第一次 工作坊

重點知識懶人包

版本號	區塊數據的版本號
Previous Hash	指向前一個區塊的 Hash
Merkle Root	區塊內所有交易計算得出的 Hash
Timestamp	區塊產生時間
Difficulty	區塊產生難度
Nonce	PoW 演算法執行次數

Block

Header

Transactions

- 版本號
- 交易輸入總額
- 交易輸入地址
- 交易輸出總額
- 交易輸出地址
- 時戳

區塊裡的重要參數

Hash

不可逆、雪崩效應

Nonce

挖礦中就是不斷更動 Nonce 值來為區塊重新計算 Hash 值。

Difficulty

每次計算 Hash 值，只要滿足 Difficulty 設定之條件，即代表成功挖到礦。Difficulty 常定義為「Hash 前面至少要出現多少個零」(每產生一些區塊會調整一次難度)

區塊鏈的工作原理

交易方以私鑰簽章

交易生成、廣播給礦工

礦工以公鑰驗證，確認未被竄改

礦工將交易放到區塊裡

挖礦不斷更動 nonce 直到區塊的 hash 符合 difficulty

將區塊放上區塊鏈

第一次 工作坊

區塊鏈實作懶人包

前置處理

1. 確認已下載 python 與 python 編譯器
2. 在編譯器開啟工作坊的**資料夾**
3. 開啟 VS code 使用內部終端機

   (或是開啟終端機進入工作坊資料夾所在位置)
4. 安裝好所需函式庫

   ex: 輸入 pip3 install sockets 或 pip3 install rsa

python 安裝教程

當礦工端執行挖礦

1. **尋找自己的 IPv4** 填入 node.py 第 14 行
2. 若想創造全新的區塊鏈， node.py 第 16 行設 **True**
   若想加入別人的區塊鏈， node.py 第 16 行設 **False**
3. 在終端機輸入 **python node.py**
4. 如果你要加入別人的區塊鏈，請輸入你要和誰拷貝區塊鏈的資料

   (填寫他的 IPv4 以及 port)
5. **跳出問題 : 之前有錢包和鑰匙了嗎?(y/n)**
   - 選擇 y 輸入你的錢包地址與私鑰
   - 選擇 n 隨機生成地址與私鑰，生成完請將資訊記在記事本
6. 現在已經開始挖礦了~可以觀察終端機看看是誰挖到新的區塊！

第一次工作坊

區塊鏈實作懶人包

當客戶端執行交易

1. 在終端機輸入 **python client.py**
2. 跳出疑問：向誰拷貝區塊鏈？

   輸入**任何已開始挖礦的人之 Ip 與 port**
3. **跳出問題 : 之前有錢包和鑰匙了嗎? (y/n)**
   - 選擇 y 輸入你的錢包地址與私鑰
   - 選擇 n 隨機生成地址與私鑰，生成完請將資訊記在記事本
4. **功能一：確認帳戶餘額**
   - 輸入 1 獲得該帳戶的餘額
5. **功能二：轉帳**
   - 輸入 2 轉帳給指定的帳戶

常見問題

1. 執行 node.py 時出現 pickle error？
   A. 嘗試更換 node.py 第 15 行的 port (1111~1119 隨便)
2. 挖礦到一半出現連線中止，但程式仍在執行中？
   A. 不用理會該 error（想一下為什麼會發生？）
3. 挖礦到一半出現 Previous hash 不符合！
   A. 這是合理的結果，請從技術面思考為甚麼會發生
4. 其餘 error 請詢問小幫手

node.py 這幾行一定要針對自己的情況填寫正確

```
12  ###############這邊每個人都要修改成自己的################
13
14  your_IP = "127.0.0.1"    #請至 cmd 輸入 ipconfig 查詢 IPv4 位址並填入
15  your_port = 1111    #從 1111~1119 都可以試試看
16  first_miner = True    #你是第一個礦工嗎? 要自己創一個鏈請填寫 True 若要連別人鏈請填寫 False
17
18  ########################################################
```

your_IP

填寫自己的 IPv4 位址，別的礦工或是客戶要傳訊息給你的時候才能透過網路找到你的電腦。

your_port

電腦有很多通訊埠(port)用來和外界信息通訊，其中1111~1119通常沒被占用，隨機填寫其中一個就好，作為連線端口。

first_miner

如果你現在要自己建立一個區塊鏈(從創世區塊區塊開始挖)，請填True；

如果你想要加入組員建立的區塊鏈，和別人一起挖同一條鏈，請填False。