Q.1) What is Blockchain? What are its key elements?

A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format.

Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions.

The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

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 duplica0tion 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 — 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.

Q.3) Discuss about the advantages and disadvantages of blockchain.

Advantages of Blockchain Technology:

1. Open: One of the major advantages of blockchain technology is that it is accessible to all means anyone can become a participant in the contribution to blockchain technology, one does not require any permission from anybody to join the distributed network.

2. Verifiable: Blockchain technology is used to store information in a decentralized manner so everyone can verify the correctness of the information by using zero-knowledge proof through which one party proves the correctness of data to another party without revealing anything about data.

3. Permanent: Records or information which is stored using blockchain technology is permanent means one needs not worry about losing the data because duplicate copies are stored at each local node as it is a decentralized network that has a number of trustworthy nodes.

4. Free from Censorship: Blockchain technology is considered free from censorship as it does not have control of any single party rather it has the concept of trustworthy nodes for validation and consensus protocols that approve transactions by using smart contracts.

5. Tighter Security: Blockchain uses hashing techniques to store each transaction on a block that is connected to each other so it has tighter security. It uses SHA 256 hashing technique for storing transactions.

6. Immutability: Data cannot be tampered with in blockchain technology due to its decentralized structure so any change will be reflected in all the nodes so one cannot do fraud here, hence it can be claimed that transactions are tamper-proof.

7. Transparency: It makes histories of transactions transparent everywhere all the nodes in the network have a copy of the transaction in the network. If any changes occur in the transaction it is visible to the other nodes.

8. Efficiency: Blockchain removes any third-party intervention between transactions and removes the mistake making the system efficient and faster. Settlement is made easier and smooth.

9. Cost Reduction: As blockchain needs no third man it reduces the cost for the businesses and gives trust to the other partner.

Disadvantages of Blockchain Technology:

1. Scalability: It is one of the biggest drawbacks of blockchain technology as it cannot be scaled due to the fixed size of the block for storing information. The block size is 1 MB due to which it can hold only a couple of transactions on a single block.

2. Immaturity: Blockchain is only a couple-year-old technology so people do not have much confidence in it, they are not ready to invest in it yet several applications of blockchain are doing great in different industries but still it needs to win the confidence of even more people to be recognized for its complete utilization.

3. Energy Consuming: For verifying any transaction a lot of energy is used so it becomes a problem according to the survey it is considered that 0.3 percent of the world's electricity had been used by 2018 in the verification of transactions done using blockchain technology.

4. Time-Consuming: To add the next block in the chain miners need to compute nonce values many times so this is a time-consuming process and needs to be speed up to be used for industrial purposes.

5. Legal Formalities: In some countries, the use of blockchain technology applications is banned like cryptocurrency due to some environmental issues they are not promoting to use blockchain technology in the commercial sector.

6. Storage: Blockchain databases are stored on all the nodes of the network creates an issue with the storage, increasing number of transactions will require more storage.

7. Regulations: Blockchain faces challenges with some financial institution. Other aspects of technology will be required in order to adopt blockchain in wider aspect.

Q.5) Explain the number Core Components of Blockchain Architecture.

Core Components of Blockchain Architecture

Node: Nodes are network participants and their devices permit them to keep track of the distributed ledger and serve as communication hubs in various network tasks. A block broadcasts all the network nodes when a miner looks to add a new block in transactions to the blockchain.

Transactions: A transaction refers to a contract or agreement and transfers of assets between parties. The asset is typically cash or property. The network of computers in blockchain stores the transactional data as copy with the storage typically referred to as a digital ledger.

Block: A block in a blockchain network is similar to a link in a chain. In the field of cryptocurrency, blocks are like records that store transactions like a record book, and those are encrypted into a hash tree.

Chain: Chain is the concept where all the blocks are connected with the help of a chain in the whole blockchain structure in the world. And those blocks are connected with the help of the previous block hash and it indicates a chaining structure.

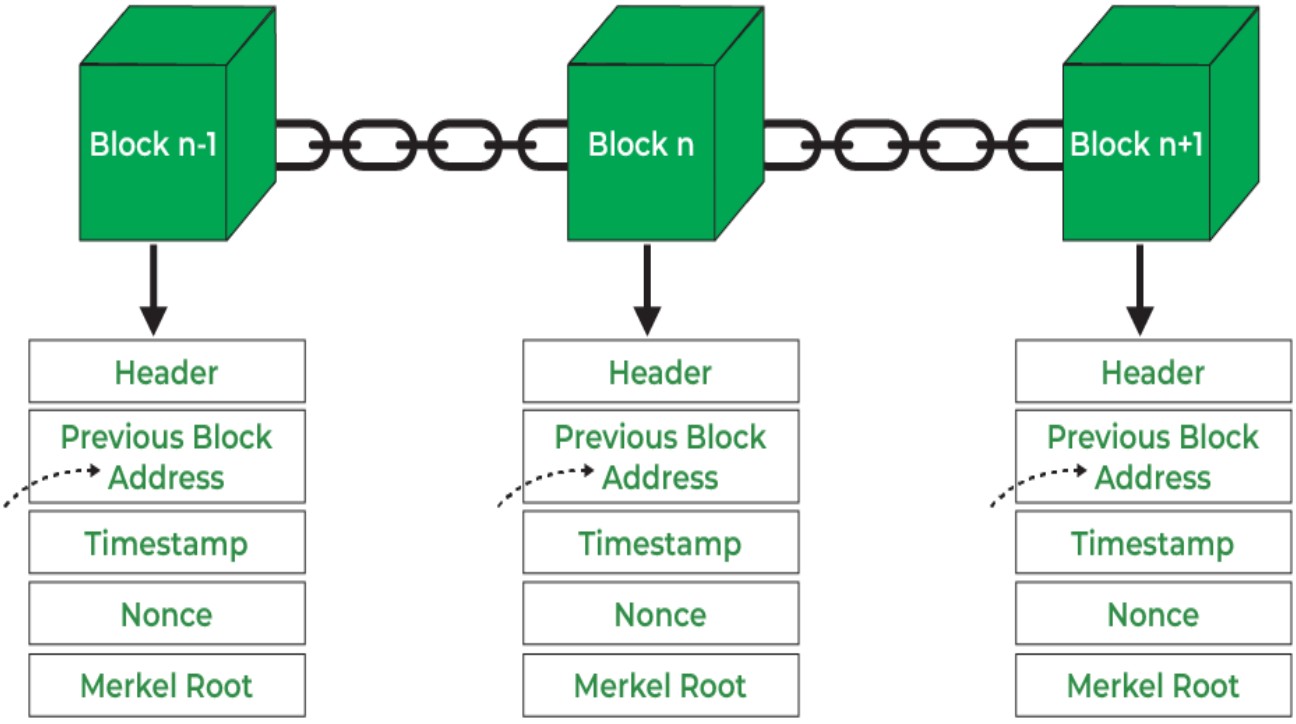
Miners: Blockchain mining is a process that validates every step in the transactions while operating all cryptocurrencies. People involved in this mining they called miners. Blockchain mining is a process to validate each step in the transactions while operating cryptocurrencies.

Consensus: A consensus is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record keeping and other things.

Q.6) Discuss architecture of Blockchain.

Blockchain Architecture

Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Verification and validation of these transactions are carried out by special kinds of nodes.



Header: It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.

Previous Block Address/ Hash: It is used to connect the $i+1^{th}$ block to the i^{th} block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

Timestamp: It is a system verify the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.

Nonce: A nonce number which uses only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.

Merkel Root: It is a type of data structure frame of different blocks of data. A merkel tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

Types of Blockchain Architecture

1. Public Blockchain:

A public blockchain is a concept where anyone is free to join and take part in the core activities of the blockchain network. Anyone can read, write, and audit the ongoing activities on a public blockchain network, which helps to achieve the self-determining, decentralized nature often authorized when blockchain is discussed.

Data on a public blockchain is secure as it is not possible to modify once they are validated.

The public blockchain is fully decentralized, it has access and control over the ledger, and its data is not restricted to persons, is always available and the central authority manages all the blocks in the chain.

2. Private Blockchain

Miners need permission to access a private blockchain. It works based on permissions and controls, which give limit participation in the network.

Only the entities participating in a transaction will have knowledge about it and the other stakeholders not able to access it.

By it works on the basis of permissions due to this it is also called a permission-based blockchain. Private blockchains are not like public blockchains it is managed by the entity that owns the network.

A trusted person is in charge of the running of the blockchain it will control who can access the private blockchain and also controls the access rights of the private chain network.

There may be a possibility of some restrictions while accessing the network of the private blockchain.

3. Consortium Blockchain

A consortium blockchain is a concept where it is permissioned by the government and a group of organizations, not by one person like a private blockchain. Consortium blockchains are more decentralized than private blockchains, due to being more decentralized it increases the privacy and security of the blocks.

Those like private blockchains connected with government organizations' blocks network. Consortium blockchains is lies between public and private blockchains. They are designed by organizations and no one person outside of the organizations can gain access. In Consortium blockchains all companies in between organizations collaborate equally.

They do not give access from outside of the organizations/ consortium network.

Q.7) Elaborate use cases of blockchain.

Applications of Blockchain are as follows:

1. Bitcoin: The primary application of Blockchain is in Cryptocurrencies like Bitcoin. Bitcoin is a decentralized digital currency introduced by Santoshi Nakamoto.

2. Banking: Nowadays, Blockchain is also replacing the existing, or we can say overtaking the **current Banking system**. With the help of Blockchain, we can transfer the fund from one person to another in a second because the transaction's validation will take place through Blockchain and cryptography. It's a possibility that Blockchain will cut down 19.8 Billion Dollars which is going for middleman cost/year. Because of the Blockchain, the hacking of accounts will become impossible.

3. Payment and Transfers: Because of Blockchain, only the wallet system has grown up so rapidly, and by using that, we can make the payment and money transfers very quickly; we don't need to enter the public key. We need to scan a unique QR code and pay soon. The amount done by Blockchain will be highly secure with no transfer fees. For blockchain transfer, no bank account is needed.

4. Healthcare: Healthcare is also a domain where **Blockchain technology** has been used for storing the details of the patients. This technology ensures that anyone accessing this Blockchain can access patients' data. This database will be highly secure and for checking the data related to the patient-doctor has to log in there with the public key and details, and he can check the patients' data.

5. Law Enforcement: The law enforcement agency is also now applying applications of Blockchain technology. So that they can create a Common Database of the criminal and the crimes committed by them with all the biometric details. Since it's highly secure, nobody can change it without proper access.

6. Voting: Blockchain can be used in the next election or Voting because of its unchanging revolutionary nature. Voting will become more secure and fail-proof with the help of Blockchain.

7. IoT(Internet of Things): Blockchain is also now used by IoT. This ensures that data that will transfer over or between the devices will be secure and encrypted without any interference.

8. Online music: Online music is one field that is increasing with the help of Blockchain technology. Companies are putting their music in a blockchain where everyone can access the music, but none can change it, and a customer can pay for a particular song and then he can download it from the Blockchain itself.

9. Real estate: Real estate is also a domain that is affected by the applications of Blockchain, and in the future, people will sell and buy property over the Blockchain.

10. Digital IDs: Blockchain is also now used by different companies for Digital Id. These digital IDs will be managed by the owner's private keys and will also help avoid excess personal information over the internet.

Q.8) Differentiate between blockchain Architecture Vs Database.

Blockchain Architecture Vs Database

Parameters	Blockchain Architecture	Database
Control	Blockchain is decentralized because there is no single point of failure and there is no central authority to control the blockchain.	The database is Centralized.
Operations	Blockchain has only an Insert operation.	The database has Create, Read, Update, and Delete operations.
Strength	It is robust technology.	The database is not fully robust technology.
Mutability	Blockchain is immutable technology and we cannot change it back or we cannot go back.	The database is a fully mutable technology, The data can be edited in the database.
Rights	Anyone with the right proof of work can write on the blockchain.	In the database reading and writing can do so.
Speed	It is slow in speed.	It is faster as compared to blockchain.

Q.1) Discuss the use of Cryptography in Cryptocurrencies

Cryptocurrencies like Bitcoin and Ethereum have gained immense popularity thanks to their decentralized, secure, and nearly anonymous nature, which supports the peer-to-peer architecture and makes it possible to transfer funds and other digital assets between two different individuals without a central authority.

The word “crypto” literally means concealed or secret. "Cryptography" means "secret writing"—the ability to exchange messages that can only be read by the intended recipient. In cryptocurrency, cryptography guarantees the security of the transactions and the participants, independence of operations from a central authority, and protection from double-spending

Cryptography technology is used for multiple purposes—for securing the various transactions occurring on the network, for controlling the generation of new currency units, and for verification of the transfer of digital assets and tokens.

A trustworthy and secure signature requires it to have the following properties:

It should be verifiable by others that it is indeed your signature;
It should be counterfeit-proof such that no one else can forge your signature, and
It should be secure from any possibility of denial by the signer later – that is, you cannot renege on a commitment once signed.

Q.2) What are the different Cryptography Methods Used in Cryptocurrencies?

Multiple methods exist for encryption in cryptography.

The first one is **Symmetric Encryption Cryptography.**

It uses the same secret key to encrypt the raw message at the source, transmit the encrypted message to the recipient, and then decrypt the message at the destination.

A simple example is representing alphabets with numbers—say, "A" is 01, "B" is 02, and so on. A message like “HELLO” will be encrypted as “0805121215,” and this value will be transmitted over the network to the recipient(s).

Once received, the recipient will decrypt it using the same reverse methodology—"08" is H, "05" is E, and so on, to get the original message value “HELLO.”

Even if unauthorized parties receive the encrypted message “0805121215,” it will be of no value to them unless they know the encryption methodology.

The second method is **Asymmetric Encryption Cryptography**, which uses two different keys —public and private—to encrypt and decrypt data.

The public key can be disseminated openly, like the address of the fund receiver, while the private key is known only to the owner.

In this method, a person can encrypt a message using the receiver’s public key, but it can be decrypted only by the receiver's private key.

This method helps achieve the two important functions of authentication and encryption for cryptocurrency transactions. The former is achieved as the public key verifies the paired private key for the genuine sender of the message, while the latter is accomplished as only the paired private key holder can successfully decrypt the encrypted message.

Q.3) Explain the Working of Cryptography.

In the simplest terms, cryptography is a technique to send secure messages between two or more participants—the sender encrypts/hides a message using a type of key and algorithm, sends this encrypted form of message to the receiver, and the receiver decrypts it to generate the original message.

Encryption keys are the most important aspect of cryptography. They make a message, transaction, or data value unreadable for an unauthorized reader or recipient, and it can be read and processed only by the intended recipient. Keys make the information “crypto”, or secret.

Many cryptocurrencies, like Bitcoin, may not explicitly use such secret, encrypted messages, as most of the information that involves Bitcoin transactions is public to a good extent.

Some of the tools that were developed as a part of cryptography have found important use in cryptocurrency. They include functions of hashing and digital signatures that form an integral part of Bitcoin processing, even if Bitcoin does not directly use hidden messages.