Blockchain

CBSA

BTA Certified Blockchain Solution Architect

QUESTION & ANSWERS
Demo

Version: 8.0

Question: 1

SHA-1 is the most commonly used SHA algorithm, and produces a _____-byte hash value(size).

A. 256
B. 128
C. 32
D. 20

Answer: D

Explanation:
SHA-1 is the most commonly used SHA algorithm, and produces a 20-byte hash value.

Question: 2

What type of attack would be considered a very large flaw in public blockchains such as Bitcoin's Blockchain where the majority of hashpower could possibly be controlled thru an attack?
What is the specific attack Bitcoin could be exposed to?

A. 51% Attacks
B. Tether Token Hack
C. DDoS Attack
D. BIP attack
E. Parity Wallet Attack

Answer: A

Question: 3

How many satoshis are in 1 bitcoin and how many wei in an Ether? (Select two.)

A. 1,000,000,000,000,000,000
B. 1,000,000,000,000,000
C. 1,000,000,000
D. 10,000
E. 1,000,000,000,000

Answer: A,B

Question: 4

In the Proof of Stake(POS) algorithm the miners are really known as _____?

A. Notary
B. Oracle
C. Forgers
D. Minters

Answer: C

Explanation:
Proof of Stake has the same goal as proof of work—to validate transactions and achieve consensus in the chain—and it uses an algorithm but with a different process. With proof of stake, the creator of a new block "is chosen in a deterministic way, depending on its wealth, also defined as a stake." Since in a proof of stake system, there is no block reward, but the miners, known as forgers, get the transaction fees. Proponents of this shift, including Ethereum co-founder Buterin, like proof of stake for the energy and cost savings realized to get to a distributed form of consensus.

Question: 5

A Byzantine failure is the loss of a system service due to a Byzantine fault in systems that requires_____.
What is required?

A. Consensus
B. Crypthography
C. Bandwidth
D. Availability

Answer: A

Explanation:
A Byzantine failure is the loss of a system service due to a Byzantine fault in systems that require consensus.

Question: 6

A _____cipher basically means it is using a fixed key which replaces the message with a pseudorandom string of characters. It is basically the encryption of each letter one at a time.
What is the cipher type?

A. Stream
B. Block
C. Parallel
D. RSA

Answer: A

Explanation:
Stream cipher basically means using a fixed key which replaces the message with a pseudorandom string of characters. It is basically the encryption of each letter one at a time.

Question: 7

You currently using the Metamask Chrome plugin and you see a selection for Etherescan in the plugin.
What is Etherscan used for?

A. A search engine that allows users to easily lookup, confirm and validate transaction that have taken place on the Ethereum Blockchain
B. A search engine that allows users to easily lookup, confirm and validate transaction that have taken place on the Bitcoin Blockchain
C. A search engine that allows users to easily lookup, confirm and validate transaction that have taken place on the Ethereum and Tokens Blockchain
D. A search engine that allows users to easily lookup, confirm and validate transaction that have taken place on any Blockchain

Answer: A

Explanation:
A search engine that allows users to easily lookup, confirm and validate transactions that have taken place on the Ethereum Blockchain

Question: 8

What are two challenges with using a Proof of Work algorithm? (Select two.)

A. Mining pools not allowed
B. Difficulty rate goes done every year.
C. Expensive
D. Power Intensive

Answer: C,D

Question: 9

Your customer is an enterprise that is focused on financial sectors. What type of blockchain would this customer likely want specified for their enterprise?

A. Permissionless
B. Decentralized
C. Hybrid
D. Permissioned

Answer: D

Explanation:
Sometimes referred to as “private” blockchains, you are required to have some sort of permission to access any or parts of that blockchain. There are a multitude of variants and hybrid permissioned/permissionless blockchains that exist.

Question: 10

Which is the following is the metaphor that describes a logical dilemma that plagues many computer networks?

A. Neo Generals’ problem
B. Byzantine Generals’ problem
C. Byzantine Admirals’ problem
D. Renaissance Generals’ problem

Answer: B

Explanation:
BFT is so-named because it represents a solution to the "Byzantine generals' problem," a logical dilemma that researchers Leslie Lamport, Robert Shostak and Marshall Pease described in an academic paper published in 1982

Question: 11

The key difference between encryption and hashing is that encrypted strings can be reversed back into their original decrypted form if you have the right key?

A. TRUE
B. FALSE

Answer: A

Question: 12

What is a logic gate in electronics and computer science?

A. A logic gate usually takes in 2 inputs and gives out 1 output. The inputs and outputs are binary values, meaning they can be both 1 and 0.
B. A logic gate usually takes in 3 inputs and gives out 2 output. The inputs and outputs are binary values, meaning they can be 1 or 0.
C. A logic gate usually takes in 2 inputs and gives out 6 output. The inputs and outputs are binary values, meaning they can be both 1 and 0.
D. A logic gate usually takes in 2 inputs and gives out 1 output. The inputs and outputs are binary values, meaning they can be 1 or 0.

Answer: D

Explanation:
A logic gate usually takes in 2 inputs and gives out 1 output. The inputs and outputs are binary values, meaning they can be 1 or 0. A XOR logic gate takes in 2 binary inputs and gives out a high output ONLY when the inputs are different. Meaning, if A and B are inputted to a XOR gate then the out C will be 1 ONLY when A is not equal to B.

Question: 13

Ethereum is considered to be a _____type of blockchain.

A. Permissionless
B. Permission Based
C. Hybrid
D. Private

Answer: A

Explanation:
Permissionless - anyone can join Anyone can run a node, run mining software/hardware, access a wallet and write data onto and transact within the blockchain (as long as they follow the rules of the bitcoin blockchain). There is no way to censor anyone, ever, on the permissionless bitcoin blockchain.

Question: 14

Your company working for is now considering the blockchain. They would like to perform a POC with R3 Cord
a. The CIO was reading about different blockchain consensus algos and would like to understand what type of consensus algos is used with Corda.
What is the best answer?
A. R3 Corda is a pluggable blockchain and allows the enterprise flexibility
B. R3 Corda is a byzantine fault tolerant blokchain
C. R3 Corda is a proof of stake based blockchain
D. R3 Corda is a proof of work based blockchain

Answer: A

Explanation:
Corda does not share the same requirements as Bitcoin: we require absolute certainty over transaction finality and we need to know who our counterparts are. So we had the freedom – and took this opportunity – to solve the consensus problem in a different way. In particular, Corda solves the privacy issue in a number of manners, primarily by allowing for separation of consensus into a service which we call the Notary Cluster. Corda was designed for business from the start. It has no cryptocurrency built into the platform and does not require mining-style consensus, which imposes great cost with little business benefit.

Question: 15

Secure Hash Algorithm (SHA-256) output is always 256 bits or 32 bytes in length regardless of the length of the input (even if input is millions of bytes). Select best answer.

A. NSA is spying on us so what's it matter.
B. Depends on input
C. False
D. True

Answer: D

Explanation:
SHA stands for Secure Hash Algorithm. This is used to prove data integrity. The same input(s) will always produce the exact same output. This output is always 256 bits or 32 bytes in length regardless of the length of the input (even if input is millions of bytes).