Congratulations! You passed!

Grade received 100%

Latest Submission Grade 100%

To pass 80% or higher

Retake the assignment in **7h 58m**

Go to next item

1. Which of the following statements characterize a Hash function? Select all that apply: **1 / 1 point**

- [x] Digests cannot be reversed to produce inputs

  Correct
  Correct. Cryptographic hash functions are one-way. It is computationally and mathematically improbable to reverse digests into inputs. Additionally, digests leak no information about the inputs that created them.

- [x] Digests cannot be described on the basis of inputs without actually running the hash function.

  Correct
  Correct. Cryptographic hash function outputs can only be obtained by running the function itself. There are no shortcuts or alternative ways to discover the output for a given input.

- [x] Hash functions deterministically transform data of arbitrary size (inputs) to data of fixed size (digests)

  Correct
  Correct. No matter the size of the input, the digest will be of the same fixed size. There are some hash functions that can output variable sized outputs, but most hash functions do not.

- [ ] Hash functions are two-way functions, so the input can be derived from the output, and vice-versa

2. Which of the following best captures elements contained in a block? **1 / 1 point**

- ( ) A nonce, a time stamp, a number used once and transaction data.
- ( ) A time stamp, a master hash and a JSON web token.
- ( ) A master hash, the list of all transactions in a certain time period, a nonce, and a database.
- (•) A timestamp, a nonce, a hash of the previous block in the chain and transaction data.

Correct
Correct, these elements are typical within a block on a blockchain.

3. Which is an accurate description of how a nonce is used by miners in proof-of-work consensus? **1 / 1 point**

- (•) The nonce is guessed by miners in order to solve the proof-of-work puzzle to create a valid blockhash in order to create a new block.
- ( ) The nonce is a miners private key and allows them to see a transaction signed using their public key.
- ( ) The nonce is an API key that a miner uses to enter the blockchain.
- ( ) The nonce is guessed by miners in order to determine the number of Bitcoin this block will generate.

Correct
Correct. Miners race to look for a nonce that will create a valid blockhash. Once a miner is able to do this, they broadcast the block data to the network for other participants to verify the validity of the block.

4. Which of the following describe ways Alice can use *public key cryptography* to send a private message to Bob, so that only he can read it? **1 / 1 point**

- ( ) Alice encrypts a message she sends to Bob using her private key and an encryption function, preventing anyone but those having Bob's public key from being able to read it.
- ( ) Alice encrypts a message she sends to Bob using her public key and an encryption function, preventing anyone but those having Bob's private key from being able to read it.
- (•) Alice encrypts a message she sends to Bob using Bob's public key and an encryption function, which prevents anyone but those having Bob's private key from being able to read it.

Correct
Correct. Alice will use Bob's public key to encrypt the message. Only the holder of Bob's private key (which, hopefully, is just Bob, the intended recipient) will be able to decrypt the cypher text into a message that can be read and understood.

5. Which of the following are accurate statements about digital signatures? *Please select all that apply.* **1 / 1 point**

- [ ] A digital signature is used when a password is hashed so that it can only be read by those with a hashing algorithm.
- [ ] A digital signature is a hashed public key that has a length of 20 bytes, and is where Ether or other tokens can be sent to.
- [x] A digital signature is the process by which a message and an encrypted hash of that message is made with a private key. Then, a public key is used to verify that the original message hash can be recovered, which indicates that the message originated with the holder of the private key.

  Correct
  Correct, a digital signature allows for the validation of the origin of a message and does not require knowledge of the private key of the signatory.

- [ ] A digital signature is a method of transforming data so that it is consistently the same length. It takes a block of data of any length and returns a string of characters that will always be the same length.

6. What makes a block valid? **1 / 1 point**

- (•) A block is valid if the hash value of the entire block is below the threshold number which is set by the difficulty.
- ( ) A block is valid if the hash value of the entire block is larger than the threshold number which is set by the difficulty.
- ( ) A block is valid as long as its hash is included in the following block.

Correct
Correct.

7. The interrelationships of the blocks through their hashes—with each block containing the previous hash—helps to make the blockchain almost entirely _____ **1 / 1 point**

immutable

Correct
Each block contains the previous block's hash, which means that every block is linearly connected back to the original genesis block. The difficulty in changing a single block—and having to find valid hashes for all the subsequent blocks—is what makes the blockchain nearly incorruptible, or immutable.

8. Which of the following are properties of *cryptographic hash functions* that make them useful? *Select all that apply.* **1 / 1 point**

- [x] Takes on input of any size and outputs a digest

  Correct
  Correct. A hash function takes as its input any kind of digital data and produces an output, called a digest or hash.

- [ ] Increases chances of successful collisions
- [ ] Authenticates a document to guarantee its origin.
- [x] Function is one-way

  Correct
  Correct. The hash output cannot be reverse-engineered to determine the input to the hash function.

9. Which of the following are true of nodes in the blockchain? *Select all that apply.* **1 / 1 point**

- [x] A node can collect transactions

  Correct
  Correct, a node can collect transactions from the mempool and can use them to try to mine a new block.

- [x] A node can create new blocks

  Correct
  Correct, if a miner tries and succeeds in mining a valid block, their block will very likely be added to the blockchain.

- [x] A node can verify blocks

  Correct
  Correct, a node can receive blocks from other nodes and verify them before adding them to their local copies of their blockchains and sending the blocks on to other nodes.

- [ ] A node can delete data from other nodes