CBSA.98q

Number: CBSA
Passing Score: 800
Time Limit: 120 min

CBSA

BTA Certified Blockchain Solution Architect

Exam A

QUESTION 1

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: https://blockgeeks.com/guides/cryptocurrencies-cryptography/

QUESTION 2
Ethereum is considered to be a _____type of blockchain.

A. Permissionless
B. Permission Based
C. Hybrid

D. Private

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: https://medium.com/@dustindreifuerst/permissioned-vs-permissionless-blockchains-acb8661ee095

QUESTION 3
Your company working for is now considering the blockchain. They would like to perform a POC with R3 Corda. 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 4
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 matters.
B. Depends on input
C. False
D. True

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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).

Reference: https://medium.com/all-things-ledger/bitcoins-implementation-of-blockchain-2be713f662c2

QUESTION 5
In the Ethereum EVM there are two types of memory areas. (Select two.)

A. Storage
B. Database
C. Memory
D. Persistent
E. Ephemeral

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html#the-ethereum-virtual-machine

QUESTION 6
What are some advantages of Proof of Stake(POS) mining over Proof of Work(POW) mining? (Select three.)

A. Energy efficient in regards to that it could consume for electricity as compared to PoW
B. Faster Hashing algorithms
C. No need for expensive compared to POW

D. Faster validations compared to POW
E. Better blockchain security compared to POW

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This eliminates the below challenges from PoW and believed to have an advantage.
No need of expensive hardware (a normal laptop or computer running the respective coin's Validator client will do as long as your laptop or computer is online)
Energy efficient as it won't consume high electricity as PoW does More loyal Validators As higher the stake the Validators have for a long time, more chances for the Validator to be picked up for "forging" and earn the transaction fee Faster validations

Reference: https://medium.com/@karthik.seshu/cryptocurrency-proof-of-work-vs-proof-of-stake-e1eee1420b10

QUESTION 7
Application Specific Integrated Circuit (ASIC) are used always in enterprise blockchains.

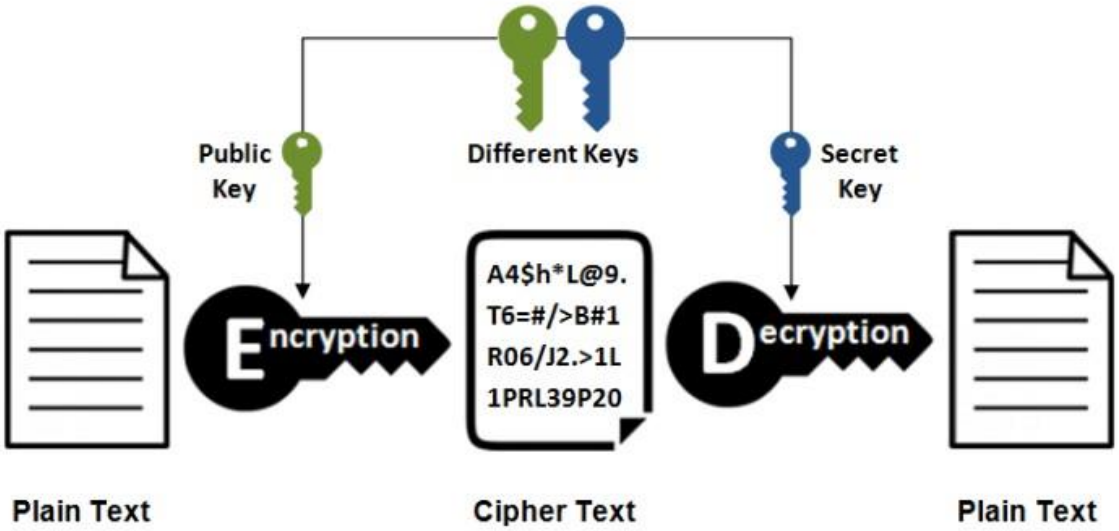
A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ASICS are generally used in blockchains such as BTC that have a Proof of Work consensus due to competition

Reference: https://www.trymining.com/pages/asic-vs-gpu

QUESTION 8
What type of encryption is shown below and is commonly used in blockchain cryptography?



A. Diffie-Hellman
B. Asymmetric Encryption
C. Synchronous
D. Asynchronous
E. Symmetric Encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Asymmetric cryptography utilizes two different keys, a public key and a private to encrypt and decrypt a particular data. The use of one key cancels out the use of the other.

Reference: https://blockgeeks.com/guides/cryptocurrencies-cryptography/

QUESTION 9
Contracts live on the blockchain in an Ethereum-specific binary format called _____?

A. EOS
B. EVM Code
C. Ether
D. Gas
E. EVM Bytecode

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Ethereum Virtual Machine (EVM) is the runtime environment for smart contracts in Ethereum. It is not only sandboxed, but actually completely isolated, which means that code running inside the EVM has no access to network, filesystem, or other processes. Smart contracts even have limited access to other smart contracts.

Reference: http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html#the-evm

QUESTION 10
Bitcoin uses what proof of work consensus system?

A. Cubehash512
B. Scrypt-Jane
C. Whirlpool
D. Scrypt-n
E. Hashcash

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Bitcoin uses the Hashcash proof of work system.

Reference: https://en.bitcoin.it/wiki/Hashcash

QUESTION 11

An _____ is a well-known service that signs transactions if they state a fact and that fact is considered to be true. They may optionally also provide the facts.

A. notary
B. oracle
C. node
D. endpoint

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An oracle is a well known service that signs transactions if they state a fact and that fact is considered to be true. They may also optionally provide the facts r 3 Corda Technical Whitepaper.

QUESTION 12
Select the two kinds of accounts in Ethereum which share the same address space. (Select two.)

A. Gas Account
B. Contract Accounts
C. External Accounts
D. Internal Accounts
E. dApp Accounts

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
The most popular Ethereum development framework is currently Truffle.

What are three features of Truffle? (Select three.)

A. Scriptable deployment & migrations framework.
B. Automated contract testing with Mocha and Chai.
C. Takes Dapp transactions via Ws-rpc, json-rpc, ipc-rpc.
D. Built-in smart contract compilation, linking, deployment and binary management.
E. Automated contract testing with Mocha only

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Truffle is a development environment, testing framework and asset pipeline for Ethereum, aiming to make life as an Ethereum developer easier.

Reference: https://github.com/trufflesuite/truffle

QUESTION 14
You are considering writing smart contracts and there are a few different languages you can consider. (Select two.)

A. Truffle
B. Serpent
C. Solidity
D. Embark

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To write smart contracts there are a few different languages: Solidity, which is like JavaScript and has .sol as a file extension, Serpent, Python-like with extension .se, and a 3rd, LLL, based on Lisp. Serpent was popular a while back but Solidity is the most popular right now and more robust, so just use Solidity. You prefer Python? Use Solidity.

Reference: https://medium.com/@ConsenSys/a-101-noob-intro-to-programming-smart-contracts-on-ethereum-695d15c1dab4

QUESTION 15
Satoshi Nakamoto invented a way to achieve Decentralized Consensus?

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.interlogica.it/en/insight-en/nakamoto-consensus/

QUESTION 16
Which of the following would NOT be true about what a smart contract gives your organization?

A. Accuracy
B. Savings
C. Autonomy
D. Trust
E. Legal Assurance

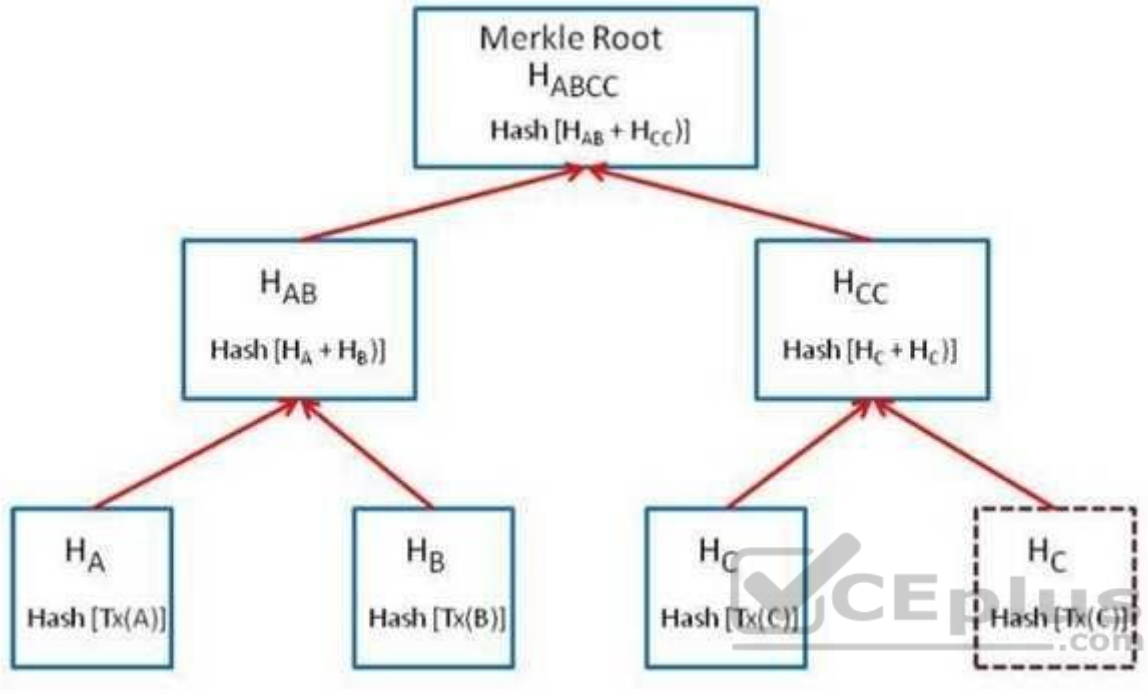
Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Smart contracts generally are not legal contracts. However, its possible that a smart contract could be accepted as a legal contract but not normally. Read more about Smart contracts here

Reference: https://blockgeeks.com/guides/smart-contracts/

QUESTION 17
The _____of the tree is the topmost node and hence this tree is represented upside down. The bottommost nodes are called as _____nodes. Each node is simply a cryptographic hash of a transaction.



Sample Merkle Tree of just 4 transactions

In the above diagram, Transaction A,B, C,C from the leaves of the tree. Select one.

A. Root, Hash
B. Root, Leaf Nodes
C. Has, Root nodes
D. Leaf nodes, Root
E. Leaf Nodes, Root

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The root of the tree is the topmost node and hence this tree is represented upside down. The bottommost nodes are called as leaf nodes. Each node is simply a cryptographic hash of a transaction. In the above diagram, Transaction A,B,C,C form the leaves of the tree.

Reference: https://medium.com/all-things-ledger/bitcoins-implementation-of-blockchain-2be713f662c2

QUESTION 18
Which of the following blockchain is NOT a permissioned blockchain?

A. Quantum
B. Ethereum
C. R3 Corda
D. Ripple
E. Hyperledger

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
What blockchain is considered Blockchain 1.0, the first blockchain?

A. Bitcoin Cash

B. Ethereum
C. Litecoin
D. Bitcoin
E. NEO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Blockchain 1.0, Grandpa Bitcoin

Reference: https://hackernoon.com/a-brief-history-in-the-evolution-of-blockchain-technology-platforms-1bb2bad8960a

QUESTION 20
In the EVM every account has a persistent key-value store mapping 256-bit words to 256-bit words called _____

A. Gas
B. Space
C. Storage
D. Datastore
E. Database

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Every account has a persistent key-value store mapping 256-bit words to 256-bit words called storage.

Reference: https://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html#the-ethereum-virtual-machine

QUESTION 21
_____ is the official Ethereum IDE that allows developers to build and deploy contracts and decentralized applications on top of the Ethereum blockchain.

A. Mist
B. Mix

C. Truffle
D. Metamask
E. Embark

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Mix is the official Ethereum IDE that allows developers to build and deploy contracts and decentralized applications on top of the Ethereum blockchain

QUESTION 22
What is the language that Solidity is using to build on the Ethereum Virtual Machines(EVM)?

A. .Net
B. Javascript
C. C++
D. Node.js
E. PHP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Javascript is the language that Solidity is using to build on the Ethereum Virtual Machine

Reference: https://www.quora.com/What-is-the-best-programming-language-to-learn-if-you-want-to-work-on-the-blockchain

QUESTION 23
What is another name for blockchains that run adjacent to the blockchains and also offer more scope for processing contracts?

A. Adchains
B. Funnelchains
C. Multichains

D. Sidechains

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sidechain is another name for blockchains that run adjacent to Bitcoin and offer more scope for processing contracts.

Reference: https://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/

QUESTION 24
What are two cryptocurrencies that you would expect to see mining equipment with ASICS? (Select two.)

A. Bitcoin
B. Ethereum
C. Neo
D. Litecoin
E. Monero

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.trymining.com/pages/asic-vs-gpu

QUESTION 25
Vitalik Buterin referred to this concept of trust beyond just currency as ‘smart contracts’ or even blockchain-based “decentralized autonomous organizations” (DAOs).

Ethereum is considered Blockchain version?

A. 2.0
B. 4.0
C. 3.0
D. 1.0

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
2.0 Ethereum came after Bitcoin. Vitalik Buterin, one of the writers for Bitcoin Magazine that tried to popularize the technology in the early 2012. He witnessed firsthand the problems in the Bitcoin implementation like wasteful mining hardware, centralized mining community, and lack of network scalability. In 2013, the then 19 year old Vitalik described his vision for Ethereum by extending the concept of Bitcoin beyond just currency. He proposed a platform where developer community and entrepreneurs to build distributed application (Dapps) for the Blockchain network. He referred to this concept of trust beyond just currency as 'smart contracts' or even blockchain-based "decentralized autonomous organizations" (DAOs).

Reference: https://hackernoon.com/a-brief-history-in-the-evolution-of-blockchain-technology-platforms-1bb2bad8960a

QUESTION 26
Ethereum is a programmable blockchain. What is one of the following reasons is NOT correct regarding Ethereum programmability?

A. Allows users to create their own operations on any complexity
B. It serves as a platform for many different types of decentralized blockchain applications
C. Does not allow users to create their own operations of any complexity
D. Ethereum also includes a peer-to-peer network protocol

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

QUESTION 27
The block creation time is set to how many minutes in Bitcoin?

A. 1
B. 10
C. 120
D. 100
E. 15
F. 150

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Remember, that the block creation time is set to 10 minutes and this can never change. So after a fixed time of approximately 2 weeks or exactly 2016 blocks the difficulty is re-adjusted. Increase in difficulty means target decreases.

Reference: https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2

QUESTION 28
In Hyperledger Fabric chaincode runs in a secured Docker container isolated from the endorsing peer process?

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://hyperledger-fabric.readthedocs.io/en/release-1.1/chaincode.html

QUESTION 29
You would like to run Ethereum DApps in a browser without a node. (No need to download blockchain.)

What could you use locally in your Chrome browser?

A. Jaxx
B. Solidity
C. Metamask
D. Mist

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Metamask is essentially a bridge.

Reference: https://blog.aion.network/introguideandwallet-57882a4066e3

QUESTION 30
You would like to start your Gethin Fast Sync Mode.
What is the command for this?

A. geth-mode—fast—cache 4096
B. geth—fast—cache 4096
C. geth—cache—fast 4096
D. geth—fast-mode—cache 4096

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://datawookie.netlify.com/blog/2018/01/ethereum-running-a-node/

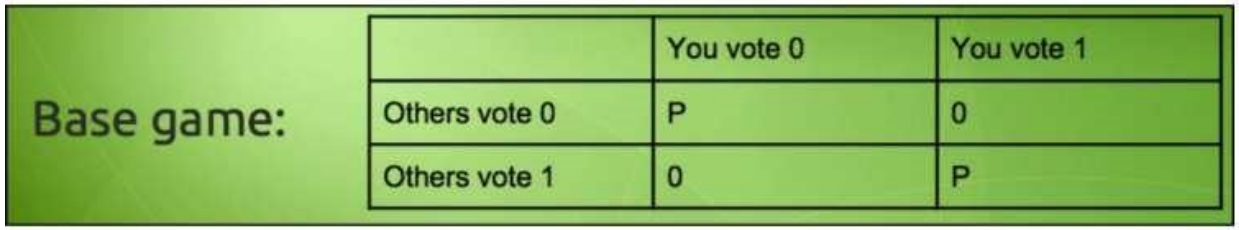
QUESTION 31
Which of the following is not considered an Ethereum testnet?

A. Ropstein
B. Rinkeby
C. Mainnet
D. Kovan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://testnet.etherscan.io/

QUESTION 32
Looking the graph below, what type of an attack is this likely?



A. 51% Attack
B. P+ Epsilon Attack
C. Blacklisting
D. Selfish Mining Attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A proof of work system is vulnerable to a particular type of attack called the “P+ epsilon attack”. In order to understand how this attack works we must define some terms before hand. Un-Coordinated Choice Model: An uncoordinated choice model is a model where all the participants don’t have the incentive to work with one another. The participants may form groups but at no time is the group big enough to become a majority.

Reference: https://blockgeeks.com/guides/hypothetical-attacks-on-cryptocurrencies/

QUESTION 33
What does the 20 in ERC20 mean or relate to?

A. BIP number
B. Release number
C. Update number
D. Proposal ID number

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ERC stands for Ethereum Request for Comments. This is an official protocol for proposing improvements to the Ethereum network. '20' is the unique proposal ID number.

Reference: https://support.exodus.io/article/108-what-is-an-erc20-token-and-does-exodus-support-it

QUESTION 34
You are considering writing a smart contract for Ethereum and would like to use a robust programming language.

Which programming language is considered the most flexible and robust for Ethereum?

A. Solidity
B. Python
C. Serpent
D. JS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To write smart contracts there are a few different languages: Solidity, which is like JavaScript and has .sol as a file extension, Serpent, Python-like with extension .se, and a 3rd, LLL, based on Lisp. Serpent was popular a while back but Solidity is the most popular right now and more robust, so just use Solidity. You prefer Python? Use Solidity.

Reference: https://medium.com/@ConsenSys/a-101-noob-intro-to-programming-smart-contracts-on-ethereum-695d15c1dab4

QUESTION 35
How many peers in the network need to endorse a transaction in a Hyperledger Fabric blockchain?

A. The number of peers required to endorse a transaction is driven by the IAM policy that is specified by the ledger.
B. The number of peers required to endorse a transaction is driven by the endorsement policy that is specified by the DApps.
C. The number of peers required to endorse a transaction is driven by the endorsement policy that is specified by the ledger.
D. The number of peers required to endorse a transaction is driven by the endorsement policy that is specified at chaincode deployment time.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The number of peers required to endorse a transaction is driven by the endorsement policy that is specified at chaincode deployment time.

Reference: http://hyperledger-fabric.readthedocs.io/en/release-1.1/Fabric-FAQ.html#endorsement

QUESTION 36
When considering a new ERC20 token its best to consider using _____.

A. Use a template from AWS
B. Audited Implementation
C. Start a new one
D. Copy from existing token

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://medium.com/@merunasgrincalaitis/gain-ethereum-ico-trust-credibility-e9e53145c331

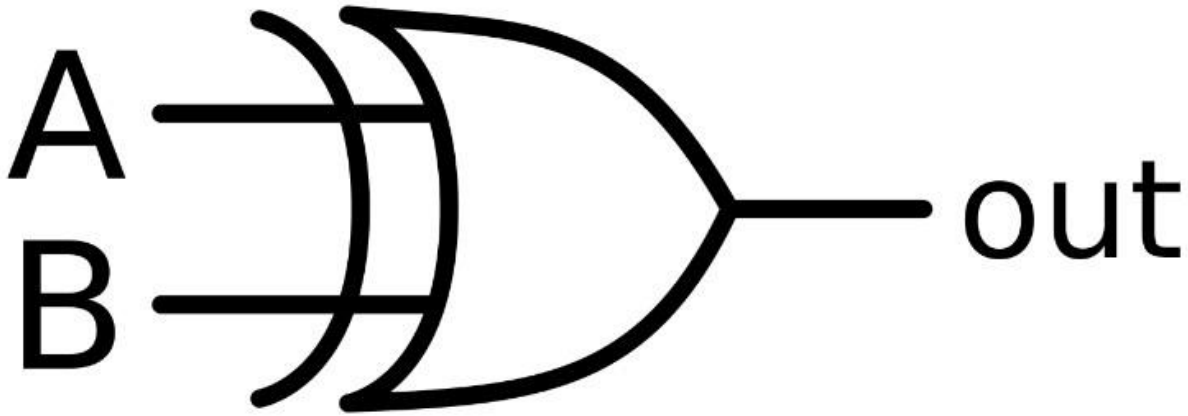
QUESTION 37
Smart Contracts are generally written in specific programming languages. Which one is NOT a language for smart contracts?

A. .Net
B. Viper
C. LLL
D. Solidity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
What is diagram referencing below?



A. AND Gate
B. XOR Gate
C. OXR Gate
D. NAND Gate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
XOR or “Exclusive OR” is a logic gate.

Reference: https://blockgeeks.com/guides/cryptocurrencies-cryptography/

QUESTION 39
Which of the following is considered the most popular public key encryption algorithm?

A. RSA
B. AES
C. MD5D. PGP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://medium.com/@ConsenSys/blockchain-underpinnings-hashing-7f4746cbd66b

QUESTION 40
Geth uses what port to expose the Ethereum RPC Service?

A. 2096
B. 8545
C. 4096
D. 2545

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://datawookie.netlify.com/blog/2018/01/ethereum-running-a-node/

QUESTION 41
In Ethereum the difficulty adjustment algorithm is coded in the _____ file.

A. calcDifficultyFrontier
B. block_validator.go
C. calcDifficultyHomesteadD. calcDifficultyvalidator.go

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dltlabs.com/how-difficulty-adjustment-algorithm-works-in-ethereum/

QUESTION 42
Which of the following is NOT a requirement of an enterprise blockchain typically?

A. Append-only distributed system of record shared across business network
B. Cost efficient blockchain
C. Transactions are endorsed by relevant participants
D. Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://developer.ibm.com/courses/all/blockchain-essentials/

QUESTION 43
Which of the following blockchain key components state how the transactions will be confirmed?

A. Distributed Ledger database
B. Validity Rules
C. Consensus Algorithm
D. Encryption

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 44
A chaincode package that was signed at creation can be handed over to other owners for inspection and signing in Hyperledger.

Is it true that the workflow supports out-of-band signing of chaincode package?

A. TRUE
B. FALSE

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:
Explanation:
A chaincode package that was signed at creation can be handed over to other owners for inspection and signing. The workflow supports out-of-band signing of chaincode package.

Reference: http://hyperledger-fabric.readthedocs.io/en/release-1.1/chaincode4noah.html

QUESTION 45
_____is advantageous because it presents scalability and low cost transactions, but like DPoS introduces a component of centralization.

What algorithm is being referenced here?

A. Byzantine Fault Tolerance
B. Hashgraph
C. Proof of Stake
D. Proof of Work
E. DAG

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
BFT 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.

Reference: https://hackernoon.com/an-overview-of-cryptocurrency-consensus-algorithms-9d744289378f

QUESTION 46
In Hashcash, miners all compete to look for a so called. "_____"which, if provided as input (together with other parts of a block header) to a hash function, yields an output that's numerically small enough to claim the next block reward.

A. Difficulty bits
B. Nonce

C. Merkle Root
D. Timestamp

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://medium.com/all-things-ledger/bitcoins-implementation-of-blockchain-2be713f662c2

QUESTION 47
You currently on a conference call with an executive from a too big to fail bank. They are validating that they want to use Quorum or another enterprise blockchain. They specifically want to know what type of consensus algo it uses and what industry for the Quorum blockchain targets.

A. BFT, cross industry
B. POS, Financial only
C. Majority voting, Financial only
D. Majority voting, cross industry
E. POW, cross industry

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.horsesforsources.com/top-5-blockchain-platforms_031618

QUESTION 48
When a consensus algo is considered to be "pluggable modularity», what does that mean?

A. Add permission as needed
B. Add user as needed
C. Select an optimal algorithm for your networks
D. Select a specific API that manages the blockchain

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

QUESTION 49
The merkle tree contains a full list of the transactions on the blockchain?

A. FALSE
B. TRUE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The merkle tree does not contain a list of all the transactions, rather a hash (digital fingerprint) of all transactions as a tree structure.

Reference: https://medium.com/all-things-ledger/bitcoins-implementation-of-blockchain-2be713f662c2

QUESTION 50
Which of the following enterprise blockchains have a pluggable framework consensus algo? (Select two.)

A. Quorum
B. R3 Corda
C. Ethereum
D. Hyperledger Fabric
E. Ripple

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.horsesforsources.com/top-5-blockchain-platforms_031618

QUESTION 51
You are using Truffle for an Ethereum contract and would like to use a default set of contracts and tests from within an empty project directory.

What is the syntax?

A. truffle defaults
B. truffle init
C. truffle test
D. truffle compile

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://github.com/trufflesuite/truffle

QUESTION 52
Gas has multiple associated terms with it: Gas Prices, Gas Cost, Gas Limit, and Gas Fees. The principle behind Gas is to have a stable value for how much a transaction or computation costs on the Ethereum network.

Which is considered to be the static value for how much a computation costs in terms of Gas?

A. Price
B. Fee
C. Cost
D. Limit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Gas Cost is a static value for how much a computation costs in terms of Gas, and the intent is that the real value of the Gas never changes, so this cost should always stay stable over time

Reference: http://ethdocs.org/en/latest/ether.html

QUESTION 53

Which of the following is NOT considered a token?

A. ICON
B. LTC
C. Golem
D. EOS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
LTC is Litecoin and is a crypto. Check Ethereum tokens here: https://etherscan.io/tokens

QUESTION 54
How are "assets" in Hyperledger Fabric represented? (Select two.)

A. JSON
B. Node
C. YAML
D. Binary
E. Deployment Manager

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Assets in Hyperledger Fabric are represented in JSON or Binary. Assets are represented in Hyperledger Fabric as a collection of key-value pairs, with state changes recorded as transactions on a Channel ledger. Assets can be represented in binary and/or JSON form.

Reference: https://hyperledger-fabric.readthedocs.io/en/release-1.3/fabric_model.html

QUESTION 55
The Hyperledger Fabric business network is divided into three categories. What are the three categories? (Select three.)

A. Membership
B. Chaincode
C. Networking
D. EVM
E. Blockchain

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
The Secure Registry Services enables Secured _____Registry of base Hyperledger images and custom images containing chaincodes.

What type of registry is implemented?

A. Docker
B. EVM
C. Kubenetes
D. VMWare

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Secure Registry Services enables Secured Docker Registry of base Hyperledger images and custom images containing chaincodes.

QUESTION 57
Hyperledger Composer has two main components. What are the two components? (Select two.)

A. Fabric
B. Sawtooth
C. Playground
D. Explorer

E. Business Network Archive
F. SDK

Correct Answer: CE
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Hyperledger Composer has following main components: 1) Business Network Archive: Capturing the core data in a business network, including the business model, transaction logic, and access controls, the Business Network Archive packages these elements up and deploys them to a runtime. Business Network Archive files are stored as ".bna" files. 2) Composer Playground: This web-based tool allows developers to learn Hyperledger Composer, model out their business network (domain), test that network, and deploy that network to a live instance of a blockchain network. The playground keeps the development model in browser storage, allowing them to be easily uploaded or downloaded. The playground also allows for CRUD (create, read, update, delete) operations to be performed on asset transactions which are created and logged. Composer playground offers a repository of sample business networks that can provide a base for building your own business network

QUESTION 58
What are two specific advantages of using Hyperledger Fabric? (Select two.)

A. No order service needed
B. Use any programming language available
C. Open Source Modular architecture
D. Allows components to be plug-and-play
E. Makes mining cryptos more efficient

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Hyperledger is an open source collaborative effort created for open industrial blockchain development. It started in December 2015 by the Linux Foundation. Linux Foundation's objectives were to create an environment in which communities of software developers and companies meet and coordinate to build blockchain frameworks.

QUESTION 59
In Hyperledger, nodes need a _____ to be able to communicate to the network.

A. Valid Certificate
B. Valid License
C. Valid YAML file D. Valid JSON file

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Hyperledger, nodes need a valid certificate to be able to communicate to the network and the participants use applications that connect to the network by way of the nodes.

QUESTION 60
What component on the blockchain maintains the "world state"?

A. .acl
B. Reputation Manager
C. Distributed Ledger
D. .bna

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Distributed Ledger manages the world state and the transaction log in the blockchain. The world state is defined as the state of all transactions on the Blockchain, where all nodes agree that all blocks on the Blockchain are at the same state. It implements three key attributes. It efficiently calculates the cryptographic hash of the entire dataset of each block. It efficiently transmits a minimal “delta” changes to the dataset, when a peer is out of sync and needs to “catch up”. It minimizes the amount of stored data required for each peer to operate.

QUESTION 61
When developing in Ethereum which is considered to be an In-Memory Blockchain simulations for rapid development?

A. Cpp-ethereum
B. Geth

C. TestRPC
D. Parity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are several redundant implementations of the Ethereum protocol to ensure the correctness of the implementation. Additionally, not all blockchain nodes operate the same way. Some are purely for developing and hold a blockchain in-memory and just simulate the mining. Real Blockchain Nodes: 1. Cpp-ethereum 2. Go-Etheruem (GETH) 3. Parity In-Memory Blockchain simulations for rapid development: 1. TestRPC 2. Ganache 3. Truffle Developer Console Clients to access the blockchain in a convenient way: 1. MetaMask browser Plugin through Infura 2. Status.IM Android/iOS app through Infura 3. MIST DApp Browser with integrated
GETH

QUESTION 62
Ethereum smart contracts can be written in what programming languages? Select all that apply.

A. Serpant
B. Cobol
C. LLL
D. LLC
E. Vyper
F. Node.js
G. IOS
H. Mutan
I. Solidity

Correct Answer: ACHI
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Ethereum Smart Contracts run on compiled bytecode, which means that there can be several high-level languages which code can be written in. In particular, Ethereum has a number of languages available: 1. Solidity – the most popular language now (2018). 2. Vyper – A Language by Vitalik Buterin with an emphasis on security 3. LLL – "Low Level Lisp-like Language" 4. Mutan – Golang-like, deprecated in 2015 5. Serpent, Python-like, but seems to be no longer maintained 6. Bamboo

QUESTION 63
Which is the right order for Ethereum Denominations?

A. Finney, Szabo, Mether, Wei
B. Gwei, Szabo, Finney, Ether
C. Finney, Szabo, Mether, Gwei
D. Wei, Finney, Szabo, Ether, Tether

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Most widely used are Wei, Gwei, Finney and Ether. With the tool https://etherconverter.online/ you can easily convert different units.

QUESTION 64
What is the nonce-field in a transaction?

A. To sum up all ethers sent from that address
B. Protects against replay attacks
C. To distribute the workloads in the EVM
D. Adds a checksum for transactions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you send off a transaction, then several fields have to be set. These include: • nonce: It is a sequence number for the sending account which counteracts replay attacks • gasprice: price offered to pay per gas • startgas: upper limit for the gas consumption • to: destination address (EoA or contract address) • value: Ether to transfer • data: Data to transfer • v, r, s: ECDA signature.

QUESTION 65
Ethereum currently uses the _____Consensus Algo and in the future it is planned to go to the _____Consensus Algo?

A. PoW, DPoS
B. PoW, PoS
C. PoS, PoW
D. DPoS, PoW

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://coingape.com/ethereum-founder-vitalik-buterin-consensus-algorithm-fight-attacks/

QUESTION 66
In Ethereum how is the block difficulty determined in Ethereum?

A. The Block Difficulty increases when the time between mined blocks is below 10 seconds, while it decreases when the time is above 20 seconds.
B. The Block Difficulty is determined by the Ethereum Committee every fortnight to reflect the average amount of transaction and it cannot be influenced by the network itself.
C. The Block Difficulty increases when the time between mined blocks is below 20 seconds, while it decreases when the tie is above 60 seconds.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

At the time of writing these lines, the Ethereum Blockchain still runs on Proof of Work. When a block is mined, the miner node selects some transactions from a pool of pending transactions. Usually they are sorted by how much gas they would bring in. These transactions are executed and incorporated in the new block. But a block also contains two very important parameters: a difficulty and a timestamp. The difficulty regulates how hard it is to find a block by the miner. The mining time is set to be between 10 and 20 seconds. If it's beyond 20 seconds, the difficulty is too high and will be automatically lowered going forward. If the mining happens below 10 seconds, then the difficulty increases. The timestamp is the time when a miner found the block. It is not automatically derived, rather it is set by the miner itself and can thus be influenced to a certain degree. The timestamp does not depend on the time zone, as it's the standard Unix timestamp.

QUESTION 67
In regards to understanding the Ethereum Virtual Machine what statement is true?

A. The EVM is extremely powerful, non-turing complete and perfect for doing computational intensive thins, because of the direct access to the graphics card.
B. The EVM is extremely powerful, turing complete and perfect for doing computational intensive things, because of the direct access to the graphics card.
C. While the EVM is Sandboxed, it isn't as powerful as the Bitcoin network, because it's not Turing Complete
D. The EVM can't access hardware layers or anything outside a blockchain node because it's sandboxed.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:
The EVM is basically a sandboxed virtual machine running on every single node. It is Turing complete and a transaction-based state machine. The nodes reach consensus by executing all transactions. Only the miner node gets the block reward, all other nodes are just checking if the miner was "honest".

QUESTION 68
Blockchain provenance is defined as _____?

A. Information sent to the blockchain and written to the blockchain.
B. Recording the history of data, from its last block to various stages of the data lifecycle
C. Recording the history of data, from its inception to various stages of the data lifecycle.
D. Once a transaction has been written and committed to the ledger it cannot be changed.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Provenance means recording the history of data, from its inception to various stages of the data lifecycle. Provenance provides a detailed record of how the data was collected, where it was stored and how it is used. Blockchain holds complete provenance details of each component of data transfer. It is accessible to all the participants in a business network. It improves the system utilization and increases trust.

QUESTION 69
Smart Contracts provide all the following benefits EXCEPT?

A. Legally Enforcable
B. Autonomy
C. Cast Savings
D. Efficiency
E. Backup

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Smart contracts generally are not legal contracts. However, its possible that a smart contract could be accepted as a legal contract but not normally.

Reference: https://blockgeeks.com/guides/smart-contracts/

QUESTION 70
There are two types of tokens in blockchain solutions. (Select two.)

A. Legal
B. Utility
C. Equity
D. Financial

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
You are currently considering blockchain solutions for your organization. You read an article about "blockless" blockchains.

What are the two benefits that could be gained over a traditional blockchain solution? (Select two.)

A. Faster Block writes
B. Greater Transaction Security
C. Faster Performance
D. Greater transaction Capacity

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://solarmagazine.com/blockchain-trading-peer-to-peer-solar-energy-trading/

QUESTION 72
In blockchains there is the concept of "Group Consensus" and how many members must agree.

A. 52%
B. 74%
C. 75%
D. 51%
E. 100%

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of these reasons is a good reason to choose a conventional database over blockchain to store application data?

A. Centralization is to be avoided
B. Databases should never be used over blockchain

C. Full history is needed for all data
D. High performance is required

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following scenarios and databases is least suited to be utilized by a blockchain solution?

A. Scenario: Law enforcement system; Dataset: Criminal Arrests, Warrants for Arrest, Conviction Date
B. Scenario: An Email campaign service; Dataset: Recipient Email, From Email; Subject, Body
C. Scenario: A family filter wifi router; Dataset: Websites Visited, Websites Blocked, Download History
D. Scenario: Credit score app; Dataset: Credit Score, Hard Inquiries; Collections, Date Removed, Date Added

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Blockchain systems can offer what advantage over centralized systems?

A. They are much easier to maintain and update
B. They have significantly higher transaction speeds
C. Their distributed ledger systems are more secure and immutable
D. All of the above

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Blockchain systems assume all parties are trusted by all other parties in the exchange or ecosystem.

A. FALSE
B. TRUE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
All blockchain networks and systems require autonomous on-chain code in order to process transactions.

A. FALSE
B. TRUE
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
The first actual known blockchain software implementation and deployment occurred:

A. In 1991 by Stuart Haber
B. In 2011 Markus Persson
C. In 2009 by Satoshi Nakamoto
D. In 1991 by Linus Torvalds

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of these technical components best represents why cryptocurrency is able to operate successfully?

A. An immutable digital ledger that is validated and distributed across many peers
B. Using API calls, cryptocurrency having a direct correlation to USD exchange rates
C. High performance computing power allows cryptocurrency to be minted just as a central government might do with fiat currency
D. Blockchain cryptocurrency transactions are always public which generates user trust and adoption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Blockchains only work to store financial transactions or other exchanges of monetary value.
A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Adding more nodes to a blockchain network has which effect?

A. Increased centralization
B. Increased security
C. Decreased costs
D. Increased performance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of following scenarios and datasets would be best suited to be utilized by a blockchain solution?

A. Scenario: Online game, Dataset: Unique Items In Game, Battles Won, Quests Completed
B. Scenario: Mobile app for inspirational quotes; Dataset: First Name, Last Name, Quote of the Day
C. Scenario: Sales (CRM) website; Dataset: Hot Lead Count, Lead Score, Lead Fullname, Today's Tasks
D. All of the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://medium.com/crowdbotics/examples-of-blockchain-games-and-how-they-work-7fb0a1e76e2e

QUESTION 83
What does the acronym DAO represent?

A. Distributed Autonomous Operations
B. Distributed Anonymous Organization
C. Distributed Anonymous Operations
D. Decentralized Autonomous Organization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

QUESTION 84
Without 100% autonomy, blockchain software and networks would serve little purpose.

A. FALSE
B. TRUE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
The reason that cryptocurrencies such as Bitcoin, Ethereum and Litecoin can be exchanged one with another is due to the fact that they all operate on the same blockchain network

A. FALSE
B. TRUE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
The difference between a decentralized and a distributed system is?

A. A decentralized system is hosted across multiple datacenters
B. Distributed and decentralized are the same thing
C. A decentralized system is not wholly owned by a single entity
D. A distributed system is not wholly owned by a single entity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462

QUESTION 87
Pending transactions on the Ethereum blockchain are always ordered by highest fee paid to lowest, and then written to the block in that order.

A. FALSE
B. TRUE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which technical feature of blockchain best promotes the notion of a blockchain being “censorship resistant”?

A. An immutable ledger of transactions
B. Permissions-based transactions
C. Smart Contracts/transactional code that is executed “on chain”
D. Consensus systems through Proof of Work and Proof of Stake

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Consider the following scenario: Due to consistent inaccuracies and outdated real estate listings, a residential real estate company wants to build a blockchain solution that accurately depicts which homes (assets) are available for purchase across all countries/provinces. All available homes should be publicly viewable by the general consumer audience, but certain details of the home, such as history of maintenance, should only be viewable by licensed real estate professionals. Which architecture would best solve the product need?

A. Public data hosted on a public blockchain, Privileged data security hoisted on a private database
B. The entire solution built on a private blockchain with proper permissions for both public and privileged data
C. Public and privileged data on hybrid blockchain will Proof of Stake consensus
D. Public data hosted on a public blockchain; Privileged data hosted on a private blockchain

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
If a product's requirements call for public autonomous on-chain code, only using open source code, using cryptographic tokens, and allowing its users the ability to earn tokens, this product should be launched on the Ethereum blockchain.

A. FALSE
B. TRUE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 91
If a company desires to create a unique cryptocurrency and launch a new blockchain network to host it.

A. They must use ERC20 standard for the token, clone the Ethereum Virtual Machine, then launch a series of nodes
B. They must use ERC20 standard for the token and can use any open source blockchain tool/system to launch a series of nodes
C. They can both create their own cryptocurrency and launch their own blockchain network with any common open source blockchain tool/system
D. None of the above

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Consider the following scenario: A solo app developer wants to create their own cryptocurrency and build a blockchain based that allows users to buy and sell second-hand items with that cryptocurrency from each other. Before the transaction is considered complete, the purchaser must put the funds in an escrow service and the sender must enter the courier tracking number into that same escrow. Time is of the essence and this developer doesn't want to worry about networking of infrastructure. This app must be fully autonomous or "decentralized". Which architecture would best solve the product need?

A. Ethereum for token creation and escrow service; User-facing features built with web technologies and deployed through IPFS
B. Ethereum for token creation; Traditional multitier API and database for escrow service; User-facing features built in web technologies then minified unto a String and deployed to an Ethereum Smart Contract
C. Hyperledger Fabric for the escrow service and token creation using chaincode; User-facing features built with Hyperledger Composer
D. The product cannot be built. Fully decentralized apps are not yet possible for user interface

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A private blockchain like Hyperledger would be the right choice for which scenario:

A. An enterprise that needs to build a scalable, secure, permissioned blockchain application
B. A network of family members who want to share passwords and other secure information with one another
C. Developers who want to rapidly prototype public blockchain solutions
D. A startup that desires to build a token and blockchain application for their users
E. All of the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Consider the following scenario: A large department store chain is being pressured by lawmakers to provide evidence that proves the store's clothing is not produced through child labor. This is no easy task currently due to the store's clothing being transferred between at least 6 different parties in between creation and placement at the storefront. The store chain is considering the use of blockchain to solve their problem. Discretion in the reading and writing of transactions is highly important to the store chain to protect its proprietary interests. Which solution would best solve the product need?

A. Use a public blockchain that supports assets, then create a new clothing asset for each item created. When the clothing item is transferred to the next party in the process, require that the associated blockchain asset be transferred to the next party's blockchain account with relevant metadata. The lawmakers can now view the transactions and transfers at any time.

B. Use a permissioned blockchain to build the technology. Require every party involved in the process to host a node on you network. Create a new clothing asset for each item created. When the clothing item is transferred to the next party in the process, have the previous party use your web portal to initialize a chaincode Smart Contract to transfer control of the asset. When the next party receives the asset have them use your web portal to initialize a chaincode Smart Contracts to acknowledge receipt of the asset. Provide read-only permissions to the lawmakers so they can receive the evidence they are looking for. C. Both options are equally suitable

D. None of the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which one of the following is true concerning Hyperledger Fabric?

A. Cryptocurrency cannot be created or used
B. because it is permissioned, companies cannot launch products on it
C. Because it is permissioned, it is impossible to display data to the general public
D. None of the above

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which scenario would it be most appropriate for a blockchain solution to implement a Proof of Work or Proof of Stake consensus?

A. When the blockchain needs to be permissioned
B. When the aim of the blockchain is to be a trustless as possible
C. When the blockchain needs to support millions of transactions
D. All of the above

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
How are blocks of data “chained” together to ensure the integrity of transactions?

A. The hash of the previous block is written to the header of the current block
B. The ID of the previous block is stored in the current block
C. A public key is stored in each block for data decryption
D. The hash of the genesis block is kept in all block headers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 98
In public key cryptography, the public key is used to:

A. Sign/approve any transaction/action that might be made by the holder of the key pair
B. Verify the digital signature of a given key pair
C. Decrypt the private key so valid transactions/actions can be performed
D. Encrypt the private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/