Back to 'Certificate Final Exam'

Started on	Monday, 23 January 2023, 5:38 AM
State	Finished
Completed on	Monday, 23 January 2023, 7:10 AM
Time taken	1 hour 31 mins
Marks	29.00/36.00
Grade	**8.06** out of 10.00 (**80.56**%)

Question **1**

Correct

Mark 1.00 out of 1.00

How does a new node connect to others on the network?

a. By randomly pinging IP addresses on Bitcoin ports looking for a response.
b. The Bitcoin core client contains "DNS seeds" to help the bootstrapping process. ✔
c. The Bitcoin core client is regularly updated with a complete copy of the network graph.

Question **2**

Correct

Mark 1.00 out of 1.00

Which of the following best describes how Bitcoins are transferred from one user to another?

a. The Bitcoin ledger is updated to debit one account and credit another
b. Every 10 mins. miners vote on the appropriate balance for every account
c. Every transaction consumes one or more outputs, UTXOs, to create new outputs ✔

Question **3**

Correct

Mark 1.00 out of 1.00

Which of the following options best describes why Bitcoin miners don't control the Bitcoin ecosystem?

a. Government regulation prevents any one area from having too large a concentration of miners
b. Bitcoin maintains a rigid governance structure which allows for others in the ecosystem to vote on who can mine Bitcoin in each cycle
c. If miners were to implement consensus rules in disagreement with the rest of the ecosystem, the merchants, exchanges, and wallets would not accept any of the Bitcoin they have earned ✔

Question **4**

Incorrect

Mark 0.00 out of 1.00

What does it mean for a blockchain to be "neutral"?

a. The blockchain will process any valid transaction regardless of sender, receiver, or content
b. The blockchain will only process neutral transactions that don't favor some miners over others ✖
c. The blockchain has a majority of nodes in countries that are permissive towards blockchain technology

Question **5**

Incorrect

Mark 0.00 out of 1.00

What does it mean when a transaction's status is "unconfirmed"?

a. It has yet to be mined and included in a block
b. The network has not yet validated the transaction
c. The miners have yet to vote on when the transaction should be included in a block ✖

Question 6
Correct
Mark 1.00 out of 1.00

Which of the following best describes how Bitcoin uses cryptographic signatures?

a. Signatures are used to encrypt transaction data as a security measure
b. Signatures are used as a fixed length unique identifier of transaction data
c. Signatures are used to assure that a message is authentic and has not been tampered with ✔

Question 7
Correct
Mark 1.00 out of 1.00

Which of the following is a sought-after feature of asymmetric encryption that has led to it being widely adopted?

a. It uses fewer server resources to encrypt and decrypt
b. It does not require a secure key transfer between users ✔
c. It uses algorithms that are more secure than other forms of encryption

Question 8
Correct
Mark 1.00 out of 1.00

Why does a private key need to remain private?

a. Anyone with a private key can encrypt data and validate the signature from a public key
b. Private keys include sensitive personal information that is required when generating the key
c. Anyone with a private key can sign messages and decrypt data encrypted with the matching public key ✔

Question 9
Correct
Mark 1.00 out of 1.00

Which of the following best describes the interaction between public keys, private keys, and Bitcoin in a standard Bitcoin transaction?

a. To move Bitcoin, a signature from both the public and private keys are required.
b. Bitcoin is locked to an address created from a public key. A signature from the corresponding private key is then required to move funds from that address. ✔
c. Bitcoin is locked to an address created from a public key. To move funds from that address, the Bitcoin must first be decrypted using the corresponding private key.

Question 10
Correct
Mark 1.00 out of 1.00

Which of the following best summarizes the relationship between Bitcoin addresses and cryptographic keys?

a. A standard Bitcoin address is derived from a public key through a series of hash functions ✔
b. A Bitcoin address is the hash of a secret number which is then encrypted with a public key
c. Both a public and the corresponding private key are required to generate a Bitcoin address

Question 11
Correct
Mark 1.00 out of 1.00

Which of the following options best describes how public and private keys are used to encrypt and decrypt data?

a. The public key is used to encrypt data that can then only be decrypted using the corresponding private key ✔
b. Both the public and private keys are used to encrypt data that can then only be accessed with the private key
c. A public key and a series of hashes are used to encrypt data, while the private key and the original hashed data is used to decrypt that data

Question 12
Correct
Mark 1.00 out of 1.00

How do cryptographic signatures help to prevent fraudulent Bitcoin transactions?

a. Three or more miners are required to sign a transaction before it is considered valid
b. Cryptographic signatures are used as a method for voting on the authenticity of any transaction on the blockchain
c. Only the person or entity in possession of the private key can create the signature necessary to produce a valid transaction ✔

Question 13
Incorrect
Mark 0.00 out of 1.00

Which of the following best describes what a digital signature is?

a. A very large prime number
b. A complex and unique mathematical formula ✖
c. Two numbers commonly referred to as the R and S values

Question 14
Incorrect
Mark 0.00 out of 1.00

Which of the following best describes what a SIGHASH is?

a. A hashing method used to hash a transaction prior to signing
b. A series of hashes applied to a signature prior to broadcasting the transaction ✖
c. A way of indicating which part of a transaction's data was used in the creation of a signature

Question 15
Correct
Mark 1.00 out of 1.00

Which of the following best describes what would happen if you made an edit to a signed message prior to checking the validity of the signature?

a. A signature validation script would return an error ✔
b. It depends on how much of the message was changed
c. It depends if the public or private key was used in the validation function

Question 16
Correct
Mark 1.00 out of 1.00

Which of the following is a feature of hashing that Bitcoin makes use of?

a. A hash function can be used to encrypt data
b. A hash can be used as a unique identifier of data ✔
c. A hash can be used to delay the release of data via its encryption functions

Question 17
Incorrect
Mark 0.00 out of 1.00

Which of the following is an accurate statement about how the Bitcoin network adjusts the mining difficulty level?

a. The hashing algorithm used in mining is adjusted by the software every two weeks ✖
b. The number of zeros that block hash must start with is voted on by all miners every 2016 blocks
c. The number of zeros that a block hash must start with is adjusted by the software every 2016 blocks

Question 18
Incorrect
Mark 0.00 out of 1.00

Which of the following is one way that Bitcoin uses hashing to summarize data?

a. Base58
b. Merkle Trees
c. Proof-of-Work ✖

Question 19
Correct
Mark 1.00 out of 1.00

What data do you need to verify a hash?

a. The hashing private key
b. The original data and the hashing algorithm used ✔
c. An array of hashes produced with the same algorithm

Question 20
Correct
Mark 1.00 out of 1.00

Merkle Trees provide a variety of utility to the Bitcoin system, including which of the following?

a. They are proof that a transaction is correctly encrypted
b. They can be used to prove that a transaction is in a block ✔
c. They are used to provide the Proof-of-Work necessary for mining a block

Question 21
Correct
Mark 1.00 out of 1.00

Which of the following is a serialization method used for signatures on Bitcoin transactions?

a. Json
b. DER ✔
c. XML

Question 22
Correct
Mark 1.00 out of 1.00

Which of the following explains why checksums are used in Bitcoin addresses?

a. A checksum is part of the address creation process
b. A checksums is a standard and easily human-readable format
c. A checksum can detect a typo in a Bitcoin address helping to prevent errors ✔

Question 23
Incorrect
Mark 0.00 out of 1.00

To link blocks together, in a chain, what data is included in a block header?

a. The previous block's hash
b. The previous 10 block's hashes
c. The previous block's Merkle root ✖

Question 24
Correct
Mark 1.00 out of 1.00

One common encoding method used in cryptography is DER. Which of the following is true of the DER encoding method?

a. DER tags are very similar to hex tags which can create some confusion
b. DER uses a Tag-Length-Value format where the tag is often the type of data ✔
c. DER tags are not widely used as they have been replaced with a key-value system

Question 25
Correct
Mark 1.00 out of 1.00

Which of the following is a reason why someone may want to run a Bitcoin full node?

a. Because they can earn money from validating transactions
b. Because they wish to be able to independently validate all transactions on the network ✔
c. Because running a full node will allow them to have their transactions treated as a priority

Question 26
Correct
Mark 1.00 out of 1.00

How does the Bitcoin daemon communicate with other programs?

a. RPC ✔
b. JSON
c. REST API

Question 27
Correct
Mark 1.00 out of 1.00

What data is contained in a wallet seed or mnemonic?

a. Only the chain code
b. The master private key plus the first 10 addresses
c. The master private key plus the master chain code ✔

Question 28
Correct
Mark 1.00 out of 1.00

The Bitcoin daemon often displays transaction data in what encoding format?

a. DER
b. Hex ✔
c. RPC

Question 29
Correct
Mark 1.00 out of 1.00

Which of the following are two types of Bitcoin transactions?

a. P2PKH P2SH ✔
b. P2KH, and HTLC
c. P2PKH and P2MH

Question 30
Correct
Mark 1.00 out of 1.00

Which of the following statements about Bitcoin transactions and scripts is true?

a. Value is locked to a script using a Bitcoin address
b. Bitcoin is tied to an address with at least two locking scripts
c. Value is locked to an address with a locking script in a transaction output ✔

Question 31
Correct
Mark 1.00 out of 1.00

When a wallet creates a new transaction, how does it then get propagated throughout the Bitcoin network?

a. The transaction is added to the official node registry
b. The wallet will tell the top 5 nodes that it is connected to, who will tell the mining nodes that they are connected to
c. The wallet will tell all the nodes that it is connected to about the transactions, who will then tell all the nodes that they are connected to ✔

Question 32
Correct
Mark 1.00 out of 1.00

Which of the following best describes the Bitcoin scripting language?

a. Bitcoin script is a fork of C++
b. Bitcoin script is a Forth-like reverse-polish notation stack-based execution language ✔
c. Bitcoin script is a Forth-like reverse-polish notation object-oriented execution language

Question 33
Correct
Mark 1.00 out of 1.00

Which nodes validate which transactions?

a. Every node validates every transaction ✔
b. Only mining nodes validate all transactions
c. Non-mining nodes validate P2PKH transactions

Question 34
Correct
Mark 1.00 out of 1.00

Which of the following best describes the difference between a hard fork and a soft fork?

a. A soft fork carries a higher risk of network partition or split than a hard fork
b. A hard fork will partition or split the network if not all nodes are updated, while a soft fork allows un-updated nodes to remain on the network ✔
c. A hard fork will partition or split the network if not all nodes are updated, while a soft fork will only partition the network if less than 80% of the nodes are updated

Question 35
Correct
Mark 1.00 out of 1.00

Why will two versions of the same transaction, a double spend, not be included in the same block?

a. A miner could only collect reduced fees on a double spend transaction
b. The network relies on the majority of miners being honest to prevent this issue
c. Miners would not benefit from including a double spend as that block would be rejected by the network ✔

Question 36
Correct
Mark 1.00 out of 1.00

When faced with conflicting data, what measure will a miner use to choose which chain to build on top of?

a. A miner will build on top of whatever block they saw first
b. A miner will build on top of the chain with the most cumulative Proof-of-Work ✔
c. A miner will build on top of the most advantageous block, for example a block that they mined and gives them a mining reward

← Previous Jump to... Next →