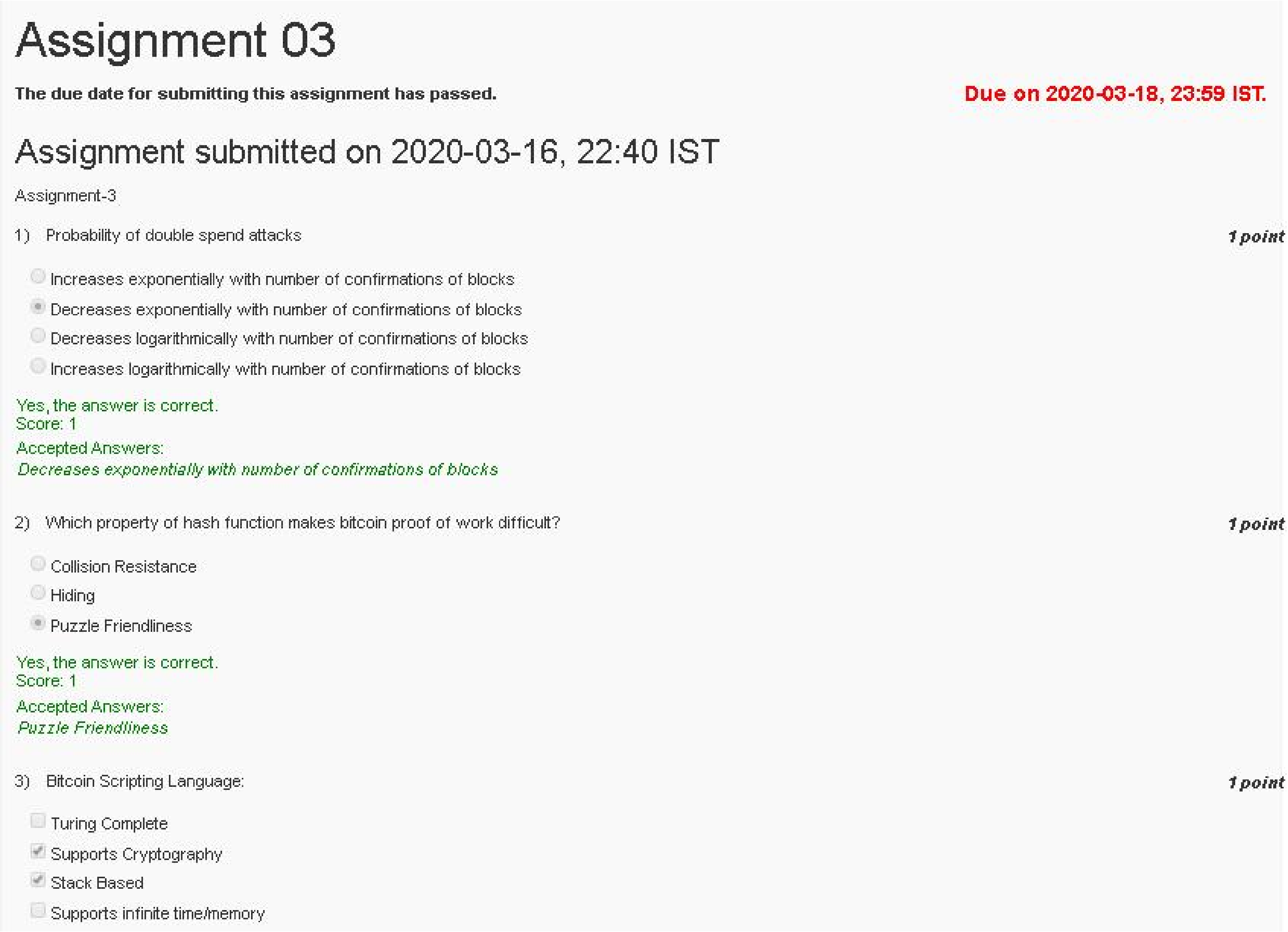


Assignment 03

The due date for submitting this assignment has passed.

Due on 2020-03-18, 23:59 IST.

Assignment submitted on 2020-03-16, 22:40 IST

Assignment-3

1) Probability of double spend attacks *1 point*

○ Increases exponentially with number of confirmations of blocks

● Decreases exponentially with number of confirmations of blocks

○ Decreases logarithmically with number of confirmations of blocks

○ Increases logarithmically with number of confirmations of blocks

Yes, the answer is correct.
Score: 1

Accepted Answers:
Decreases exponentially with number of confirmations of blocks

2) Which property of hash function makes bitcoin proof of work difficult? *1 point*

○ Collision Resistance

○ Hiding

● Puzzle Friendliness

Yes, the answer is correct.
Score: 1

Accepted Answers:
Puzzle Friendliness

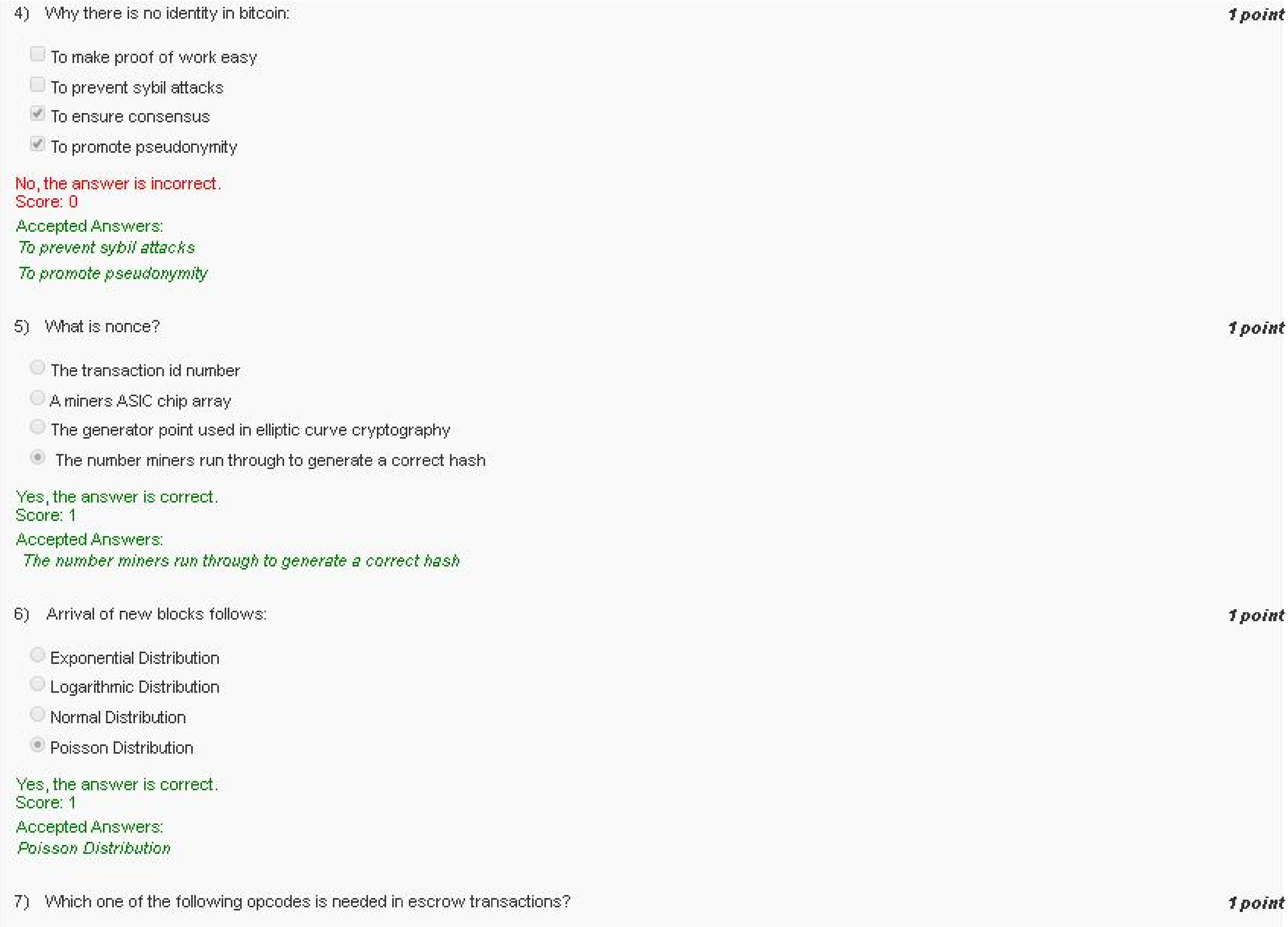
3) Bitcoin Scripting Language: *1 point*

□ Turing Complete

☑ Supports Cryptography

☑ Stack Based

□ Supports infinite time/memory



4) Why there is no identity in bitcoin: **1 point**

☐ To make proof of work easy

☐ To prevent sybil attacks

☑ To ensure consensus

☑ To promote pseudonymity

No, the answer is incorrect.
Score: 0

Accepted Answers:
To prevent sybil attacks

To promote pseudonymity

5) What is nonce? **1 point**

○ The transaction id number

○ A miners ASIC chip array

○ The generator point used in elliptic curve cryptography

● The number miners run through to generate a correct hash

Yes, the answer is correct.
Score: 1

Accepted Answers:
The number miners run through to generate a correct hash

6) Arrival of new blocks follows: **1 point**

○ Exponential Distribution

○ Logarithmic Distribution

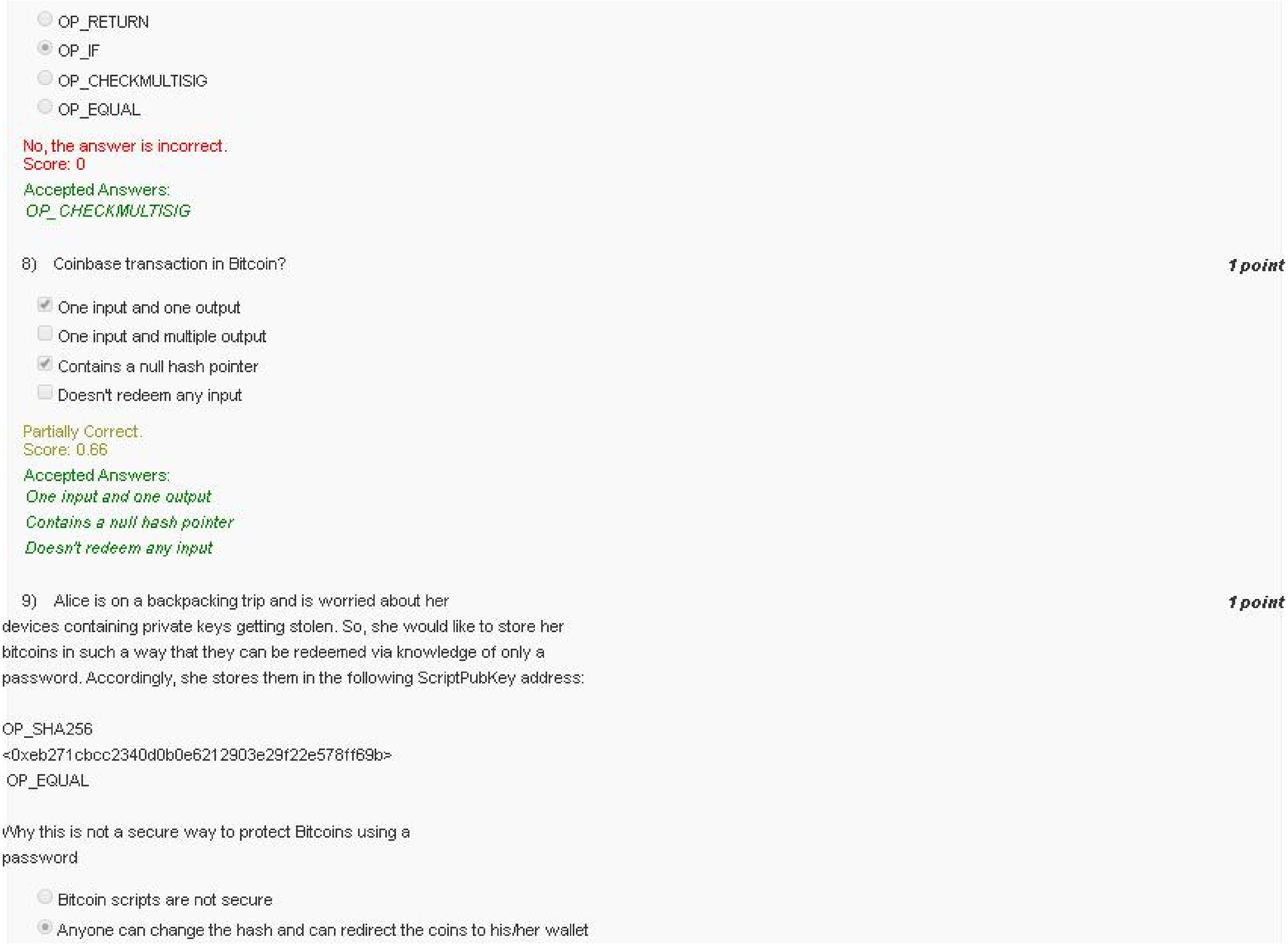
○ Normal Distribution

● Poisson Distribution

Yes, the answer is correct.
Score: 1

Accepted Answers:
Poisson Distribution

7) Which one of the following opcodes is needed in escrow transactions? **1 point**



○ OP_RETURN

● OP_IF

○ OP_CHECKMULTISIG

○ OP_EQUAL

No, the answer is incorrect.
Score: 0

Accepted Answers:
OP_CHECKMULTISIG

8) Coinbase transaction in Bitcoin? **1 point**

☑ One input and one output

□ One input and multiple output

☑ Contains a null hash pointer

□ Doesn't redeem any input

Partially Correct.
Score: 0.66

Accepted Answers:
One input and one output
Contains a null hash pointer
Doesn't redeem any input

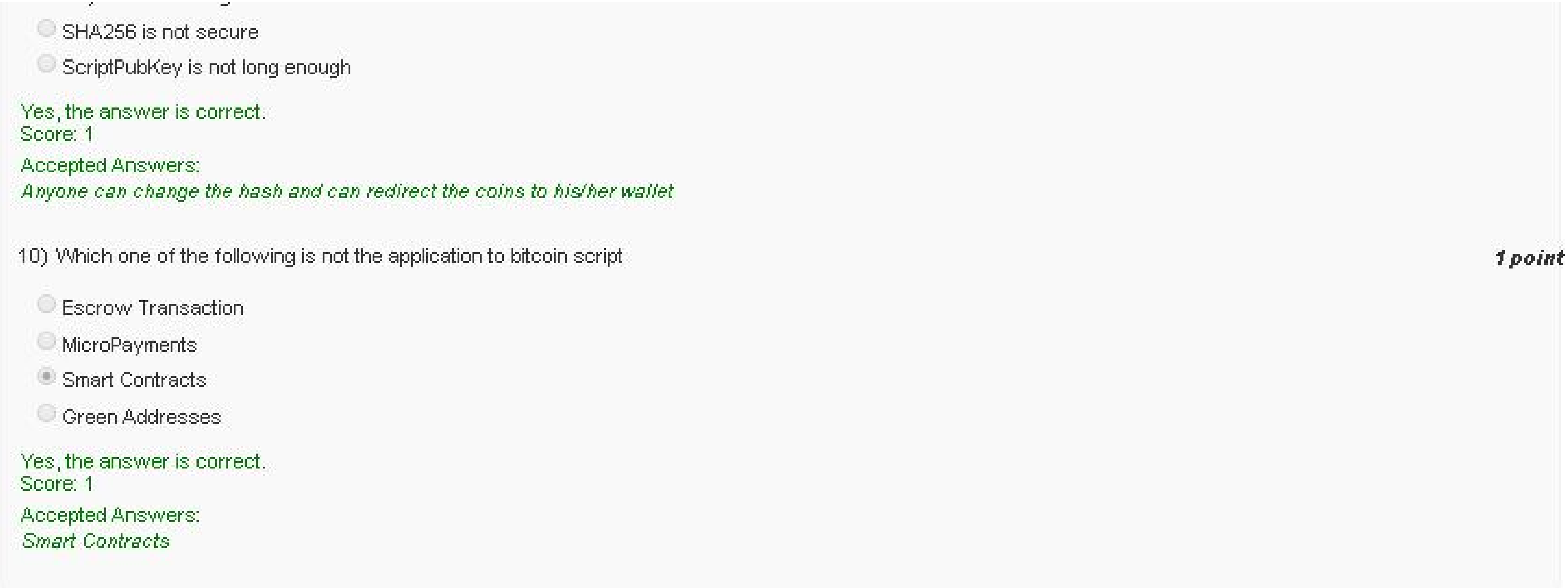
9) Alice is on a backpacking trip and is worried about her devices containing private keys getting stolen. So, she would like to store her bitcoins in such a way that they can be redeemed via knowledge of only a password. Accordingly, she stores them in the following ScriptPubKey address: **1 point**

```
OP_SHA256
<0xeb271cbcc2340d0b0e6212903e29f22e578ff69b>
 OP_EQUAL
```

Why this is not a secure way to protect Bitcoins using a password

○ Bitcoin scripts are not secure

● Anyone can change the hash and can redirect the coins to his/her wallet



○ SHA256 is not secure

○ ScriptPubKey is not long enough

Yes, the answer is correct.
Score: 1

Accepted Answers:
Anyone can change the hash and can redirect the coins to his/her wallet

10) Which one of the following is not the application to bitcoin script **_1 point_**

○ Escrow Transaction

○ MicroPayments

● Smart Contracts

○ Green Addresses

Yes, the answer is correct.
Score: 1

Accepted Answers:
Smart Contracts