

Subject: Block-chain Technology

1. What is Blockchain technology?

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

2. What Is Ethereum (ETH)?

Ethereum is an open-source software platform based on Blockchain technology that enables developers to build and deploy decentralized applications (i.e., applications that are not controlled by a single entity). You may construct a decentralized application in which the participants are the ones who make the decisions.

3. What is a Blockchain Explorer?

A blockchain explorer is a piece of software that draws data from a blockchain using an API and a blockchain node, then uses a database to organize the data and present it to the user in a searchable format.

4. What Is Hashing in Blockchain?

The process of making an input item of any length represents an output item of a fixed length is referred to as hashing in the blockchain. Take, for example, the use of blockchain in cryptocurrencies, where transactions of varying lengths are run through a given hashing algorithm and all produce a fixed-length performance.

5. What are the different types of Blockchain?

The blockchain is classified into four types

- Public Blockchains
- Private Blockchains

- Consortium Blockchains
- Hybrid Blockchains.

6. What are some of the popular Cryptocurrencies?

The most popular Cryptocurrencies are:

- Bitcoin(BTC)
- Ethereum(ETH)
- Ripple(XRP)
- Litecoin(LTC)
- Bitcoin Cash(BCH)

7. What is a 51% Attack?

A miner or a group of miners attempting to control more than 50% of a network's hashing capacity, processing power, or hash rate is known as a 51 percent attack on a blockchain network. The attacker may prevent new transactions from taking place or being verified in this attack. They can also reverse transactions that have already been verified while in charge of the network, resulting in a double-spending problem.

8. Compare Blockchain with relational database

Criteria	Blockchain	RDBMS
Unit of data	Block	Table
Single point of failure	Does not exist	Exists
Centralized control	No	Yes
Editing/deleting data	Not possible	Possible

9. What do you mean by blocks in Blockchain technology?

In the Blockchain, a block is simply a set of records. The term “blockchain” refers to the process of joining these lists together. For example, if a company has 100 ledger books, the total is known as Blockchain, and each ledger is referred to as a block.

10. How does a block is recognized in the Blockchain approach?

Any block in this online ledger consists primarily of a hash pointer that serves as a connection to the previous block, transaction data, and a time stamp.

11. Are there any network-specific conditions for using Blockchain technology in an organization?

No, there isn't any such restriction on using it. However, under the worried protocols, the network must be a peer-to-peer network. It effectively validates the new block and assists businesses in keeping up with the pace in this area without relying on third-party applications.

12. Is it possible to modify the data once it is written in a block?

No, it is not possible to do that. If any customization is needed, the company simply needs to delete the details from all other blocks as well. Data must be treated with extreme caution when using this system for no other reason than this.

13. How Does Blockchain Create Blocks?

When the block size is reached, the blockchain creates blocks automatically. Since the block is a file, the transactions are saved until the file is complete. They are linked in such a way that the most recent block is connected to the previous one. A hash value is created using a mathematical function to identify a block. It also shows any modifications made to a block.

14. Can Anyone Remove Blocks from A Blockchain?

The manner in which blocks are removed from a blockchain is entirely dependent on how they are treated. Manually removing a block is not possible. If it is destroyed, however, the blockchain may attempt to restore the database using other peers.

They can be removed after they've been checked to reduce the blockchain's size since they don't need someone to perform regular operations. It can be re-downloaded if necessary. This process is called pruning.

15. What is encryption? What is its role in Blockchain?

Encryption is a technique that is used to keep the data secure. The data is encoded to some level before being sent out of a network by the sender in this process. Only the receiver will be able to decode it. This approach is useful in Blockchain because it simply adds to the overall protection and validity of blocks, making them more stable.

16. What exactly do you know about the security of a block?

Any users on a network cannot customize a block. As a result, it offers a high degree of security. Furthermore, every block is protected by cryptography, which is yet another vote in this case. As a result, there is no need to be concerned about the protection of data in a block.

17. Why is Blockchain a trusted approach?

For a variety of purposes, blockchain can be trusted. Because of its open-source existence, the first thing that comes to mind is its compatibility with other business applications. The second factor is its safety. Since it was designed to be used for online transactions, the developers paid particular attention to keeping up with the times in terms of protection. Blockchain will help despite the type of company one owns.

18. How does Bitcoin use Blockchain?

A transaction is a value transfer that is recorded in the blockchain between Bitcoin wallets. Bitcoin wallets store a private key, also known as a seed, which is used to sign transactions and provide mathematical proof that they came from the wallet's owner.

19. Is Blockchain an incorruptible ledger?

Yes, Blockchain is an incorruptible ledger. According to the inventor, the blockchain database cannot be tampered with.

20. What are blockchain requirements?

Blockchain is a truly disruptive technology that has the potential to change business networks. So, the requirements for a blockchain is as follows:

- Smart contracts
- Ledgers
- Cryptography
- Consensus Protocol

21. In what order are the blocks linked in the blockchain?

Each block in the blockchain is always linked in reverse order. To put it another way, blockchain connects each block to the one before it. Hence, blocks are linked in the backward direction.

That's it for the list of top Blockchain questions for beginners. Let's move to the next section of intermediate Blockchain Technology interview questions.

22. What are Block Identifiers?

A blockchain has a unique identifier for each block. The hash value is used to create a unique identifier. As a result, no two block identifiers would be the same. In Blockchain, blocks can be identified by the *block header hash* and the *block height*.

23. Name the common type of ledgers that can be considered by users in Blockchain?

There are three common types of a ledger that can be considered by users in the blockchain:

1. Centralized Network
2. Decentralized Network
3. Distributed Network

24. How is a blockchain ledger different from an ordinary ledger?

The key distinction between blockchain ledger and ordinary ledger is that Blockchain is a distributed database that can be conveniently decentralized. This method has a much lower risk of error than a traditional ledger. An ordinary ledger is one that is created by hand or by human effort, while the Blockchain automates all of its processes. All you have to do now is set it up properly and according to the instructions.

25. Can you define what is an off-chain transaction?

A transaction that takes place outside of the blockchain is known as an off-chain transaction. An on-chain transaction – often referred to as simply “a transaction” – modifies the blockchain and relies on the blockchain to establish its legitimacy, while off-chain transaction records and validates the transaction using other methods.

Section B

1. Give real-life use case of blockchain.

- **Supply chain management:** Blockchain can provide reduced cost and risk across the supply chain. It can also provide increased supply chain transparency.
- **Healthcare:** To keep a record of patient's data. The ledger technology manages the medicine supply chain, facilitates the secure transfer of patient medical records.
- **Digital voting:** The token-based system created using blockchain technology will ensure the system of ‘one unchangeable vote per person.
- **Real Estate:** Ownership and title details are stored on the blockchain, thereby making it easier to transfer ownership and trace ownership.
- **Media:** Blockchain can maintain data integrity, allowing advertising agencies to target the right customers, and musicians to receive proper royalties for original works.

2. What are the components of a blockchain architecture?

- **Node:** User/computer within the blockchain architecture.
- **Transaction:** It is the smallest building block of the blockchain system.
- **Block:** It is used for maintaining a set of transactions that are distributed to all the nodes in the network.
- **Chain:** The sequence of blocks.
- **Miners:** Specific nodes that perform a block verification process before adding to the blockchain structure.
- **Consensus Protocol:** Set of rules to carry out blockchain operations.

3. What is Blockchain Wallet and How Does It Work?

A blockchain wallet is a piece of digital software that stores private and public keys, as well as tracks and records all transactions involving those keys on the blockchain. A blockchain wallet, in theory, does not store cryptocurrency; instead, all records belonging to these keys are stored on the blockchain on which the wallet is hosted.

Blockchain wallets have public and private keys. A public key and a private key are used in a similar way in blockchain wallets. A public key is similar to an email address in that it can be shared with others. When your wallet is created, a public key is created as well, which you can share with others to obtain funds. The private key is a closely guarded secret. It's similar to your password in that it shouldn't be compromised, and you shouldn't share it.

4. What are Smart Contracts and how do they work?

A smart contract is a computer code-based agreement between two individuals. They are stored on a public ledger and cannot be modified because they run on the blockchain. A smart contract's transactions are handled by the blockchain, which means they can be submitted automatically without the involvement of a third party.

The Smart contracts are secure, transparent, third-party-free, autonomous, and accurate.

Let me use an example to demonstrate how smart contracts work. If Alex decides to sell his home to Bob. Then they would pay a slew of fees to third parties such as real estate agents, banks, and attorneys, and others. However, with a smart contract, they can simply write a statement stating that if Bob pays this amount of money, he will be given ownership of the property. Hence, smart contracts can cut down the actual process and give us trustable options for transactions.

5. What Is Cryptocurrency Mining and how Bitcoin mining works?

The word "crypto mining" refers to the process of obtaining cryptocurrencies by the use of computers to solve cryptographic equations. Validating data blocks and applying transaction records to a public record (ledger) is also a part of this method.

Bitcoin mining is not just the process of putting new bitcoins into circulation, but it is also an important part of the blockchain ledger's upkeep and growth. It is carried out with the assistance of highly advanced computers that solve extremely difficult computational math problems.

6. What are the benefits of Blockchain Technology?

Blockchain technology has the following benefits:

- Blockchain technology employs advanced security compared to other networks or record-keeping systems. Prior to being recorded, all transactions must be agreed upon. A transaction is encrypted and connected to the previous transaction after it has been authorized.
- Blockchain offers transparency. As one of the major problems in the new industry is transparency. An organization may use blockchain to create a completely decentralized network that eliminates the need for a centralized authority, increasing the system's transparency.
- Blockchain helps in reducing costs. Organizations will save a lot of money by using the blockchain instead of paying third-party vendors.
- Blockchain automates time-consuming processes in order to increase performance. With the aid of automation, it also eliminates human errors. As a result, blockchain increases efficiency and speed.
- The blockchain allows for immediate traceability. It generates an audit trail that records an asset's provenance at each stage of its journey which prevents fraud.

7. Name some popular Blockchain Platforms for Blockchain Applications?

The following are the list of widely-used platforms for blockchain-based applications

- IBM Blockchain
- EOS
- OpenLedger
- Corda
- Ripple
- Ethereum
- IOTA
- Quorum
- OpenChain
- Hyperledger Sawtooth

8. What is the difference between Blockchain and Hyperledger?

- Blockchain is a technology that allows us to build decentralized systems. When we break down blockchain, the “block” refers to information stored in a digital format, while “chain” refers to the database where that information is stored.
- Hyperledger is a type of blockchain platform. It’s a blockchain-based open-source network. These blockchains each have their own storage routines and consensus, as well as smart contracts, identity, and access management.
- Since hyperledger is a product of the blockchain platform, they have a few in common. However, due to hyperledger’s unique features, both are different.

Mostly, blockchain is classified into public and private types. And Hyperledger is an example of private blockchain.

9. What is a ledger? What is the difference between a distributed ledger and a traditional ledger?

A ledger is a constantly growing file. It maintains a permanent record of all transactions between two parties on the blockchain network.

A distributed ledger is a database of digital data that is replicated, exchanged, and synchronized across multiple sites in a network.

Distributed ledgers, unlike traditional ledgers (think banks, governments, and accountants), provide a system of synchronized databases that have an auditable background of information that is accessible to everyone inside the network.

10. What type of records can be kept in Blockchain? Is there any restriction on the same?

In the Blockchain method, there are no limitations on the number of records that can be held. It is important to remember that record keeping is not limited to these applications.

The following are examples of the types of information that can be held on them:

1. Health transaction records

2. Managing your identity
3. Production of transactions
4. Organizational events and management tasks
5. Documentation is required.

11. What are Blockchain Durability and robustness?

1. Bitcoin was founded in the year 2008. Since then, there has been no major damage to the Bitcoin network. For nearly 30 years, the internet has proved to be a reliable resource. It's a track record that bodes well for the future development of blockchain technology.
2. In the same way, as the internet has built-in robustness, blockchain technology does as well. The blockchain can't be managed by any single individual since it stores blocks of information that are similar across its network. There should be no single failure point in the blockchain.

12. How is a blockchain ledger different from an ordinary ledger?

The key distinction between blockchain ledger and ordinary ledger is that Blockchain is a distributed database that can be conveniently decentralized. This method has a much lower risk of error than a traditional ledger. An ordinary ledger is one that is created by hand or by human effort, while the Blockchain automates all of its processes. All you have to do now is set it up properly and according to the instructions.

13. What is Double Spending? Is it possible to double spend in a Blockchain system?

It occurs when a single digital token is used several times since the token is typically made up of a digital file that can be easily cloned. It simply causes inflation, and businesses are forced to take a significant loss. One of the main goals of Blockchain technology is to eradicate this method as much as possible.

Blockchain avoids double-spending by requiring several parties to validate a transaction before it is written to the ledger. It's no exaggeration to claim that bitcoin's entire structure of Blockchain, mining, proof of work, complexity, and so on exists to create this history of transactions that is computationally impractical to change.

14. Explain the significance of blind signature and how it is useful?

A blind signature is a form of digital signature in which the contents of a message are hidden (blinded) before they're signed. As with a standard digital signature, the resulting blind signature can be publicly validated against the original, unblinded message.

Blind signatures are often used in privacy-related protocols where the signer and message author are not the same individual. Cryptographic voting systems and digital cash schemes are two examples.

15. Can you define what is an off-chain transaction?

A transaction that takes place outside of the blockchain is known as an off-chain transaction. An on-chain transaction – often referred to as simply “a transaction” – modifies the blockchain and relies on the blockchain to establish its legitimacy, while off-chain transaction records and validates the transaction using other methods.

16. What are the key principles in Blockchain that are helpful in eliminating the security threats that need to be followed?

To eliminate the security threats, The key Principles that are needed to follow are as follows. All these principles are fundamental and simple to apply. They are helpful in making transaction documents more valuable.

1. Auditing
2. Securing applications
3. Securing testing and similar approaches
4. Database security
5. Continuity planning
6. Digital workforce training

17. Name the steps that are involved in the Blockchain project implementation?

There is a total of six steps involved in the blockchain project implementation process and they are:

1. Identifying the requirements
2. Consideration of screen ideas
3. Blockchain project production
4. Analysis of the Security Implementation's Feasibility
5. Managing and overseeing the project

18. What is a Public Key?

The cryptographic algorithm that enables peers in a blockchain to obtain funds in their wallet uses a public key. A pair of keys is created when a public key is connected to a private key. The private-public key pair is used to ensure that the blockchain's security is maintained. A public key is a string of alphanumeric characters that is unique to a specific node or address.

19. What is a Private Key?

A private key is an alphanumeric term that is used to encrypt and decrypt data associated with a public key. In blockchain security, It is also a component of the cryptographic algorithms. The key has been allocated to the key generator and can only be used by him. If he fails to do so, someone can gain access to the wallet's information or data, as well as the address for which the private key is stored.

20. What Are the Drawbacks of Blockchain?

Some disadvantages of Blockchains are listed below.

- Some Blockchain Solutions Use So Much Energy Because Blockchain Isn't a Distributed Computing System
- It's difficult to incorporate and manage complex technologies.
- There are also problems with scalability.
- Data is unchangeable.
- It can be inefficient at times because network speed and transaction costs fluctuate.

- Human error has not yet been eradicated.
- Not entirely secure.

21. What is Transparent and incorruptible in blockchain?

Every ten minutes, the blockchain network checks in with itself to ensure that it is in a state of consensus. The network, which functions as a self-auditing ecosystem of digital value, reconciles any transaction that occurs in ten-minute intervals. A “block” refers to a collection of these transactions. As a result, two critical properties emerge from this they are:

Transparency data is embedded in the network as a whole, and it is available by definition. It can’t be tampered with because changing every single unit of data on the blockchain will require a massive amount of computational power to circumvent the entire network.

22. What Is Consensus Algorithm?

The method of gaining consensus on a change of data over the system or any distributed network is known as a consensus algorithm. They are widely used in blockchains because they enable the network of unknown nodes to reach consensus on the data that is being stored or shared. Proof-of-Stake (PoS) and Proof-of-Work(PoW) are the most popular consensus algorithms.

23. Is the Blockchain Totally Different from Traditional Banking Ledger?

Banking ledgers are used to ensure that the transactions can take place correctly. That’s why they trace and timestamp transactions. The significant difference between a banking ledger and a blockchain is how they are governed. The blockchain is decentralized in nature; however, banking ledgers are completely centralized as banks govern them.

The blockchain is completely transparent and trustworthy when compared to bank ledgers. Banks are keen on blockchain technology to automate most of their banking functionalities and provide a trustworthy approach. However, they are more likely to use federated blockchain or private blockchain to ensure that they still control their operations.

24. What Are the Key Features/Properties of Blockchain?

There are many key features of blockchain. They include the following.

- Blockchain as a data structure: Blockchain can act as a data structure and store different types of data, including identity information, insurance, medical, and so on.
- Immutability: The data, once stored in the blockchain, is immutable. This gives the blockchain tamper detection property as well.
- Data protection: As the owner of the data is the source peer itself, data protection is completely dependent on the source. The absence of third-party actors also means that it is secure and offers the best data protection

- Decentralized ledger technology: Decentralized ledger technology is the most important feature of a blockchain. It can be used by a private organization or public in a variety of use-cases.
- Better user anonymity: Users are relatively hidden compared to other traditional networks.
- Double spending: Blockchain solves double-spending problems using consensus algorithms and distributed ledger technology.

25. *What Type of Records You Can Keep in A Blockchain?*

Blockchain acts as a data structure, which means that it can be used to store any form of data. Industries can make proper use of blockchain record types as they can completely take advantage of what it has to offer. The most common types of records/data that can be kept in blockchain are as follows.

- Identity management
- Transaction processing
- Documentation
- Medical records
- Management activities
- Business transactions

SECTION C

1. Differentiate between Blockchain and Hyperledger.

Blockchain is a decentralized technology of immutable records called blocks, which are secured using cryptography. Hyperledger is a platform or an organization that allows people to build private Blockchain.

Using Blockchain you can build public and private Blockchain whereas with Hyperledger you can only build private Blockchains.

Blockchain is divided into public, private, and consortium Blockchains and Hyperledger is a private Blockchain technology with access to Blockchain data and is limited to predefined users, configurations, and programming.

Blockchain can be used in multiple fields such as business, government, healthcare, etc. while Hyperledger is primarily used for enterprise-based solutions. Wherever we talk about public Blockchain, it refers to the usage of Blockchain on the internet, and Hyperledger-based Blockchain solutions are solutions meant for usage on the intranet, within an organization.

2. How do you explain Blockchain technology to someone who doesn't know it?

Blockchain technology is a distributed ledger, which stores transaction details in the form of immutable records or non-modifiable records (called blocks) which are secured using cryptography.

Let's consider the example of a school where Blockchain is similar to a digital report card of a student. Say, each block contains a student record that has a label (stating the date and time) of when the record was entered. Neither the teacher nor the student will be able to modify the details of that block or the record of report cards. Also, the teacher owns a private key that allows him/her to make new records and the student owns a public key that allows him to view and access the report card at any time. So basically, the teacher owns the right to update the record while the student only has the right to view the record. This method makes the data secure.

3. What is Merkel Tree?

Merkel Tree is a data structure that is used for verifying a block. It is in the form of a binary tree containing cryptographic hashes of each block. A Merkle tree is structured similarly to a binary tree where each leaf node is a hash of a block of transactional data and each non-leaf node is a hash of its leaf node. The Merkle root or hash root is the final hash root of all the transaction hashes. It encompasses all the transactions that are underlying all the non-leaf nodes.

4. What do you mean by blocks in Blockchain technology?

Blockchain is a distributed database of immutable records called blocks, which are secured using cryptography. Refer to the video to see the various attributes of a block.

There are a previous hash, transaction details, nonce, and target hash value. A block is like a record of the transaction. Each time a block is verified, it gets recorded in chronological order in the main Blockchain. Once the data is recorded, it cannot be modified.

5. How is Blockchain distributed ledger different from a traditional ledger?

- A Blockchain distributed ledger is highly transparent as compared to a traditional ledger.
- Blockchain distributed ledgers are irreversible. Information registered on a distributed ledger cannot be modified whereas on a traditional ledger it is reversible.
- A distributed ledger is more secure. It uses cryptography and every transaction is hashed and recorded whereas in traditional ledger security can be compromised.
- In a distributed ledger, there is no central authority. It is a distributed system and the participants hold the authority to maintain the sanity of the network and are responsible for validating the transactions. Traditional ledgers are based on the concept of centralized control, which controls all transactions.

- In a distributed ledger, identities are unknown and hidden whereas in traditional ledger identities of all participants have to be known before the transactions happen.
- In a distributed ledger, there is no single point of failure as the data is distributed and information is shared across multiple nodes. If one node fails, the other nodes carry the same copy of the information. In comparison, traditional ledgers have a single point of failure. If a single system crashes, the entire network comes to a standstill.
- In a distributed ledger, data modification or change cannot be done but for a traditional ledger, it is possible.
- In a distributed ledger, validation is done by the participants in the network while in a traditional ledger, validation is done by a centralized authority.
- The copy of the ledger is shared amongst participants in a distributed ledger while in a traditional ledger, a single copy is maintained in a centralized location. It is not shared amongst the participants.

6. How can you identify a block?

Every block consists of four fields -

- The hash value of the previous block (thereby getting linked in a blockchain)
- It contains details of several transaction data
- It has a value called the nonce. The nonce is a random value which is used to vary the value of the hash in order to generate hash value less than the target
- Hash of the block itself. It is the digital signature of the block and an alphanumeric value used to identify a block

The hash address is the unique identification of the block. It is a hex value of 64 characters that have both letters and digits. It is obtained by using the SHA - 256 algorithms.

Refer to the video to see how a block is structured. The hash of the previous block, transaction data, and the nonce consolidate the header of the block. They are together passed through a hashing function and then the hash value is generated.

7. What is cryptography? What is its role in Blockchain?

Blockchain uses cryptography to secure users' identities and ensure transactions are done safely with a hash function.

Cryptography uses public and private keys in order to encrypt and decrypt data. In the Blockchain network, a public key can be shared with all the Bitcoin users but a private key (just like a password) is kept secret with the users.

Blockchain uses SHA - 256 which is secure and provides a unique hash output for every input. The basic feature of this algorithm is whatever input you pass, it will give you a standard alphanumeric output of 64 characters. It is a one-way function from which you can derive an encrypted value from the input, but not vice-versa.

8. What are the different types of Blockchain?

There are three different types of Blockchain - Public, Private, and Consortium Blockchain.

Public Blockchain ledgers are visible to all the users on the internet and any user can verify and add a block of transactions to the Blockchain. Examples, Bitcoin, and Ethereum.

Private Blockchain ledgers are visible to users on the internet but only specific users in the organization can verify and add transactions. It's a permissioned blockchain, although the information is available publicly, the controllers of the information are within the organization and are predetermined. Example, Blockstack.

In Consortium Blockchain, the consensus process is controlled by only specific nodes. However, ledgers are visible to all participants in the consortium Blockchain. Example, Ripple.

9. What is a Genesis Block?

- The genesis block is the first block in the Blockchain which is also known as block 0
- In Blockchain, it is the only block that doesn't refer to its previous block.
- It defines the parameters of the Blockchain such as,
 - level of difficulty,
 - consensus mechanism etc. to mine blocks

10. How is the hash (Block signature) generated?

The process of generating a block signature involves:

- Passing transaction details through a one-way hash function i.e., SHA-256.
- Running the output value through a signature algorithm (like ECDSA) with the user's private key.
- Following these steps, the encrypted hash, along with other information (such as the hashing algorithm), is called the digital signature.

11. List down some of the extensively used cryptographic algorithms.

Here are a few popular algorithms:

- SHA - 256
- RSA (Rivest-Shamir-Adleman)
- Triple DES
- Ethash
- Blowfish

12. What is a smart contract and list some of its applications?

Smart contracts are self-executing contracts which contain the terms and conditions of an agreement between the peers

Some of the applications are:

Transportations: Shipment of goods can be easily tracked using smart contracts

Protecting copyrighted content: Smart contracts can protect ownership rights such as music or books

Insurance: Smart contracts can identify false claims and prevent forgeries

Employment contract: Smart contracts can be helpful to facilitate wage payments

13. What is the Ethereum network and how many Ethereum networks are you familiar with?

Ethereum is a blockchain-based distributed computing platform featuring smart contract functionality that enables users to create and deploy their decentralized applications

There are three types of networks in Ethereum:

- Live network (main network) - Smart contracts are deployed on the main network
- Test network (like Ropsten, Kovan, Rinkeby) - Allow users to run their smart contracts with no fees before deploying it on the main network
- Private network - Are those which are not connected to the main network. They run within the premises of the organization but carry the features of an Ethereum network.

14. Where do nodes run a smart contract code?

Nodes run smart contracts code on Ethereum Virtual Machine (EVM). It is a virtual machine designed to operate as a runtime environment for Ethereum-based smart contracts.

EVM is operated in a sandboxed environment (isolated from the main network). This is a perfect testing environment.

You can download the EVM, run your smart contract locally in an isolated manner and once you have tested and verified it, you can deploy it on the main network.

15. What is a Dapp and how is it different from a normal application?

Dapp:

- A Dapp is a decentralized application which is deployed using smart contract
- A Dapp has its back-end code (smart contract) which runs on a decentralized peer-to-peer network
- Process:
 - Front-end
 - Smart contract (backend code)
 - Blockchain (P2P contract)

Normal application:

- Normal application has a back-end code which runs on a centralized server
- It's a computer software application that is hosted on a central server
- Process:
 - Front-end
 - API
 - Database (runs on the server)

16. What is the difference between Bitcoin and Ethereum?

Criteria	Bitcoin	Ethereum

Concept	P2P currency	P2P currency and smart contract
Consensus mechanism	Proof of work	Proof of work/ Proof of stake
Hashing Algorithm	SHA-256	Ethash
Time is taken to mine a block	10 Minutes (approx.)	12-15 seconds
Reward	12.5 BTC	3 ETH
Transaction fee	Optional	A fee is calculated in gas
Value (8/21/18)	1 BTC = 6934.34 USD	1 ETH = 278.98 USD

17. Name the steps that are involved in the Blockchain project implementation.

Requirement identification:

- Identify the problem and goal
- Identify the most suitable consensus mechanism
- Identify the most suitable platform
- Account for implementation and deployment costs

Planning stage

- In this stage an individual evaluates all requirements and decides a suitable blockchain platform to be implemented.

Development and implementation of a project

- Designing the architecture
- Designing the user interface
- Building the APIs

Controlling and monitoring the project

- Applying Proof of Concept (POC)
- Identifying and fixing issues

18. List and explain the parts of EVM memory.

The memory of an EVM is divided into three types:

Storage:

- Storage values are stored permanently on the Blockchain network
- It is extremely expensive

Memory:

- Memory is a temporary modifiable storage
- It can be accessed only during contract execution. Once the execution is finished, its data is lost

Stack:

- A stack is temporary and non-modifiable storage.
- Here, when the execution completes, the content is lost.

19. What is the fork? What are some of the types of forking?

In simple terms, updating a cryptocurrency protocol or code is called forking. Fork implies that a Blockchain splits into two branches. It can happen when the participants of the network cannot come to an agreement with regards to the consensus algorithm and new rules to validate transactions.

There are three types of forking:

- Hard forks
- Soft forks
- Accidental forks

20. Differentiate between Proof of Work vs Proof of Stake.

Proof of Work (PoW):

In Blockchain, PoW is the process of solving a complex mathematical puzzle called mining. Here, the probability of mining a block is based upon the amount of computational work done by a miner. Miners spend a lot of computing power (with hardware) for solving the cryptographic puzzle.

Proof of Stake (PoS):

PoS is an alternative to PoW in which the Blockchain aims to achieve distributed consensus. The probability of validating a block relies upon the number of tokens you own. The more tokens you have, the more chances you get to validate a block. It was created as a solution to minimize the use of expensive resources spent in mining.

21. What are function modifiers in Solidity? Mention the most widely used modifiers.

In Solidity, function modifiers are used to easily modify the behavior of your smart contract functions. In simple terms, it can build additional features or apply restrictions on the function of smart contracts. The most extensively used function modifiers in solidity are:

- View, which are functions that cannot modify the state of a smart contract. They are read-only functions. Refer to our video to see an example of a View function

Pure, which are functions that neither read nor write the state of a smart contract. They return the same result determined by its input values. Refer to our video to see an example of a Pure function.

22. What are the features provided by Blockchain?

- **Decentralized:** Blockchain is a decentralized technology. There is no central governing authority that manages the network. Rather every node has a copy of the ledger and each node contribute to maintaining the Blockchain network.
- **Immutable:** Data stored in a blockchain cannot be altered or manipulated. Once a transaction is added to the ledger, it resides there permanently.
- **Security:** Blockchain provides security to the data as it is not easy to hack and by this, we mean that it is actually very tough because the data block is added to the chain only after it is validated by more than half of the participating nodes. It uses a strong encryption algorithm like SHA-256 which ensures another layer of security.
- **Open Ledger:** The ledger is the record of transactions done and because it is visible to everyone, therefore is called an open ledger. Every node in the network has a copy of the ledger. So there is trust among participants as they can clearly check what is happening in the network.
- **Consensus Mechanism:** Blockchain works on some consensus protocols. A consensus algorithm is a procedure through which all the nodes of the Blockchain network reach a common agreement about the present state of the distributed ledger.

23. What is the Consensus mechanism in Blockchain?

Consensus is basically a set of protocols that regulate the blockchain network. It ensures no duplicate block is added to the chain and the block is added only after it is agreed upon by all other nodes in the network. It helps to achieve reliability and trust among the peer nodes.

There are different consensus algorithms:

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Elapsed Time
- Proof of Capacity
- Proof of Burn

24. What is the difference between Ethereum and Bitcoin?

Bitcoin	Ethereum
Bitcoin was introduced by Satoshi Nakamoto in 2008	Ethereum was introduced in the year 2013 by Vitalik Buterin
Bitcoin is a cryptocurrency	Ethereum is also a cryptocurrency but it contains executable codes and smart contract that are used for making DApps
The average block time is 10 min	The average block time is 10-15 sec
Bitcoin is Turing incomplete	Ethereum is Turing complete
It uses Proof of Work (PoW)	It uses Proof of Work (PoW)

Its native cryptocurrency is
Bitcoin (BTC)

Its native cryptocurrency is Ether (ETH)

25. What are some different types of Blockchain?

- **Public Blockchain:** A public blockchain is an open network where anyone can join the network and make transactions. Example- Bitcoin, Ethereum, Litecoin.
- **Private Blockchain:** A private blockchain is a permissioned blockchain that enforces some restrictions on users. It does not allow everyone to join the network. Also, the ledger is visible to only permissioned users of the organization. Example- Hyperledger, Multichain.
- **Consortium Blockchain:** It is like a private or permissioned blockchain where instead of a single organization, more than one organization governs the network. Example- Quorum, Corda.
- **Hybrid Blockchain:** It is a combination of both public and private blockchain. It provides control as well as freedom by using features of both types of blockchain. Example- Dragonchain.