

Unit 4 - WEEK 1

Course outline
How does an NPTEL online course work?
Week 0
WEEK 1
<div><div><div></div><div>Lecture 01</div></div><div><div></div><div>Lecture 02</div></div><div><div></div><div>Quiz : Assignment 01</div></div><div><div></div><div>Assignment 01 Solution</div></div><div><div></div><div>Feedback For Week 1</div></div></div>
WEEK 2
WEEK 3
WEEK 4
WEEK 5
WEEK 6
WEEK 7
WEEK 8
Lecture Notes
DOWNLOAD VIDEOS
Text Transcripts

Assignment 01

The due date for submitting this assignment has passed.
As per our records you have not submitted this assignment.

Due on 2020-03-04, 23:59 IST.

1) Which is NOT a part of asymmetric encryption?

Mining

Public key

Passphrase

Private Key

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

1 point

2) What are the properties of Blockchain?

Decentralized Systems

Distributed ledger

Double spending

No, the answer is incorrect.
Score: 0
Accepted Answers:
Decentralized Systems
Distributed ledger

1 point

3) Suppose you have eight data points -- 1 to 8. The post-order traversal of the Merkle Tree is given by (here 1 means hash of 1, 12 means the combined hash of 1 and 2, and so on):

{1,2,12,3,4,34,1234,5,6,56,7,8,78,5678,12345678}

{1,12,2,1234,3,34,4,12345678,5,56,6,5678,7,78,8}

{12345678,1234,12,1,2,34,3,4,5678,56,5,6,78,7,8}

{12345678,1234,5678,12,34,56,78,1,2,3,4,5,6,7,8}

No, the answer is incorrect.
Score: 0
Accepted Answers:
{1,2,12,3,4,34,1234,5,6,56,7,8,78,5678,12345678}

1 point

4) Disadvantage of the Symmetric key cryptology?

fast

key exchange

slow

key management

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

1 point

5) Which of the following is a *wrong* statement about a *cryptographic hash function*:

given the same message the hash function would return the same hash

it is difficult to generate the original message from the hash

a small change in the message does not impact the hash

it is difficult to find two different messages with same hash

No, the answer is incorrect.
Score: 0
Accepted Answers:
a small change in the message does not impact the hash

1 point

6) In order to prove "Transaction B" is a part of this merkle tree. What all hashes are needed?

Root Hash / Merkle Root

Hash AB

Hash CD

Hash A

Hash B

Hash C

Hash D

Transaction A

Transaction B

Transaction C

Transaction D

Hash B, Hash AB, Hash ROOT

Hash A, Hash AB, Hash CD

Hash A, Hash CD

Hash B, Hash CD

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

1 point

7) Security features of hash function?

puzzle-friendly

hiding

collision free

No, the answer is incorrect.
Score: 0
Accepted Answers:
puzzle-friendly
hiding
collision free

1 point

8) Which of the followings are negatives of Bitcoin?

High power Consumption

Highly Volatile

Repudiation

None

No, the answer is incorrect.
Score: 0
Accepted Answers:
High power Consumption
Highly Volatile

1 point

9) Can we use Memory Pointers to point to previous block in blockchain?

True

False

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

1 point

10) In which of the following cases we need Blockchain?

1. Do you need to store state?

2. Are there multiple writers?

3. Are all writers trusted?

4. Data need to be temper evident?

1. Yes

2. Yes

3. Yes

4. No

1. Yes

2. Yes

3. No

4. Yes

1. Yes

2. No

3. No

4. Yes

1. Yes

2. Yes

3. Yes

4. Yes

No, the answer is incorrect.
Score: 0
Accepted Answers:
1. Yes
2. Yes
3. No
4. Yes

1 point