) to record product status at each stage of production. The records are permanent and immutable. They make it possible to trace each product to its source. Global retailer Walmart uses blockchain to track sales of pork in China. Its system lets the company see where each piece of meat comes from, each processing and storage step in the supply chain, and the products’ sell-by date. In the event of a product recall, the company can also see which batches are affected and who bought them.

#### **Electric Power Micro-grids**

This example shows how entities of any size can use blockchain. In other words, blockchain is not just for the big players. Smart contracts are being used to redistribute excess power from solar panels. The Transactive Grid is an application running on blockchain to monitor and redistribute energy in a neighbourhood micro-grid. The program automates the buying and selling of green energy to save costs and pollution. The process uses the Ethereum blockchain platform, designed specifically for building and executing smart contracts.

#### **RFID-driven Contract Bids and Execution**

RFID tags are commonly used in supply chain to store information about products. IT systems can read the tags automatically and then process them. Therefore, the logic goes; why not use them for smart contracts in logistics?

The possible setup could be as follows. RFID tags for cartons or pallets store information on delivery location and date. Logistics partners run applications to look for these tags and bid for a delivery contract. The partner offering optimal price and service gets the business. A smart contract then tracks status and final delivery performance.

#### **Cold Chain Monitoring**

Food and pharmaceutical products often have specialised storage needs. Moreover, enterprises see the value in sharing warehouses and distribution centres instead of each one paying for its own. Sensors on sensitive products can record temperature, humidity, vibration, and other environmental conditions.

These readings can then be stored on a blockchain. They are permanent and tamper-proof. If a storage condition deviates from what is agreed, each member of the blockchain will see it. A smart contract can trigger a response to correct the situation. For instance, depending on the size of the deviation, the action may be to adjust the storage. However, it could also extend to changing “use-by” dates, declaring products unfit, or applying penalties.

#### **Blockchain and Internet of Things**

Other ambitious ideas come from using blockchain and the IoT. One suggestion is for smart contracts to manage rentals of driverless cars. A smart contract could check for rental payments. If there has been no payment or the rental agreement reaches the end of its term, the smart contract could lock the car and tell it to drive itself back to the hire company’s premises.

#### **Challenges to Be Met**

Blockchain of course, is still an emerging technology and is, therefore, not without its share of potential issues. Enterprises that want to harness blockchain power for their supply chain will need to watch out and be ready for the following challenges.

#### **Ecosystem Still in Progress**

The first telephone was useless until the second one arrived. In time, the phone spread across the world, and now we cannot do without it. The situation is similar for blockchain and companies that want to do business with specific partners. Those partners will need to buy into blockchain as well.

For example, Tomcar can currently execute Bitcoin payment for about 2% of the parts it buys. However, niche uses of blockchain are on the rise. It may be just a matter of time until businesses “join the dots” for widespread acceptance.

#### **Currency Volatility**

Bitcoin is an easy way to start using blockchain. The problem is that the rate of exchange between Bitcoin and other currencies can change rapidly. Payment terms must be short enough or flexible enough to be able to cash in Bitcoin and recover the value expected.