upGrad

Interview Questions:
Architecting DeFi Applications

Q1	What are the best practices while defining the DeFi app architecture?
Answer	• Upgradable smart contracts for security • Multiple nodes for scalability

Q2	What happens if a 51% attack takes place?
Answer	Data is rolled back as per the longest chain.

Q3	What are block confirmations?
Answer	Due to the possibility of a 51% attack, it is advisable to wait for 'n' number of blocks after the transaction is included in the block, before actually considering the transaction as the final payment.

Q4	What are the different Ether units in an Ethereum smart contract?

Answer	i. 1 wei = 1 ii. 1 szabo = 1e12 iii. 1 finney = 1e15 iv. 1 ether = 1e18

Q5	Can you store Ethereum in a smart contract?
Answer	Yes, we can store Ethereum in a smart contract.

Q6	Which Solidity function is used to verify a signature?
Answer	ecrecover()

Q7	What is a library in Solidity?
Answer	• A library is a piece of code that can be reused by other smart contracts. There are two types of libraries, which are as follows: 1. Deployed library 2. Embedded library • Deployed libraries have their own address, and also they can be used by several other contracts. Embedded libraries do not have their own address and are deployed as part of the code of the smart contract that uses them.

Q8	How can we produce a hash of multiple values in Solidity?
Answer	The following line of code can be used for the required purpose: keccak256(abi.encodePacked(a, b, c))

Q9	What is the ABIEncoderV2 pragma statement?
Answer	This is a pragma statement used to enable experimental features that are not yet enabled in standard Solidity. For instance, it enables to return a struct from a function that is called externally, which is not yet possible in standard Solidity (0.5.x).

Q10	How can we get the address of a smart contract that was deployed from another smart contract?
Answer	We can get the required address by the following code: address childAddress = address(new Child())

Q11	How would you optimally order uint128, bytes32, and another uint128 to save gas?
Answer	• Order 1. uint128 2. uint128 3. Bytes32 • Explanation The EVM stores variables in 32-byte slots. However, Solidity is smart enough to pack several variables into a single slot if they can fit together. For this optimization to work, packed variables have to be defined next to each other. In the example given above, the two uint128 will be placed in the same 256-bit slots (128 + 128 = 256).

Q12	Mention three ways to save gas.
Answer	a. Put less data on-chain. b. Use events instead of storage. c. Ensure an optimal order for variable declaration.

Q13	Is it necessary to make an address payable to transfer ERC20 tokens?

Answer	No. The payable requirement is only required for a native Ether. Ethereum has no knowledge of ERC20 tokens. For Ethereum, this is simply a variable in a smart contract, similar to any other variables.

Q14	What is the difference between an address and address payable?
Answer	Only address payable can receive money.

Q15	What are the four memory locations of Solidity?
Answer	Storage, Memory, Stack, and Calldata

Q16	What is the use of account nonce in smart contract transactions?
Answer	Each account has a transaction counter. It prevents replay attacks where a transaction sending, for example, 20 coins, from A to B can be replayed by B over and over to continually drain A's balance.

Q17	What are HD wallets?
Answer	• Hierarchical Deterministic wallets (or HD wallets) were introduced by BIP 32 (BIPs stand for Bitcoin Improvement Proposals) and later improved by BIP 44. While HD wallets were introduced by the Bitcoin community, it is a wallet structure that supports many coins. HD wallets can allow for an entire suite of crypto wallets to be

	generated from a single seed phrase, although not a commonly used feature. • But, what is an HD wallet? Simply put, an HD wallet is a public/private key tree starting from a root node (master node). • To generate key pairs 1. Mnemonic + m / purpose' / coin_type' / account' / chain / address_index

Q18	How to cancel a transaction?
Answer	Once a transaction has been done, nobody can prevent it from being mined and validated by a miner. However, you can still send another transaction preventing the first one from working if it is mined before the first transaction. This second transaction will have the following properties: 1. It will have the exact same nonce (an incrementing integer that is sent in each transaction, specific to each Ethereum address). 2. It will have a higher gas price than the first one. 3. It will also send a tiny amount of Ether to another address.

Q19	What is the benefit of publishing a smart contact on explorers such as Etherscan?
Answer	Publishing a smart contact on explorers such as Etherscan helps in ensuring that smart contract code is exactly the same as what is being deployed onto the blockchain. It also allows the public to read and audit the contract.

Q20	What will happen to the existing smart contracts after ETH2.0's launch?
Answer	Nothing; everything will work as it is. Only the mining algorithm will be different, which has no impact on a smart contract's data.