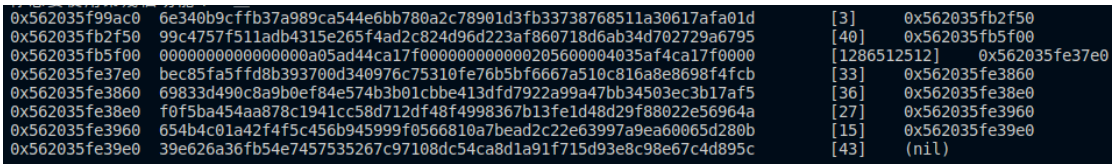
Result_report #4

通訊三、109208001、曾翎喬

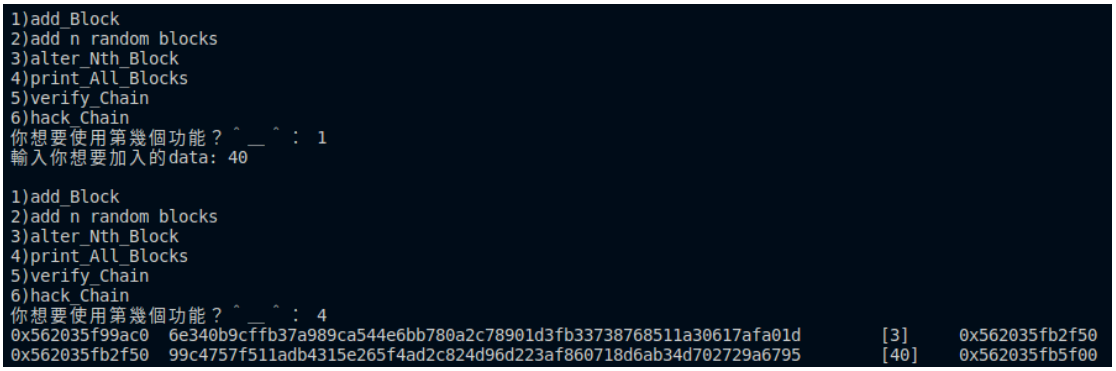
主要在建立 blockchain，共有六種功能，使用者可以根據想使用哪種功能，輸入對應的數字。

每次執行回圈一次，若印出 block chain 如下圖，則依序對應到的意義分別為：這個 block 的名稱，這個 block 的 hash 簽名，這個 block 包含的 data，這個 block 連接的下一個 block 的名稱，若接地則印出 nil。



【功能 1】：add_Block，輸入想要加入的 block data（以一個空的 chain 加入 data=3 為例，配合功能 4，可以看到這個 chain 有一個 block data=[3]）

（若再加入一個 block，則會加在尾端，而不是頭，3 的後面，非前面）

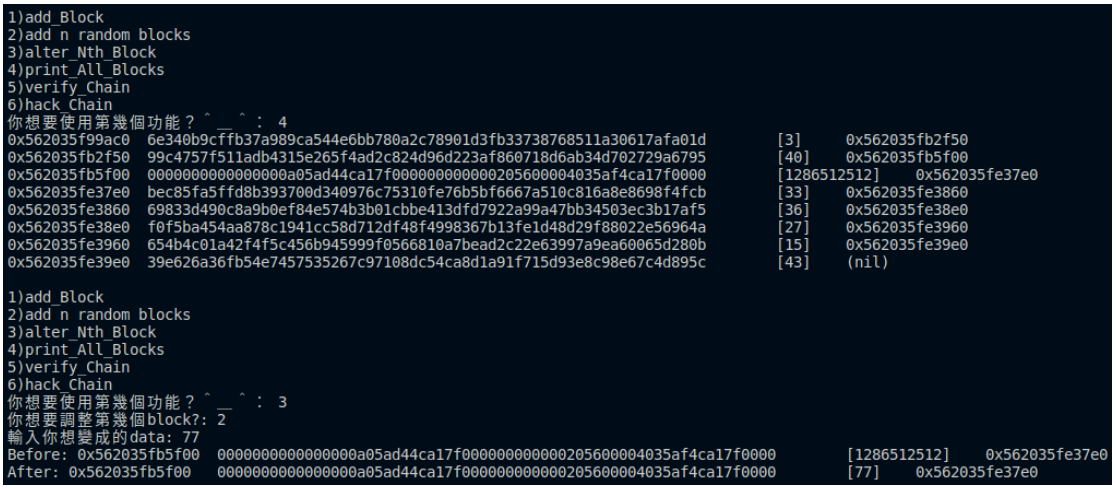


【功能 2】： add a random blocks，輸入想要加入幾個 block（以輸入想加入 5 (n)個 block 為例，則系統會隨機產生介在 0 ~ n*10 = 50 之間的五個 data，並將他們加入 blockchain 當中）

＊＊值得注意的是，當產生多個 block 時，我的程式設計會自動產生一個不可能的值，此例子為（1286512512）會被辨認不能加入 block 中，之後的功能五會用到這個設計。

【功能 3】：alter_Nth_Block，替換 data，輸入想要調整的 block 和想變成的 data。（若我想換第三個 data（[1286512512]），就輸入 block 2，因為 block 是從 0 開始計算）

＊＊可以發現，在調整前後，他的 block 名稱不會改變，表示前後連接的節點不變。他的簽名 hash 也不會改變。只有改變 block 的 data 而已。



【功能 4】：print_All_Blocks，就是印出現在 blockchain 的連接情形。

```
1)add_Block
2)add n random blocks
3)alter_Nth_Block
4)print_All_Blocks
5)verify_Chain
6)hack_Chain
你想要使用第幾個功能？ ^ __ ^ : 4
0x562035f99ac0  6e340b9cffb37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d        [3]     0x562035fb2f50
0x562035fb2f50  99c4757f511adb4315e265f4ad2c824d96d223af860718d6ab34d702729a6795        [40]    0x562035fb5f00
0x562035fb5f00  0000000000000000a05ad44ca17f0000000000002056000004035af4ca17f0000      [77]    0x562035fe37e0
0x562035fe37e0  bec85fa5ffd8b393700d340976c75310fe76b5bf6667a510c816a8e8698f4fcb        [33]    0x562035fe3860
0x562035fe3860  69833d490c8a9b0ef84e574b3b01cbbe413dfd7922a99a47bb34503ec3b17af5        [36]    0x562035fe38e0
0x562035fe38e0  f0f5ba454aa878c1941cc58d712df48f4998367b13fe1d48d29f88022e56964a        [27]    0x562035fe3960
0x562035fe3960  654b4c01a42f4f5c456b945999f0566810a7bead2c22e63997a9ea60065d280b        [15]    0x562035fe39e0
0x562035fe39e0  39e626a36fb54e7457535267c97108dc54ca8d1a91f715d93e8c98e67c4d895c        [43]    (nil)
```

【功能 5】：Verify_Chain，這邊是最難的地方！若簽名不同，則表示這個不是我要的交易，會印出「verification failed!」無法辨識。

＊＊延續上圖印出的結果，我們知道這個 chain 由八個 block 組成，然而事實上第三筆資料 77，原本是系統的亂數（1286512512），而後這個亂數再被 77 取代，所以 77 的（由前面幾個 block 產生的 hash）-（這個 block 指到的 hash 不一樣）兩個 hash 不一樣，表示這個 block 可能是別的買賣亂加的，不是我們要的正確交易。

＊＊因為第一筆資料（3）前面不會指到 block，所以此處由第二個 block（40）指到的 hash 開始印。

```
1)add_Block
2)add n random blocks
3)alter_Nth_Block
4)print_All_Blocks
5)verify_Chain
6)hack_Chain
你想要使用第幾個功能？ ^ __ ^ : 5
1       [40]    99c4757f511adb4315e265f4ad2c824d96d223af860718d6ab34d702729a6795 - 99c4757f511adb4315e265f4ad2c824d96d223af860718d6ab34d702729a6795 Verified!
2       [77]    010f8d9e83f87075c2e82bde5fa048148a733f9018a2f464f0ddb76e4de34c7b - 0000000000000000a05ad44ca17f0000000000002056000004035af4ca17f0000 Verificati
on Failed
3       [33]    5514b59a7b14840b2c7b67d7af831a6a539ba51f04ec510ba603ede9b6cee21d - bec85fa5ffd8b393700d340976c75310fe76b5bf6667a510c816a8e8698f4fcb Verificati
on Failed
4       [36]    69833d490c8a9b0ef84e574b3b01cbbe413dfd7922a99a47bb34503ec3b17af5 - 69833d490c8a9b0ef84e574b3b01cbbe413dfd7922a99a47bb34503ec3b17af5 Verified!
5       [27]    f0f5ba454aa878c1941cc58d712df48f4998367b13fe1d48d29f88022e56964a - f0f5ba454aa878c1941cc58d712df48f4998367b13fe1d48d29f88022e56964a Verified!
6       [15]    654b4c01a42f4f5c456b945999f0566810a7bead2c22e63997a9ea60065d280b - 654b4c01a42f4f5c456b945999f0566810a7bead2c22e63997a9ea60065d280b Verified!
7       [43]    39e626a36fb54e7457535267c97108dc54ca8d1a91f715d93e8c98e67c4d895c - 39e626a36fb54e7457535267c97108dc54ca8d1a91f715d93e8c98e67c4d895c Verified!
```

【功能 6】：hack_Chain，從錯誤的 hash（data=77）那邊開始，產生一系列新的 hash（如下圖一）。再次執行 verify，會發現所有的 block 都變成可辨識了～（如下圖二）

＊＊如果是一個想要賺這筆交易的 gas fee 的駭客，他想要讓大家相信這是一個合法的交易，所以他就由他自己加入的錯誤交易開始（1286512512），自己偽造一系列的簽名，讓別人都來加入他的 chain，這樣就可從中獲得 mining 的費用了。（這邊引用我自己推測的比特幣觀點～）

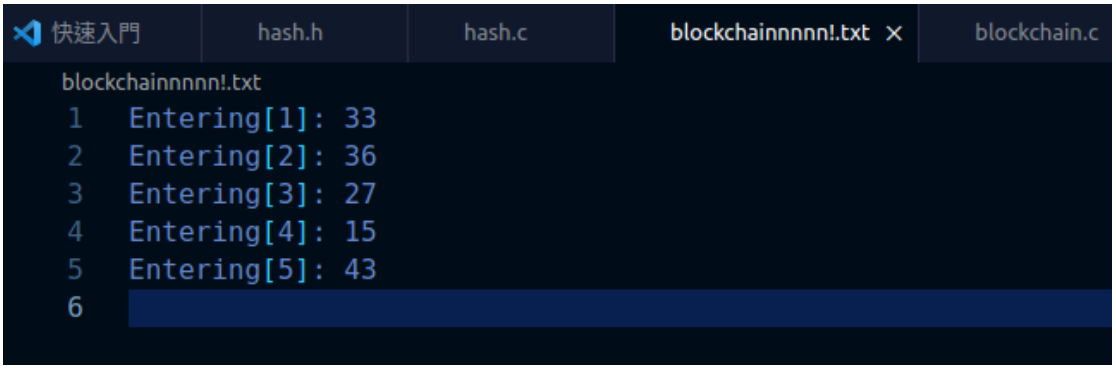
```
1)add_Block
2)add_n_random_blocks
3)alter_Nth_Block
4)print_All_Blocks
5)verify_Chain
6)hack_Chain
你想要使用第幾個功能？ ^__^ : 6
010f8d9e83f87075c2e82bde5fa048148a733f9018a2f464f0ddb76e4de34c7b
293c85c0620d94a8fee03a8a6ab49e9f0682e00391321611acfa3e53fbd931fa
6f3ee65879fe5c8ea03b0ff784dec81abcb0da681f4e8ff9bc784ac1a7da56f0
55c430d5347c440d71ffdbec8efaf10aab173c3da0274041c2fb3c9c97d054fa
e7156153fb24b9658666e9dcbcd79c33a99c09d116fb24fe8a9ac6031bd7e9dd
92a8e5659839b5779378884fc2db703ce77a926af8d0e3374197f91e73918f1a
```

（圖一）

```
1)add_Block
2)add_n_random_blocks
3)alter_Nth_Block
4)print_All_Blocks
5)verify_Chain
6)hack_Chain
你想要使用第幾個功能？ ^__^ : 5
1       [40]    99c4757f511adb4315e265f4ad2c824d96d223af860718d6ab34d702729a6795 - 99c4757f511adb4315e265f4ad2c824d96d223af860718d6ab34d702729a6795 Verified!
2       [77]    010f8d9e83f87075c2e82bde5fa048148a733f9018a2f464f0ddb76e4de34c7b - 010f8d9e83f87075c2e82bde5fa048148a733f9018a2f464f0ddb76e4de34c7b Verified!
3       [33]    293c85c0620d94a8fee03a8a6ab49e9f0682e00391321611acfa3e53fbd931fa - 293c85c0620d94a8fee03a8a6ab49e9f0682e00391321611acfa3e53fbd931fa Verified!
4       [36]    6f3ee65879fe5c8ea03b0ff784dec81abcb0da681f4e8ff9bc784ac1a7da56f0 - 6f3ee65879fe5c8ea03b0ff784dec81abcb0da681f4e8ff9bc784ac1a7da56f0 Verified!
5       [27]    55c430d5347c440d71ffdbec8efaf10aab173c3da0274041c2fb3c9c97d054fa - 55c430d5347c440d71ffdbec8efaf10aab173c3da0274041c2fb3c9c97d054fa Verified!
6       [15]    e7156153fb24b9658666e9dcbcd79c33a99c09d116fb24fe8a9ac6031bd7e9dd - e7156153fb24b9658666e9dcbcd79c33a99c09d116fb24fe8a9ac6031bd7e9dd Verified!
7       [43]    92a8e5659839b5779378884fc2db703ce77a926af8d0e3374197f91e73918f1a - 92a8e5659839b5779378884fc2db703ce77a926af8d0e3374197f91e73918f1a Verified!
```

（圖二）

<u>最後，每一次執行功能二都會印出一開始的 blockchain</u>



這次的專題好可惜，本來想要用 javascript 建立的 bitcoin 開源，甚至為了他看了好多天的 javascript 教學影片，但是我用的開源好像不能用 vscode 編譯，自己能改開源的地方也有限，受限於不太懂 javascript 語法。不過不能說毫無收穫，我也從觀看比特幣的一系列影片中，學習到比特幣的公鑰、私鑰的加密、block 連接，還有 P2P Network、socket 的概念，儘管最後沒有成功實踐，之後修獻聰的網概也可以再做一次這個主題～～