EXIN Blockchain

FOUNDATION

Certified by
EXIN

Sample Exam

Edition 202001

Content

Introduction

This is the EXIN Blockchain Foundation (BLOCKCHAINF.EN) sample exam. The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is correct.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth 1 point. You need 26 points to pass the exam.

The time allowed for this exam is 60 minutes.

Good luck!

Sample Exam

1 / 40
What is an advantage of a public blockchain?

A) It does not use disinterested third parties to secure blocks, as all participants have a vested interest.
B) It is more resilient against fraud, because it uses federated nodes to combat fraud.
C) It is open to everyone in the world without permission and licensing requirements.
D) Its networks are built by for-profit companies and the working of the network is guaranteed.

2 / 40
What is a blockchain?

A) A centralized database that holds a subset of all transactions on all nodes.
B) A client-server database existing on a limited number of nodes at the same time.
C) A distributed database with a record of all transactions on the network.
D) A standalone database with history of all transactions on various nodes.

3 / 40
What is the function of a lightweight node within a blockchain network?

A) It stores a complete history of every transaction on the network.
B) It stores purchased cryptocurrency for users of a blockchain network.
C) It verifies transactions by piggybacking on the work of full nodes.

4 / 40
What is **not** a classification for a node?

A) Full node
B) Lightweight node
C) Merkle node
D) Miner node

5 / 40
A bearer instrument used to transfer value between two parties over a blockchain network.

What is this instrument?

A) A DApp
B) A hash
C) A node
D) A token

What is a **key** characteristic of a public blockchain?

A) Allowing a user to elect nodes to process transactions
B) Allowing anyone to participate in the blockchain network
C) Allowing control over who can participate and at what level
D) Allowing only trusted parties to operate their blockchain

What is an example of the use of cryptography in a blockchain?

A) Accessing private or hybrid blockchains by using a private key
B) Creating cryptocurrency as a reward for mining nodes
C) Keeping blockchains secure from 51% attacks by corrupt nodes
D) Securing transfers of cryptocurrency between recipients

How do blockchains use private and public-key cryptography?

A) Asymmetric encryption allows a sender to transfer cryptocurrency to a public key. The recipient can then access these funds with their private key and hold it in their wallet.
B) In public-key cryptography, one key is used to encrypt and decrypt transaction. The sender uses this key to send cryptocurrency and the recipient's wallet holds it after decryption.
C) Symmetric encryption allows a sender to transfer cryptocurrency to another user. The recipient can then access their funds when the sender grants access to their private key.
D) The algorithm in the blockchain encrypts and stores private and public keys to all user's wallets. Cryptocurrency then accesses their funds through their twenty-word passphrase key.

How do hybrid blockchain networks combat 51% attacks?

A) Through a central controller ensuring the security of each node in the network
B) Through a Proof of Work (PoW) algorithm, which allows miners to secure the network
C) Through incentivization, where miners receive currency for securing the network
D) Through Merkle tree roots, that allow the network to restore itself to its last valid block

How do blockchains function like ledgers?

A) They hold a record of all transactions that have ever occurred on a network.
B) They hold vast amounts of transaction data as a centralized database.
C) They periodically update all balances of each wallet to the blockchain.

11 / 40
What is the task of miners in a blockchain network?

A) Miners act as a single third party to aggregate records and provide trust in the network by the miners' authority.
B) Miners are computers that allow access to the blockchain, ensuring the number of corrupt nodes will stay low.
C) Miners are nodes that compete for a reward by calculating the correct nonce to make a transaction possible.
D) Miners determine the consensus rules that should be followed and interfere when these rules are broken.

12 / 40
Which description fits **only** the Proof of Work (PoW) consensus algorithm?

A) A collaborative consensus algorithm, where approved accounts do the validation.
B) A collaborative consensus algorithm that is facilitated by farmers, who offer leftover memory of their computer to make transactions possible.
C) A consensus algorithm, where the validation is done for the entire transaction flow, including not only the correctness, but also the sequence of transactions.
D) A low-cost and fast algorithm, where a node needs to deposit cryptocurrency to guarantee the transaction.
E) A noncompetitive consensus algorithm, where validation is done by elected nodes, which send cryptocurrency to an address, from which it cannot be retrieved.
F) An algorithm that involves collaborative validation, performed by validators, which are chosen outside of the consensus.
G) An algorithm that works in a trusted execution environment and proves the time when the transaction has taken place.
H) An intensive and expensive, competitive algorithm where each mining node on the blockchain is competing to secure blocks.

13 / 40
A competitive consensus algorithm that was developed because blockchains had difficulty meeting the transaction speed demands.

Which consensus algorithm is this?

A) Delegated Proof of Stake (DPoS)
B) Proof of Burn (PoB)
C) Proof of Stake (PoS)
D) Proof of Work (PoW)

14 / 40
Which consensus algorithm is the **least** energy efficient?

A) Delegated Proof of Stake (DPoS)
B) Proof of Authority (PoA)
C) Proof of Space (PoSpace)
D) Proof of Work (PoW)

15 / 40
What is an advantage of using the consensus algorithm Proof of Elapsed Time (PoET) instead of Proof of Work (PoW)?

A) PoET can often be used in a permissionless blockchain more easily than PoW, because PoET's lottery system for node selection is secure.
B) PoET has generally lower transaction costs than PoW, because the hardware needed is more generic than the hardware needed for PoW.
C) PoET is much more secure than PoW, because PoET supports the trusted execution environment (TEE) by time-stamping the transactions.
D) PoET is usually faster than PoW, because fewer nodes compete for validation than in PoW, since PoET randomly selects the nodes.

16 / 40
An attacker tries to corrupt the transaction history of a blockchain to be able to spend a token or a cryptocurrency twice.

What is the **most** likely thing this attacker did?

A) The attacker changed the transaction on his node and propagated it in the network.
B) The attacker edited the smart contract and recovered investor's cryptocurrency.
C) The attacker gained control of more than 51% of the network's computing power.
D) The attacker hard-forked the network and created a new blockchain network.

17 / 40
Blockchain networks are vulnerable to 51% attacks.

Which network would incentivize hackers **most** to break the network?

A) Bitcoin
B) Fabric
C) Factom
D) Ripple

One of the greatest threats to the blockchain community is the narcissism of small differences.

What is the result of this narcissism of small differences?

A) One community group makes fun of another community group over small things, resulting in greater collaboration.
B) The community cares about and works to resolve small differences that cannot be perceived by outside groups.
C) The community has developed many similar projects and these fight with one another over small differences.
D) The community has grown closer and works together in a collaborative fashion to solve common problems.

How do fraudsters use a Ponzi scheme?

A) A fraudster convinces a victim to pay for receiving something of greater value later on.
B) A fraudster finds investors, then dumps the tokens of the investors to crash the market.
C) A fraudster pays dividends to initial investors using the funds of subsequent investors.
D) A fraudster steals credit cards and uses them to buy money, goods or property.

Which characteristic of a blockchain network is also its protection?

A) The greater the number of full independent nodes, the harder it is to compromise the data in the blockchain.
B) The lower the number of miners in the blockchain, the higher the incentive is for securing the network.
C) The more centralized the control of the blockchain is, the harder it is to secure the data and avoid fraud.
D) The more complicated the Proof of Work (PoW) algorithm is, the more rewarding it is to secure the network.

How can information be secured in a blockchain?

A) By using a closed peer-to-peer (P2P) network, sharing information across platforms
B) By using a distribution of cryptocurrencies over miners through the network
C) By using asymmetric cryptography, consisting of a public and private key
D) By using distributed ledger technology (DLT), which records transactions at the source

22 / 40
In what way do blockchains use a public witness?

A) A digital courthouse or library acts as a public witness to store information to reference.
B) A node on a blockchain network attests to the accuracy and truthfulness of information.
C) A person sends a transaction over a public network to earn rewards as a public witness.
D) A preferred node can be elected to attest to the accuracy and truthfulness of information.

23 / 40
Blockchain enables self-sovereign identity.

How does blockchain do this?

A) It enables centralized third parties to offer easy-to-use and valid identity information.
B) It enables each person to have exclusive control of their money, property and identity.
C) It enables governments to effortlessly issue identities with advanced digital certificates.
D) It enables only internet companies to offer world-class secure personal identity repositories.

24 / 40
Public blockchains give an incentive to encourage users to mine blocks and secure the network.

What incentive is this?

A) Public blockchains allow users to create tokens to sell on secondary markets.
B) Public blockchains do not offer rewards, because they are open source.
C) Public blockchains offer cash rewards for running mining nodes.
D) Public blockchains offer rewards for mining in the form of cryptocurrency.

25 / 40
An organization wants to develop smart contracts, based on blockchain technology. The organization does not wish to burden employees with maintaining the security of the blockchain.

What blockchain technology fits the organization **best**?

A) A hybrid blockchain
B) A private blockchain
C) A public blockchain

26 / 40
What is a **key** characteristic of the Hyperledger network?

A) It is a public blockchain network and one of the oldest networks, existing since 2009.
B) It is private, open sourced and can run everyone's own distributed ledger technology (DLT).
C) It utilizes cryptocurrency as a reward mechanism, which makes the network more secure.
D) It utilizes the Proof of Stake (PoS) consensus algorithm as its main security measure.

27 / 40
What is the **best** use case for smart contracts?

A) Digitalize and automate legally binding contracts using artificial intelligence (AI)
B) Enforce the execution of contracts in the legal system using cryptocurrencies
C) Ensure automatic payments by predetermined actions or events in insurance contracts
D) Extend the Bitcoin blockchain, the best-known smart contract platform, to the judicial system

28 / 40
In which scenario is a smart contract the **best** solution to the problem?

A) A bartender wants to force customers to pay for their drinks by transferring cryptocurrency to his wallet.
B) A chief financial officer wants her smart watch to notify her when her partner enters their front door.
C) An energy company wants to automatically buy power when the price reaches a predetermined rate.
D) An insurance company wants to pay out a farmer whenever the case manager feels it is best to do so.

29 / 40
What are DApps designed to do?

A) Execute smart contracts with the business logic in the front-end of a standalone application
B) Manage cryptocurrencies only, without any embedded voting system for governance of the blockchain
C) Run applications on a peer-to-peer (P2P) network expanding smart contracts beyond simple value transfer
D) Support applications that run on multiple public cloud providers avoiding any vendor lock-in and fraud

30 / 40
What is the role of a DAO (decentralized autonomous organization)?

A) Address the principal-agent dilemma with collaboration and acceptance of actions within agreed rules
B) Embed regulated online smart contracts with the current judicial system, using public blockchains
C) Offer complex online smart contracts without any link to tangible and intangible offline assets
D) Provide a private blockchain contract platform on which users can run their online applications

31 / 40
How can blockchain technology **best** help securing identity data?

A) By eliminating third parties through providing secured-data storage at a user's server
B) By encoding all the health data and save it on a private and permissionless blockchain
C) By protecting data that has been submitted on the internet using a cryptographic algorithm
D) By providing information personal data without disclosing the actual data that proves it

32 / 40
What is the value of using blockchain networks with Internet of Things (IoT)?

A) Allowing blockchain users to follow self-driving cars and access these cars
B) Avoiding a spoofing attack using the secured identity that is stored on a blockchain
C) Enabling software that programs itself to solve problems without human intervention
D) Solving expensive and complex calculations using Hyperledger Fabric mining

33 / 40
Blockchain technology has made decentralized marketplaces possible.

What is a benefit of a decentralized marketplace?

A) It is based on open-source technology, so it can be used without any investment
B) It is not under a paid license to operate and therefore it is managed better
C) It is relatively cheap due to the use of cryptocurrency and is very accessible
D) It is tamper-proof, resilient to being shut down and trustworthy due to smart contracts

34 / 40
How does blockchain improve supply chains?

A) By automatically creating trade agreements between two parties
B) By creating safe centralized marketplaces to trade goods on
C) By stabilizing the national currencies of the countries involved
D) By transferring tokenized ownership through a software system

35 / 40
The Monetary Authority of Singapore (MAS) and blockchain company R3 partnered together.

What did they achieve together?

A) The creation of smart contracts and stable coins
B) The facilitation of interbank transmission of messages
C) The first interbank payments without limitations of time zones
D) The launch of wire transfers using cryptography

36 / 40
What is digital fiat currency?

A) A digital form of currency, that represents a country's financial reserves
B) An e-currency, that creates a transparent and borderless debt market
C) An online system, that enables making transactions without a bank account

37 / 40
How does blockchain technology benefit the insurance industry?

A) By avoiding compliance requirements of national authorities, which reduces overhead
B) By ensuring accuracy of data and automating micro insurances, which reduces costs
C) By introducing flexible premiums to be paid by customers, which increases profits
D) By setting up a digital mode of payment, which simplifies claims settlement

38 / 40
How does blockchain technology help to protect intellectual property rights (IP)?

A) It allows a user to include IP transactions in smart contracts.
B) It allows a user to record an event and establish the timeline.
C) It allows a user to record the creation of software packages.
D) It allows a user to send a transaction and receive IP ownership.

39 / 40
What is an example of how a government is actively promoting the use of blockchain?

A) China has created a regulatory sandbox that allows them to closely monitor the experiments in blockchain mining and create their own cryptocurrency.
B) Estonia offers e-Residency software, which is available to anyone in the world interested in operating a business online and from within the European Union.
C) Singapore's Monetary Authority (MAS) is creating central bank digital money for payments between banks using distributed ledger technology (DLT).

40 / 40
Why is blockchain described as the technology that adds a layer of trust to the internet?

A) It allows individuals and groups to work together without having to trust each other or establish authority.
B) It creates a dedicated virtual private network (VPN) tunnel between two or more parties to carry out online fund transfers.
C) It provides mechanism for the government to create their own digital fiat currency as a replacement of physical currency.
D) It provides multifactor authentication to create and update records of cryptocurrency transactions securely.

Answer Key

1 / 40
What is an advantage of a public blockchain?

A) It does not use disinterested third parties to secure blocks, as all participants have a vested interest.
B) It is more resilient against fraud, because it uses federated nodes to combat fraud.
C) It is open to everyone in the world without permission and licensing requirements.
D) Its networks are built by for-profit companies and the working of the network is guaranteed.

A) Incorrect. This is an advantage of permissioned blockchain nodes. Permissioned blockchain nodes are private networks that use some blockchain technology but not all. Most do not incorporate mining and do not have a native cryptocurrency. Thus, there are no disinterested third parties. The blocks and transactions are processed by known participants.
B) Incorrect. Federated nodes can exist in both public and private blockchains. Public blockchains can also exist without federation. Federation is when the system, or rather the user of a system, elects nodes to process transactions.
C) Correct. This is an advantage of public blockchains. Public blockchains are open to anyone in the world to participate in the functions of the network, only limited by their access to the internet, hardware, and electricity. (Literature: A, Chapter 1.1)
D) Incorrect. Public blockchains are by definition held in an open license such as the Apache or MIT license. There are no gating mechanisms, no one to ask permission and no licensing fee.

2 / 40
What is a blockchain?

A) A centralized database that holds a subset of all transactions on all nodes.
B) A client-server database existing on a limited number of nodes at the same time.
C) A distributed database with a record of all transactions on the network.
D) A standalone database with history of all transactions on various nodes.

A) Incorrect. Blockchain is a decentralized, peer-to-peer (P2P) distributed database where every node holds record of all transactions.
B) Incorrect. Blockchain consists of P2P distributed databases.
C) Correct. It is a P2P distributed time-stamped database that holds a record of all transactions that have ever occurred on the network. (Literature: A, Chapter 1.1)
D) Incorrect. Blockchain is a decentralized, P2P distributed database with history of all transactions.

3 / 40

What is the function of a lightweight node within a blockchain network?

A) It stores a complete history of every transaction on the network.
B) It stores purchased cryptocurrency for users of a blockchain network.
C) It verifies transactions by piggybacking on the work of full nodes.

A) Incorrect. A node does not necessarily store a complete history of every transaction on the network. That is only true for a full node.
B) Incorrect. A node does not store cryptocurrency itself, but it stores blocks that contain a record of all transactions.
C) Correct. Lightweight nodes verify transactions by piggybacking on the work of full nodes. (Literature: A, Chapter 1.1)

4 / 40

What is **not** a classification for a node?

A) Full node
B) Lightweight node
C) Merkle node
D) Miner node

A) Incorrect. Full nodes need all new transaction records. They keep all block headers. Block headers identify a unique block and contain a hash of the previous block. All this data adds up and takes up a lot of room.
B) Incorrect. Lightweight nodes verify transactions by piggybacking on the work of full nodes. They only download the headers of all blocks and then check transactions utilizing a system called simplified payment verification (SPV).
C) Correct. Merkle tree root is not a node classification. It is a hash that allows a hybrid blockchain to restore itself to its last known valid block in case its network is attacked. (Literature: A, Chapter 1.1)
D) Incorrect. A miner is a type of node that is adding transactions to new blocks. Miners compete to win the right to create a new complete block by solving a complex mathematical problem. Each miner will write their answer in the block header and if they are correct, they are then rewarded with cryptocurrency.

A bearer instrument used to transfer value between two parties over a blockchain network.

What is this instrument?

A) A DApp
B) A hash
C) A node
D) A token

A) Incorrect. DApps are applications that run on a peer-to-peer (P2P) network instead of a single system. DApps are built with smart contracts but use other services such as secure messaging and often allow an unlimited number of participants to interact within a given rule set.
B) Incorrect. A hash function is used to secure all the data in a block of transactions. A hash is the output of this mathematical process that creates a string of numbers and letters of a fixed size.
C) Incorrect. A node is a computer that is connected to a blockchain network. It runs the software for the network and keeps the network healthy by transferring information across the network to other nodes.
D) Correct. A token is a bearer instrument used to transfer value between two parties over a blockchain network. (Literature: A, Chapter 1.1)

What is a **key** characteristic of a public blockchain?

A) Allowing a user to elect nodes to process transactions
B) Allowing anyone to participate in the blockchain network
C) Allowing control over who can participate and at what level
D) Allowing only trusted parties to operate their blockchain

A) Incorrect. Federated blockchain nodes can exist in both public blockchains and private blockchains. Federation is when the system, or rather the user of a system, elects nodes to process transactions.
B) Correct. Public blockchains allow anyone to participate in the network as long as they have access to the internet, hardware and electricity. (Literature: A, Chapter 1.1)
C) Incorrect. Hybrid blockchains control who can participate and at what level of participation each node is allowed to operate.
D) Incorrect. Private blockchains only allow trusted parties to operate their blockchain.

What is an example of the use of cryptography in a blockchain?

A) Accessing private or hybrid blockchains by using a private key
B) Creating cryptocurrency as a reward for mining nodes
C) Keeping blockchains secure from 51% attacks by corrupt nodes
D) Securing transfers of cryptocurrency between recipients

A) Incorrect. Cryptography is not used to enter hybrid or private blockchains, even if they use private and public keys.
B) Incorrect. Some blockchain networks reward mining nodes with cryptocurrency. However, this is not what cryptography does.
C) Incorrect. Cryptography helps secure blockchains, but not necessarily against a 51% attack.
D) Correct. The asymmetric encryption blockchain technology uses, allows a sender to transfer cryptocurrency to the recipient without someone else being able to steal it. (Literature: A, Chapter 2.1)

How do blockchains use private and public-key cryptography?

A) Asymmetric encryption allows a sender to transfer cryptocurrency to a public key. The recipient can then access these funds with their private key and hold it in their wallet.
B) In public-key cryptography, one key is used to encrypt and decrypt transaction. The sender uses this key to send cryptocurrency and the recipient's wallet holds it after decryption.
C) Symmetric encryption allows a sender to transfer cryptocurrency to another user. The recipient can then access their funds when the sender grants access to their private key.
D) The algorithm in the blockchain encrypts and stores private and public keys to all user's wallets. Cryptocurrency then accesses their funds through their twenty-word passphrase key.

A) Correct. Asymmetric cryptography allows anyone to encrypt a message using the recipient's public key, whilst the encrypted message can only be read using the recipient's private key. Asymmetric encryption allows a sender to transfer cryptocurrency to the recipient without someone else being able to steal it. It allows them to do this without having met or exchanged information. As long as the sender has the public key of the recipient, they can send them cryptocurrency. (Literature: A, Chapter 2)
B) Incorrect. Public-key cryptography uses two keys, a public and a private key. Users that wish to send cryptocurrency to a new address would sign the transaction with their private key and then send it to the public key, known as the address. The recipient would then use their private keys to access the funds.
C) Incorrect. Blockchains do not use this type of encryption as there is only one key with this type of encryption and the users will have to meet to exchange information.
D) Incorrect. Blockchains only have the public address for cryptocurrency. The private key is held securely by the owner. Passphrases can be used to recover private keys if they are lost.

9 / 40

How do hybrid blockchain networks combat 51% attacks?

A) Through a central controller ensuring the security of each node in the network
B) Through a Proof of Work (PoW) algorithm, which allows miners to secure the network
C) Through incentivization, where miners receive currency for securing the network
D) Through Merkle tree roots, that allow the network to restore itself to its last valid block

A) Incorrect. Merkle Tree roots are a way to secure hybrid networks. Hybrid blockchains do not go through a central controller.
B) Incorrect. Encryption is a generic security functionality of any kind of blockchain and is not specific to hybrid networks.
C) Incorrect. An incentivization mechanism works well for public blockchains, but not for hybrid blockchains.
D) Correct. Hybrid blockchain networks are secured through Merkle tree root hashes, which allow the network to restore itself to its last known valid block in case of corruption. (Literature: A, Chapter 1.1)

10 / 40

How do blockchains function like ledgers?

A) They hold a record of all transactions that have ever occurred on a network.
B) They hold vast amounts of transaction data as a centralized database.
C) They periodically update all balances of each wallet to the blockchain.

A) Correct. Blockchains are widely distributed public accounts that let anyone see who has what cryptocurrency and the full history of that coin over time. Every transaction can be found as well as the parties involved in these transactions. (Literature: A, Chapter 2.1)
B) Incorrect. Blockchain are widely distributed ledgers that hold a limited amount of transaction data. The size limit is restricted because they are distributed, and it is impractical to share and reconcile vast quantities of data.
C) Incorrect. Wallets do not keep a private ledger. They pull in balance data from a blockchain.

What is the task of miners in a blockchain network?

A) Miners act as a single third party to aggregate records and provide trust in the network by the miners' authority.
B) Miners are computers that allow access to the blockchain, ensuring the number of corrupt nodes will stay low.
C) Miners are nodes that compete for a reward by calculating the correct nonce to make a transaction possible.
D) Miners determine the consensus rules that should be followed and interfere when these rules are broken.

A) Incorrect. Needing a single third party was exactly what Satoshi wanted to avoid by introducing blockchain technology.
B) Incorrect. Miners are not responsible for access to the blockchain.
C) Correct. Miners compete for a reward by trying to calculate the nonce. (Literature: A, Chapter 1.1)
D) Incorrect. Miners do not determine the rules in blockchain. Miners operate in the playing field determined by the rules.

12 / 40
Which description fits **only** the Proof of Work (PoW) consensus algorithm?

A) A collaborative consensus algorithm, where approved accounts do the validation.
B) A collaborative consensus algorithm that is facilitated by farmers, who offer leftover memory of their computer to make transactions possible.
C) A consensus algorithm, where the validation is done for the entire transaction flow, including not only the correctness, but also the sequence of transactions.
D) A low-cost and fast algorithm, where a node needs to deposit cryptocurrency to guarantee the transaction.
E) A noncompetitive consensus algorithm, where validation is done by elected nodes, which send cryptocurrency to an address, from which it cannot be retrieved.
F) An algorithm that involves collaborative validation, performed by validators, which are chosen outside of the consensus.
G) An algorithm that works in a trusted execution environment and proves the time when the transaction has taken place.
H) An intensive and expensive, competitive algorithm where each mining node on the blockchain is competing to secure blocks.

A) Incorrect. This is the definition of Proof of Authority (PoA).
B) Incorrect. This is the definition of Proof of Capacity (PoC) and Proof of Space (PoSpace).
C) Incorrect. This is the definition of Hyperledger Fabric.
D) Incorrect. This is the definition of Proof of Stake (PoS).
E) Incorrect. This is the definition of Proof of Burn (PoB).
F) Incorrect. This is the definition of Delegated Proof of Stake (DPoS).
G) Incorrect. This is the definition of Proof of Elapsed Time (PoET).
H) Correct. This is the definition of PoW. (Literature: A, Chapter 3.1)

13 / 40

A competitive consensus algorithm that was developed because blockchains had difficulty meeting the transaction speed demands.

Which consensus algorithm is this?

A) Delegated Proof of Stake (DPoS)
B) Proof of Burn (PoB)
C) Proof of Stake (PoS)
D) Proof of Work (PoW)

A) Incorrect. DPoS is a collaborative effort. Nodes that are validating transactions are rewarded equally. Stakeholders elect witnesses who will validate transactions and create blocks for the network.
B) Incorrect. PoB is a noncompetitive consensus algorithm.
C) Correct. PoS is a competitive consensus algorithm. It was created as an alternative to the PoW because blockchains had difficulty meeting the transaction speed demands. PoS nodes do not mine cryptocurrency. Users can put some of their cryptocurrency, from a blockchain, in a retainer. This retainer allows the user to "stake" that they will process transactions honestly and by the rules of the consensus system. If the user fails to do so, they will forfeit their cryptocurrency. (Literature: A, Chapter 3.2)
D) Incorrect. PoW is a competitive consensus algorithm where each mining node on the blockchain is competing to secure blocks. It allows anyone to participate at any level in the creation and maintenance of the system but is very competitive. Nodes that hope to be competitive and be rewarded with cryptocurrency will need to operate specialized equipment. PoS was created as an alternative to the PoW that required high transaction speed demands.

14 / 40

Which consensus algorithm is the **least** energy efficient?

A) Delegated Proof of Stake (DPoS)
B) Proof of Authority (PoA)
C) Proof of Space (PoSpace)
D) Proof of Work (PoW)

A) Incorrect. Delegated Proof of Stake (DPoS) is a collaborative effort, and nodes that are validating transactions are rewarded equally in this consensus system. It is energy efficient and does not burn electricity when mining.
B) Incorrect. Proof of Authority (PoA) blockchains have a collaborative consensus algorithm. In this system, transactions and blocks are validated by approved accounts. The validator nodes run consensus software, allowing them to put transactions in blocks. Because of the limited number of validators, it is energy efficient.
C) Incorrect. Instead of using processing power to compete to secure the blockchain, it uses leftover memory. Proof of Space (PoSpace) blockchains may be a fairer and greener alternative to other blockchains. They can be used to build applications and transfer value.
D) Correct. This algorithm is, by design, energy intensive and expensive. The expense and difficulty of obtaining bitcoins was an intentional part of the token economics. Much like mining gold, it is not cheap nor easy to mine, and the difficulty and scarcity of bitcoins is thought to drive part of the value of the asset. (Literature: A, Chapter 3.1)

What is an advantage of using the consensus algorithm Proof of Elapsed Time (PoET) instead of Proof of Work (PoW)?

A) PoET can often be used in a permissionless blockchain more easily than PoW, because PoET's lottery system for node selection is secure.
B) PoET has generally lower transaction costs than PoW, because the hardware needed is more generic than the hardware needed for PoW.
C) PoET is much more secure than PoW, because PoET supports the trusted execution environment (TEE) by time-stamping the transactions.
D) PoET is usually faster than PoW, because fewer nodes compete for validation than in PoW, since PoET randomly selects the nodes.

A) Incorrect. PoET is used mostly in a permissioned network as the nodes need to identify themselves. Furthermore, PoET's lottery system has security issues.
B) Incorrect. POeT does have lower transaction costs, but the cause is not generic hardware as PoET needs specific hardware.
C) Incorrect. PoET is not more secure than PoW and even if it were, it would have nothing to do with time stamping as this mechanism only works in an environment where the nodes are known.
D) Correct. The lower number of competing nodes makes PoET faster. (Literature: A, Chapter 3.1 and 3.5)

An attacker tries to corrupt the transaction history of a blockchain to be able to spend a token or a cryptocurrency twice.

What is the **most** likely thing this attacker did?

A) The attacker changed the transaction on his node and propagated it in the network.
B) The attacker edited the smart contract and recovered investor's cryptocurrency.
C) The attacker gained control of more than 51% of the network's computing power.
D) The attacker hard-forked the network and created a new blockchain network.

A) Incorrect. Other nodes will not accept this transaction because it would create a sidechain that is shorter than the existing chain. The attacker does not have enough mining power with one node to get enough mining power to create a longer chain.
B) Incorrect. It is not likely that a smart contract was hacked, because the attacker tries to spend tokens twice.
C) Correct. This is what happened in an attack to the Ethereum Classic network. The attacker was a bad miner and rolled back the history of transactions. The attacker did this by gaining control of more than 51% of the network's computing power (51% attack). (Literature: A, Chapter 10.1)
D) Incorrect. No hard-forking of the network took place, because there was no radical modification to the network's protocol.

Blockchain networks are vulnerable to 51% attacks.

Which network would incentivize hackers **most** to break the network?

A) Bitcoin
B) Fabric
C) Factom
D) Ripple

A) Correct. Miners must use their computing power and electricity to generate new cryptocurrency like bitcoins. If a network becomes too concentrated, criminal miners can corrupt the network with impunity. This particular type of vulnerability is called a 51% attack. 51% is the number that creates a tipping point for many blockchains. If fewer nodes are independent, a network will be rolled back. (Literature: A, Chapter 10.1)

B) Incorrect. Hyperledger's Fabric does not have cryptocurrency. With little to steal, hackers are less incentivized to break the network.

C) Incorrect. Factom does not use mining but has a native cryptocurrency Factoids. The federated nodes are rewarded with Factoids. The nodes can sell Factoids back into the market to those who wish to use the Factom blockchain. An anchoring technique is used to take a snapshot of this blockchain in the form of a hash and every ten minutes store in large networks such as bitcoin. If an attacker takes control of 51% of the network, he cannot change the history. This attack would be detected and the blockchain could be forked by the 49% to regain control.

D) Incorrect. Unlike bitcoin, that does not require users to trust or know other individuals on the network, the whole infrastructure of Ripple requires that all parties trust and know one another to some extent. A financial participant must trust the issuers of assets it holds, and a node operator must trust that the other nodes in its validator list will not collude to block valid transactions from being confirmed. Since trust and aligned incentives for cooperation are built in, this network is less likely to suffer a 51% attack.

18 / 40

One of the greatest threats to the blockchain community is the narcissism of small differences.

What is the result of this narcissism of small differences?

A) One community group makes fun of another community group over small things, resulting in greater collaboration.
B) The community cares about and works to resolve small differences that cannot be perceived by outside groups.
C) The community has developed many similar projects and these fight with one another over small differences.
D) The community has grown closer and works together in a collaborative fashion to solve common problems.

A) Incorrect. There is no collaboration. The rifts in the communities go all the way down to the code and this has divided the community repeatedly.
B) Incorrect. The communities are more likely to ridicule and mock one another and become hypersensitive to small things.
C) Correct. Communities with adjoining territories and close relationships are more likely to fight. (Literature: A, Chapter 10.2)
D) Incorrect. The opposite happens. Communities are more likely to ridicule and mock one another than collaborate.

19 / 40

How do fraudsters use a Ponzi scheme?

A) A fraudster convinces a victim to pay for receiving something of greater value later on.
B) A fraudster finds investors, then dumps the tokens of the investors to crash the market.
C) A fraudster pays dividends to initial investors using the funds of subsequent investors.
D) A fraudster steals credit cards and uses them to buy money, goods or property.

A) Incorrect. This is an advance fee scheme scam.
B) Incorrect. This is a market manipulation scam.
C) Correct. In old-school Ponzi schemes, the fraudster pays dividends to initial investors using the funds of subsequent investors. (Literature: A, Chapter 10.3)
D) Incorrect. This is an identity theft and credit card fraud scam.

20 / 40
Which characteristic of a blockchain network is also its protection?

A) The greater the number of full independent nodes, the harder it is to compromise the data in the blockchain.
B) The lower the number of miners in the blockchain, the higher the incentive is for securing the network.
C) The more centralized the control of the blockchain is, the harder it is to secure the data and avoid fraud.
D) The more complicated the Proof of Work (PoW) algorithm is, the more rewarding it is to secure the network.

A) Correct. Distribution is one of the main security safeguards in a blockchain. (Literature: A, Chapter 1.1)
B) Incorrect. The incentive for miners is not the security of the blockchain.
C) Incorrect. A central controller can create more security of the blockchain by working with only trusted nodes.
D) Incorrect. PoW complexity does not contribute to security of the blockchain.

21 / 40
How can information be secured in a blockchain?

A) By using a closed peer-to-peer (P2P) network, sharing information across platforms
B) By using a distribution of cryptocurrencies over miners through the network
C) By using asymmetric cryptography, consisting of a public and private key
D) By using distributed ledger technology (DLT), which records transactions at the source

A) Incorrect. P2P is the type of network being used, it is not a security measure in itself.
B) Incorrect. Cryptocurrency is the value that is being exchanged, it is not a security tool.
C) Correct. Asymmetric cryptography allows anyone to encrypt a message using a public key, whilst the encrypted message can only be read with the correct private key. (Literature: A, Chapter 2.1)
D) Incorrect. DLT is the overall technology of blockchain, it is not a security measure in itself.

22 / 40
In what way do blockchains use a public witness?

A) A digital courthouse or library acts as a public witness to store information to reference.
B) A node on a blockchain network attests to the accuracy and truthfulness of information.
C) A person sends a transaction over a public network to earn rewards as a public witness.
D) A preferred node can be elected to attest to the accuracy and truthfulness of information.

A) Incorrect. Blockchains are in essence a digital archive, but they do not need a separate digital courthouse or library to act as a public witness. That is what the nodes do.
B) Correct. Each node on a blockchain network witnesses information. All nodes attest to its accuracy and truthfulness at a later date, much like how court houses, libraries and archives are places where people store information to reference at another point in time. (Literature: A, Chapter 2.4)
C) Incorrect. Nodes act as public witnesses, not persons. The nodes do not always earn rewards to act as a public witness.
D) Incorrect. Each node on a blockchain network is witnessing information, not just preferred nodes.

23 / 40
Blockchain enables self-sovereign identity.

How does blockchain do this?

A) It enables centralized third parties to offer easy-to-use and valid identity information.
B) It enables each person to have exclusive control of their money, property and identity.
C) It enables governments to effortlessly issue identities with advanced digital certificates.
D) It enables only internet companies to offer world-class secure personal identity repositories.

A) Incorrect. Centralized systems can be compromised, and documents can be faked or changed, making it difficult to verify identities. Facebook hit the news headlines in 2018 after it shared the personal data of more than 87 million customers with Cambridge Analytica, which is a third party. That information was then used to manipulate individual's behavior. Convenience and ease of use has compromised many people's identities and financial information.
B) Correct. Blockchain technology has allowed for a shift in the concepts of self-ownership. It has sparked new life into social movements around the moral and natural rights of each person to have exclusive control of their money, property, and identity. (Literature: A, Chapter 6.1)
C) Incorrect. A self-sovereign identity is one that is managed by an individual and not a third party. A person would authenticate herself and not rely on a third party to validate and corroborate her credentials.
D) Incorrect. There is only a small group of companies that have control over issuing website security certificates and curating and cultivating online identities. This centralization has caused huge volumes of personal data to be housed on centralized servers for everyone who uses the internet. These servers can and do get hacked.

24 / 40
Public blockchains give an incentive to encourage users to mine blocks and secure the network.

What incentive is this?

A) Public blockchains allow users to create tokens to sell on secondary markets.
B) Public blockchains do not offer rewards, because they are open source.
C) Public blockchains offer cash rewards for running mining nodes.
D) Public blockchains offer rewards for mining in the form of cryptocurrency.

A) Incorrect. Usually, miners earn cryptocurrency directly.
B) Incorrect. Even though they are based on an open license and are open source, the public blockchains still offer rewards for mining.
C) Incorrect. Miners are given cryptocurrency, not regular currency.
D) Correct. Public blockchains usually give cryptocurrency as a reward for mining. (Literature: A, Chapter 1.1)

An organization wants to develop smart contracts, based on blockchain technology. The organization does not wish to burden employees with maintaining the security of the blockchain.

What blockchain technology fits the organization **best**?

A) A hybrid blockchain
B) A private blockchain
C) A public blockchain

A) Incorrect. For a hybrid blockchain the level of participation of each node can be controlled. If the organizations do not wish to use its employees to secure the blockchain, this is not the best option.
B) Incorrect. Private blockchains are more like trust networks. The members of the network are known, and contracts can be changed. They offer improvements compared to paper-based business processes, but they do not have the same finality or enforceability as public networks.
C) Correct. A public blockchain minimizes the possibility to change the smart contracts in the blockchain. The security of a public blockchain does not rely on a small number of employees and therefore fits with the organization's wish. (Literature: A, Chapter 1 and 10.1)

26 / 40
What is a **key** characteristic of the Hyperledger network?

A) It is a public blockchain network and one of the oldest networks, existing since 2009.
B) It is private, open sourced and can run everyone's own distributed ledger technology (DLT).
C) It utilizes cryptocurrency as a reward mechanism, which makes the network more secure.
D) It utilizes the Proof of Stake (PoS) consensus algorithm as its main security measure.

A) Incorrect. Hyperledger is not a public blockchain network and it was set-up in 2015 by Linux foundation.
B) Correct. Hyperledger is a private but open-sourced network and therefore helps people to spin up their own DLT. (Literature: A, Chapter 4.4)
C) Incorrect. Hyperledger does not utilize the cryptocurrency mechanism as rewards and for security.
D) Incorrect. Hyperledger does not use the PoS consensus algorithm.

What is the **best** use case for smart contracts?

A) Digitalize and automate legally binding contracts using artificial intelligence (AI)
B) Enforce the execution of contracts in the legal system using cryptocurrencies
C) Ensure automatic payments by predetermined actions or events in insurance contracts
D) Extend the Bitcoin blockchain, the best-known smart contract platform, to the judicial system

A) Incorrect. Smart contracts are created by developers and enforced with Boolean logic, mathematics, and encryption. A legally binding contract, on the other hand, is created by a lawyer and enforced by a judicial system. Most smart contracts are not legally binding. AI and smart contracts might be used together, but this is not the best use case.
B) Incorrect. Legal contracts are enforced by a judicial system; they do not have the same limitations as smart contracts. If a court order to pay somebody is violated, even in a civil lawsuit, it is possible to be charged with contempt and go to prison, or funds can be automatically withdrawn from an account. Laws are more flexible, and software is more rigid. Laws and contracts are interpreted by people who have legal options. Code is usually only interpreted one way, and if it executes unexpectedly it means there is a bug that needs to be fixed.
C) Correct. A farming smart contract can ensure insurance payments are made automatically. If the temperature goes down and damages crops, the farmer will receive payment. (Literature: A, Chapter 5.1)
D) Incorrect. The Bitcoin blockchain is less known for smart contracts, but the white paper that originally proposed the Bitcoin network alluded to their creation. Smart contracts on Bitcoin use what is known as "opcode", which was introduced by Peter Todd as Bitcoin Improvement Proposal (BIP) 65.

In which scenario is a smart contract the **best** solution to the problem?

A) A bartender wants to force customers to pay for their drinks by transferring cryptocurrency to his wallet.
B) A chief financial officer wants her smart watch to notify her when her partner enters their front door.
C) An energy company wants to automatically buy power when the price reaches a predetermined rate.
D) An insurance company wants to pay out a farmer whenever the case manager feels it is best to do so.

A) Incorrect. This is not a scenario in which a smart contract would be useful. Smart contracts do not force another party to release funds.
B) Incorrect. A smart contract is a contract between two or more parties. In this scenario, there is no second party and therefore a smart contract is not the best solution for this.
C) Correct. This is a good example of a smart contract being useful. (Literature: A, Chapter 5.1)
D) Incorrect. Smart contracts get triggered by predetermined events. The willingness of a company to pay is not an optimal way to use a smart contract, because this does not automatically trigger the code.

What are DApps designed to do?

A) Execute smart contracts with the business logic in the front-end of a standalone application
B) Manage cryptocurrencies only, without any embedded voting system for governance of the blockchain
C) Run applications on a peer-to-peer (P2P) network expanding smart contracts beyond simple value transfer
D) Support applications that run on multiple public cloud providers avoiding any vendor lock-in and fraud

A) Incorrect. Smart contracts are the backend and often only make up a small part of a DApp.
B) Incorrect. DApps are divided into three broad categories based on their function: 1) DApps that manage money; 2) DApps that utilize money but are built for another purpose, such as a game; 3) Apps for governance, such as a voting system. These governance applications are called "decentralized autonomous organizations" which is normally just shortened to DAOs.
C) Correct. DApps expand smart contracts beyond simple A-to-B value transfers. DApps are built with smart contracts but use other services such as secure messaging and often allow an unlimited number of participants to interact within a given rule set. (Literature: A, Chapter 5.3)
D) Incorrect. Decentralized applications - often just referred to as DApps - are applications that run on a P2P network instead of a single system. DApps can be tools, programs, games, and more that connect users and providers directly.

30 / 40
What is the role of a DAO (decentralized autonomous organization)?

A) Address the principal-agent dilemma with collaboration and acceptance of actions within agreed rules
B) Embed regulated online smart contracts with the current judicial system, using public blockchains
C) Offer complex online smart contracts without any link to tangible and intangible offline assets
D) Provide a private blockchain contract platform on which users can run their online applications

A) Correct. The concept of a DAO was created to address what in economics is referred to as the "principal-agent problem". The principal-agent problem is a dilemma that occurs when an "agent" can make decisions on behalf of another agent but is influenced by their own self-interest. The "agent" may choose to take more risk, because they do not actually carry the cost of that risk. (Literature: A, Chapter 5.4)
B) Incorrect. The code and capabilities of DAOs do not absolve individuals from complying with regulations and laws.
C) Incorrect. DAOs run through rules encoded within their smart contracts. They live completely online but can govern assets that are offline, like real estate or natural resources.
D) Incorrect. All public blockchains are DAOs. These include Bitcoin, Ethereum, Factom, and others. DAOs can be more than public networks. They can be used to manage all types of human organizations such as corporations, investment funds, or even governments.

How can blockchain technology **best** help securing identity data?

A) By eliminating third parties through providing secured-data storage at a user's server
B) By encoding all the health data and save it on a private and permissionless blockchain
C) By protecting data that has been submitted on the internet using a cryptographic algorithm
D) By providing information personal data without disclosing the actual data that proves it

A) Incorrect. It makes no sense to use a blockchain at the user's server. Blockchain is supposed to be a distributed ledger.
B) Incorrect. Encoding personal data at a permissionless blockchain makes no sense as a permissionless blockchain is not well-enough secured for this.
C) Incorrect. It makes no sense to protect information that has been submitted on the internet before, as it might have been compromised already.
D) Correct. Providing information without disclosing the actual data is one of the important functions of a blockchain. (Literature: A, Chapter 6.1)

32 / 40
What is the value of using blockchain networks with Internet of Things (IoT)?

A) Allowing blockchain users to follow self-driving cars and access these cars
B) Avoiding a spoofing attack using the secured identity that is stored on a blockchain
C) Enabling software that programs itself to solve problems without human intervention
D) Solving expensive and complex calculations using Hyperledger Fabric mining

A) Incorrect. This would be a dangerous situation where self-driving cars would be open to spoofing attacks or hacks. There are many companies developing technologies that utilize blockchain to protect IoT devices.
B) Correct. IoT can utilize blockchain secured identity to prevent a spoofing attack where a malicious party impersonates another device to launch an attack to steal data or cause some other disorder. (Literature: A, Chapter 6.3)
C) Incorrect. This is the value of using blockchain networks with AI.
D) Incorrect. There is no mining in Hyperledger Fabric. Matrix Artificial Intelligence (AI) is providing a solution that makes it easy to combine machine learning and smart contracts. The platform modifies how smart contracts are executed, and improves their speed, flexibility, ease and security. Matrix uses its mining power to solve expensive and complex AI computations.

Blockchain technology has made decentralized marketplaces possible.

What is a benefit of a decentralized marketplace?

A) It is based on open-source technology, so it can be used without any investment
B) It is not under a paid license to operate and therefore it is managed better
C) It is relatively cheap due to the use of cryptocurrency and is very accessible
D) It is tamper-proof, resilient to being shut down and trustworthy due to smart contracts

A) Incorrect. The use of open-source technology does not determine whether investment is needed. Moreover, not all blockchains are based on open-source code.
B) Incorrect. Being under a paid license does not determine whether a product is managed well.
C) Incorrect. It is not necessarily true that decentralized marketplaces are cheaper than other marketplaces.
D) Correct. The blockchain ensures that everyone is who they say they are and secures the transfer of value, without the need for a third party. (Literature: A, Chapter 6.5)

34 / 40
How does blockchain improve supply chains?

A) By automatically creating trade agreements between two parties
B) By creating safe centralized marketplaces to trade goods on
C) By stabilizing the national currencies of the countries involved
D) By transferring tokenized ownership through a software system

A) Incorrect. Trade agreements can be programmed into smart contracts, but blockchain does not create these.
B) Incorrect. Blockchain can help making decentralized marketplaces more secure, but it definitely does not help to create centralized marketplaces.
C) Incorrect. Blockchain does not help stabilizing national currencies.
D) Correct. Blockchain can transfer value, or tokenized ownership through just a software system. (Literature: A, Chapter 7.1)

35 / 40

The Monetary Authority of Singapore (MAS) and blockchain company R3 partnered together.

What did they achieve together?

A) The creation of smart contracts and stable coins
B) The facilitation of interbank transmission of messages
C) The first interbank payments without limitations of time zones
D) The launch of wire transfers using cryptography

A) Incorrect. Everex is involved in the development of smart contracts and stable coins to support the digital currency initiatives of commercial and central banks.
B) Incorrect. The global network for the Society of Worldwide Interbank Financial Telecommunication (SWIFT) became the entity responsible for most international payments. Although it does not move money, the network facilitates the transmission of messages between banks, effectively allowing banks to get in direct communication to make the international money transfer process easier.
C) Correct. The Monetary Authority of Singapore partnered with blockchain company R3 and conducted the first interbank payments using blockchain technology in 2016. The project showed that banks could transact and settle round-the-clock and were no longer limited by time zones and office hours. (Literature: A, Chapter 7.2)
D) Incorrect. Western Union was founded, and they launched the wire transfer. This process uses electronic funds transfer from one person or entity to another through its telegraph network, effectively helping to move money within and across borders. Western Union still handles the majority of personal remittances globally.

36 / 40

What is digital fiat currency?

A) A digital form of currency, that represents a country's financial reserves
B) An e-currency, that creates a transparent and borderless debt market
C) An online system, that enables making transactions without a bank account

A) Correct. Digital fiat currency is defined as the representation in the digital form of a currency of a particular nation and is issued and regulated by the competent monetary authority of the country. (Literature: A, Chapter 8.1)
B) Incorrect. Digital fiat currency has nothing to do with debt markets.
C) Incorrect. Digital fiat currency works only for people with a bank account. It is aimed at international payment balance, not individual transactions.

37 / 40
How does blockchain technology benefit the insurance industry?

A) By avoiding compliance requirements of national authorities, which reduces overhead
B) By ensuring accuracy of data and automating micro insurances, which reduces costs
C) By introducing flexible premiums to be paid by customers, which increases profits
D) By setting up a digital mode of payment, which simplifies claims settlement

A) Incorrect. Blockchain activities must comply with legislation and regulations.
B) Correct. Blockchain technology enables insurance companies to provide more value to the contacts they already have. (Literature: A, Chapter 8.3)
C) Incorrect. Blockchain does not define the premium for customers.
D) Incorrect. Blockchain does not define the mode of payment to the insurance company.

38 / 40
How does blockchain technology help to protect intellectual property rights (IP)?

A) It allows a user to include IP transactions in smart contracts.
B) It allows a user to record an event and establish the timeline.
C) It allows a user to record the creation of software packages.
D) It allows a user to send a transaction and receive IP ownership.

A) Incorrect. A smart contract acts as an online contract between two or more parties. Smart contracts are digital agreements or sets of rules governing the IP access.
B) Correct. IP is grounded in a concept of fairness, "who did what when" and the first person that did something should have the right to the commercial benefit for those efforts. Using blockchain, it is possible to establish that something existed at a given point in time and third parties can verify that information. (Literature: A, Chapter 8.4)
C) Incorrect. Blockchain technology is used to record an event regarding creation of an IP.
D) Incorrect. It is not possible to establish ownership over an IP by simply sending a transaction.

What is an example of how a government is actively promoting the use of blockchain?

A) China has created a regulatory sandbox that allows them to closely monitor the experiments in blockchain mining and create their own cryptocurrency.
B) Estonia offers e-Residency software, which is available to anyone in the world interested in operating a business online and from within the European Union.
C) Singapore's Monetary Authority (MAS) is creating central bank digital money for payments between banks using distributed ledger technology (DLT).

A) Incorrect. Blockchain technology has had a love-hate relationship with China. In 2017 blockchain mining and ICOs were expelled from the country and professionals in the space were arrested. At the same time, China's government has invested heavily in blockchain development. They are leading in innovation and cracking down on blockchain systems they cannot control. However, China does not have its own cryptocurrency.
B) Incorrect. Estonia launched digital ID cards for online services and has offered citizenship as a service by being the first country to offer e-Residency. They create a digital identity, available to anyone in the world interested in operating a business online and through the European Union. However, the e-Residency is not software that is distributed. It is also not solely promoting blockchain technology.
C) Correct. The MAS are creating central bank digital money using DLT. The first phase of the project started in 2016 where they proved the ability to conduct a domestic inter-bank payment using a central bank-issued Singapore Dollar (SGD) equivalent token. (Literature: A, Chapter 9.2)

Why is blockchain described as the technology that adds a layer of trust to the internet?

A) It allows individuals and groups to work together without having to trust each other or establish authority.
B) It creates a dedicated virtual private network (VPN) tunnel between two or more parties to carry out online fund transfers.
C) It provides mechanism for the government to create their own digital fiat currency as a replacement of physical currency.
D) It provides multifactor authentication to create and update records of cryptocurrency transactions securely.

A) Correct. It allows for individuals, governments, and businesses to work together in a fair and open manner, without first establishing trust, ownership, and authority. (Literature: A, Chapter 9.4)
B) Incorrect. VPN is not an application of blockchain technology.
C) Incorrect. Digital fiat currency is one of the applications of blockchain technology.
D) Incorrect. Blockchain technology makes use of cryptographic hash functions to provide the trait of immutability.

Evaluation

The table below shows the correct answers to the questions in this sample exam.

Question	Answer	Question	Answer
1	C	21	C
2	C	22	B
3	C	23	B
4	C	24	D
5	D	25	C
6	B	26	B
7	D	27	C
8	A	28	C
9	D	29	C
10	A	30	A
11	C	31	D
12	H	32	B
13	C	33	D
14	D	34	D
15	D	35	C
16	C	36	A
17	A	37	B
18	C	38	B
19	C	39	C
20	A	40	A

Contact EXIN

www.exin.com