Certified Blockchain Solutions Architect (CBSA)

Practice Test

Question 1

Question: In what year was the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto, which outlines a solution to the double-spending problem, published?

a. 2008

b. 2009

c. 2011

d. 2012

Correct Answer(s): A. 2008

Explanation: In 2008, the whitepaper was published by Satoshi Nakamoto and outlines a solution to the double-spending problem. The following year, Bitcoin was released to the public.

Question 2

Question: Blockchain technology is built from which of the following sets of technologies?

a. P2P Networks, Public Key Encryption and Programs

b. Centralized Networks, RSA Encryption and Programs

c. P2P Networks, RSA Encryption and Enforcement

d. P2P Networks, Private Key Encryption and Contracts

e. Centralized Networks, RSA Encryption and Contracts

Correct Answer(s): A. P2P Networks, Public Key Encryption and Programs

Explanation: Blockchains are not using revolutionary technology but are built from these technologies used in a complementary fashion. P2P Networks Private Key Enc P2P Networks, Private Key Encryption and Programs

Question 3

Question: Blockchain technology is revolutionary in all of the following ways EXCEPT?

a. Blockchain is not new technology but a syncing of technologies that now make sense.

b. Trust is at the center and essentially removes intermediaries.

c. The tamperproof public ledger of value.

d. It is nondisruptive to the status quo.

e. It is a platform with numerous use cases.

Correct Answer(s): D. It is nondisruptive to the status quo.

Explanation: Blockchain is proving to be very disruptive to the status quo. Intermediaries such as payment processors, financial institutions, and other industries are seeing the blockchain as a disruptive force to their legacy business, but also as creating other opportunities for their business.

Question 4

Question: When the distributed ledger has been updated and all nodes maintain their own identical copy of the ledger, the nodes have reached which point?

a. Consensus

b. Agreement

c. Distributed

d. Immutable

Correct Answer(s): A. Consensus

Explanation: Consensus is when the distributed ledger has been updated and all nodes maintain their own identical copy of the ledger. This is also known as the "World State" in some blockchains.

This architecture allows for a new capacity as a system of recordkeeping that goes beyond being a simple database.

Question 5

Question: Which of the following blockchain key components state how the transactions will be confirmed?

a. Validity rules

b. Consensus algorithm

c. Encryption

d. Shared digital ledger

Correct Answer(s): A. Validity rules

Explanation: Validity rules (validation) state how the user and the transactions will be validated. This is predetermined by the consensus algorithm.

Question 6

Question: Which of the following are NOT considered to be benefits of a "public" blockchain?

a. Open Read and Write

b. Ledger is distributed

c. Secure due to mining (51% rule)

d. Faster transactions

Correct Answer(s): D. Faster transactions

Explanation: There are several public blockchain benefits, such as Open Read and Write, ledger is distributed, censorship resistant, and is secure due to mining (51% rule). Faster transactions is not correct because Private or Permissioned blockchains are more efficient in consensus, for example.

Question 7

Question: Establishing Trust in a Public Blockchain generally means to the users that all transaction data on a chained block is assumed to be trustworthy. The users base this trust on which of the following trust-related concerns? Select two.

a. This block data has not been tampered with.

b. The ledger is distributed.

c. The blockchain is immutable.

d. Data is still centralized in blockchains.

Correct Answer(s): A. This block data has not been tampered with, and C. The blockchain is immutable.

Explanation: Blockchain technology is about storing some kind of data, which are transactions in case of the Bitcoin blockchain. Users expect that, because there is no centralized control, that the blockchain is immutable.

Blockchain is essentially transferring trust from an intermediary to technology (software code).

Question 8

Question: What type of fork describes a major modification to the blockchain protocol which makes previously invalid blocks or transactions valid?

a. Hard fork

b. Soft fork

c. Either hard or soft forks

d. Segwit Fork

Correct Answer(s): A. Hard fork

Explanation: A hard fork is a term that describes a major change modification to the blockchain protocol, which makes previously invalid blocks or transactions valid.

This requires all nodes to upgrade to the latest version of the protocol software if they want to use the new coin or blockchain.

Question 9

Question: What is the main purpose of a blockchain implementing a Segregated Witness?

a. By removing signatures, this frees up capacity to add more transactions to each block on the chain.

b. By removing signatures, this frees up capacity to add more signatures to the chain.

c. It creates efficiency by removing signatures and also reduces security threats.

d. It does not enable off chain protocols.

Correct Answer(s): A. By removing signatures, this frees up capacity to add more transactions to each block on the chain.

Explanation: Segregated Witness, or Segwit for short, separates transaction signatures to increase blocksize on the chain.

Question 10

Question: When discussing Ethereum with your customers, what would be the best statement to use when comparing to cryptocurrencies?

a. Ethereum is the platform and Ether is its cryptocurrency.

b. Ether is a platform and Ethereum is the cryptocurrency for Ether.

c. Ethereum is a platform and Ether is the test platform. Bitcoin is used as the cryptocurrency for Ethereum.

d. None of the above.

Correct Answer(s): A. Ethereum is the platform and Ether is its cryptocurrency.

Explanation: When comparing blockchains and cryptos, it is important understand the platform versus the cryptocurrencies. For example, when comparing platforms to what is being enabled, Blockchain is essentially the train track; otherwise, the platform (platforms are the enabler).

Cryptos, like BTC, are essentially trains on the track or the platform (Applications are enabled).

Question 11

Question: What consensus algorithm's decision is represented by a system of "longest chain wins"?

a. Proof of Work

b. Proof of Stake

c. DPOS

d. Proof of Authority

Correct Answer(s): A. Proof of Work

Explanation: Proof of Work miners have to deal with a non-computational problem where their random guesses as to the "nonce" are most efficient.

Question 12

Question: What consensus algorithm is advantageous because it presents scalability and low-cost transactions, but, like Delegated Proof of Consensus (DPoS), introduces a component of centralization? Select One

a. Proof of Work

b. Proof of Stake

c. Practical Byzantine Fault Tolerance (PBFT)

d. Proof of Authority

Correct Answer(s): C. Practical Byzantine Fault Tolerance (PBFT)

Explanation: PBFT is notably implemented by Ripple (where validators are pre-selected by the Ripple foundation) and Stellar (where anyone can be a validator and trust is established by the community). BFT is advantageous because it presents scalability and low-cost transactions, but, like DPoS, introduces a component of centralization. .

Question 13

Question: The Bitcoin and Ethereum blockchains use which public key encryption algorithm?

a. ECDSA

b. MD5

c. AES

d. RSA

Correct Answer(s): A. ECDSA

Explanation: ECDSA (Elliptic Curve Digital Signature Algorithm) is the public key encryption algorithm used by both the bitcoin and Ethereum blockchains.

Question 14

Question: Which of the following is the BEST definition of Decentralization?

a. Peer-to-Peer data sharing, hosting hardware owned by many not few, fault tolerant, secure, lower performance

b. Peer-to-Peer data sharing, hosting hardware owned by a few not many, fault tolerant, secure, lower performance

c. Distributed data sharing, hosting hardware owned by many not few, fault tolerant, secure, lower performance

d. Peer-to-Peer data sharing, hosting hardware owned by many not few, fault tolerant, secure, higher performance

Correct Answer(s): A. Peer-to-Peer data sharing, hosting hardware owned by many not few, fault tolerant, secure, lower performance

Explanation: Peer-to-Peer essentially uses data sharing, hosting hardware owned by many not few, fault tolerant, secure, lower performance. It's common way to share files—a good example was Napster. Peer-to-peer (P2P) file sharing is the distribution of digital media such as software, videos, music, and images through an informal network in order to upload and download files. Typically, P2P software enables users to select which files to share. These files are indexed on a central server, making them available for other users to find and download.

Question 15

Question: Which of the following would NOT be true about what a smart contract gives your organization?

a. Autonomy

b. Trust

c. Legal assurance

d. Savings

Correct Answer(s): C. Legal assurance

Explanation: While smart contracts can be written to complement or substitute for legal contracts, their legal enforceability is not yet agreed upon by all state governments. .

Question 16

Question: Ethereum has four main components. Which of the following components executes smart contracts?

a. EVM

b. Node

c. Smart Contract code

d. dApps

Correct Answer(s): A.EVM

Explanation: Ethereum Virtual Machine (EVM) is built into the Ethereum blockchain and runs the Ethereum protocol.

Question 17

Question: The Ethereum blockchain is a _____type of machine?

a. Transactionless based

b. Stateless based

c. Stateful based

d. Transaction based

Correct Answer(s): D. Transaction based

Explanation: As described in the "yellow paper," Ethereum blockchain is a transaction-based state machine.

In computer science, a state machine refers to something that will read a series of inputs and, based on those inputs, will transition to a new state.

Question 18

Question: The Ethereum protocol design process follows a number of principles. These principles are all involved in guiding Ethereum development, but they are not absolute. Which of the following is NOT an Ethereum design principle?

a. Agile

b. Freedom

c. Sandwich Complexity Model

d. We have no features

Correct Answer(s): A. Agile

Explanation: Agile is not a principle. The Ethereum protocol design process follows a number of principles which are all involved in guiding Ethereum development, but they are not absolute.

Question 19

Question: Ethereum is a _____type of blockchain.

a. Permissionless

b. Permissioned

c. Hybrid

d. Private

Correct Answer(s): A. Permissionless

Explanation: Permissionless means 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 20

Question: Ethereum uses what type of cryptographic hashing algorithm hash algorithm?

a. SHA-256

b. Ehash

c. SHA-2 384

d. RSA

Correct Answer(s): B. Ehash

Explanation: Ethereum uses both public key cryptography and cryptographic hashing. The hashing algorithm is used for chaining blocks together.

Question 21

Question: There are two types of functions which are required in a smart contract. What are they? Select two.

a. Constructor

b. Fallback

c. Failback

d. String

Correct Answer(s): A. Constructor, and B. Fallback.

Explanation: The Constructor is called only once, when you deploy the smart contract.

The Fallback function is one without a name (literally no name, defined as function (){ code... }) which is invoked when someone sends Ether to the address of your smart contract. Without this function, Ether sent to the smart contract will be rejected

---

Question 22

Question: Which of the following is NOT a property of an Ethereum Smart Contract?

a. Automatically enforce obligations

b. Legally enforceable

c. Several smart contracts can make up a dapp

d. Defines the rules and penalties around an agreement in the same way that a traditional contract does

Correct Answer(s): B. Legally enforceable

Explanation: Smart Contracts are not meant to be legally enforceable in Ethereum. Smart contracts define the rules and penalties around an agreement in the same way that a traditional contract does. .

Question 23

Question: Dapps are open sourced and are accessed via what browser?

a. Mist

b. Internet Explorer

c. Composer

d. Chrome

Correct Answer(s): A. Mist

Explanation: Mist is the end-user interface for Ethereum. It's the tool of choice for browsing and using Dapps and is specifically designed for non-technical user base.

Question 24

Question: Using the Ethereum network requires you to pay for the write privilege in what type of format?

a. Gas

b. Ether

c. BTC

d. Coinbase

Correct Answer(s): A. Gas

Explanation: Gas is a measurement roughly equivalent to computational steps for Ethereum.

Every transaction is required to include a gas limit and a fee that it is willing to pay per gas.

Question 25

Question: The Ethereum Virtual Machine (EVM) is agile enough to run any code defined by the developer or the user of the EVM. What is the term for this type of VM used in Ethereum?

a. Quasi-Turing Complete

b. VMWare

c. Stateful

d. Stateless

Correct Answer(s): A. Quasi-Turing Complete

Explanation: The EVM Ethereum Virtual Machine is a computer software that runs at an abstraction layer straight above the underlying hardware.

Ethereum uses a Turing Complete Virtual Machine for running and compiling the codes.

The term "Turing Complete" states that this software is agile enough to run any code defined by the developer or user.

Question 26

Question: A limitation of the EVM not associated with other types of virtual state machines is that the EVM is intrinsically bound by which variable parameter ?

a. Gas

b. CPU

c. Code Base

d. Location

Correct Answer(s): A. Gas

Explanation: The only limitation the EVM has that a typical Turing complete machine does not is that the EVM is intrinsically bound by gas, which limits the amount of computation that can be performed.

Question 27

Question: When joining the Ethereum network, you have the option of running various types of nodes. Which of the following is NOT an option?

a. Secure

b. Light

c. Full

d. Archive

Correct Answer(s): A. Secure

Explanation: Ethereum Node Types defined: Full nodes verify block that is broadcast onto the network; Light nodes do not verify every block or transaction and do not have a copy of the current blockchain state; Archive nodes are full nodes that preserve the entire history of transactions.

Question 28

Question: Inter-Planetary File System (IPFS) is a decentralized filesystem and peer peer-to-peer hypermedia protocol that is similar to which solution?

a. BitTorent

b. FUSE

c. Dropbox

d. EVM

Correct Answer(s): A. BitTorent

Explanation: The Inter-Planetary File System (IPFS) is a decentralized filesystem and peer-to-peer hypermedia protocol.

Compare to a single BitTorrent swarm exchanging and sharing data through multiple nodes storing parts of the same file.

Question 29

Question: What protocol is IPFS designed to replace?

a. FTP

b. HTTP

c. SSL

d. RDP

Correct Answer(s): B. HTTP

Explanation: IPFS is designed to be P2P with no Centralized Point of Failure. Features of IPFS are: It can be used to view documents such as on the Web; Files can be accessible via HTTP; hash-addressed content guarantees authenticity; browsers or extensions can learn to use the URL Scheme. Essentially replaces HTTP.

Question 30

Question. Ethereum development uses some specific tools for backend development. What are two of the tools that are supported? Select two.

a. Solidity

b. Viper

c. C++

d. Java

Correct Answer(s): A. Solidity, and B. Viper.

Explanation: Solidity, the language behind Ethereum, is specifically designed to utilize the Ethereum Virtual Machine or EVM.

Ethereum-based applications and Smart Contracts are written in Solidity.

Viper is the successor to Serpent. It is under active development. Serpent has been deprecated. .

Question 31

Question: You're developing a program and want it to talk to an Ethereum node from inside a JavaScript application to interface RPC. What API library do you use?

a. web3.js

b. JSON

c. C++

d. Node,Js

Correct Answer(s): A. Web3.js

Explanation: JSON is a lightweight data-interchange format. It can represent numbers, strings, ordered sequences of values, and collections of name/value pairs.

To talk to an Ethereum node from inside a JavaScript application, use the web3.js library, which provides a convenient interface for the RPC methods.

Question 32

Question: The Hyperledger Project consists of the following EXCEPT?

a. Management

b. Infrastructure

c. Frameworks

d. Tools

Correct Answer(s): A Management

Explanation: Management is not correct. The Hyperledger Project consists of the following:

Infrastructure: Ecosystems that accelerate open development and commercial adoption

Frameworks: A portfolio of differentiated approaches to business blockchain frameworks developed by a growing community of communities

Tools: Typically built for one framework, and through common license and community-of-communities approach, ported to other frameworks .

Question 33

Question: Which part of the Hyperledger Project has the marketing responsibility for commercial adoption of the Hyperledger Solutions?

a. Management

b. Infrastructure

c. Frameworks

d. Tools

Correct Answer(s): B. Infrastructure

Explanation: Infrastructure refers to the ecosystems that accelerate open development and commercial adoption.

Question 34

Question: The Hyperledger Project Framework of blockchains is meant for specific use cases for enterprise. Which blockchain includes a novel consensus algorithm, Proof of Elapsed Time (PoET)?

a. Hyperledger Sawtooth

b. Hyperledger Fabric

c. Hyperledger Iroha

d. Hyperledger Indy

Correct Answer(s): A. Hyperledger Sawtooth

Explanation : Hyperledger Sawtooth is a modular platform for building, deploying, and running distributed ledgers.

Hyperledger Sawtooth includes a novel consensus algorithm, Proof of Elapsed Time (PoET), which targets large distributed validator populations with minimal resource consumption

Question 35

Question: You're currently investigating Hyperledger and would like to confirm that there is a set of collaboration tools for building blockchain business networks that accelerate the development of smart contracts and blockchain applications. What is the solution that meets the requirement?

a. Hyperledger Composer

b. Hyperledger Explorer

c. Hyperledger Quilt

d. Hyperledger Cello

Correct Answer(s): A Hyperledger Composer

Explanation: Hyperledger Composer (contributed by IBM and Oxchains) is a set of collaboration tools for building blockchain business networks that accelerate the development of smart contracts and blockchain applications, as well as their deployment across a distributed ledger.

Question 36

Question: The Hyperledger Project has a modular umbrella schema to its organization which includes three parts of the organizational schema. As part of the organizational schema, it includes an "Infrastructure" Module that is structured with four layers. What layer below is NOT part of the structure?

a. Architecture

b. Technical

c. Legal

d. Organizational

Correct Answer(s): A. Architecture

Explanation: The Infrastructure Module includes the following four modules: Technical, Legal, Marketing, and Organizational.

Question 37

Question: What is provided by the Hyperledger Fabric to facilitate network communications?

a. SDK

b. API

c. GOLANG

d. Middleware

Correct Answer(s): A. SDK

Explanation: Hyperledger Fabric provides a Node.js and a Java SDK to facilitate network communications functionality.

Question 38

Question: The advantages of using Hyperledger Fabric include which of the following? Select one.

a. Having a modular component structure

b. Ability to use your programs from SQL

c. Having a native token to use for payments

d. Having a POW mining algorithm

Correct Answer(s): A. Having a modular component structure

Explanation: Hyperledger Fabric has a modular component structure and an extensible plug and play framework.

Question 39

Question: Hyperledger fabric business network is divided into which of the following categories?

a. Sawtooth, Fabric, and Indy

b. Composer, Fabric, and Chaincode

c. Blockchain, Chaincode, and Membership

d. Blockchain, Registration, Identity

Correct Answer(s): A. Blockchain, Chaincode, and Membership

Explanation: The Hyperledger Fabric business network is divided into three categories: Blockchain, Membership, and Chaincode.

Question 40

Question: Hyperledger can best be described as which of the following?

a. A newer version of Proof of Work

b. Having a single blockchain in the framework

c. An effort to advance cross-industry blockchain technologies

d. A newer version of Proof of Stake

Correct Answer(s): C. An effort to advance cross-industry blockchain technologies.

Explanation: Under an "Umbrella Strategy," Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies

Question 41

Question: The chaincode's interface implements which of the following functions?

a. Invoke and init

b. Open and close

c. Close and shut

d. Invoke and revoke

Correct Answer(s): Invoke and Init

Explanation: Hyperledger supports the following two types of transactions.

Code deploying transaction: A code deploying transaction submits, updates, or terminates a chaincode.

Code invoking transaction: A code invoking transaction is an API call to a chaincode function.

Question 42

Question: Proof of Stake consensus aims to do all of the following EXCEPT?

a. Improving transaction capacity

b. Improving security by removing the Nothing at Stake Issues

c. Improving performance

d. Reducing hardware requirements for nodes

Correct Answer(s): B. Improving security by removing the Nothing at Stake Issues

Explanation: Proof of Stake removes the guessing game from the validation of blocks so mining no longer requires powerful and specialized hardware. Therefore, it requires less energy for processing. Proof of Stake consensus uses a system where "Validator" nodes each give or pay a stake in order to validate transactions. When it's time for group consensus, all who wish to participate lock up funds in a stake. The key difference with this consensus is that no computing is ever performed during consensus; only wagering and any kind of device can wager, regardless of computing power. One potential vulnerability of the Proof of Stake is the Nothing at Stake problem, where a validator node approves all transactions on both sides of a ledger after a hard fork has occurred.

Question 43

Question: What type of organization can be thought of as a corporation run without any human involvement under the control of an incorruptible set of business rules?

a. Decentralized Autonomous Organization (DAO)

b. Limited Liability Corporation

c. Corporation

d. Forked Organization

Correct Answer(s): A. Decentralized Autonomous Organization (DAO)

Explanation: Decentralized Autonomous Organization (DAO) can be thought of as a corporation run without any human involvement under the control of an incorruptible set of business rules. A DAO can also be seen as the most complex form of a smart contract, where the bylaws of the decentralized organization are embedded into the code of the smart contract, using complex token governance rules.

Question 44

Question: What is the process of turning cipher-text back into plaintext called?

a. Decryption

b. Hashing

c. Encoding

d. Encryption

Correct Answer(s): A. Decryption

Explanation: Decryption is the process of turning cipher-text back into plaintext. Encryption is the process of turning a clear-text message (plaintext) into a data stream (cipher-text), which looks like a meaningless and random sequence of bits.

Question 45

Question: What is the process called when two parallel blockchains are created, where one of the two is the winning blockchain?

a. Fork

b. Merger

c. Bridge

d. EVM

Correct Answer(s): A. Fork

Explanation: A fork is the creation of an ongoing alternative version of the blockchain, by creating two blocks simultaneously on different parts of the network. It creates two parallel blockchains, where one of the two is the winning blockchain

---

Question 46

Question: A _____ is a digital identity for something that can be owned.

a. Token

b. Coin

c. Cryptocurrency

d. Key

Correct Answer(s): A. Token

Explanation: A token is a digital identity for something that can be owned. Cryptocurrency is a form of digital currency based on mathematics, where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds

Question 47

Question: All of the following are key terms in Cryptography EXCEPT

a. Secret

b. Function

c. Root Hash

d. Cypher

Correct Answer(s): C. Root Hash

Explanation: Cryptography is used in Blockchain to address the issues and concerns of privacy. Cryptography is the study of how to send information back and forth securely in the presence of adversaries. A cryptographic function is a function for encoding or encrypting data to protect the contents from others. The following components are the basis of a cryptographic function:

- ✓ The Secret: The data which we are trying to protect
- ✓ The Key: A piece of data used for encrypting and decrypting the secret
- ✓ The Function: The process or function used to encrypt the secret
- ✓ The Cipher: The encrypted secret data, output of the function

The Secret and the Key are passed into the Function to create a Cipher

---

Question 48

Question: Group Consensus is reached when how many members agree?

a. 51%

b. 50%

c. 75%

d. 100%

Correct Answer(s): A. 51%

Explanation: The truth is assumed to be the version of the ledger that 51% or more of the tribe members present agree on.

Question 49

Question: What is a file called that contains a collection of private keys?

a. Wallet

b. Hashgraph

c. Block

d. Ledger

Correct Answer(s): A. Wallet

Explanation: A wallet is a file that contains a collection of private keys. These wallets could be online, offline, paper, or hardware.

Question 50

Question: What type of ledger refers to a distributed ledger that doesn't require a native currency to operate?

a. Tokenless

b. Private

c. Enterprise

d. Centralized

Correct Answer(s): A. Tokenless

Explanation: A tokenless ledger refers to a distributed ledger that doesn't require a native currency to operate.