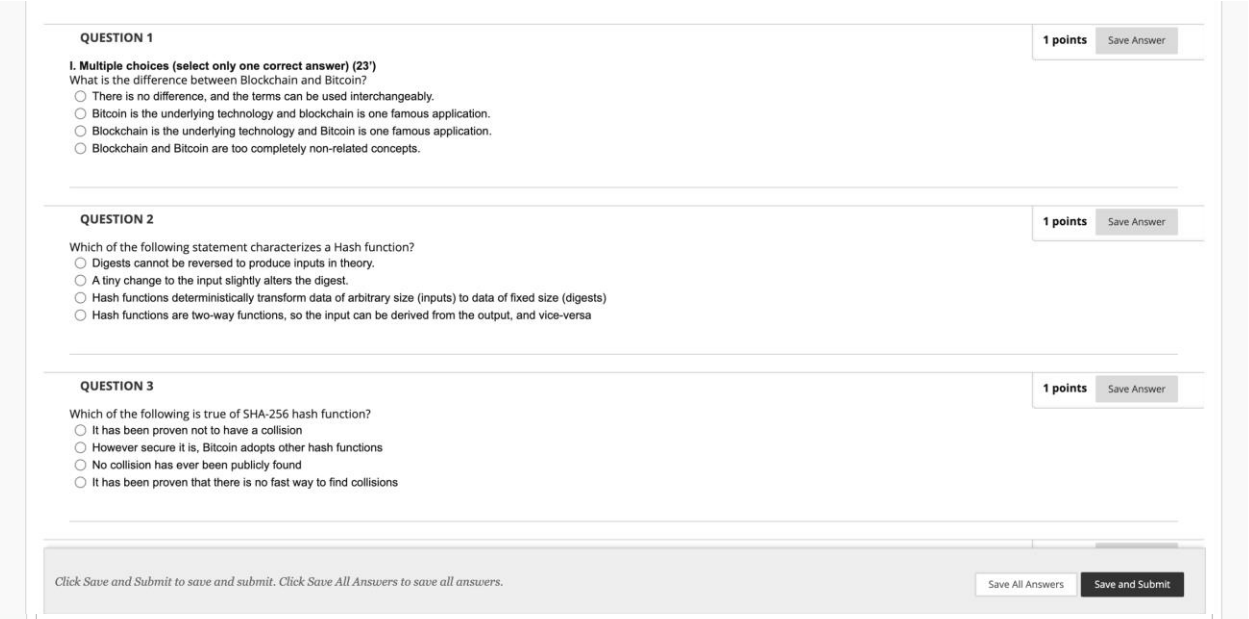


QUESTION 1

I. Multiple choices (select only one correct answer) (23')
What is the difference between Blockchain and Bitcoin?

○ There is no difference, and the terms can be used interchangeably.
○ Bitcoin is the underlying technology and blockchain is one famous application.
○ Blockchain is the underlying technology and Bitcoin is one famous application.
○ Blockchain and Bitcoin are too completely non-related concepts.

QUESTION 2

Which of the following statement characterizes a Hash function?

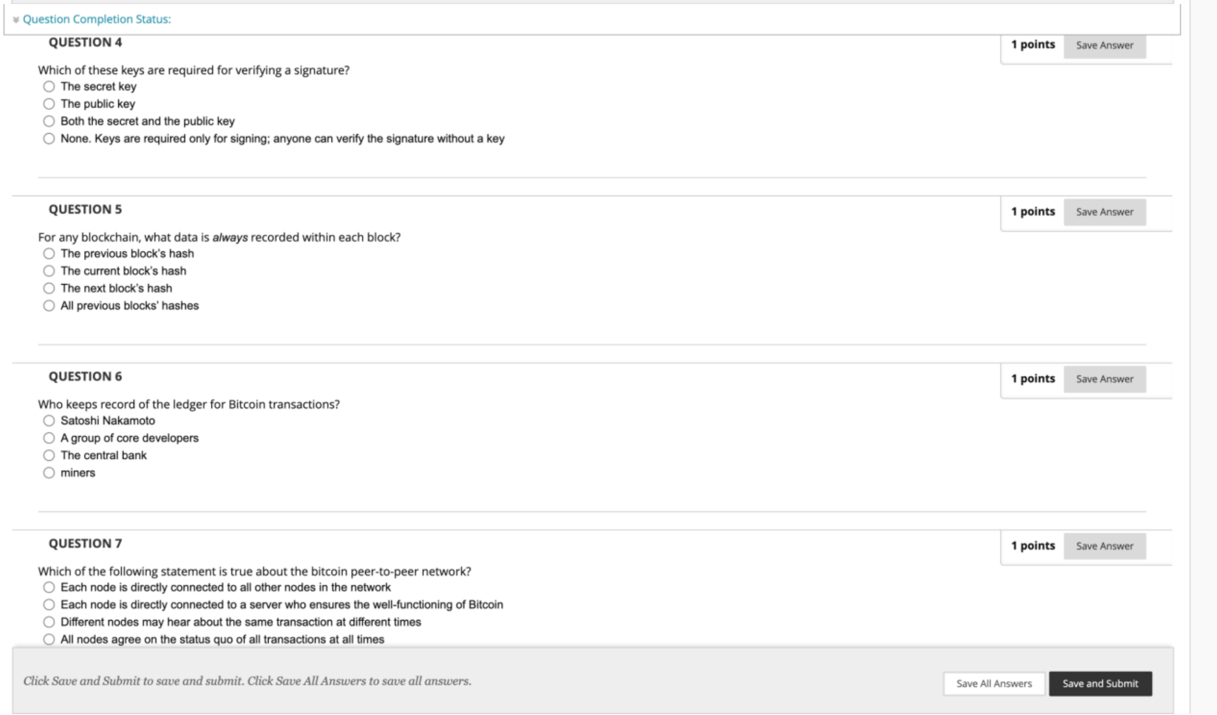
○ Digests cannot be reversed to produce inputs in theory.
○ A tiny change to the input slightly alters the digest.
○ Hash functions deterministically transform data of arbitrary size (inputs) to data of fixed size (digests)
○ Hash functions are two-way functions, so the input can be derived from the output, and vice-versa

QUESTION 3

Which of the following is true of SHA-256 hash function?

○ It has been proven not to have a collision
○ However secure it is, Bitcoin adopts other hash functions
○ No collision has ever been publicly found
○ It has been proven that there is no fast way to find collisions

Click Save and Submit to save and submit. Click Save All Answers to save all answers.



QUESTION 4

Which of these keys are required for verifying a signature?

○ The secret key
○ The public key
○ Both the secret and the public key
○ None. Keys are required only for signing; anyone can verify the signature without a key

QUESTION 5

For any blockchain, what data is *always* recorded within each block?

○ The previous block's hash
○ The current block's hash
○ The next block's hash
○ All previous blocks' hashes

QUESTION 6

Who keeps record of the ledger for Bitcoin transactions?

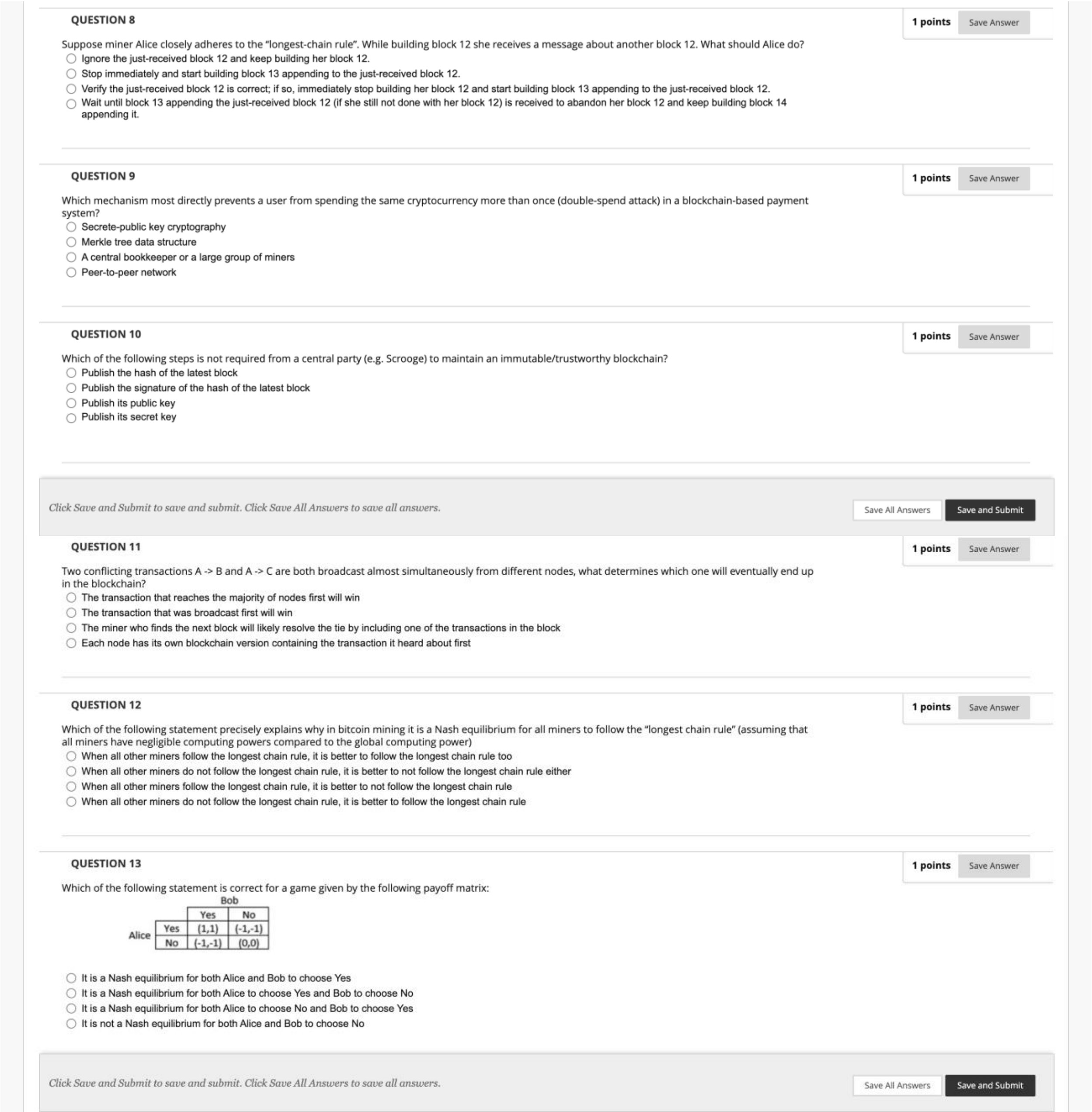
○ Satoshi Nakamoto
○ A group of core developers
○ The central bank
○ miners

QUESTION 7

Which of the following statement is true about the bitcoin peer-to-peer network?

○ Each node is directly connected to all other nodes in the network
○ Each node is directly connected to a server who ensures the well-functioning of Bitcoin
○ Different nodes may hear about the same transaction at different times
○ All nodes agree on the status quo of all transactions at all times

Click Save and Submit to save and submit. Click Save All Answers to save all answers.



QUESTION 8

Suppose miner Alice closely adheres to the “longest-chain rule”. While building block 12 she receives a message about another block 12. What should Alice do?

○ Ignore the just-received block 12 and keep building her block 12.
○ Stop immediately and start building block 13 appending to the just-received block 12.
○ Verify the just-received block 12 is correct; if so, immediately stop building her block 12 and start building block 13 appending to the just-received block 12.
○ Wait until block 13 appending the just-received block 12 (if she still not done with her block 12) is received to abandon her block 12 and keep building block 14 appending it.

QUESTION 9

Which mechanism most directly prevents a user from spending the same cryptocurrency more than once (double-spend attack) in a blockchain-based payment system?

○ Secrete-public key cryptography
○ Merkle tree data structure
○ A central bookkeeper or a large group of miners
○ Peer-to-peer network

QUESTION 10

Which of the following steps is not required from a central party (e.g. Scrooge) to maintain an immutable/trustworthy blockchain?

○ Publish the hash of the latest block
○ Publish the signature of the hash of the latest block
○ Publish its public key
○ Publish its secret key

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

QUESTION 11

Two conflicting transactions A -> B and A -> C are both broadcast almost simultaneously from different nodes, what determines which one will eventually end up in the blockchain?

○ The transaction that reaches the majority of nodes first will win
○ The transaction that was broadcast first will win
○ The miner who finds the next block will likely resolve the tie by including one of the transactions in the block
○ Each node has its own blockchain version containing the transaction it heard about first

QUESTION 12

Which of the following statement precisely explains why in bitcoin mining it is a Nash equilibrium for all miners to follow the “longest chain rule” (assuming that all miners have negligible computing powers compared to the global computing power)

○ When all other miners follow the longest chain rule, it is better to follow the longest chain rule too
○ When all other miners do not follow the longest chain rule, it is better to not follow the longest chain rule either
○ When all other miners follow the longest chain rule, it is better to not follow the longest chain rule
○ When all other miners do not follow the longest chain rule, it is better to follow the longest chain rule

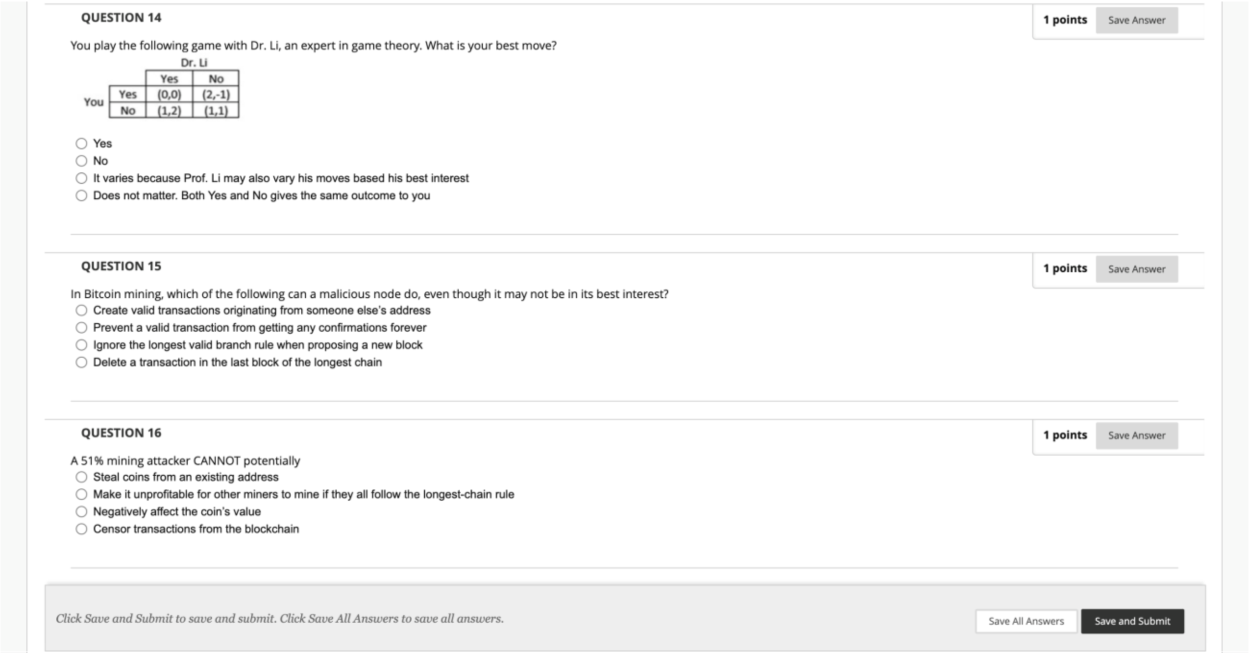
QUESTION 13

Which of the following statement is correct for a game given by the following payoff matrix:

		Bob	
		Yes	No
Alice	Yes	(1,1)	(-1,-1)
	No	(-1,-1)	(0,0)

○ It is a Nash equilibrium for both Alice and Bob to choose Yes
○ It is a Nash equilibrium for both Alice to choose Yes and Bob to choose No
○ It is a Nash equilibrium for both Alice to choose No and Bob to choose Yes
○ It is not a Nash equilibrium for both Alice and Bob to choose No

Click Save and Submit to save and submit. Click Save All Answers to save all answers.



QUESTION 14

You play the following game with Dr. Li, an expert in game theory. What is your best move?

		Dr. Li	
		Yes	No
You	Yes	(0,0)	(2,-1)
	No	(1,2)	(1,1)

○ Yes
○ No
○ It varies because Prof. Li may also vary his moves based his best interest
○ Does not matter. Both Yes and No gives the same outcome to you

QUESTION 15

In Bitcoin mining, which of the following can a malicious node do, even though it may not be in its best interest?

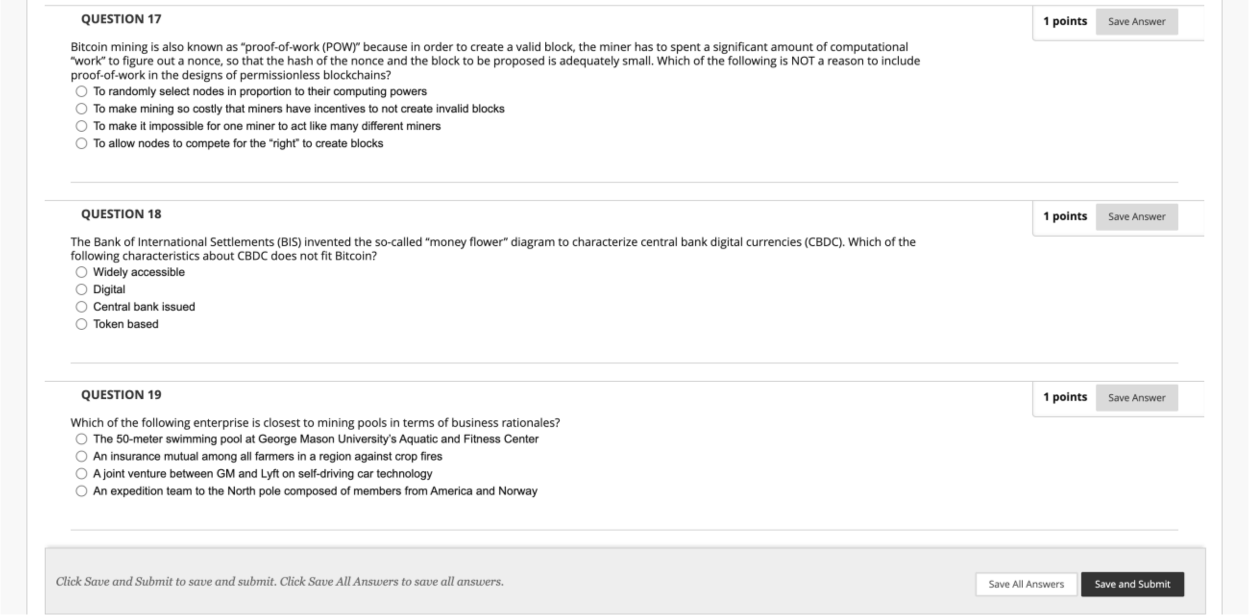
○ Create valid transactions originating from someone else's address
○ Prevent a valid transaction from getting any confirmations forever
○ Ignore the longest valid branch rule when proposing a new block
○ Delete a transaction in the last block of the longest chain

QUESTION 16

A 51% mining attacker CANNOT potentially

○ Steal coins from an existing address
○ Make it unprofitable for other miners to mine if they all follow the longest-chain rule
○ Negatively affect the coin's value
○ Censor transactions from the blockchain

Click Save and Submit to save and submit. Click Save All Answers to save all answers.



QUESTION 17

Bitcoin mining is also known as "proof-of-work (POW)" because in order to create a valid block, the miner has to spent a significant amount of computational "work" to figure out a nonce, so that the hash of the nonce and the block to be proposed is adequately small. Which of the following is NOT a reason to include proof-of-work in the designs of permissionless blockchains?

○ To randomly select nodes in proportion to their computing powers
○ To make mining so costly that miners have incentives to not create invalid blocks
○ To make it impossible for one miner to act like many different miners
○ To allow nodes to compete for the "right" to create blocks

QUESTION 18

The Bank of International Settlements (BIS) invented the so-called "money flower" diagram to characterize central bank digital currencies (CBDC). Which of the following characteristics about CBDC does not fit Bitcoin?

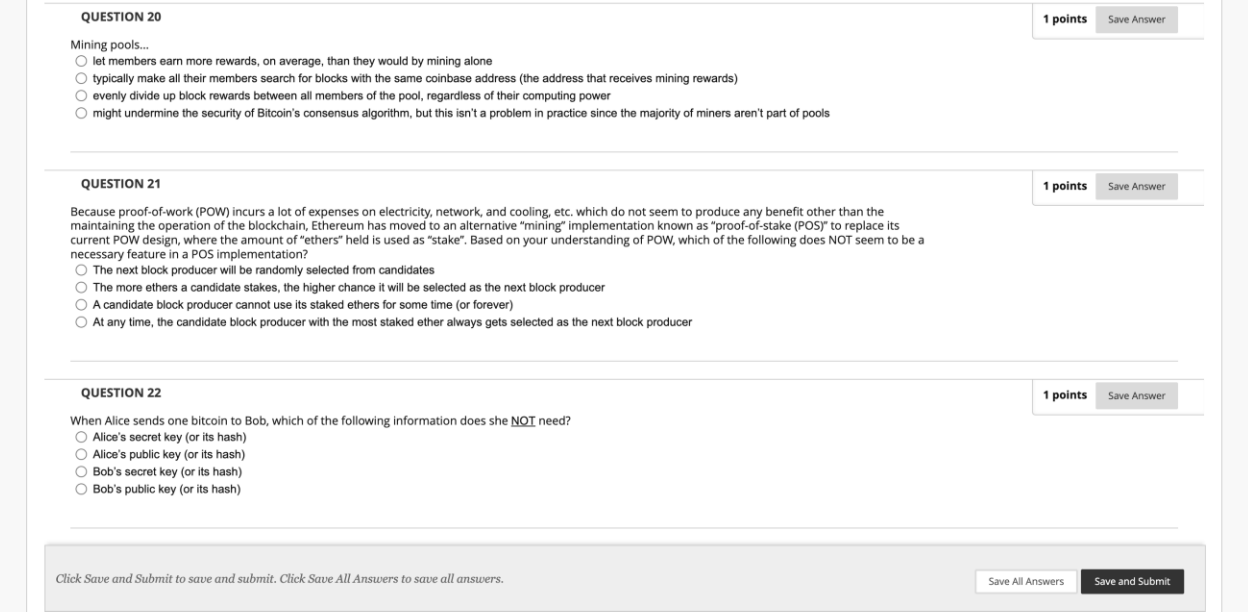
○ Widely accessible
○ Digital
○ Central bank issued
○ Token based

QUESTION 19

Which of the following enterprise is closest to mining pools in terms of business rationales?

○ The 50-meter swimming pool at George Mason University's Aquatic and Fitness Center
○ An insurance mutual among all farmers in a region against crop fires
○ A joint venture between GM and Lyft on self-driving car technology
○ An expedition team to the North pole composed of members from America and Norway

Click Save and Submit to save and submit. Click Save All Answers to save all answers.



QUESTION 20

Mining pools...

○ let members earn more rewards, on average, than they would by mining alone
○ typically make all their members search for blocks with the same coinbase address (the address that receives mining rewards)
○ evenly divide up block rewards between all members of the pool, regardless of their computing power
○ might undermine the security of Bitcoin's consensus algorithm, but this isn't a problem in practice since the majority of miners aren't part of pools

QUESTION 21

Because proof-of-work (POW) incurs a lot of expenses on electricity, network, and cooling, etc. which do not seem to produce any benefit other than the maintaining the operation of the blockchain, Ethereum has moved to an alternative "mining" implementation known as "proof-of-stake (POS)" to replace its current POW design, where the amount of "ethers" held is used as "stake". Based on your understanding of POW, which of the following does NOT seem to be a necessary feature in a POS implementation?

○ The next block producer will be randomly selected from candidates
○ The more ethers a candidate stakes, the higher chance it will be selected as the next block producer
○ A candidate block producer cannot use its staked ethers for some time (or forever)
○ At any time, the candidate block producer with the most staked ether always gets selected as the next block producer

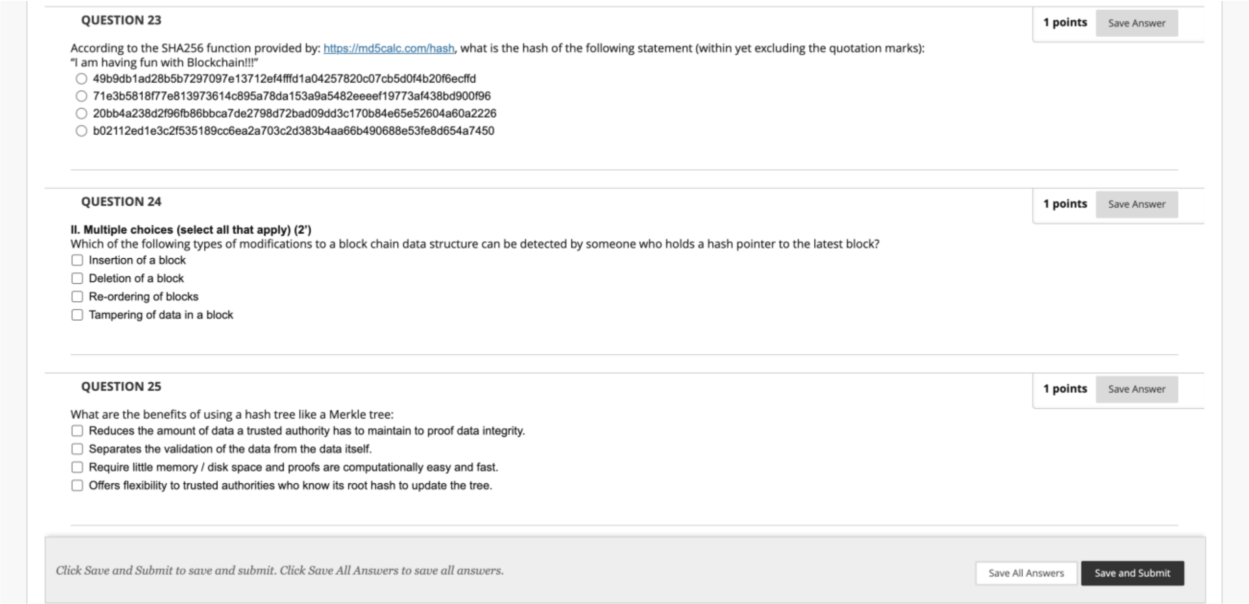
QUESTION 22

When Alice sends one bitcoin to Bob, which of the following information does she NOT need?

○ Alice's secret key (or its hash)
○ Alice's public key (or its hash)
○ Bob's secret key (or its hash)
○ Bob's public key (or its hash)

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Website for question 23: https://md5calc.com/hash



QUESTION 23

According to the SHA256 function provided by: https://md5calc.com/hash, what is the hash of the following statement (within yet excluding the quotation marks):
"I am having fun with Blockchain!!!"

○ 49b9db1ad28b5b7297097e13712ef4fffd1a04257820c07cb5d0f4b20f6ecffd
○ 71e3b5818f77e813973614c895a78da153a9a5482eeeef19773af438bd900f96
○ 20bb4a238d2f96fb86bbca7de2798d72bad09dd3c170b84e65e52604a60a2226
○ b02112ed1e3c2f535189cc6ea2a703c2d383b4aa66b490688e53fe8d654a7450

QUESTION 24

II. Multiple choices (select all that apply) (2')
Which of the following types of modifications to a block chain data structure can be detected by someone who holds a hash pointer to the latest block?

□ Insertion of a block
□ Deletion of a block
□ Re-ordering of blocks
□ Tampering of data in a block

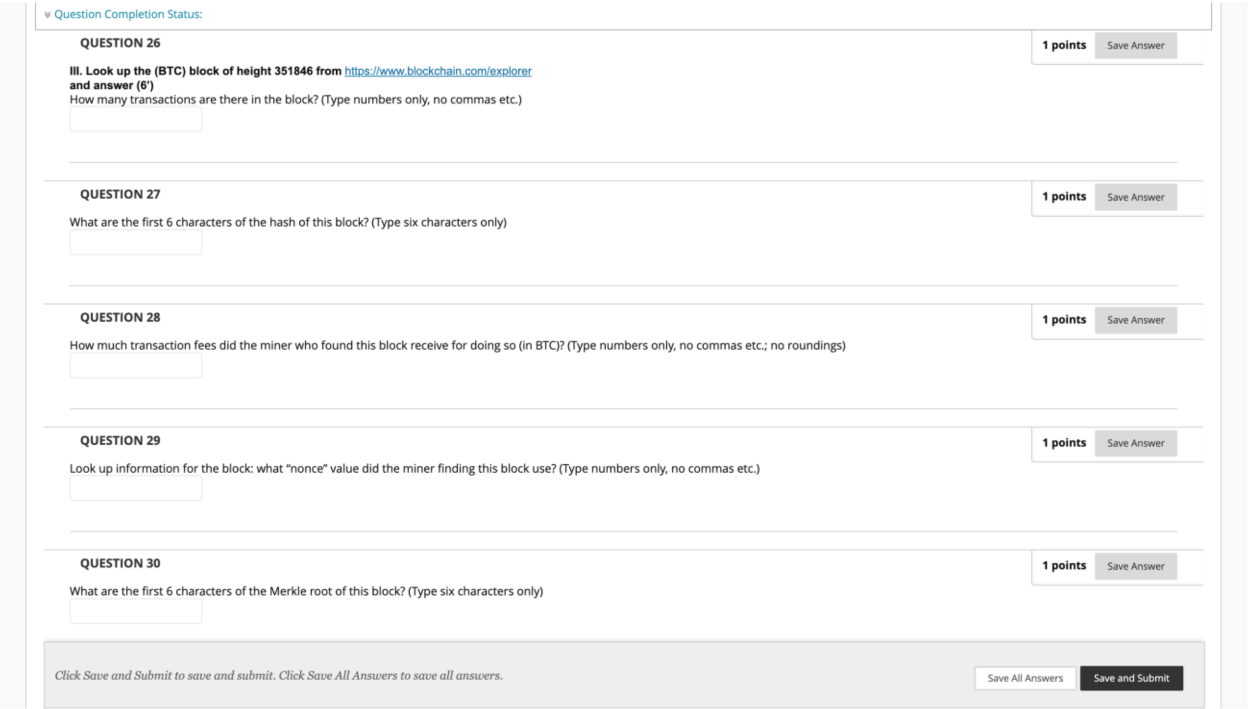
QUESTION 25

What are the benefits of using a hash tree like a Merkle tree:

□ Reduces the amount of data a trusted authority has to maintain to proof data integrity.
□ Separates the validation of the data from the data itself.
□ Require little memory / disk space and proofs are computationally easy and fast.
□ Offers flexibility to trusted authorities who know its root hash to update the tree.

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Website for question 26 to 31: https://www.blockchain.com/explorer



QUESTION 26

III. Look up the (BTC) block of height 351846 from https://www.blockchain.com/explorer
and answer (6')
How many transactions are there in the block? (Type numbers only, no commas etc.)

QUESTION 27

What are the first 6 characters of the hash of this block? (Type six characters only)

QUESTION 28

How much transaction fees did the miner who found this block receive for doing so (in BTC)? (Type numbers only, no commas etc.; no roundings)

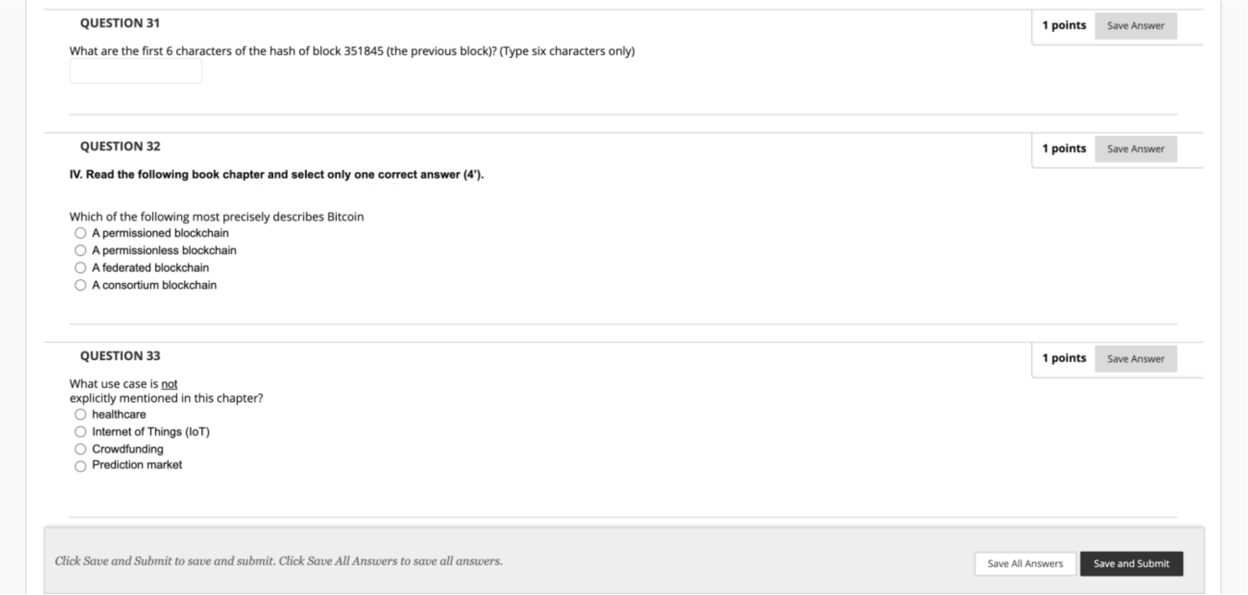
QUESTION 29

Look up information for the block: what "nonce" value did the miner finding this block use? (Type numbers only, no commas etc.)

QUESTION 30

What are the first 6 characters of the Merkle root of this block? (Type six characters only)

Click Save and Submit to save and submit. Click Save All Answers to save all answers.



QUESTION 31

What are the first 6 characters of the hash of block 351845 (the previous block)? (Type six characters only)

QUESTION 32

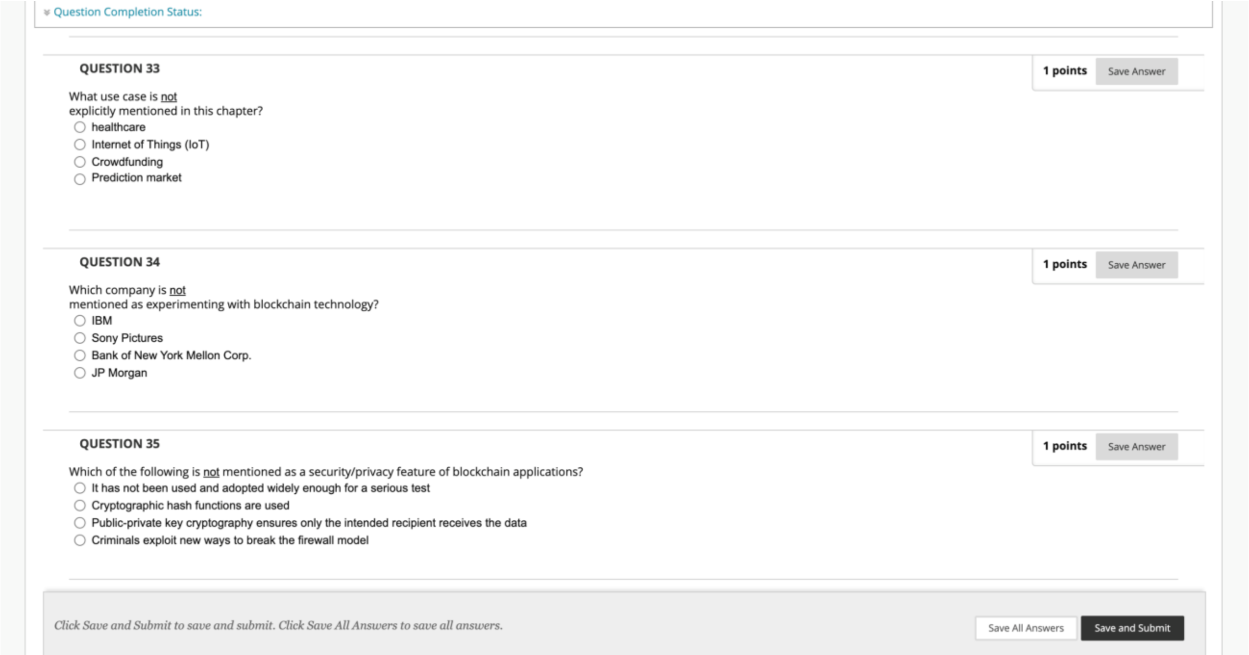
IV. Read the following book chapter and select only one correct answer (4').

Which of the following most precisely describes Bitcoin
○ A permissioned blockchain
○ A permissionless blockchain
○ A federated blockchain
○ A consortium blockchain

QUESTION 33

What use case is not
explicitly mentioned in this chapter?
○ healthcare
○ Internet of Things (IoT)
○ Crowdfunding
○ Prediction market

Click Save and Submit to save and submit. Click Save All Answers to save all answers.



QUESTION 33

What use case is not
explicitly mentioned in this chapter?

○ healthcare
○ Internet of Things (IoT)
○ Crowdfunding
○ Prediction market

QUESTION 34

Which company is not
mentioned as experimenting with blockchain technology?

○ IBM
○ Sony Pictures
○ Bank of New York Mellon Corp.
○ JP Morgan

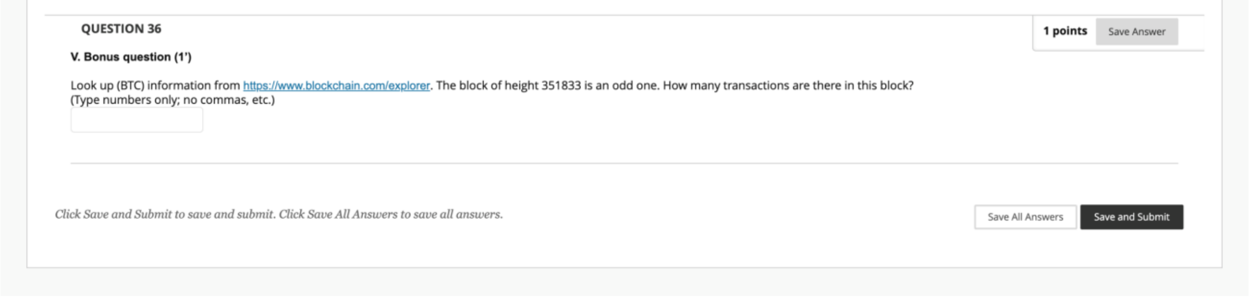
QUESTION 35

Which of the following is not mentioned as a security/privacy feature of blockchain applications?

○ It has not been used and adopted widely enough for a serious test
○ Cryptographic hash functions are used
○ Public-private key cryptography ensures only the intended recipient receives the data
○ Criminals exploit new ways to break the firewall model

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Website for question 36: https://www.blockchain.com/explorer



QUESTION 36

V. Bonus question (1')

Look up (BTC) information from https://www.blockchain.com/explorer. The block of height 351833 is an odd one. How many transactions are there in this block?
(Type numbers only; no commas, etc.)

Click Save and Submit to save and submit. Click Save All Answers to save all answers.