DUMPSARENA

EC-CouncilBlockchain Fintech CertificationB|FC exam

ECCouncil 312-82

Version Demo

Total Demo Questions: 6

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Blockchain and FinTech	2
Topic 2, Understanding Blockchain	15
Topic 3, Understanding Cryptocurrency	11
Topic 4, Understanding Smart Contracts	7
Topic 5, Understanding DApps	6
Topic 6, Understanding Blockchain Platforms	5
Topic 7, Understanding Blockchain Use Cases	10
Topic 8, Blockchain and FinTech: Challenges and Future	4
Total	60

QUESTION NO: 1

A healthcare network is considering storing complete patient records directly on a shared blockchain. Which two concerns make an off-chain record repository with on-chain references and consent information more appropriate? (Select two.)

A. Patient records may require correction or updating

B. Sensitive information should not be replicated broadly among network participants

C. Blockchain nodes cannot record timestamps for access events

D. A blockchain cannot store references to external records

ANSWER: A B

Explanation:

Patient records may require correction or updating and **sensitive information should not be replicated broadly among network participants** are correct. Blockchain records are designed to be durable and tamper-evident, which makes direct storage of mutable clinical records difficult. Healthcare information also has stringent confidentiality requirements, and replicating complete records to multiple ledger nodes can create unnecessary privacy exposure.

On-chain hashes, pointers, consent records, and access-audit events can support integrity and traceability while the protected record is retained in an appropriate off-chain system. Encryption is important, but it does not remove the need to consider replication, access control, retention, and correction requirements.

QUESTION NO: 2

_____is one of the most widely used enterprise blockchain frameworks applicable across different industries.

A. Hyperledger Fabric

B. Microsoft Azure

C. Bitcoin

D. Ethereum

ANSWER: A

Explanation:

Hyperledger Fabric is one of the most widely used enterprise blockchain frameworks because it was specifically designed for permissioned business networks. Hosted by the Linux Foundation's Hyperledger project, Fabric supports known and authenticated participants, which lets organizations apply identity, access-control, governance, privacy, and audit requirements that are common in cross-organizational enterprise use cases. Its modular architecture allows network operators to select components such as membership services and consensus mechanisms according to operational requirements. Fabric also supports channels and private data capabilities, enabling authorized organizations to limit the visibility of sensitive transaction information while sharing a common ledger where appropriate. These characteristics make it suitable for applications in supply-chain traceability, trade finance, healthcare, manufacturing, retail, and other industries where multiple trusted organizations need to transact and maintain a tamper-evident record. The Hyperledger project describes Fabric as an enterprise-grade, permissioned distributed-ledger platform, and its documentation details its modular design and private-data features. See the Hyperledger Fabric project page and the Hyperledger Fabric documentation.

QUESTION NO: 3

Which two statements correctly distinguish Type I and Type II decentralized applications in the commonly used DApp classification? (Select two.)

A. A Type I DApp operates on its own blockchain

B. A Type II DApp uses the blockchain of a Type I DApp

C. A Type II DApp must always operate its own validator network

D. A Type I DApp can only be used for cryptocurrency exchange

E. A Type III DApp is the blockchain on which Type I DApps operate

ANSWER: A B

Explanation:

A Type I DApp operates on its own blockchain and **a Type II DApp uses the blockchain of a Type I DApp** are correct. Type I applications provide their own blockchain infrastructure and consensus environment. Type II applications are built on an existing Type I blockchain, such as a protocol or application deployed using Ethereum smart contracts.

A Type II DApp does not need to create a separate blockchain merely because it has its own token or specialized function. A Type III DApp is generally described as using the protocol of a Type II application, rather than serving as the blockchain foundation for all other DApps.

QUESTION NO: 4

Distributed ledger technology or DLT is a word used to describe technologies which store, distribute and facilitate the exchange of value between users, either privately or publicly.

A. Blockchain

B. Distributed Ledger Technology

C. Cryptocurrency

D. Consensus Mechanisms

ANSWER: B

Explanation:

“Distributed Ledger Technology” is correct because it is the umbrella term for systems in which records are shared, replicated, and synchronized across multiple network participants rather than maintained solely by one central administrator. These systems can record transfers of assets, ownership, credentials, and other forms of value, while providing participants with a consistent ledger state. DLT may be deployed in public, permissionless environments, where anyone can potentially participate under network rules, or in private/permissioned environments, where participation and access are controlled by an organization or consortium. This flexibility is why the term applies to technologies supporting value exchange in both public and private settings. Blockchain is one important implementation of DLT, but DLT is broader than a single data structure or network design. Depending on the implementation, a distributed ledger can use different methods to validate updates, establish agreement among participants, and preserve an auditable transaction history. The European Union Blockchain Observatory and Forum describes distributed ledger technologies as systems that enable the recording and sharing of data across multiple locations, participants, or entities, while NIST discusses blockchain as a type of distributed ledger technology. See the European Commission’s blockchain and distributed-ledger overview and NISTIR 8202, Blockchain Technology Overview.

QUESTION NO: 5

What is the primary way blockchain could help in the food industry?

A. Streamlining management

B. Eliminating food born illness

C. Making transactions more transparent

D. Making transport safer

ANSWER: C

Explanation:

Making transactions more transparent is the primary food-industry benefit because blockchain can provide a shared, tamper-evident record of relevant events as food moves through the supply chain. Producers, processors, distributors, retailers, regulators, and—in some implementations—consumers can access consistent provenance information, such as a product's source, batch, processing history, shipment details, and handling records. This visibility supports rapid traceability: when a quality or safety concern is identified, organizations can more efficiently determine the affected product path and isolate the relevant lots. It also helps participants substantiate claims about origin, ingredients, certifications, and handling, strengthening accountability across organizations that do not necessarily share a single internal database.

In food supply chains, the value is therefore not simply recording a payment or shipment; it is increasing trusted transparency and traceability among multiple parties. IBM describes blockchain-based food traceability as providing end-to-end visibility and enabling participants to trace food through the supply chain more quickly. The U.S. Food and Drug Administration likewise emphasizes traceability records as a means to identify the movement of foods and support faster removal of potentially contaminated products. See IBM Food Trust and the FDA Food Traceability Rule.

QUESTION NO: 6

An auditor must monitor the balances and incoming payments of a company's hierarchical deterministic wallet without being able to authorize any transfer. Which two items can the company provide to support this requirement? (Select two.)

A. The relevant public addresses

B. An extended public key

C. The recovery seed phrase

D. A private spending key

E. A transaction identifier from a previous payment

ANSWER: A B

Explanation:

The relevant public addresses and **an extended public key** are correct. A public address can be used to inspect the associated on-chain activity. An extended public key can derive a sequence of public keys and addresses for a hierarchical deterministic wallet, allowing an auditor to monitor multiple receiving addresses without receiving the corresponding private keys.

A private key or recovery seed would allow spending authority and must not be supplied to an observer. A transaction identifier identifies a particular transaction, but it does not provide continuing visibility into future activity for the wallet.