Progress

Course outline

course work?

Week 0

WEEK 1

WEEK 2

WEEK 3

Lecture 6

Lecture 7

Lecture 8

Lecture 9

Lecture 10

WEEK 4

WEEK 5

WEEK 6

WEEK 7

WEEK 8

Lecture Notes

Text Transcripts

DOWNLOAD VIDEOS

Ouiz: Assignment 03

Assignment 03 Solution

Feedback For Week 3

NPTEL » Introduction to Blockchain Technology and Applications

1 point

Unit 6 - WEEK 3

How does an NPTEL online

The due date for submitting this assignment has passed. As per our records you have not submitted this assignment.	Due on 2020-03-18, 23:59 I
Assignment-3	
Probability of double spend attacks	1
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	
No, the answer is incorrect. Score: 0	
Accepted Answers: Decreases exponentially with number of confirmations of blocks	
2) Which property of hash function makes bitcoin proof of work difficult?	1
Collision Resistance	
Hiding	
Puzzle Friendliness	
No, the answer is incorrect.	
Score: 0 Accepted Answers:	
Puzzle Friendliness	
3) Bitcoin Scripting Language:	1
Turing Complete	
Supports Cryptography	
Stack Based	
Supports infinite time/memory	
No, the answer is incorrect. Score: 0	
Accepted Answers: Supports Cryptography	
Stack Based	
4) Why there is no identity in bitcoin:	1
☐ 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	
E) What is pages?	
5) What is nonce?	1
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 bash	
The number miners run through to generate a correct hash	
No, the answer is incorrect. Score: 0	
Accepted Answers:	

Score: 0 Accepted Answers: Poisson Distribution

Normal Distribution

Poisson Distribution

No, the answer is incorrect.

Arrival of new blocks follows:

Exponential Distribution

Logarithmic Distribution

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

OP_RETURN OP_IF

The number miners run through to generate a correct hash

OP_CHECKMULTISIG

OP_EQUAL

No, the answer is incorrect. Score: 0

Accepted Answers: OP_CHECKMULTISIG

8) Coinbase transaction in Bitcoin?

One input and one output

One input and multiple output Contains a null hash pointer

Doesn't redeem any input

Score: 0 Accepted Answers:

No, the answer is incorrect.

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:

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

No, the answer is incorrect. Score: 0

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 Escrow Transaction

 MicroPayments Smart Contracts

Green Addresses

No, the answer is incorrect. Score: 0 Accepted Answers:

Smart Contracts