

WEB 3.0 SECURITY INTERVIEW QUESTIONS & ANSWERS

Prepared by HANIM EKEN

<https://ie.linkedin.com/in/hanimeken>

<https://ie.linkedin.com/in/hanimeken>

1. What are smart contracts, and how do they differ from traditional contracts?

Smart contracts are self-executing contracts with the terms and conditions of an agreement directly written into code. They run on blockchain platforms like Ethereum. Unlike traditional contracts, smart contracts automatically execute when predefined conditions are met, removing the need for intermediaries and ensuring trust through code and cryptography.

2. Explain the role of gas in Ethereum smart contracts.

Gas is a unit of measurement for the computational work required to execute a transaction or smart contract on the Ethereum network. Users pay gas fees to incentivize miners to include their transactions in blocks. Smart contract developers must optimize their code to use as little gas as possible to make transactions cost-effective for users.

3. Explain the concept of a blockchain and how it differs from traditional databases.

A blockchain is a distributed, immutable ledger that records transactions across a network of nodes. It differs from traditional databases by its decentralized nature, immutability, transparency, and the use of cryptographic hashes to secure data. Transactions on a blockchain are tamper-proof once confirmed, making it suitable for trustless applications.

4. What are smart contracts, and how do they work in the context of Web3 development?

Smart contracts are self-executing agreements with code that automatically enforces and executes predefined rules when specific conditions are met. In Web3 development, smart contracts are deployed on blockchain networks and interact with DApps. They enable trustless, automated, and transparent transactions.

5. Can you describe the Ethereum Virtual Machine (EVM) and its role in Web3 development?

The Ethereum Virtual Machine (EVM) is the runtime environment for executing smart contracts on the Ethereum blockchain. It's responsible for processing and executing code on the network. Web3 developers interact with the EVM through various libraries and frameworks to deploy and interact with smart contracts.

6. Explain the difference between public and private blockchains and their use cases.

Public blockchains, like Ethereum, are open to anyone and offer transparency and decentralization. Private blockchains are permissioned and typically used by organizations for internal purposes. Public blockchains are suitable for open DApps, while private blockchains are more focused on controlled access and privacy.

7. How do you handle security concerns in Web3 development, especially when dealing with smart contracts?

Security in Web3 development is critical. Best practices include code audits, input validation, handling exceptions, using established libraries, and following security standards like the OpenZeppelin library. Additionally, developers should stay updated on security vulnerabilities and consider formal verification methods.

8. Can you explain what a decentralized application (DApp) is and provide an example of a DApp you've worked on?

A DApp is an application that runs on a decentralized network, typically utilizing smart contracts. Mention a DApp project you've worked on, highlighting its purpose, the blockchain platform used, your role, and the technologies employed.

9. Can you explain the concept of token standards in blockchain, such as ERC-20 and ERC-721?

Token standards define the rules and standards that a token on a blockchain must adhere to. ERC-20 is a standard for fungible tokens (e.g., cryptocurrencies), while ERC-721 is a standard for non-fungible tokens (NFTs), which represent unique assets like collectibles and digital art. These standards ensure interoperability and compatibility with various platforms and wallets.

10. How do you handle security concerns in smart contract development?

Security in smart contract development is crucial. Best practices include code audits, following the "Principle of Least Authority," implementing access controls, using external libraries cautiously, and thoroughly testing contracts on testnets. Developers should also stay updated on security vulnerabilities and community recommendations.

11. What are decentralized identifiers (DIDs) and their significance in web3 development?

DIDs are a new type of identifier that enable verifiable, self-sovereign digital identities. They play a significant role in web3 development by allowing users to control and own their identities across different applications and platforms without relying on centralized authorities.