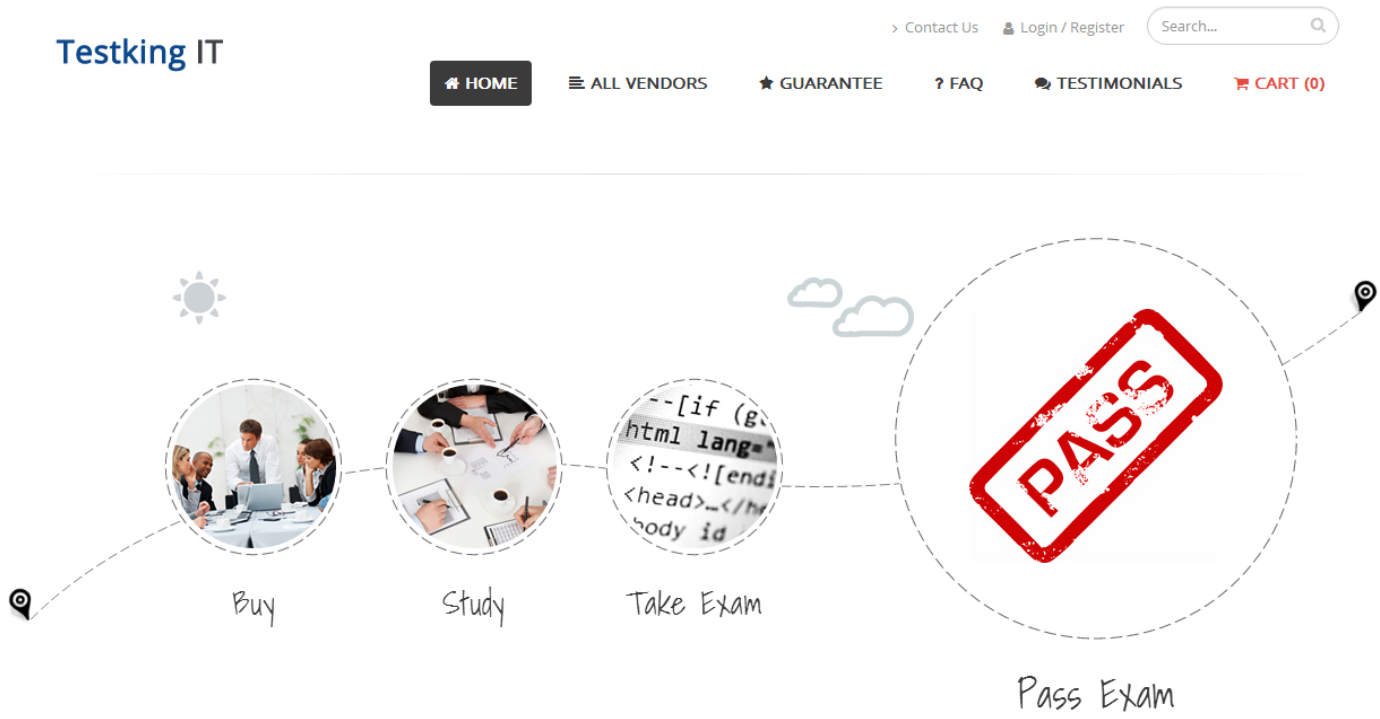
TestkingIT



Try **Desktop Test Engine** before you buy

We're not the only ones **happy** about TestKingsIT Practice Material ...

48236+ customers in 100+ countries use TestKingsIT Test Engine. Meet our customers.

iMessenger VOREED GetCustom JET ORANGE iCompany Paradoxx

http://www.testkingit.com/

Latest practice material - Exam Cram - TestKingIT

Exam : **HFCP**

Title : Hyperledger Fabric Certified Practitioner (HFCP) Exam

Vendor : Linux Foundation

Version : DEMO

NO.1 In Hyperledger Fabric, what data structures manage sensitive information between organizations?

A. Private data collections

B. State database

C. Ordering service

D. Endorsement policies

Answer: A

Explanation:

In Hyperledger Fabric, "private data collections" are used to manage sensitive information between organizations. This feature allows specified subsets of data to be shared among a defined group of network participants while keeping it hidden from others, thus maintaining confidentiality and privacy across the network. Private data collections enable organizations to transact privately without having to establish a separate channel, significantly reducing the overhead associated with channel management .

NO.2 What is the difference between chaincode, transaction, and block events?

A. Use setEvent, setTransactionEvent, setBlockEvent to emit chaincode, transaction and block events in the chaincode.

B. Chaincode events must be programmed in the smart contract, transaction and block events work out of the box

C. They are pretty much the same both regarding functionality and programming effort as well.

D. Block events must be programmed in the smart contract, chaincode events work out of the box.

Answer: B

Explanation:

In Hyperledger Fabric, chaincode events, transaction events, and block events serve different purposes and are emitted differently. Chaincode events must be explicitly programmed into the smart contract. Developers need to use thesetEventmethod within the chaincode to emit custom events that applications can listen to. On the other hand, transaction and block events are generated by the system automatically. These events notify listening applications of new blocks added to the chain or transactions included in blocks, without requiring any additional programming effort within the smart contracts.

NO.3 What happens if the user submits a transaction with no matching function?

A. The peer will have rejected the transaction.

B. Nothing, the transaction is ignored.

C. The first transaction function is called.

D. The unknownTransaction function is called.

Answer: D

Explanation:

In Hyperledger Fabric, if a user submits a transaction with no matching function specified in the smart contract, theunknownTransactionfunction is invoked by default. This function serves as a catch-all method that can be used to handle cases where the transaction type is not recognized, providing a mechanism to manage or log these occurrences effectively .

NO.4 Which ordering does Pluggable Consensus support for Hyperledger Fabric?

A. CFT (Crash Fault Tolerant) only

B. PCFT (Pure Crash Fault-Tolerant)

C. BFT (Byzantine Fault-Tolerant) only

D. Proof of BFT (Byzantine Fault-Tolerant)

Answer: A

Explanation:

Hyperledger Fabric supports pluggable consensus mechanisms that allow the system to be tailored to specific trust assumptions of a deployment. The platform allows for the implementation of various consensus protocols, including Crash Fault Tolerant (CFT) and Byzantine Fault Tolerant (BFT). However, the specific support for only CFT or BFT would depend on the implementation choice within the context of the deployment's trust model. Fabric's modular architecture supports well-established consensus protocols for both CFT and BFT .

NO.5 When creating a gRPC connection to the Gateway peer using Transport Layer Security (TLS), what information must be supplied by the client application?

A. The Gateway peer host name, service port number, and a TLS host name override.

B. A common connection profile that includes the Gateway peer address and TLS certificate.

C. The endpoint address of the Gateway peer and the certificate of the TLS certificate authority.

D. The client private key and the public key of the TLS certificate authority.

Answer: C

Explanation:

When creating a gRPC connection to the Gateway peer in Hyperledger Fabric using Transport Layer Security (TLS), the client application must supply the endpoint address of the Gateway peer and the certificate of the TLS certificate authority. This configuration is essential to establish a secure communication channel. The endpoint address specifies where the Gateway peer is located, which the client uses to connect. The certificate of the TLS certificate authority is crucial for validating the identity of the Gateway peer, ensuring that the connection is secure and that the data being transmitted is encrypted. This setup helps prevent man-in-the-middle attacks and ensures that sensitive data remains confidential during transmission.

NO.6 Each peer in the Hyperledger Fabric network hosts a copy of the ledger, which also belongs to what component?

A. The membership services

B. The Ordering node

C. The NoSQL databases

D. A member channel

Answer: D

Explanation:

In Hyperledger Fabric, each peer in the network hosts a copy of the ledger, which is associated with a member channel. The ledger itself is comprised of a blockchain to store the immutable, sequenced record in blocks, and a state database to maintain the current state of the ledger. There is one ledger per channel, and each peer maintains a copy of the ledger for each channel of which they are a member .