

- TA依照以下標準斟酌給分，若有總分算錯，或對評分方式有疑問，請找TA討論。

1.[8%] What advantages does a “decentralized” system have?

基本敘述對：+6

有寫到分散風險：+2

2.[8%] Explain the difference between permissioned distributed ledger and permissionless distributed ledger.

permissioned distributed ledger 的使用者需經過認證才可以參與網路 (挖礦 or 瀏覽帳本 or 交易 or ...)

3.[8%] Describe the relation between private key, public key, public key hash, and address.

private key → (ECDSA) public key

public key → (hash160) public key hash

public key hash ← → (base58 encode) address

一個箭頭：+2

加密演算法名稱不扣分

4.[8%] Without using a block explorer, how to find out the sender's address through a given transaction hash? (Hint: The rpc “getrawtransaction” can get the transaction's raw data.)

hw0 內容.

1. tx input裡面沒有address訊息(unlocking script 不需附上address), 需找出input tx id之後再拿一次getrawtransaction取得前一筆tx的output, 裏頭會有address.
2. 從tx input 裡取得public key, 透過hash160 + base58checksum 取得address.

5.

[3%](a). What is UTXO?

unspent transaction output : +3

以中文解釋 : +3

寫的很像, e.g. unspent output : +1

[5%](b). How does wallet-software get the balance of an address?

加總address的UTXO : +5

只提到掃blockchain : +2

只提到用API like getbalance來查詢 : +1

6. [10%] Describe how Bitcoin verify transaction's inputs. (Hint : Locking Script and Unlocking Script)

提到把locking script及unlocking script合起來檢查 : +5

提到用stack來evaluate locking script & unlocking script : +5

7.

[3%](a). Given a Transaction, how can we get its fee?

$\text{sum}(\text{inputs amount}) - \text{sum}(\text{outputs amount}) : +3$

寫反了, 寫成 $\text{sum}(\text{outputs amount}) - \text{sum}(\text{inputs amount}) : +2$

誤解成如何取得fee(miner挖礦可獲得reward) : +1

[5%](b). Describe why fee is necessary to bitcoin.

提到預防spam Tx及DDoS : +5

提到獎勵miner : +4

提到除了以上兩個以外有道理的理由 : +1

只提到「為了安全」: +2

8.

[8%](a). List the five types of "Standard Transactions".

P2PKH, Pay to PubKey, P2SH, Multisig, OP_RETURN, 少一個扣一分(所以就算沒寫也送你3分)

[6%](b). What is the purpose for OP_RETURN type transaction?

提到「用來紀錄info/data」 : +6

只提到替代fake UTXO : +3

提到save memory : +3