Smart Contracts and Game Theory – Quiz

Cryptoeconomics

Question 1

What is a smart contract?

A. A legal document
B. Self-executing code on blockchain that enforces agreements
C. A trading bot
D. A wallet type

Question 1

What is a smart contract?

A. A legal document
B. Self-executing code on blockchain that enforces agreements
C. A trading bot
D. A wallet type

Answer: B
Smart contracts are programs stored on blockchain that automatically execute when conditions are met.

Question 2

Which blockchain platform popularized Turing-complete smart contracts?

A. Bitcoin
B. Ethereum
C. Litecoin
D. Ripple

Question 2

Which blockchain platform popularized Turing-complete smart contracts?

A. Bitcoin
B. Ethereum
C. Litecoin
D. Ripple

Answer: B
Ethereum, launched in 2015, popularized Turing-complete smart contracts. The term 'smart contract' was coined by Nick Szabo in 1994. Bitcoin has limited scripting capabilities but is not Turing-complete.

Question 3

What is Solidity?

A. A cryptocurrency
B. The primary programming language for Ethereum smart contracts
C. A consensus mechanism
D. A wallet

Question 3

What is Solidity?

A. A cryptocurrency
B. The primary programming language for Ethereum smart contracts
C. A consensus mechanism
D. A wallet

Answer: B
Solidity is the main programming language used to write smart contracts on Ethereum and EVM-compatible chains.

Question 4

What is a 'Nash equilibrium' in game theory?

A. Maximum profit point
B. A state where no player benefits from unilaterally changing strategy
C. Network balance
D. Token distribution

Question 4

What is a 'Nash equilibrium' in game theory?

A. Maximum profit point
B. A state where no player benefits from unilaterally changing strategy
C. Network balance
D. Token distribution

Answer: B
Nash equilibrium occurs when each player's strategy is optimal given all other players' strategies.

Question 5

What is 'mechanism design'?

A. Hardware engineering
B. Designing rules and incentives to achieve desired outcomes
C. Smart contract coding
D. Token creation

Question 5

What is 'mechanism design'?

A. Hardware engineering
B. Designing rules and incentives to achieve desired outcomes
C. Smart contract coding
D. Token creation

Answer: B
Mechanism design creates incentive structures that align individual self-interest with system goals.

Question 6

What is the 'Prisoner's Dilemma' relevant to in blockchain?

A. Mining efficiency
B. Understanding why self-interested actors might not cooperate optimally
C. Wallet security
D. Token pricing

Question 6

What is the 'Prisoner's Dilemma' relevant to in blockchain?

A. Mining efficiency
B. Understanding why self-interested actors might not cooperate optimally
C. Wallet security
D. Token pricing

Answer: B
The Prisoner's Dilemma illustrates how rational self-interest can lead to suboptimal outcomes without proper incentive design.

Question 7

What is 'gas' in Ethereum?

A. Fuel for mining rigs
B. The unit measuring computational work for transactions
C. A token type
D. Network speed

Question 7

What is 'gas' in Ethereum?

A. Fuel for mining rigs
B. The unit measuring computational work for transactions
C. A token type
D. Network speed

Answer: B
Gas measures computational effort; users pay gas fees in ETH to compensate validators for execution.

Question 8

What is a 'reentrancy attack'?

A. Logging in twice
B. Exploiting a contract that makes external calls before updating state
C. DDoS attack
D. Brute force attack

Question 8

What is a 'reentrancy attack'?

A. Logging in twice
B. Exploiting a contract that makes external calls before updating state
C. DDoS attack
D. Brute force attack

Answer: B
Reentrancy attacks exploit contracts that call external addresses before updating internal state, allowing repeated withdrawals.

Question 9

What is an 'oracle' in blockchain?

A. A prediction market
B. A service that provides external data to smart contracts
C. A mining pool
D. A wallet provider

Question 9

What is an 'oracle' in blockchain?

A. A prediction market

B. A service that provides external data to smart contracts

C. A mining pool

D. A wallet provider

Answer: B
Oracles bridge real-world data (prices, weather, events) to on-chain smart contracts.

Question 10

What is the ERC-20 standard?

A. A consensus algorithm
B. A standard interface for fungible tokens on Ethereum
C. A wallet format
D. A mining protocol

Question 10

What is the ERC-20 standard?

A. A consensus algorithm
B. A standard interface for fungible tokens on Ethereum
C. A wallet format
D. A mining protocol

Answer: B
ERC-20 defines a common interface for tokens, enabling interoperability across wallets and exchanges.

Question 11

What is 'incentive compatibility'?

A. Hardware compatibility
B. When honest behavior is the rational self-interested choice
C. Token compatibility
D. Network compatibility

Question 11

What is 'incentive compatibility'?

A. Hardware compatibility
B. When honest behavior is the rational self-interested choice
C. Token compatibility
D. Network compatibility

Answer: B
A mechanism is incentive compatible when participants maximize their utility by acting honestly.

Question 12

What is a 'Sybil attack'?

A. A virus
B. Creating multiple fake identities to gain disproportionate influence
C. A mining attack
D. A wallet hack

Question 12

What is a 'Sybil attack'?

A. A virus
B. Creating multiple fake identities to gain disproportionate influence
C. A mining attack
D. A wallet hack

Answer: B
Sybil attacks use multiple pseudonymous identities to subvert reputation or voting systems.

Question 13

What does 'code is law' mean in smart contracts?

A. Coding is legally required
B. Contract execution follows code exactly, regardless of intent
C. Lawyers must learn coding
D. All laws are coded

Question 13

What does 'code is law' mean in smart contracts?

A. Coding is legally required

B. Contract execution follows code exactly, regardless of intent

C. Lawyers must learn coding

D. All laws are coded

Answer: B

Code is law means smart contracts execute exactly as written, with no human interpretation or intervention. The 2016 DAO hack challenged this philosophy when Ethereum hard-forked to reverse an exploit, showing that social consensus can override code execution in exceptional cases.

Question 14

What is the ERC-721 standard?

A. A fungible token standard
B. The standard for non-fungible tokens (NFTs) on Ethereum
C. A stablecoin standard
D. A governance token standard

Question 14

What is the ERC-721 standard?

A. A fungible token standard
B. The standard for non-fungible tokens (NFTs) on Ethereum
C. A stablecoin standard
D. A governance token standard

Answer: B
ERC-721 defines NFTs - unique tokens representing ownership of distinct assets.

Question 15

What is 'frontrunning' in blockchain?

A. Running a node
B. Inserting transactions ahead of others after seeing pending transactions
C. Mining first
D. Leading a team

Question 15

What is 'frontrunning' in blockchain?

A. Running a node
B. Inserting transactions ahead of others after seeing pending transactions
C. Mining first
D. Leading a team

Answer: B
Frontrunning exploits visibility of pending transactions to profit by executing trades first.

Question 16

What is MEV (Maximal Extractable Value)?

A. Maximum transaction value
B. Value extractable by reordering, including, or excluding transactions
C. Mining efficiency value
D. Market exchange value

Question 16

What is MEV (Maximal Extractable Value)?

A. Maximum transaction value

B. Value extractable by reordering, including, or excluding transactions

C. Mining efficiency value

D. Market exchange value

Answer: B

MEV is the value validators can extract by manipulating transaction ordering in blocks. Originally 'Miner Extractable Value' pre-Merge (Sept 2022), renamed to 'Maximal' after Ethereum's transition to PoS.

Question 17

What is an 'immutable' smart contract?

A. A contract that can be updated
B. A contract whose code cannot be changed after deployment
C. A temporary contract
D. A test contract

Question 17

What is an 'immutable' smart contract?

A. A contract that can be updated

B. A contract whose code cannot be changed after deployment

C. A temporary contract

D. A test contract

Answer: B

Immutable contracts cannot be modified once deployed, ensuring trustless and predictable behavior. Immutability also means bugs cannot be fixed. This trade-off drives the use of proxy patterns for upgradeable contracts, though those introduce trust assumptions.

Question 18

What is a 'proxy contract' pattern?

A. A voting contract
B. A pattern enabling upgradeable smart contracts
C. A mining contract
D. A token contract

Question 18

What is a 'proxy contract' pattern?

A. A voting contract
B. A pattern enabling upgradeable smart contracts
C. A mining contract
D. A token contract

Answer: B
Proxy contracts separate storage and logic, allowing the logic to be upgraded while preserving state.

Question 19

What is 'commit-reveal' scheme used for?

A. Version control
B. Fair voting or auctions by hiding choices until reveal phase
C. Transaction signing
D. Mining coordination

Question 19

What is 'commit-reveal' scheme used for?

A. Version control
B. Fair voting or auctions by hiding choices until reveal phase
C. Transaction signing
D. Mining coordination

Answer: B
Commit-reveal prevents frontrunning in votes/auctions by first committing to hashed choices, then revealing.

Question 20

What is a 'time-lock' in smart contracts?

A. A security feature
B. A mechanism that delays execution until a specified time
C. Transaction speed limit
D. Mining timeout

Question 20

What is a 'time-lock' in smart contracts?

A. A security feature
B. A mechanism that delays execution until a specified time
C. Transaction speed limit
D. Mining timeout

Answer: B
Time-locks delay actions, providing security by allowing review before irreversible operations.

Question 21

A validator observes a large pending transaction that will buy Token X on a DEX, causing its price to spike. The validator places their own buy order for Token X before including the user's transaction, then sells after the price rises. What is this scenario?

A. Reentrancy attack
B. Sandwich attack (MEV extraction)
C. Sybil attack
D. Flash loan attack

Question 21

A validator observes a large pending transaction that will buy Token X on a DEX, causing its price to spike. The validator places their own buy order for Token X before including the user's transaction, then sells after the price rises. What is this scenario?

A. Reentrancy attack
B. Sandwich attack (MEV extraction)
C. Sybil attack
D. Flash loan attack

Answer: B
This is a sandwich attack, a form of MEV where validators profit by placing their own transactions before and after a victim's trade. The validator buys before (frontrunning), the victim's buy pushes the price up, then the validator sells (backrunning) for a profit.

Question 22

A DAO proposal to upgrade the treasury contract receives 60% support. However, 10 large whales who collectively hold 45% of tokens did not vote. Under what mechanism would their non-participation prevent the upgrade from executing?

A. Simple majority voting
B. Quorum requirement with absolute threshold
C. Quadratic voting
D. Conviction voting

Question 22

A DAO proposal to upgrade the treasury contract receives 60% support. However, 10 large whales who collectively hold 45% of tokens did not vote. Under what mechanism would their non-participation prevent the upgrade from executing?

A. Simple majority voting

B. Quorum requirement with absolute threshold

C. Quadratic voting

D. Conviction voting

Answer: B

A quorum requirement sets a minimum participation threshold (e.g., 50% of all tokens must vote) for a proposal to be valid. If the quorum is not met, the proposal fails regardless of support percentage. Here, if only 55% voted and quorum requires ¿60%, the upgrade would not execute despite having 60% approval among participants.

Question 23

In a blockchain mining game, two miners each choose to either cooperate (share resources) or defect (mine alone). If both cooperate, each gets 3 rewards. If both defect, each gets 1 reward. If one defects while the other cooperates, the defector gets 5 and the cooperator gets 0. What is the Nash equilibrium?

A. Both cooperate (3,3)
B. Both defect (1,1)
C. One cooperates, one defects
D. No Nash equilibrium exists

Question 23

In a blockchain mining game, two miners each choose to either cooperate (share resources) or defect (mine alone). If both cooperate, each gets 3 rewards. If both defect, each gets 1 reward. If one defects while the other cooperates, the defector gets 5 and the cooperator gets 0. What is the Nash equilibrium?

A. Both cooperate (3,3)
B. Both defect (1,1)
C. One cooperates, one defects
D. No Nash equilibrium exists

Answer: B
This is the classic Prisoner's Dilemma. Both defecting (1,1) is the Nash equilibrium because neither player can improve by unilaterally changing strategy. If either switches to cooperate, they get 0 (worse than 1). Despite (3,3) being better for both, it's unstable without coordination mechanisms.

Question 24

A DEX uses an automated market maker with the constant product formula x * y = k. If the pool has 1000 ETH and 2,000,000 USDC, and a trader swaps 100 ETH into the pool (ignoring fees), approximately what USDC do they receive?

A. 200,000 USDC
B. 181,818 USDC
C. 190,476 USDC
D. 166,667 USDC

Question 24

A DEX uses an automated market maker with the constant product formula x * y = k. If the pool has 1000 ETH and 2,000,000 USDC, and a trader swaps 100 ETH into the pool (ignoring fees), approximately what USDC do they receive?

A. 200,000 USDC

B. 181,818 USDC

C. 190,476 USDC

D. 166,667 USDC

Answer: B

k = 1000 * 2,000,000 = 2,000,000,000. After adding 100 ETH: new_x = 1100, so new_y = 2,000,000,000 / 1100 1,818,182. USDC received = 2,000,000 - 1,818,182 = 181,818 USDC. The constant product formula naturally creates slippage for large trades.

Question 25

A smart contract holds 100 ETH in a multisig wallet requiring 3-of-5 signatures. Three signers collude to submit a withdrawal to their own address. What game-theoretic assumption failed?

A. Incentive compatibility
B. Nash equilibrium stability
C. Independence of signers (no collusion assumption)
D. Mechanism design optimality

Question 25

A smart contract holds 100 ETH in a multisig wallet requiring 3-of-5 signatures. Three signers collude to submit a withdrawal to their own address. What game-theoretic assumption failed?

A. Incentive compatibility
B. Nash equilibrium stability
C. Independence of signers (no collusion assumption)
D. Mechanism design optimality

Answer: C
Multisig security assumes signers are independent and won't collude. If 3 signers can collude, they form a majority and the multisig offers no protection. This highlights the importance of signer diversity and the distinction between cryptographic security (math) and game-theoretic security (incentives/behavior).

Question 26 (True/False)

Smart contracts can be modified after deployment.

A. True
B. False

Question 26 (True/False)

Smart contracts can be modified after deployment.

A. True

B. False

Answer: False

Smart contracts are generally immutable after deployment - their code cannot be changed. This ensures trustless execution but also means bugs cannot be fixed. Proxy patterns can enable upgradeability but introduce trust assumptions.

Question 27 (True/False)

Nash equilibrium means all players are satisfied.

A. True
B. False

Question 27 (True/False)

Nash equilibrium means all players are satisfied.

A. True

B. False

Answer: False

Nash equilibrium means no player can unilaterally improve their outcome by changing strategy. Players may not be satisfied - the equilibrium can be suboptimal for everyone (like in Prisoner's Dilemma).

Question 28 (True/False)

MEV stands for Maximal Extractable Value.

A. True
B. False

Question 28 (True/False)

MEV stands for Maximal Extractable Value.

A. True

B. False

Answer: True

MEV (Maximal Extractable Value) is value that validators can extract by reordering, including, or excluding transactions. Originally called 'Miner Extractable Value' before Ethereum's Merge to PoS in September 2022.

Question 29 (True/False)

DAOs are controlled by a single entity.

A. True
B. False

Question 29 (True/False)

DAOs are controlled by a single entity.

A. True

B. False

Answer: False

DAOs (Decentralized Autonomous Organizations) are governed by smart contracts and token holder voting, not by a single centralized entity. Decision-making is distributed among participants.

Question 30 (True/False)

Front-running is a form of MEV extraction.

A. True
B. False

Question 30 (True/False)

Front-running is a form of MEV extraction.

A. True

B. False

Answer: True

Front-running (inserting transactions ahead of others after seeing pending transactions) is a common MEV extraction technique. Validators profit by reordering transactions to their advantage.

Question 31 (True/False)

Solidity is the only language for writing smart contracts.

A. True
B. False

Question 31 (True/False)

Solidity is the only language for writing smart contracts.

A. True

B. False

Answer: False

While Solidity is the most popular language for Ethereum smart contracts, other languages exist: Vyper (Python-like for Ethereum), Rust (for Solana), Move (for Sui/Aptos), and Cairo (for StarkNet).

Question 32 (Fill in the Blank)

___ **equilibrium is when no player can improve by changing strategy.** *Hint: Named after a mathematician...*

Question 32 (Fill in the Blank)

___ equilibrium is when no player can improve by changing strategy. *Hint: Named after a mathematician...* **Answer:**

Nash
Nash equilibrium occurs when each player's strategy is optimal given all other players' strategies.

Question 33 (Fill in the Blank)

MEV stands for Maximal Extractable ___. *Hint: What validators extract...*

Question 33 (Fill in the Blank)

MEV stands for Maximal Extractable ___. *Hint: What validators extract...* **Answer: Value**

MEV (Maximal Extractable Value) is value that validators can extract by reordering, including, or excluding transactions.

Question 34 (Fill in the Blank)

A ___ is a decentralized autonomous organization. *Hint: Three letters...*

Question 34 (Fill in the Blank)

A ___ is a decentralized autonomous organization. *Hint: Three letters...* **Answer: DAO**

DAO (Decentralized Autonomous Organization) is governed by smart contracts and token holder voting.