ECCouncil.312-82.by.Hathoi.26q

Number: 312-82
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 312-82

Exam Name: EC-Council Blockchain Fintech Certification

Exam A

QUESTION 1
_______is a computer program that runs stop a blockchain and embedded within it are governance and business logic rules

A. Dapps
B. DaS
C. DAO
D. DAC

Correct Answer: A
Section:
Explanation:
Decentralized Applications (Dapps) are applications that run on a blockchain network and include embedded governance and business logic rules. Unlike traditional applications, Dapps are decentralized, meaning they operate on a peer-to-peer network rather than a centralized server, leveraging smart contracts to automatically enforce rules and protocols without intermediaries.
Key Details:
Characteristics of Dapps: Dapps are open-source, operate autonomously, and store data on a blockchain. They utilize smart contracts to handle various functions, from transaction processing to enforcing governance rules and executing business logic.
Smart Contracts: The embedded rules within Dapps are typically coded as smart contracts, which are self-executing contracts with the terms of the agreement directly written into lines of code. This ensures that all transactions and operations within the Dapp are transparent, immutable, and automatically enforced.
Use Cases: Dapps are commonly found in areas such as decentralized finance (DeFi), gaming, supply chain management, and social media, offering users more control and transparency compared to traditional applications.
In conclusion, Dapps (A) is the correct answer as it refers to computer programs running on a blockchain with embedded governance and business logic rules.

QUESTION 2
In this method users permanently destroy a certain quantity of bitcoin in proportion to the quantity of altcoin to be demand. What is this method?

A. Side block
B. Proof of Burn
C. Side-chaining
D. Proof of ownership

Correct Answer: B
Section:
Explanation:
Proof of Burn (PoB) is a consensus mechanism where users permanently destroy (or 'burn') a certain quantity of cryptocurrency, such as Bitcoin, to gain the right to mine or acquire an altcoin. This process proves commitment to the network and secures it by effectively sacrificing one asset to obtain another.
Key Details:
Burning Process: In PoB, participants send a certain amount of cryptocurrency to an unspendable address, effectively removing it from circulation. This act serves as proof that they have invested in the network by reducing the supply of the original cryptocurrency.
Purpose and Use Cases: PoB is used by networks that want to incentivize long-term commitment and reduce total supply. It is often seen in new blockchain projects that allow miners or users to trade value in established currencies like Bitcoin for the native token of the new network.
Security: By requiring participants to destroy value, PoB helps prevent spam attacks and promotes network stability.
Therefore, B. Proof of Burn is the correct answer, as it describes the method where users destroy a certain amount of cryptocurrency to receive or mine another asset.

QUESTION 3
__________is a blockchain based predictions market that uses the Ethereum blockchain.

A. Augur
B. IBM Blockchain
C. STEEM
D. DASH

Correct Answer: A
Section:
Explanation:
Augur is a decentralized, blockchain-based predictions market built on the Ethereum network. It enables users to create and participate in markets based on the outcome of real-world events, using smart contracts to automate the process and secure transactions.
Key Details:
Ethereum-Based: Augur utilizes the Ethereum blockchain to facilitate the creation and settlement of prediction markets. It leverages Ethereum's smart contracts to ensure transparency, immutability, and trustless interactions.
Decentralized Prediction Market: In Augur, users can bet on the outcome of various events, ranging from sports to elections. The decentralized nature of the platform ensures that no central authority controls the markets, providing a level of censorship resistance.
Token Usage: Augur uses a token called REP (Reputation) that holders use to report and dispute outcomes of events on the platform. This ensures that the market outcomes are validated in a decentralized manner.
Thus, A. Augur is the correct answer, as it is a blockchain-based prediction market built on Ethereum.

QUESTION 4
______is designed to allow easy deployment of bloodchains.

A. Composer
B. Cello
C. Caliper
D. Quit

Correct Answer: B
Section:
Explanation:
Hyperledger Cello is designed to facilitate the deployment and management of blockchain networks. It provides an easy-to-use framework for creating, managing, and scaling blockchain networks, making it suitable for rapid deployment and operation. Although the term 'bloodchains' might be a typo or intended for 'blockchains,' Cello indeed simplifies the blockchain setup process for various applications.
Key Details:
Deployment and Management: Cello offers a suite of tools that automates blockchain deployment, operation, and monitoring, making it accessible for businesses looking to adopt blockchain technology with minimal effort.
Modular Approach: It supports various blockchain frameworks, including Hyperledger Fabric, and is aimed at reducing the complexity involved in blockchain management.
Use Cases: Hyperledger Cello is useful for enterprise blockchain applications, as it allows administrators to manage blockchain networks with tools that support configuration, monitoring, and scaling.
Thus, B. Cello is the correct answer, as it simplifies blockchain deployment and management.

QUESTION 5
What is a DEX?

A. A distributed exchange that covers multiple nationalities
B. A cryptocurrency exchange such as coinbase
C. A decentralized exchanged that allows users to exchange cryptocurrency directly
D. A Decentralized finance app or DApp

Correct Answer: C
Section:
Explanation:

A Decentralized Exchange (DEX) is a platform that allows users to trade cryptocurrencies directly with one another without the need for a central intermediary or custodian. On a DEX, trades are facilitated using smart contracts on a blockchain, which automate transactions and ensure transparency. This decentralized model allows for peer-to-peer trading, often providing users with greater privacy and control over their funds compared to centralized exchanges.
Key Details:
Functionality of DEXs: DEXs enable users to connect their wallets and trade assets directly from their accounts. There is no central authority controlling the funds, reducing the risk of hacks and giving users full control over their private keys.
Examples of DEXs: Popular DEXs include Uniswap, SushiSwap, and PancakeSwap, which are commonly built on blockchain networks like Ethereum and Binance Smart Chain. These platforms operate through automated market makers (AMMs) or order book systems, which facilitate trading without centralized management.
Comparison with Centralized Exchanges (CEXs): Unlike centralized exchanges, which act as intermediaries and hold user funds, DEXs do not hold custody of funds. This reduces the risk of theft and enables users to trade directly from their wallets.
Therefore, the correct answer is C. A decentralized exchange that allows users to exchange cryptocurrency directly.

QUESTION 6
Self-executing computer programs which facilitate transaction automation and eliminates the need for intermediaries are called what?

A. Cryptocurrencies
B. Bitcoin mining
C. Distributed ledgers
D. Smart contracts

Correct Answer: D
Section:
Explanation:
Smart Contracts are self-executing computer programs that automatically enforce, verify, and facilitate the terms of a contract when certain conditions are met. These programs run on blockchain networks and eliminate the need for intermediaries by automating transactions based on predefined rules coded into the contract.

Key Details:
Automation and Trust: Smart contracts are crucial in blockchain technology because they enable trustless transactions, meaning parties can transact directly without relying on intermediaries. The code controls the execution, and transactions are transparent and irreversible.
Use Cases: Smart contracts are foundational to decentralized finance (DeFi) applications, supply chain management, digital identity, and more. They facilitate various operations such as lending, borrowing, insurance, and automated asset transfers.
Example in Ethereum: Ethereum popularized smart contracts by providing a platform with Turing-complete scripting capabilities. This allowed developers to create sophisticated decentralized applications that execute on the blockchain.
In conclusion, D. Smart contracts is the correct answer as it refers to the technology that automates transactions and eliminates the need for intermediaries.

QUESTION 7
Which of the following is a language for working with Ethereum?

A. Mist
B. Rikeby
C. Solidity
D. Kovan

Correct Answer: C
Section:
Explanation:
Solidity is the primary programming language used for developing smart contracts on the Ethereum blockchain. It is a statically typed, high-level language similar to JavaScript and C++, and it is specifically designed for creating contracts that run on the Ethereum Virtual Machine (EVM).
Key Details:
Purpose of Solidity: Solidity was created by the Ethereum team to enable the development of smart contracts that automate the execution of blockchain-based applications. Its syntax is designed to be familiar to developers

experienced in other programming languages, which helps in onboarding and learning.

Compatibility and Flexibility: As a Turing-complete language, Solidity allows for the development of complex smart contracts and decentralized applications (DApps) with conditional logic, loops, and more. It is widely used in the DeFi space and beyond.

Ethereum Test Networks: Other options listed, such as Rinkeby and Kovan, refer to Ethereum test networks where developers test smart contracts, but they are not languages themselves. Mist is an Ethereum wallet interface, not a programming language.

Thus, C. Solidity is the correct answer, as it is the language specifically designed for working with Ethereum smart contracts.

QUESTION 8

________implements the interledger protocol, which facilitates interoperability across different distributed and non-distributed ledger networks.

A. Composer
B. Cello
C. Quit
D. Caliper

Correct Answer: C
Section:
Explanation:

The answer is (C) Quilt.

Hyperledger Quilt is a Java implementation of the Interledger Protocol (ILP). ILP is designed to transfer value across different ledgers, whether they are distributed ledgers (like blockchains) or traditional non-distributed ledgers.

Here's why the other options aren't the best fit:

Composer: Hyperledger Composer was a tool for building blockchain applications, but it has been deprecated.

Cello: Hyperledger Cello aims to provide a modular blockchain platform, making it easier to deploy and manage blockchain networks.

Caliper: Hyperledger Caliper is a benchmarking tool used to measure the performance of different blockchain implementations.

Quilt's primary function is to enable interoperability between different ledger systems, which is crucial for the broader adoption and integration of blockchain technology.

QUESTION 9

Public blockchains most often use_________ as a consensus mechanism.

A. PoS
B. PoB
C. PoW
D. PoET

Correct Answer: C
Section:
Explanation:

Public blockchains most commonly use Proof of Work (PoW) as their consensus mechanism, especially in well-established networks such as Bitcoin and, until recently, Ethereum. PoW is a protocol that relies on network participants (miners) solving complex mathematical problems to validate and add transactions to the blockchain. This process ensures the integrity and security of the network, as it requires substantial computational power and resources, making it difficult for any single entity to control the blockchain.

Key Details:

Proof of Work (PoW): PoW, used primarily by Bitcoin, operates by having participants (often referred to as miners) compete to solve cryptographic puzzles. The first to solve the puzzle adds the next block of transactions to the blockchain and is rewarded with newly minted coins. This system is energy-intensive but is widely recognized for its security and resistance to tampering.

Transition in Other Networks: While Ethereum initially used PoW, it transitioned to Proof of Stake (PoS) in 2022 with Ethereum 2.0, due to PoS's lower energy requirements and increased scalability. However, Bitcoin, the most prominent public blockchain, still relies on PoW.

Other Consensus Mechanisms: Alternatives such as Proof of Stake (PoS) and Proof of Burn (PoB) are used by other blockchain networks that aim for different trade-offs in terms of energy efficiency, scalability, and security.

Proof of Elapsed Time (PoET) is another mechanism mostly associated with permissioned (private) blockchains rather than public blockchains.

Why PoW for Public Blockchains?: Public blockchains prioritize decentralization and security. PoW provides a robust way to achieve this, despite its high energy consumption. Its high level of security and historical success in

Bitcoin's network often make it the go-to choice for public blockchains.
In summary, the dominance of PoW in public blockchains is due to its established security and proven track record, although PoS and other mechanisms are increasingly gaining popularity for their efficiency in newer blockchain projects.

QUESTION 10
Is a Microsoft blockchain development platform that allows the creation of custom private blockchains.

A. Sratis
B. Corda
C. Azure
D. Fabric

Correct Answer: C
Section:
Explanation:
Microsoft Azure is a blockchain development platform that enables the creation of custom private blockchains. Azure Blockchain Service provides tools and services that allow organizations to set up and manage consortium blockchain networks, customize smart contracts, and create tailored blockchain applications. Azure supports multiple blockchain frameworks, including Ethereum and Hyperledger Fabric, making it versatile for both private and public network needs.
Key Details:
Azure Blockchain Service: This service facilitates the deployment of managed blockchain networks on the cloud, leveraging Azure's infrastructure to deliver scalability, security, and reliability for private and consortium blockchain applications.
Private Blockchain Capabilities: As a private blockchain service, Azure allows businesses to operate their blockchain in a controlled, permissioned environment. This offers greater control over data and participants, making it ideal for enterprise use cases like supply chain management, finance, and legal contracts.
Blockchain Framework Compatibility: Although Azure supports a variety of blockchain protocols, it primarily focuses on private blockchain deployments, allowing for detailed control over network participants and data visibility.
In summary, Microsoft Azure stands out as a flexible and comprehensive platform for private blockchain development, catering to enterprises with tailored solutions and extensive cloud-based services.

QUESTION 11
Proof of work algorithms are best described as being used for what?

A. Executing transactions
B. Proof that adequate computational resources have been sent.
C. Bitcoin mining
D. Proving the user has invested enough in the system

Correct Answer: B
Section:
Explanation:
Proof of Work (PoW) algorithms are primarily used to demonstrate that sufficient computational resources have been expended by a participant to validate transactions and add them to the blockchain. In PoW, miners compete to solve a cryptographic puzzle, which requires significant computational power. This effort helps secure the network by making it prohibitively expensive for any individual or group to alter the blockchain's history.
Key Details:
Mechanism of PoW: The essence of PoW is to prove that a certain amount of computational work has been performed. This ''work'' is measured by the effort miners invest in solving the cryptographic puzzle. The process requires miners to find a nonce that, when hashed with the block's data, results in a hash that meets the network's difficulty requirements.
Security and Integrity: By proving computational work, PoW ensures that miners cannot simply fabricate or alter transactions without a significant investment of resources. This mechanism deters attacks and makes blockchain networks resistant to tampering and double-spending.
Association with Bitcoin Mining: Although PoW is often associated with Bitcoin mining (as miners expend computational resources to validate and record transactions), its broader purpose is to establish a cost for participation in the network, ensuring that all entries to the blockchain are trustworthy and secure.
Therefore, PoW is best described as a mechanism for proving that adequate computational resources have been expended, aligning with the correct answer B.

QUESTION 12
_________is used to split up the tasks into multiple chunks that are then processed by multiple nodes.

A. Sharding
B. Parsing
C. Partitioning
D. Fragmenting

Correct Answer: A
Section:
Explanation:
Sharding is a scalability technique that splits tasks or data into smaller, more manageable pieces called 'shards.' These shards are then processed in parallel by multiple nodes in a network. By dividing the workload, sharding can significantly enhance the efficiency and speed of blockchain networks, which is especially beneficial for handling large transaction volumes and complex computations.
Key Details:
Purpose of Sharding: The main goal of sharding is to address blockchain scalability issues. By enabling the network to process transactions and data in parallel, it reduces the load on individual nodes, thus increasing the overall throughput of the blockchain.
How Sharding Works: In a sharded blockchain, each node only needs to process a portion of the total data rather than every single transaction on the network. Each shard is responsible for a subset of data and transactions, and only nodes within a particular shard need to validate its transactions.
Relevance in Blockchain: Sharding is crucial in large-scale blockchain networks like Ethereum, where high transaction volumes can lead to congestion. Ethereum 2.0, for example, incorporates sharding as a core feature to improve its scalability and transaction processing capacity.
Sharding is, therefore, the correct answer, as it directly refers to the method of dividing tasks for parallel processing in a distributed environment.

QUESTION 13
These wallets store keys in a tree structure derived from a seed.

A. Brain Wallets
B. Hierarchical Deterministic Wallets
C. Deterministic Wallets
D. Non-Deterministic Wallets

Correct Answer: B
Section:
Explanation:
Hierarchical Deterministic (HD) Wallets are wallets that generate private and public keys in a tree structure, starting from a single seed phrase. This seed phrase can generate multiple key pairs, allowing users to back up and recover all their wallet addresses using one phrase, which enhances security and convenience.
Key Details:
Tree Structure: HD wallets use a root seed to derive an entire hierarchy of keys. Each branch in the tree can create new sub-branches, generating separate addresses for different transactions without reusing them, which provides better privacy.
Seed-Based Recovery: Users can restore all wallet addresses with the original seed phrase, making HD wallets more secure and easy to back up compared to non-deterministic wallets, which would require individual backups for each key.
Compatibility with Blockchain Standards: HD wallets adhere to the BIP32 and BIP44 standards, which outline the derivation paths and formats used by these wallets. This compatibility allows for interoperability among different wallet providers.
In conclusion, Hierarchical Deterministic Wallets (answer B) best describes wallets that store keys in a tree structure derived from a seed.

QUESTION 14
Which of the following are likely use cases for blockchain in the energy industry? (Select two.)

A. Safety in energy production

B. Energy trading
C. Safety in energy transport
D. Smart power grids

Correct Answer: B, D
Section:
Explanation:
Blockchain technology has significant potential in the energy industry, particularly in energy trading and smart power grids. By providing a transparent, decentralized, and secure platform for transactions, blockchain can facilitate peer-to-peer energy trading and improve the efficiency and reliability of smart grids.
Key Details:
Energy Trading: Blockchain enables peer-to-peer energy trading where individuals and companies can buy and sell excess energy (such as solar or wind power) directly to each other. This decentralized model reduces the need for intermediaries and allows consumers to benefit from direct energy sales and purchases.
Smart Power Grids: Blockchain can enhance smart grid systems by enabling real-time data sharing and automated decision-making. With blockchain, smart grids can securely record and share data related to energy production, consumption, and storage, thereby improving grid management, reducing waste, and optimizing energy distribution.
Enhanced Transparency and Security: By recording all transactions in an immutable ledger, blockchain ensures transparency and security, reducing the risks of fraud and discrepancies in the energy market. This is especially beneficial in energy trading where trust and accurate record-keeping are essential.
Thus, Energy trading (B) and Smart power grids (D) are the most likely use cases for blockchain in the energy industry.

QUESTION 15
________uses a Trusted Execution environment (TEE) to provide randomness and safety in the leader election process via a guaranteed wait time.

A. PoET
B. PoD
C. PoA
D. PoI

Correct Answer: A
Section:
Explanation:
Proof of Elapsed Time (PoET) is a consensus mechanism that uses a Trusted Execution Environment (TEE) to ensure randomness and safety in the leader election process by enforcing a guaranteed wait time. Developed by Intel, PoET is particularly used in permissioned blockchain networks where a TEE can securely run code to determine which node is elected to propose the next block. This mechanism is efficient in terms of energy consumption and provides a fair method for selecting a leader without requiring intensive computational power.
Key Details:
Role of TEE in PoET: The TEE ensures that nodes wait for a random period before being eligible to propose a new block. This waiting period is verified by the TEE, which acts as a trusted third party to confirm that nodes have adhered to the assigned wait time.
Randomness and Security: PoET provides randomness in the leader selection process, reducing the chances of any node gaining an unfair advantage. It also promotes security by leveraging the TEE, which is designed to prevent tampering with the waiting time calculations.
Use Cases: PoET is mainly used in permissioned blockchain environments like Hyperledger Sawtooth, where nodes are pre-approved, and there is a need for a scalable yet secure consensus mechanism.
In summary, PoET is the correct answer as it directly refers to a consensus mechanism that utilizes a Trusted Execution Environment for leader election.

QUESTION 16
A_________in a new chain and requires clients to upgrade in order to participate on the new blockchain.

A. Hard fork
B. Soft fork
C. Sharding
D. Sub chain

Correct Answer: A
Section:
Explanation:
A hard fork occurs when there is a fundamental change in a blockchain's protocol, resulting in the creation of a new chain that is incompatible with the previous one. After a hard fork, nodes must upgrade to the new version of the blockchain's software to continue participating in the network. A hard fork can be used to implement new features, fix security issues, or change core aspects of the blockchain.
Key Details:
Differences from Soft Forks: Unlike a soft fork, which is backward-compatible and allows nodes on the previous version to still participate, a hard fork splits the blockchain into two distinct paths, with the upgraded path requiring new software.
Examples: Notable hard forks include Bitcoin Cash from Bitcoin and Ethereum Classic from Ethereum. These forks occurred due to disagreements within the community on how to handle certain protocol changes, leading to the creation of separate blockchains.
Upgrade Requirements: Participants on the blockchain who wish to continue on the new chain after a hard fork must update their software. Those who do not upgrade remain on the original chain, which continues as a separate, incompatible blockchain.
Thus, the correct answer is Hard fork (A), as it directly refers to a blockchain split that requires client upgrades for participation.

QUESTION 17
A Type II DAPP is categorized by its_______

A. Using the protocol of a type II DApp
B. Using the blockchain and protocol of a type I
C. Using another blockchain such as Ethereum
D. Using the block chain of a type I but not the protocol

Correct Answer: B
Section:
Explanation:

A Type II DApp is a decentralized application that uses both the blockchain and protocol of a Type I DApp. Type I DApps are the foundational blockchain-based platforms, such as Ethereum, that operate with their own blockchain. Type II DApps build on these platforms, using the existing blockchain and protocol, but offering specific functionalities or services.
Key Details:
Type I DApps: These are fundamental blockchain platforms, like Bitcoin or Ethereum, which have their own blockchain and provide a foundation for other applications.
Characteristics of Type II DApps: Type II DApps leverage the infrastructure of Type I DApps but add additional functionality through smart contracts or protocols. For example, protocols such as ERC-20 tokens or ERC-721 NFTs are built on Ethereum and utilize Ethereum's underlying blockchain and consensus protocol.
Integration: By utilizing both the blockchain and protocol of a Type I DApp, Type II DApps inherit the security, decentralization, and features of the underlying Type I platform, which simplifies their development and ensures compatibility.
In summary, B. Using the blockchain and protocol of a type I accurately describes the categorization of Type II DApps.

QUESTION 18
__________change the blockchain layout from a linearly sequential model.

A. Side chains
B. Fork chains
C. Sub chains
D. Tree chains

Correct Answer: D
Section:
Explanation:
Tree Chains modify the standard blockchain structure from a linear sequence to a tree-like structure, where blocks can have multiple branches instead of forming a single sequential chain. This structure can improve scalability and enable parallel processing, as multiple chains can be validated simultaneously.
Key Details:

Tree Structure: In tree chains, blocks can have multiple child blocks, which allows transactions to be processed across several branches concurrently. This reduces bottlenecks associated with linear block validation and enhances throughput.
Benefits Over Linear Chains: Traditional blockchain models process blocks in a strict sequence. Tree chains allow for more flexibility and higher transaction throughput, as multiple blocks can be validated simultaneously across different branches.
Use Cases: This structure is advantageous for complex applications that require parallel transaction processing, such as large-scale blockchain networks or systems needing high transaction speeds.
Thus, D. Tree chains is the correct answer, as it refers to the blockchain model that diverges from a linear structure.

QUESTION 19
According to a study be Deloitte, which of the following are benefits of blockchain for the insurance industry (pick two)?

A. More efficient claims processing
B. Supporting strategic initiatives
C. Comprehensive interoperable health records
D. Lower costs

Correct Answer: A, D
Section:
Explanation:
According to studies conducted by Deloitte and other industry research, blockchain offers several benefits for the insurance industry, particularly in more efficient claims processing and lower costs. Blockchain's capabilities in data immutability, transparency, and automation play key roles in streamlining insurance processes and reducing operational expenses.
Key Details:
Efficient Claims Processing: Blockchain enables quicker verification and processing of claims by automating workflows through smart contracts. This reduces paperwork, minimizes errors, and speeds up the claims process, improving customer satisfaction.
Lower Costs: By reducing intermediaries and leveraging automation, blockchain lowers administrative costs. It minimizes the need for manual verification and fraud detection, which traditionally consume significant resources in the insurance industry.
Transparency and Fraud Reduction: Blockchain provides an immutable and transparent record of all transactions. This helps prevent fraud, as all stakeholders have access to the same data, reducing discrepancies and the need for extensive audits.
In conclusion, A. More efficient claims processing and D. Lower costs are the correct answers, as these are key benefits of blockchain for the insurance industry identified in Deloitte's research.

QUESTION 20
The Financial Action Task force defines virtual asset service providers as companies that (choose two):

A. Sell products for virtual currency
B. Purchase virtual currency
C. Exchange virtual assets for fiat currency
D. Transfer virtual assets

Correct Answer: C, D
Section:
Explanation:
According to the Financial Action Task Force (FATF), Virtual Asset Service Providers (VASPs) are entities or companies that facilitate activities related to virtual assets. Specifically, VASPs include businesses that exchange virtual assets for fiat currency and transfer virtual assets. These activities are regulated to prevent money laundering, terrorist financing, and other illicit activities.
Key Details:
Exchange of Virtual Assets for Fiat Currency: VASPs often act as intermediaries that enable the conversion between virtual assets (like cryptocurrencies) and traditional fiat currencies. This function is central to enabling liquidity and usability of cryptocurrencies within the traditional financial system.
Transfer of Virtual Assets: VASPs may also provide services that involve the transfer of virtual assets from one user to another, which includes activities such as facilitating peer-to-peer transactions, wallet services, or custodial services.
FATF Standards and Compliance: The FATF has established guidelines for VASPs to enhance transparency and ensure compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations.
Thus, the correct answers are C. Exchange virtual assets for fiat currency and D. Transfer virtual assets, as these are the core activities defined for VASPs by the FATF.

QUESTION 21
The financial Action Task force defines virtual asset providers as companies that (choose two):

A. Sell products for virtual currency
B. Purchase virtual currency
C. Exchange virtual assets for fiat currency
D. Transfer virtual assets

Correct Answer: C, D
Section:
Explanation:
The Financial Action Task Force (FATF) defines Virtual Asset Service Providers (VASPs) in its guidelines to include entities that engage in the exchange of virtual assets for fiat currency and the transfer of virtual assets. This categorization is part of the FATF's efforts to regulate and monitor the flow of virtual assets to mitigate risks associated with illicit activities.
Key Details:
Exchange and Conversion Services: FATF recognizes companies that offer exchange services between virtual assets and fiat currencies as VASPs. These services are critical for converting virtual assets into forms that can be readily used in traditional markets.
Transfer Services: VASPs that facilitate the transfer of virtual assets are also within the FATF's regulatory scope. This includes services that manage, transfer, or act as intermediaries in the movement of virtual assets between users, ensuring these transactions are conducted transparently and within regulatory frameworks.
Therefore, C. Exchange virtual assets for fiat currency and D. Transfer virtual assets are the correct answers, as they align with the FATF's definition of VASPs.

QUESTION 22
A_________represents a transfer of value from one address to another, Transaction in a blockchain network can be defined also as a record of an event or the ''transfer of value from one account to another''

A. Hash function
B. Block
C. Signature
D. transaction

Correct Answer: D
Section:
Explanation:
In blockchain terminology, a transaction represents the transfer of value from one address to another. Each transaction is recorded on the blockchain as an immutable entry, often representing a movement of digital assets or a record of an event.
Key Details:
Nature of Transactions: A blockchain transaction involves a digital asset or token being sent from one blockchain address (wallet) to another. The transaction is broadcast to the network, validated by nodes, and then recorded on the blockchain ledger.
Transfer of Value: Blockchain transactions serve as proof of the transfer of value, which could represent cryptocurrency movement, digital asset exchange, or a specific record of an event, depending on the blockchain's purpose.
Inclusion in Blocks: Each transaction is grouped into blocks, which are then cryptographically linked together, forming the blockchain. This ensures all transactions are secure, traceable, and verifiable.
Thus, D. Transaction is the correct answer, as it describes the fundamental concept of transferring value on a blockchain.

QUESTION 23
When using ___________ the chain of ownership is established by a chain of digital signatures as each owner signs when transferring ownership.

A. NFTS
B. ETHASH
C. PoET
D. UTXO

Correct Answer: D
Section:
Explanation:
The UTXO (Unspent Transaction Output) model establishes a chain of ownership by using digital signatures. In this model, each transaction consists of inputs (from previous UTXOs) and outputs (new UTXOs), and ownership is transferred by the current owner signing the transaction. This digital signature is then verified by the recipient, ensuring a secure and traceable chain of ownership.
Key Details:
Functionality of UTXO: UTXO is a fundamental part of Bitcoin's transaction model. When a transaction occurs, it consumes previous outputs as inputs, generating new UTXOs. Each UTXO can only be spent once, and ownership is verified through cryptographic signatures.
Chain of Ownership: The UTXO model inherently creates a clear and verifiable chain of ownership, as each output is signed by the current owner and used as input for future transactions, maintaining a continuous and transparent record of asset transfers.
Security through Digital Signatures: UTXO-based transactions rely on digital signatures to authenticate and authorize asset transfers, ensuring that only the rightful owner can initiate a transaction.
Thus, D. UTXO is the correct answer, as it accurately describes the model where ownership is established through a chain of digital signatures.

QUESTION 24
Who first proposed blind signatures to build an untraceable digital currency?

A. David Chaum
B. Satoshi Nakamoto
C. Wei Dai
D. Nick Szabo

Correct Answer: A
Section:
Explanation:
David Chaum first proposed the concept of blind signatures in the early 1980s as a way to create an untraceable digital currency. Chaum's work laid the groundwork for digital privacy in financial transactions by enabling transactions to be signed without revealing the actual content of the transaction, thus maintaining user privacy.
Key Details:
Blind Signatures: A blind signature is a form of digital signature in which the content of a message is hidden (or 'blinded') before being signed. This allows for privacy-preserving digital transactions, as the signer cannot see the actual content they are signing.
Application in Digital Currency: Chaum's idea was foundational for the development of anonymous electronic cash systems. His work led to the creation of DigiCash in 1989, one of the earliest forms of digital currency focused on user privacy.
Influence on Modern Cryptocurrencies: Although Chaum's DigiCash was not a blockchain-based system, his concepts of privacy and anonymous transactions greatly influenced the development of later cryptographic currencies and protocols, including Bitcoin.
Therefore, A. David Chaum is the correct answer, as he pioneered the use of blind signatures for anonymous digital currency.

QUESTION 25
When you purchase bitcoins, how are they stored?

A. In an exchange
B. As a file
C. As a hash
D. In a bitcoin wallet

Correct Answer: D
Section:
Explanation:
When you purchase bitcoins, they are stored in a bitcoin wallet. A bitcoin wallet is a digital tool that stores the cryptographic keys necessary to access and manage your Bitcoin holdings. It does not store physical bitcoins but instead holds the keys to access them on the blockchain.
Key Details:

Functionality of Bitcoin Wallets: Bitcoin wallets manage private and public keys. The private key is required to sign transactions, while the public key generates addresses that allow for receiving bitcoins. Without access to the private key, the user cannot spend or transfer their bitcoins.
Types of Bitcoin Wallets: Wallets can be software-based (such as mobile or desktop apps) or hardware-based (physical devices like a Ledger or Trezor). There are also online (custodial) wallets provided by exchanges, but these still technically store bitcoins within a wallet.
Not a Physical Storage: Bitcoins do not exist as physical files or objects. The wallet is an interface that interacts with the blockchain, where the actual records of ownership are maintained.
Thus, D. In a bitcoin wallet is the correct answer, as bitcoins are stored in wallets that hold the keys necessary to interact with the Bitcoin blockchain.

QUESTION 26
________is a word use to describe technologies which store, distribute and facilitate the exchange of value between users, either privately or publicly

A. DAO
B. Ledger
C. DLT
D. Blockchain

Correct Answer: C
Section:
Explanation:
Distributed Ledger Technology (DLT) is a broad term used to describe technologies that store, distribute, and facilitate the exchange of value between users, either privately or publicly. DLT encompasses various types of ledgers, including blockchains, where data is replicated, shared, and synchronized across a distributed network.
Key Details:
Definition and Scope: DLT refers to a digital system for recording transactions across multiple locations simultaneously. It allows for decentralized data management and reduces the need for a central authority to maintain a ledger.
Private and Public Ledgers: DLT can be implemented in both private (permissioned) and public (permissionless) networks. In public DLT, anyone can participate, while private DLT restricts access to authorized participants only.
Examples of DLT: Blockchain is one form of DLT, but other types include Directed Acyclic Graphs (DAGs) and Hashgraph. Each of these has unique mechanisms for data storage and consensus.
Therefore, C. DLT is the correct answer, as it is the term that broadly covers technologies used for the exchange and storage of value in distributed systems.