Eccouncil

312-82 Exam

EC-Council Blockchain Fintech Certification (BFC) Exam

Questions & Answers
Demo

Version: 4.0

Question: 1

Public blockchains most often use_____ as a consensus mechanism.

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

Answer: C

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: 2

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

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

Answer: C

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: 3

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

Answer: B

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: 4

_____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

Answer: A

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: 5

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

Answer: B

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.