

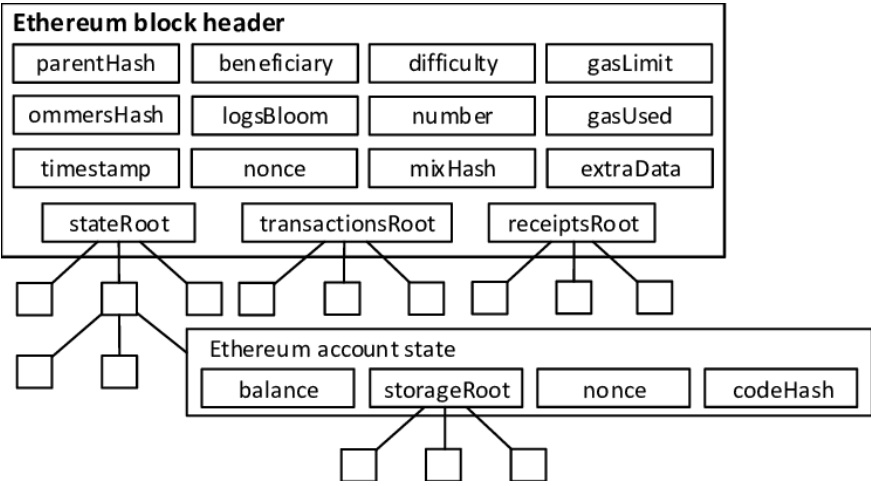
Interview Questions: Ethereum Fundamentals

| | |
|------------------|--|
| Q1 | Name two main consensus algorithms, and state the difference between the two as well as their pros and cons. |
| Reference | https://www.geeksforgeeks.org/difference-between-proof-of-work-pow-and-proof-of-stake-pos-in-blockchain/ |
| Ans | <ul style="list-style-type: none">a. Proof of Work (PoW): PoW is one of the most popular and mostly used consensus algorithms in permissionless blockchains such as Bitcoin, Ethereum and Litecoin. PoW involves finding a nonce value for the block that satisfies a specific condition (number of leading zeroes) set by the algorithm. Proof of Work enables consensus in the system by eliminating double Spending attack, race attack, etc. The disadvantages include usage of extremely high electricity costs, possibility of centralisation of miners owing to specialised hardware such as ASICs and requirement of a high capital investment.b. Proof of Stake (PoS): PoS is a common alternative to Proof of Work, and this consensus algorithm does not involve the concept of mining. Proof of Stake overcomes numerous problems faced in Proof of Work such as high electricity usage and high capital investments. In this algorithm, nodes invest in the native cryptocurrency, and validators are selected for each block proportionate to their staked investment. The selected nodes validate the validity of the newly submitted transactions and blocks. However, nodes can validate more than one block at a specific time and, hence, might lead to forks. This phenomenon is usually known as the 'Nothing at Stake' problem. |

| | |
|-----------|---|
| Q2 | What is the difference between externally owned accounts and contract accounts? How are they created? |
|-----------|---|

| | |
|------------|--|
| Ans | Externally owned accounts belong to a user and are controlled by a private key, whereas contract accounts are controlled by their contract code. |
|------------|--|

| | |
|-----------|--|
| Q3 | What are the different components of an Ethereum block header? |
|-----------|--|

| | |
|------------|--|
| Ans |  <p>The diagram illustrates the structure of an Ethereum block header and its associated account state. The Ethereum block header is a container for the following fields:</p> <ul style="list-style-type: none"> parentHash, beneficiary, difficulty, gasLimit ommersHash, logsBloom, number, gasUsed timestamp, nonce, mixHash, extraData stateRoot, transactionsRoot, receiptsRoot <p>Below the header, the Ethereum account state is shown, which includes:</p> <ul style="list-style-type: none"> balance, storageRoot, nonce, codeHash <p>The diagram uses boxes to represent these fields and lines to show the hierarchical relationships between them, such as the stateRoot pointing to a Merkle tree structure of account states.</p> |
|------------|--|

| | |
|-----------|--|
| Q4 | What are Ommer blocks and how do they make sense in the Ethereum blockchain? |
|-----------|--|

| | |
|------------|---|
| Ans | <p>In the case of Proof-of-Work mining, many miners are trying to mine the same set of transactions at the same time. Since the block mining time is extremely short (approximately 15 seconds in the case of ethereum), there is a possibility that more than one block is mined within a quite short interval. The block that is mined first is added to the main chain, but the effort of the miner who mined the other block is not simply let off. These competing blocks are called orphaned blocks.</p> <p>Ethereum paper states that “An ommer is a block whose parent is equal to the current block’s parent’s parent.” Miners are rewarded for mining orphaned blocks. This is the basic purpose of ommers. The</p> |
|------------|---|

| | |
|--|---|
| | <p>ommer blocks will be rewarded only if they are valid. Validity of an ommer means that it should be within the 6th generation or smaller to the current block. After 6, the orphaned blocks cannot be referenced. Ommer blocks do not receive the full reward, instead it receives a smaller reward. This incentive is introduced to Ethereum to promote mining in the network.</p> |
|--|---|

| | |
|------------|--|
| Q5 | What is a genesis block? Write a basic genesis config file. |
| Ans | <p>The first block of the Ethereum blockchain is called the genesis block. The following code details out the components of a genesis block. Note : Addresses given in the code are random. It does not imply anything.</p> <pre>// genesis.json { "alloc": { "0xca843569e3427144cead5e4d5999a3d0ccf92b8e": { "balance": "10000000000000000000000000000000" }, "0xfbd5c686b912d7722dc86510934589e0aaf3b55a": { "balance": "10000000000000000000000000000000" } }, "config": { "chainID": 68, "homesteadBlock": 0, "eip155Block": 0, "eip158Block": 0 }, "nonce": "0x0000000000000000", "difficulty": "0x0400",</pre> |

| | |
|--|---|
| | <pre> "mixhash": "0x00", "coinbase": "0x00", "timestamp": "0x00", "parentHash": "0x00", "extraData": "0x43a3dfdb4j343b428c638c19837004b5ed33adb3db69cb db7a38e1e50b1b82fa", "gasLimit": "0xffffffff" } </pre> |
|--|---|

| | |
|------------|---|
| Q6 | <p>What is the homesteadBlock parameter in the genesis config file?</p> <p>What is the value of the homesteadBlock parameter and what is its significance?</p> |
| Ans | <ol style="list-style-type: none"> Homestead is the second major version release of the Ethereum platform, which includes several protocol changes and a networking change that gives us the ability to carry out further network upgrades: EIP-2 Main homestead hardfork changes EIP-7 Hard Fork EVM update: DELEGATECALL EIP-8 devp2p forward compatibility |

| | |
|-----------|---|
| Q7 | <p>What is the difference between an Ethereum Address and an Ethereum public key?</p> |
|-----------|---|

| | |
|------------------|---|
| Reference | https://ethereum.stackexchange.com/questions/33171/ethereum-address-vs-public-key |
| Ans | An Ethereum address represents an account. For external-owned accounts, the address is derived as the last 20 bytes of the public key controlling the account, e.g., cd2a3d9f938e13cd947ec0i8um67fe734df8d886l. This is a hexadecimal format (base 16 notation), which is often indicated explicitly by prepending 0x to the address. Since each byte of the address is represented by 2 hex characters, a prefixed address is 42 characters long. |

| | |
|------------------|---|
| Q8 | What are the differences among the State Trie, the Receipt Trie and the Account Trie? |
| Reference | https://medium.com/cybermiles/diving-into-ethereums-world-state-c893102030ed |
| Ans | <ul style="list-style-type: none"> a. The state trie contains a key and value pair for every account that exists on the Ethereum network. b. Each Ethereum block has its own separate transaction trie. A block contains many transactions. c. The account state contains information about an Ethereum account. |

| | |
|------------|---|
| Q9 | What is the world state / global state in Ethereum? Fill in the blank. The world state in Ethereum is stored in a data structure called the _____ trie. |
| Ans | <ul style="list-style-type: none"> a. The world state is a mapping between addresses (accounts) and account states. The world state is not stored on the blockchain, but the Yellow Paper states its expected implementations to store this data in a trie (also referred as the state database or state trie). The world state can be seen as the global state that is constantly updated by transaction executions. The Ethereum |

| | |
|--|---|
| | <p>network is similar to a decentralised computer, and the world state is considered to be this computer's hard drive.</p> <p>b. The world state in Ethereum is stored in a data structure called the Merkle Patricia trie.</p> |
|--|---|

| | |
|------------------|--|
| Q10 | How does POW work in Ethereum? |
| Reference | https://eth.wiki/en/fundamentals/mining |
| Ans | <p>The proof of work algorithm used is called Ethash (a modified version of Dagger-Hashimoto) and involves finding a nonce input to the algorithm so that the result is below a certain threshold depending on the difficulty.</p> <p>Ethash PoW is memory-hard, making it ASIC-resistant. This means that calculating the PoW requires choosing subsets of a fixed resource depending on the nonce and block header. This resource (a few gigabyte size data) is called a directed acyclic graph (DAG). The DAG is entirely different every 30,000 blocks (a 100-hour window called an epoch) and takes some time to generate. Since the DAG only depends on the block height, it can be pregenerated, but if it is not, the client needs to wait until the end of this process to produce a block. Until clients precache DAGs in advance, the network may experience a massive block delay on each epoch transition. Note that the DAG does not need to be generated for verifying the PoW, essentially allowing for verification with both low CPU and small memory.</p> |

| | |
|------------------|---|
| Q11 | How does proof of authority work? |
| Reference | https://blockonomi.com/proof-of-authority/ |
| Ans | First, PoA was proposed by a group of developers in March 2017 (the term was coined by Gavin Wood) as a blockchain based on the |

| | |
|--|---|
| | <p>Ethereum protocol. It was developed primarily as a solution to the problem of spam attacks on Ethereum's Ropsten test network. The new network was named Kovan and is a primary test network available to all Ethereum users today.</p> <p>PoA consensus is an optimised Proof-of-Stake model that leverages identity as the form of stake rather than staking tokens. The identity is staked by a group of <i>validators</i> (authorities) that are pre-approved to validate transactions and blocks within the respective network. The group of validators is usually supposed to remain fairly small (~25 or lower) in order to ensure efficiency and manageable security of the network.</p> |
|--|---|

| | |
|------------------|---|
| Q12 | What is EVM? |
| Reference | https://www.bitdegree.org/learn/ethereum-virtual-machine#:~:text=Ethereum%20virtual%20machine%2C%20or%20EVM,created%20objects%20safe%20from%20modifying. |
| Ans | EVM stands for Ethereum Virtual Machine. It is a decentralised virtual machine capable of handling scripts using the public nodes network. It is also Turing complete and utilises Gas as an internal pricing mechanism. |

| | |
|------------------|---|
| Q13 | Explain the various layers of an Ethereum network. |
| Reference | https://www.ifourtechnolab.com/blog/blockchain-and-architecture |
| Ans | The Ethereum network can be broadly classified into the following layers: |

- | | |
|--|---|
| | <ol style="list-style-type: none">1) Storage layer: Any type of data created can be stored in a basic file system or a database. Usually, Ethereum uses databases such as LevelDB or RockDB to store the state of the whole network and other data.2) Network layer: Information such as transaction details is sent from one node to another in a Blockchain network. This can be done using different messaging protocols. In Ethereum, we use a protocol called JSON-RPC to communicate between nodes.3) Protocol layer: Data and network layers are present in any normal network. How do we differentiate between any network and a Blockchain network? This is defined by the protocol layer. This layer is majorly composed of the consensus protocols of the Blockchain network.4) Application layer: This is the layer that differentiates between Bitcoin and Ethereum. The application layer defines various types of conditions that can be written on top of the three layers for any particular application. It includes smart contracts that define your application logic. |
|--|---|