

100% Money Back
Guarantee

Vendor:Blockchain

Exam Code:CBSP

Exam Name:BTA Certified Blockchain Security
Professional

Version:Demo

QUESTION 1

Which of the following is designed to allow someone to prove they know a secret without revealing it?

- A. Confidential Transaction
- B. Ring Signature
- C. Zero-Knowledge Proof
- D. Stealth Address

Correct Answer: C

QUESTION 2

Which of the following attacks were enabled by design decisions made by the blockchain's developers? Select all that apply

- A. Bitcoin
- B. EOS
- C. Verge
- D. List

Correct Answer: CD

QUESTION 3

The Bitcoin hack demonstrated that there are circumstances in which the principles of blockchain must be violated to protect the blockchain.

- A. True
- B. False

Correct Answer: A

QUESTION 4

Which of the following is a takeaway from the pigeocoin/Bitcom Core hack?

- A. Importance of scanning code for common vulnerabilities
- B. Importance of cryptanalysis of algorithms used
- C. Import of system-level analysis

D. Import of a robust change management process

Correct Answer: A

QUESTION 5

Malware infections of blockchain nodes can compromise the security of the blockchain's consensus algorithm.

A. True

B. False

Correct Answer: A

QUESTION 6

Which of the following is NOT an essential part of Confidential Transactions?

A. Zero-Knowledge Proof

B. Ring Signature

C. Elliptic Curve Cryptography

D. Pederson Commitment

Correct Answer: A

QUESTION 7

Transactions can be added to DAG-based distributed ledgers without being validated but the same is not true for blockchain.

A. True

B. False

Correct Answer: A

QUESTION 8

Sidechains can benefit the mainchain in what ways? Select all that apply

A. Speed

B. Functionality

C. Scalability

D. Security

Correct Answer: BC

QUESTION 9

Which of the following blockchains uses a channel-focused architectural design?

A. Hyperledger

B. Corda

C. Ethereum

Correct Answer: A

QUESTION 10

Which of the following features were exploited as part of the Verge cryptocurrency hack? Select all that apply.

A. Mining Difficulty Update Function

B. Multiple Hash Functions

C. Timestamp Flexibility

D. Short Addresses

Correct Answer: AD

QUESTION 11

This sample code is vulnerable to which of the following attacks? Select all that apply A. Arithmetic

```
1 function withdraw(uint _amount) {
2     require(balances[msg.sender] - _amount > 0);
3     msg.sender.transfer(_amount);
4     balances[msg.sender] -= _amount;
5 }
```

B. Race Conditions

C. Unchecked Return Values

D. Short Addresses

Correct Answer: A

QUESTION 12

A blockchain-based solution best achieves which of the following goals?

A. Data control

B. Data deletion

C. Data retention

D. Data privacy

Correct Answer: C