



BLOCKCHAIN

Interview Guide



Ace Your Blockchain Interview

Blockchain provides an extremely secure method of storing data and conducting transactions. Companies and organizations are starting to take notice since, according to these statistics provided by Techjury, 90 percent of US and European banks explored blockchain in 2018. The worldwide blockchain technology market is projected to amass revenues of \$20 billion by 2024. According to **101blockchains**, the three economies that have embraced blockchain the most are the United States, China, and Switzerland. The US currently has the most blockchain activity and interest, but that will no doubt change in the coming years. Furthermore, as the Internet of

Things (IoT) continues to gain acceptance and usage, it is increasingly adopting blockchain technology. The value of IoT devices is expected to exceed \$50 billion by 2020. This development spells good news for blockchain and also translates into greater demand for blockchain professionals.

If you want to start a career in Blockchain, you will come across various in-depth learning interviews. Worried? Don't, because we have clubbed a list of the 30+ most popular questions you can expect in an interview. So prepare ahead of time, and crack your Blockchain Interview in the first go.

Topics Covered

- Hyperledger
- Merkle Tree
- Cryptography
- Types of Blockchain
- Smart Contracts
- Ethereum
- Distributed Applications
- Blockchain Mining
- Proof of Work
- Proof of Stake

Blockchain Interview Questions - Beginner Level

Q: Differentiate between Blockchain and Hyperledger.

A: **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.

Q: How do you explain Blockchain technology to someone who doesn't know it?

A: 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 which 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**.

Q: What is Merkel Tree?

A: 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 Merkel 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.

Q: What do you mean by blocks in Blockchain technology?

A: 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.

Q: How is Blockchain distributed ledger different from a traditional ledger?

- A**
- ✓ 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.

Q: How can you identify a block?

A: 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 **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.

Q: What is cryptography? What is its role in Blockchain?

A: 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 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.

Q: What are the different types of Blockchain?

A: 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**.

Q: What happens when you try to deploy a file with multiple contracts?

A: In Blockchain, deploying a file with multiple contracts is not possible. The compiler only deploys the last contract from the uploaded file and the remaining contracts are neglected.

Q: What is a Genesis Block?

- A**
- ✔ 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

Blockchain Interview Questions - Intermediate level

Q: How is the hash (Block signature) generated?

A: 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.

Q: List down some of the extensively used cryptographic algorithms.

A: Here are a few popular algorithms:

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

Q: What is a smart contract and list some of its applications?

A: 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

Q: What is Ethereum network and how many Ethereum networks are you familiar with?

A: 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.

Q: Where do nodes run a smart contract code?

A: 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.

Q: What is a Dapp and how is it different from a normal application?

A: 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)

Q: Name some leading open source platforms for developing Blockchain applications.

- A** ✓ Ethereum is one of the popular platforms for building Blockchain-based applications
- ✓ Eris is used for building enterprise-based solutions

Some of the other widely used platforms for building Blockchain include Hyperledger, Multichain, Open chain.

Q: What is the very first thing you must specify in a Solidity file?

- A:** It is necessary to specify the version number of Solidity at the beginning of code as it eliminates incompatibility errors that can arise while compiling with another version. This is a mandatory clause that has to be there at the top of any Solidity code you write. You also need to mention the correct version number for the code.

Q: What is the difference between Bitcoin and Ethereum?**A:**

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

Q: What is nonce and how is it used in mining?

A: In Blockchain, mining is a process to validate transactions by solving a difficult mathematical puzzle called proof of work. Now, proof of work is the process to determine a number (nonce) along with a cryptographic hash algorithm to produce a hash value lower than a predefined target. The nonce is a random value that is used to vary the value of hash so that the final hash value meets the hash conditions.

Blockchain Interview Questions - Expert Level

Q: Name the steps that are involved in the Blockchain project implementation.

A: 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

Q: Explain a real-life use-case where Blockchain is being used.

A: In supply chain management, smart contracts provide permanent transparency and validation of transactions shared by multiple supply chain partners. Check out our diagrammatic display of supply chain management using Blockchain in our video.

Q: List and explain the parts of EVM memory.

A: 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.

Q: What happens if the execution of a smart contract costs more than the specified gas?

A: Initially, your transaction will be executed, but if the execution of a smart contract costs more than the specified gas, then the miners will stop validating your contract. The Blockchain will record the transaction as failed, also the user doesn't get a refund.

Q: 5. What does the gas usage in a transaction depend on and how is the transaction fee calculated?

A: Gas usage depends upon the amount of storage and set of instructions (codes) used in a smart contract. The transaction fee is calculated in Ether, which is given as:

$$\text{Ether} = \text{Tx Fees} = \text{Gas Limit} * \text{Gas Price}$$

Q: 6. What is the fork? What are some of the types of forking?

A: 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

Q: Differentiate between Proof of Work vs Proof of Stake.

A: 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.

Q: What is a 51% attack?

A: In Blockchain, 51% attack refers to a vulnerability where an individual or group of people control the majority of the mining power (hash rate). This allows attackers to prevent new transactions from being confirmed. Further, they can double-spend the coins. In a 51% attack, smaller cryptocurrencies are being attacked.

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

A: 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.

Next Step to Success

With these Blockchain interview questions and answers, you will be able to sail through your blockchain interview with confidence. However, if you want to gain in-depth knowledge of blockchain, our **Blockchain Certification Training Course** will help you decipher the global buzz surrounding Blockchain, Bitcoin, and cryptocurrency. By developing a strong grasp of core Blockchain platforms, you will be motivated to create apps with Ethereum and become an expert in this emerging technology.



INDIA

Simplilearn Solutions Pvt Ltd.
53/1 C, Manoj Arcade, 24th Main,
Harlunkute, 2nd Sector, HSR Layout
Bangalore: 560102
Call us at: 1800-212-7688

USA

Simplilearn Americas, Inc.
201 Spear Street, Suite 1100,
San Francisco, CA 94105
United States
Phone No: +1-844-532-7688