Blockchain Foundations – Quiz

20 Multiple-Choice Questions

Prof. Dr. J. Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

Quiz Questions 1–5

Q1. What is the "double-spending problem" in digital payments?
A) Paying twice the normal fee B) Spending the same digital coin more than once
C) Two miners finding a block simultaneously D) A user creating two wallets

Quiz Questions 1–5

Q1. What is the "double-spending problem" in digital payments?
A) Paying twice the normal fee B) Spending the same digital coin more than once
C) Two miners finding a block simultaneously D) A user creating two wallets
Answer: B – Digital data can be copied, so without consensus, the same coin could be sent to multiple people.

Q2. On the trust spectrum shown in the lecture, what does moving from left to right represent?
A) Increasing transaction speed B) Replacing human trust with technical mechanisms
C) Increasing transaction fees D) Moving from digital to physical assets

Quiz Questions 1–5

Q1. What is the "double-spending problem" in digital payments?
A) Paying twice the normal fee B) Spending the same digital coin more than once
C) Two miners finding a block simultaneously D) A user creating two wallets
Answer: B – Digital data can be copied, so without consensus, the same coin could be sent to multiple people.

Q2. On the trust spectrum shown in the lecture, what does moving from left to right represent?
A) Increasing transaction speed B) Replacing human trust with technical mechanisms
C) Increasing transaction fees D) Moving from digital to physical assets
Answer: B – Each step rightward removes a layer of human trust and replaces it with a verifiable rule.

Q3. Which three words best summarize what a blockchain is?
A) Fast, private, centralized B) Shared, permanent, decentralized
C) Encrypted, anonymous, instant D) Cheap, scalable, regulated

Quiz Questions 1–5

Q1. What is the "double-spending problem" in digital payments?
A) Paying twice the normal fee B) Spending the same digital coin more than once
C) Two miners finding a block simultaneously D) A user creating two wallets
Answer: B – Digital data can be copied, so without consensus, the same coin could be sent to multiple people.

Q2. On the trust spectrum shown in the lecture, what does moving from left to right represent?
A) Increasing transaction speed B) Replacing human trust with technical mechanisms
C) Increasing transaction fees D) Moving from digital to physical assets
Answer: B – Each step rightward removes a layer of human trust and replaces it with a verifiable rule.

Q3. Which three words best summarize what a blockchain is?
A) Fast, private, centralized B) Shared, permanent, decentralized
C) Encrypted, anonymous, instant D) Cheap, scalable, regulated
Answer: B – A blockchain is a shared notebook that everyone can read, nobody can erase, and no single person controls.

Q4. What is the "avalanche effect" in hash functions?
A) Hash outputs grow larger over time B) A tiny input change produces a completely different output
C) Multiple inputs always produce the same hash D) Hashing becomes slower as the blockchain grows

Quiz Questions 1–5

Q1. What is the "double-spending problem" in digital payments?
A) Paying twice the normal fee B) Spending the same digital coin more than once
C) Two miners finding a block simultaneously D) A user creating two wallets
Answer: B – Digital data can be copied, so without consensus, the same coin could be sent to multiple people.

Q2. On the trust spectrum shown in the lecture, what does moving from left to right represent?
A) Increasing transaction speed B) Replacing human trust with technical mechanisms
C) Increasing transaction fees D) Moving from digital to physical assets
Answer: B – Each step rightward removes a layer of human trust and replaces it with a verifiable rule.

Q3. Which three words best summarize what a blockchain is?
A) Fast, private, centralized B) Shared, permanent, decentralized
C) Encrypted, anonymous, instant D) Cheap, scalable, regulated
Answer: B – A blockchain is a shared notebook that everyone can read, nobody can erase, and no single person controls.

Q4. What is the "avalanche effect" in hash functions?
A) Hash outputs grow larger over time B) A tiny input change produces a completely different output
C) Multiple inputs always produce the same hash D) Hashing becomes slower as the blockchain grows
Answer: B – Changing "Hello" to "hello" produces a completely different SHA-256 fingerprint.

Q5. Alice has 1 BTC and broadcasts two transactions: 1 BTC to Bob and 1 BTC to Carol. What does the network do?
A) Duplicates the coin so both receive 1 BTC B) Rejects both transactions
C) Accepts one transaction and rejects the other D) Splits the coin into 0.5 BTC each

Quiz Questions 1–5

Q1. What is the "double-spending problem" in digital payments?
A) Paying twice the normal fee B) Spending the same digital coin more than once
C) Two miners finding a block simultaneously D) A user creating two wallets
Answer: B – Digital data can be copied, so without consensus, the same coin could be sent to multiple people.

Q2. On the trust spectrum shown in the lecture, what does moving from left to right represent?
A) Increasing transaction speed B) Replacing human trust with technical mechanisms
C) Increasing transaction fees D) Moving from digital to physical assets
Answer: B – Each step rightward removes a layer of human trust and replaces it with a verifiable rule.

Q3. Which three words best summarize what a blockchain is?
A) Fast, private, centralized B) Shared, permanent, decentralized
C) Encrypted, anonymous, instant D) Cheap, scalable, regulated
Answer: B – A blockchain is a shared notebook that everyone can read, nobody can erase, and no single person controls.

Q4. What is the "avalanche effect" in hash functions?
A) Hash outputs grow larger over time B) A tiny input change produces a completely different output
C) Multiple inputs always produce the same hash D) Hashing becomes slower as the blockchain grows
Answer: B – Changing "Hello" to "hello" produces a completely different SHA-256 fingerprint.

Q5. Alice has 1 BTC and broadcasts two transactions: 1 BTC to Bob and 1 BTC to Carol. What does the network do?
A) Duplicates the coin so both receive 1 BTC B) Rejects both transactions
C) Accepts one transaction and rejects the other D) Splits the coin into 0.5 BTC each
Answer: C – The network reaches consensus on which transaction is valid; the duplicate is rejected.

Quiz Questions 6–10

Q6. Block 100 has fingerprint `abc123`. **Block 101 stores "previous =** `abc123`**." An attacker changes Block 100. What happens?**
A) Block 101 updates automatically B) Block 100's fingerprint changes, creating a mismatch with Block 101
C) Nothing visible changes D) The network deletes both blocks

Quiz Questions 6–10

Q6. Block 100 has fingerprint `abc123`. Block 101 stores "previous = `abc123`." An attacker changes Block 100. What happens?
A) Block 101 updates automatically B) Block 100's fingerprint changes, creating a mismatch with Block 101
C) Nothing visible changes D) The network deletes both blocks
Answer: B – Tampering changes the hash, breaking the chain link; all subsequent blocks detect the mismatch.

Q7. In Proof of Work, a miner spends $50,000 on electricity and submits a valid block worth $300,000. What is the profit?
A) $50,000 B) $250,000 C) $300,000 D) $350,000

Quiz Questions 6–10

Q6. Block 100 has fingerprint `abc123`. Block 101 stores "previous = `abc123`." An attacker changes Block 100. What happens?
A) Block 101 updates automatically B) Block 100's fingerprint changes, creating a mismatch with Block 101
C) Nothing visible changes D) The network deletes both blocks
Answer: B – Tampering changes the hash, breaking the chain link; all subsequent blocks detect the mismatch.

Q7. In Proof of Work, a miner spends $50,000 on electricity and submits a valid block worth $300,000. What is the profit?
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = reward ($300,000) minus electricity cost ($50,000) = $250,000.

Q8. A blockchain prioritizes high throughput and strong security but uses only 20 validators. Which trilemma property is sacrificed?
A) Security B) Scalability C) Decentralization D) Privacy

Quiz Questions 6–10

Q6. Block 100 has fingerprint `abc123`. Block 101 stores "previous = `abc123`." An attacker changes Block 100. What happens?
A) Block 101 updates automatically B) Block 100's fingerprint changes, creating a mismatch with Block 101
C) Nothing visible changes D) The network deletes both blocks
Answer: B – Tampering changes the hash, breaking the chain link; all subsequent blocks detect the mismatch.

Q7. In Proof of Work, a miner spends $50,000 on electricity and submits a valid block worth $300,000. What is the profit?
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = reward ($300,000) minus electricity cost ($50,000) = $250,000.

Q8. A blockchain prioritizes high throughput and strong security but uses only 20 validators. Which trilemma property is sacrificed?
A) Security B) Scalability C) Decentralization D) Privacy
Answer: C – Fewer validators means less decentralization; this is how chains like Solana achieve high speed.

Q9. Bitcoin processes about 7 transactions per second while Visa handles 65,000. According to the lecture, what explains this gap?
A) Bitcoin uses older hardware B) The price of achieving decentralized consensus
C) Visa uses blockchain internally D) Bitcoin deliberately limits users

Quiz Questions 6–10

Q6. Block 100 has fingerprint `abc123`. Block 101 stores "previous = `abc123`." An attacker changes Block 100. What happens?
A) Block 101 updates automatically B) Block 100's fingerprint changes, creating a mismatch with Block 101
C) Nothing visible changes D) The network deletes both blocks
Answer: B – Tampering changes the hash, breaking the chain link; all subsequent blocks detect the mismatch.

Q7. In Proof of Work, a miner spends $50,000 on electricity and submits a valid block worth $300,000. What is the profit?
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = reward ($300,000) minus electricity cost ($50,000) = $250,000.

Q8. A blockchain prioritizes high throughput and strong security but uses only 20 validators. Which trilemma property is sacrificed?
A) Security B) Scalability C) Decentralization D) Privacy
Answer: C – Fewer validators means less decentralization; this is how chains like Solana achieve high speed.

Q9. Bitcoin processes about 7 transactions per second while Visa handles 65,000. According to the lecture, what explains this gap?
A) Bitcoin uses older hardware B) The price of achieving decentralized consensus
C) Visa uses blockchain internally D) Bitcoin deliberately limits users
Answer: B – Getting 50,000 computers to agree without a leader is far slower than one company processing payments.

Q10. A company where only one department controls all data considers using blockchain. The decision tree says:
A) Use blockchain for better encryption B) Use a database — single-party control does not need blockchain
C) Use blockchain to impress investors D) Use blockchain because it is newer technology

Quiz Questions 6–10

Q6. Block 100 has fingerprint `abc123`. Block 101 stores "previous = `abc123`." An attacker changes Block 100. What happens?
A) Block 101 updates automatically B) Block 100's fingerprint changes, creating a mismatch with Block 101
C) Nothing visible changes D) The network deletes both blocks
Answer: B – Tampering changes the hash, breaking the chain link; all subsequent blocks detect the mismatch.

Q7. In Proof of Work, a miner spends $50,000 on electricity and submits a valid block worth $300,000. What is the profit?
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = reward ($300,000) minus electricity cost ($50,000) = $250,000.

Q8. A blockchain prioritizes high throughput and strong security but uses only 20 validators. Which trilemma property is sacrificed?
A) Security B) Scalability C) Decentralization D) Privacy
Answer: C – Fewer validators means less decentralization; this is how chains like Solana achieve high speed.

Q9. Bitcoin processes about 7 transactions per second while Visa handles 65,000. According to the lecture, what explains this gap?
A) Bitcoin uses older hardware B) The price of achieving decentralized consensus
C) Visa uses blockchain internally D) Bitcoin deliberately limits users
Answer: B – Getting 50,000 computers to agree without a leader is far slower than one company processing payments.

Q10. A company where only one department controls all data considers using blockchain. The decision tree says:
A) Use blockchain for better encryption B) Use a database — single-party control does not need blockchain
C) Use blockchain to impress investors D) Use blockchain because it is newer technology
Answer: B – The decision tree exits at "multiple parties with trust deficit"; one trusted party should use a database.

Quiz Questions 11–15

Q11. The first real-world purchase using Bitcoin was 10,000 BTC for two pizzas in 2010. This event proved that:
A) Bitcoin is too expensive for daily use B) Digital scarcity works — those coins could only be spent once
C) Pizza is the ideal blockchain use case D) Bitcoin's price never changes

Quiz Questions 11–15

Q11. The first real-world purchase using Bitcoin was 10,000 BTC for two pizzas in 2010. This event proved that:
A) Bitcoin is too expensive for daily use B) Digital scarcity works — those coins could only be spent once
C) Pizza is the ideal blockchain use case D) Bitcoin's price never changes
Answer: B – The pizza transaction demonstrated that digital coins enforced by consensus have real purchasing power.

Q12. A cheating miner spends $50,000 on electricity and submits a fraudulent block. The network rejects it. What is the outcome?
A) The miner earns half the reward B) The miner loses $50,000 with no reward
C) The network shuts down temporarily D) Other miners share the lost reward

Quiz Questions 11–15

Q11. The first real-world purchase using Bitcoin was 10,000 BTC for two pizzas in 2010. This event proved that:
A) Bitcoin is too expensive for daily use B) Digital scarcity works — those coins could only be spent once
C) Pizza is the ideal blockchain use case D) Bitcoin's price never changes
Answer: B – The pizza transaction demonstrated that digital coins enforced by consensus have real purchasing power.

Q12. A cheating miner spends $50,000 on electricity and submits a fraudulent block. The network rejects it. What is the outcome?
A) The miner earns half the reward B) The miner loses $50,000 with no reward
C) The network shuts down temporarily D) Other miners share the lost reward
Answer: B – Cheating wastes the electricity cost with zero return; honesty is the profitable strategy.

Q13. Mt. Gox lost $450M in Bitcoin in 2014, yet the Bitcoin blockchain continued operating. What does this distinction reveal?
A) Bitcoin is immune to all attacks B) Centralized services built on blockchain are the actual points of failure
C) Exchanges are unnecessary in crypto D) The stolen Bitcoin was recovered automatically

Quiz Questions 11–15

Q11. The first real-world purchase using Bitcoin was 10,000 BTC for two pizzas in 2010. This event proved that:
A) Bitcoin is too expensive for daily use B) Digital scarcity works — those coins could only be spent once
C) Pizza is the ideal blockchain use case D) Bitcoin's price never changes
Answer: B – The pizza transaction demonstrated that digital coins enforced by consensus have real purchasing power.

Q12. A cheating miner spends $50,000 on electricity and submits a fraudulent block. The network rejects it. What is the outcome?
A) The miner earns half the reward B) The miner loses $50,000 with no reward
C) The network shuts down temporarily D) Other miners share the lost reward
Answer: B – Cheating wastes the electricity cost with zero return; honesty is the profitable strategy.

Q13. Mt. Gox lost $450M in Bitcoin in 2014, yet the Bitcoin blockchain continued operating. What does this distinction reveal?
A) Bitcoin is immune to all attacks B) Centralized services built on blockchain are the actual points of failure
C) Exchanges are unnecessary in crypto D) The stolen Bitcoin was recovered automatically
Answer: B – The blockchain layer was secure; the centralized exchange's own security was the weak point.

Q14. The lecture states that Bitcoin's security budget exceeds $15 billion per year. Why does a larger budget make attacks harder?
A) The money is used to hire security guards B) An attacker must outspend the entire network's computing power to rewrite blocks
C) The budget pays for software updates D) Larger budgets mean fewer validators are needed

Quiz Questions 11–15

Q11. The first real-world purchase using Bitcoin was 10,000 BTC for two pizzas in 2010. This event proved that:
A) Bitcoin is too expensive for daily use B) Digital scarcity works — those coins could only be spent once
C) Pizza is the ideal blockchain use case D) Bitcoin's price never changes
Answer: B – The pizza transaction demonstrated that digital coins enforced by consensus have real purchasing power.

Q12. A cheating miner spends $50,000 on electricity and submits a fraudulent block. The network rejects it. What is the outcome?
A) The miner earns half the reward B) The miner loses $50,000 with no reward
C) The network shuts down temporarily D) Other miners share the lost reward
Answer: B – Cheating wastes the electricity cost with zero return; honesty is the profitable strategy.

Q13. Mt. Gox lost $450M in Bitcoin in 2014, yet the Bitcoin blockchain continued operating. What does this distinction reveal?
A) Bitcoin is immune to all attacks B) Centralized services built on blockchain are the actual points of failure
C) Exchanges are unnecessary in crypto D) The stolen Bitcoin was recovered automatically
Answer: B – The blockchain layer was secure; the centralized exchange's own security was the weak point.

Q14. The lecture states that Bitcoin's security budget exceeds $15 billion per year. Why does a larger budget make attacks harder?
A) The money is used to hire security guards B) An attacker must outspend the entire network's computing power to rewrite blocks
C) The budget pays for software updates D) Larger budgets mean fewer validators are needed
Answer: B – A 51% attack requires more computing power than the rest of the network combined, which costs more than any gain.

Q15. Terra/Luna collapsed in 2022, destroying $40 billion. The lecture says the blockchain "worked perfectly." What actually failed?
A) The consensus mechanism B) The economic design of the algorithmic stablecoin
C) The hash function used by the chain D) The number of validators was too low

Quiz Questions 11–15

Q11. The first real-world purchase using Bitcoin was 10,000 BTC for two pizzas in 2010. This event proved that:
A) Bitcoin is too expensive for daily use B) Digital scarcity works — those coins could only be spent once
C) Pizza is the ideal blockchain use case D) Bitcoin's price never changes
Answer: B – The pizza transaction demonstrated that digital coins enforced by consensus have real purchasing power.

Q12. A cheating miner spends $50,000 on electricity and submits a fraudulent block. The network rejects it. What is the outcome?
A) The miner earns half the reward B) The miner loses $50,000 with no reward
C) The network shuts down temporarily D) Other miners share the lost reward
Answer: B – Cheating wastes the electricity cost with zero return; honesty is the profitable strategy.

Q13. Mt. Gox lost $450M in Bitcoin in 2014, yet the Bitcoin blockchain continued operating. What does this distinction reveal?
A) Bitcoin is immune to all attacks B) Centralized services built on blockchain are the actual points of failure
C) Exchanges are unnecessary in crypto D) The stolen Bitcoin was recovered automatically
Answer: B – The blockchain layer was secure; the centralized exchange's own security was the weak point.

Q14. The lecture states that Bitcoin's security budget exceeds $15 billion per year. Why does a larger budget make attacks harder?
A) The money is used to hire security guards B) An attacker must outspend the entire network's computing power to rewrite blocks
C) The budget pays for software updates D) Larger budgets mean fewer validators are needed
Answer: B – A 51% attack requires more computing power than the rest of the network combined, which costs more than any gain.

Q15. Terra/Luna collapsed in 2022, destroying $40 billion. The lecture says the blockchain "worked perfectly." What actually failed?
A) The consensus mechanism B) The economic design of the algorithmic stablecoin
C) The hash function used by the chain D) The number of validators was too low
Answer: B – The blockchain executed code correctly; the flawed incentive design caused the collapse.

Quiz Questions 16–20

Q16. The lecture places cash, banks, PayPal, and blockchain on a trust spectrum. What pattern emerges as you move toward blockchain?
A) Transaction costs decrease steadily B) Each step replaces one more layer of human trust with a technical mechanism
C) Privacy increases at every step D) Transaction speed increases at every step

Quiz Questions 16–20

Q16. The lecture places cash, banks, PayPal, and blockchain on a trust spectrum. What pattern emerges as you move toward blockchain?
A) Transaction costs decrease steadily B) Each step replaces one more layer of human trust with a technical mechanism
C) Privacy increases at every step D) Transaction speed increases at every step
Answer: B – The spectrum shows a progressive shift from institutional trust to cryptographic verification.

Q17. A Bitcoin block header is 80 bytes, but the block body can be up to 4 MB. Why is this separation important?
A) It allows miners to skip transaction verification B) Light clients can verify block validity without downloading the full body
C) The header is encrypted while the body is not D) It reduces the total energy cost of mining

Quiz Questions 16–20

Q16. The lecture places cash, banks, PayPal, and blockchain on a trust spectrum. What pattern emerges as you move toward blockchain?
A) Transaction costs decrease steadily B) Each step replaces one more layer of human trust with a technical mechanism
C) Privacy increases at every step D) Transaction speed increases at every step
Answer: B – The spectrum shows a progressive shift from institutional trust to cryptographic verification.

Q17. A Bitcoin block header is 80 bytes, but the block body can be up to 4 MB. Why is this separation important?
A) It allows miners to skip transaction verification B) Light clients can verify block validity without downloading the full body
C) The header is encrypted while the body is not D) It reduces the total energy cost of mining
Answer: B – The small header size enables mobile phones and lightweight devices to participate in verification.

Q18. China's e-CNY uses blockchain technology but is centrally controlled. How does this contradict Bitcoin's original design goal?
A) e-CNY is faster, which proves centralization is better B) CBDCs retain central authority to freeze accounts, the exact power Bitcoin was designed to eliminate
C) Bitcoin and e-CNY serve identical purposes D) e-CNY is more decentralized because the government represents everyone

Quiz Questions 16–20

Q16. The lecture places cash, banks, PayPal, and blockchain on a trust spectrum. What pattern emerges as you move toward blockchain?
A) Transaction costs decrease steadily B) Each step replaces one more layer of human trust with a technical mechanism
C) Privacy increases at every step D) Transaction speed increases at every step
Answer: B – The spectrum shows a progressive shift from institutional trust to cryptographic verification.

Q17. A Bitcoin block header is 80 bytes, but the block body can be up to 4 MB. Why is this separation important?
A) It allows miners to skip transaction verification B) Light clients can verify block validity without downloading the full body
C) The header is encrypted while the body is not D) It reduces the total energy cost of mining
Answer: B – The small header size enables mobile phones and lightweight devices to participate in verification.

Q18. China's e-CNY uses blockchain technology but is centrally controlled. How does this contradict Bitcoin's original design goal?
A) e-CNY is faster, which proves centralization is better B) CBDCs retain central authority to freeze accounts, the exact power Bitcoin was designed to eliminate
C) Bitcoin and e-CNY serve identical purposes D) e-CNY is more decentralized because the government represents everyone
Answer: B – Bitcoin aimed to remove central control; CBDCs use the same technology to strengthen it.

Q19. Five international aid organizations want to share transparent donation records but do not trust each other. Evaluate whether blockchain is appropriate.
A) No — a shared spreadsheet is always sufficient B) Yes — multiple untrusted parties needing a shared immutable record is an ideal blockchain use case
C) No — blockchain cannot store financial records D) Yes — but only if they mine their own cryptocurrency

Quiz Questions 16–20

Q16. The lecture places cash, banks, PayPal, and blockchain on a trust spectrum. What pattern emerges as you move toward blockchain?
A) Transaction costs decrease steadily B) Each step replaces one more layer of human trust with a technical mechanism
C) Privacy increases at every step D) Transaction speed increases at every step
Answer: B – The spectrum shows a progressive shift from institutional trust to cryptographic verification.

Q17. A Bitcoin block header is 80 bytes, but the block body can be up to 4 MB. Why is this separation important?
A) It allows miners to skip transaction verification B) Light clients can verify block validity without downloading the full body
C) The header is encrypted while the body is not D) It reduces the total energy cost of mining
Answer: B – The small header size enables mobile phones and lightweight devices to participate in verification.

Q18. China's e-CNY uses blockchain technology but is centrally controlled. How does this contradict Bitcoin's original design goal?
A) e-CNY is faster, which proves centralization is better B) CBDCs retain central authority to freeze accounts, the exact power Bitcoin was designed to eliminate
C) Bitcoin and e-CNY serve identical purposes D) e-CNY is more decentralized because the government represents everyone
Answer: B – Bitcoin aimed to remove central control; CBDCs use the same technology to strengthen it.

Q19. Five international aid organizations want to share transparent donation records but do not trust each other. Evaluate whether blockchain is appropriate.
A) No — a shared spreadsheet is always sufficient B) Yes — multiple untrusted parties needing a shared immutable record is an ideal blockchain use case
C) No — blockchain cannot store financial records D) Yes — but only if they mine their own cryptocurrency
Answer: B – The decision tree confirms: multiple parties + trust deficit + need for immutability = blockchain is appropriate.

Q20. Bitcoin uses 150 TWh/year (comparable to Argentina), while Proof of Stake reduces energy by 99.95%. Should all blockchains switch to Proof of Stake?
A) Yes — energy waste is never justified B) No — Proof of Work is always superior
C) It depends on whether the security model and decentralization trade-offs are acceptable for each network's goals D) The comparison is irrelevant because blockchains do not use energy

Quiz Questions 16–20

Q16. The lecture places cash, banks, PayPal, and blockchain on a trust spectrum. What pattern emerges as you move toward blockchain?
A) Transaction costs decrease steadily B) Each step replaces one more layer of human trust with a technical mechanism
C) Privacy increases at every step D) Transaction speed increases at every step
Answer: B – The spectrum shows a progressive shift from institutional trust to cryptographic verification.

Q17. A Bitcoin block header is 80 bytes, but the block body can be up to 4 MB. Why is this separation important?
A) It allows miners to skip transaction verification B) Light clients can verify block validity without downloading the full body
C) The header is encrypted while the body is not D) It reduces the total energy cost of mining
Answer: B – The small header size enables mobile phones and lightweight devices to participate in verification.

Q18. China's e-CNY uses blockchain technology but is centrally controlled. How does this contradict Bitcoin's original design goal?
A) e-CNY is faster, which proves centralization is better B) CBDCs retain central authority to freeze accounts, the exact power Bitcoin was designed to eliminate
C) Bitcoin and e-CNY serve identical purposes D) e-CNY is more decentralized because the government represents everyone
Answer: B – Bitcoin aimed to remove central control; CBDCs use the same technology to strengthen it.

Q19. Five international aid organizations want to share transparent donation records but do not trust each other. Evaluate whether blockchain is appropriate.
A) No — a shared spreadsheet is always sufficient B) Yes — multiple untrusted parties needing a shared immutable record is an ideal blockchain use case
C) No — blockchain cannot store financial records D) Yes — but only if they mine their own cryptocurrency
Answer: B – The decision tree confirms: multiple parties + trust deficit + need for immutability = blockchain is appropriate.

Q20. Bitcoin uses 150 TWh/year (comparable to Argentina), while Proof of Stake reduces energy by 99.95%. Should all blockchains switch to Proof of Stake?
A) Yes — energy waste is never justified B) No — Proof of Work is always superior
C) It depends on whether the security model and decentralization trade-offs are acceptable for each network's goals D) The comparison is irrelevant because blockchains do not use energy
Answer: C – Each consensus mechanism involves different trade-offs; the right choice depends on the network's priorities.