開始日時	2023年 06月 8日(木曜日) 10:55
状態	終了
完了日時	2023年 06月 8日(木曜日) 11:04
所要時間	9 分 18 秒
評点	**36.00** / 100.00

問題 **1**

正解

6.00 / 6.00

Which instruction enables the implementation of escrow transactions

a. OP_CheckMultiSig: Checks multi-signatures ✔

b. OP_Hash216: Compute the hashes of three parties

c. OP_IdentitalVerify: Returns true if the inputs are identical

d. OP_Trip: Triples the top item on the stack

Your answer is correct.

正解:
OP_CheckMultiSig: Checks multi-signatures

問題 **2**

不正解

0.00 / 6.00

Which is not a consideration in choosing the location to setup a mining center for a cryptocurrency?

a. Electricity cost

b. Popularity of that cryptocurrency in that country

c. Network speed

d. Climate ✖

Your answer is incorrect.

正解:
Popularity of that cryptocurrency in that country

問題 **3**

不正解

0.00 / 6.00

Which is NOT true about Bitcoin’s language Script

- a. It is Turing incomplete ✖
- b. It has a set of basic arithmetic, basic logic and cryptographic instructions
- c. It is stack-based
- d. It can contain loops

Your answer is incorrect.

正解:
It can contain loops

問題 **4**

正解

6.00 / 6.00

Which is a form of consensus in Bitcoin

- a. Consensus about core developers
- b. Consensus about rules ✔
- c. Consensus about future blocks
- d. Consensus about the exchange rate

Your answer is correct.

正解:
Consensus about rules

問題 **5**

正解

6.00 / 6.00

Which is not a part of a Bitcoin transaction?

a. Input(s)

b. Metadata

c. Output(s)

d. Smart contract ✔

Your answer is correct.

正解:
Smart contract

問題 **6**

不正解

0.00 / 6.00

Which is not a major risk to handle for Bitcoin exchanges

a. Exchange range might fluctuate

b. It can be hacked

c. Too many people may show up ✖

d. It might lead to a Ponzi scheme

Your answer is incorrect.

正解: Exchange range might fluctuate

問題 **7**

不正解

0.00 / 8.00

What is true about virtual mining

- a. We need to spend real resources for security ✖
- b. It leads to centralization faster than other cryptocurrencies
- c. It is researched a lot scientifically
- d. It is better for the environment than traditional mining

Your answer is incorrect.

正解: It is better for the environment than traditional mining

問題 **8**

正解

6.00 / 6.00

Which is an advantage of GPU over CPU in mining Bitcoin

- a. Several of them can be cooled more systematically
- b. It can parallel-compute multiple hashes ✔
- c. GPU can compute floating points in SHA256
- d. It can be used by amateurs

Your answer is correct.

正解:
It can parallel-compute multiple hashes

問題 **9**

正解

6.00 / 6.00

Which is not a required property for general hash functions?

- a. It should be difficult to compute ✔
- b. Output should be a string of a fixed size
- c. It should be easy to verify
- d. It should be efficiently computable

Your answer is correct.

正解:
It should be difficult to compute

問題 **10**

正解

6.00 / 6.00

Which is true about the anonymity of Bitcoin

- a. It's anonymity is always good for the society
- b. It is anonymous
- c. It is pseudonymous ✔
- d. Its transactions are unlinkable

Your answer is correct.

正解:
It is pseudonymous

問題 **11**

不正解

0.00 / 6.00

Which is true about mining pools

- a. Pools contribute to decentralization because amateur individuals cannot compete ASICs but they can combine their power in pools ✖
- b. In reality, a pool member can easily leave the pool anytime
- c. Pool mechanism increases the variance in finding solutions increasing the chance to find more blocks
- d. System upgrade is made easier

Your answer is incorrect.

正解:
System upgrade is made easier

問題 **12**

不正解

0.00 / 6.00

Which is true?

- a. Bitcoin's puzzle is not memory hard
- b. We don't know any puzzle to be memory hard in solving but memory easy in verifying
- c. A cryptocurrency with a memory-hard and memory-bound puzzle is ASIC resistant ✖
- d. If we have a memory hard puzzle, we don't need powerful processors

Your answer is incorrect.

正解:
Bitcoin's puzzle is not memory hard

問題 **13**

不正解

0.00 / 6.00

Which is true?

- a. SHA-256 accepts fixed size input but applying Merkle-Damgard transformation, it can be used for cryptocurrency
- b. SHA-256 accepts fixed size input, so it can never be used for cryptocurrency
- c. SHA-256 is not collision-resistant but applying Merkle-Damgard transformation, it can be used for cryptocurrency
- d. SHA-256 accepts any arbitrary size input ✖

Your answer is incorrect.

正解:
SHA-256 accepts fixed size input but applying Merkle-Damgard transformation, it can be used for cryptocurrency

問題 **14**

不正解

0.00 / 6.00

Which is true about the anonymity of Bitcoin

- a. Minimizing the taint score implies a better anonymity ✖
- b. Side channels are good for deanonymization
- c. Unlinkability should be defined with respect to any general adversary
- d. Pseudonymity implies unlinkability

Your answer is incorrect.

正解:
Side channels are good for deanonymization

問題 **15**

不正解

0.00 / 6.00

Which is true about Bitcoin

a. Due to imperfections in the network, latency, etc., less than 51% of the hash rate can be sufficient to hack

b. Coins are fungible ✖

c. Miners check all fields of a transaction to verify it

d. History of coins does not matter

Your answer is incorrect.

正解:
Due to imperfections in the network, latency, etc., less than 51% of the hash rate can be sufficient to hack

問題 **16**

不正解

0.00 / 8.00

What is the core reason that ASIC resistance honey-moon took longer for Litecoin than that of Bitcoin?

a. Bitcoin was launched earlier

b. In Litecoin, every new block is found in 2.5 mins, while in 10 mins. in Bitcoin ✖

c. Bitcoin has always been more popular

d. Memory technology advances slower than processor technology

Your answer is incorrect.

正解:
Memory technology advances slower than processor technology

◄ 2023-1-BC-Presentation-Schedule

移動 ...