1.請解釋什麼是區塊鏈。(15分)

區塊練最早的概念是由Nakamoto Satoshi所發表的一篇” Bitcoin: A Peer-to-Peer Electronic Cash System”中所提出，當中提出了一種完全的點對點的電子現金系統，使的線上支付不需通過任何的金融機構，該網路以隨機散列的方式，將每一次的虛擬貨幣交易放入區塊當中，區塊鏈是交易紀錄的資料庫，是由區塊所構成，並且區塊鏈是由所有節點所共享，區塊產生並且串接到區塊鏈的過程即稱為挖礦，而產生區塊的電腦或人稱為礦工。

2.請解釋區塊鏈的交易為何可以避免被竄改。(15分)

只要大多數的CPU沒有合作起來對全網進行攻擊，那麼誠實的結點將會生程最常的，超過攻擊者的鏈條，只要誠實的結點控制了網路，檢驗機制就依然有效運作。

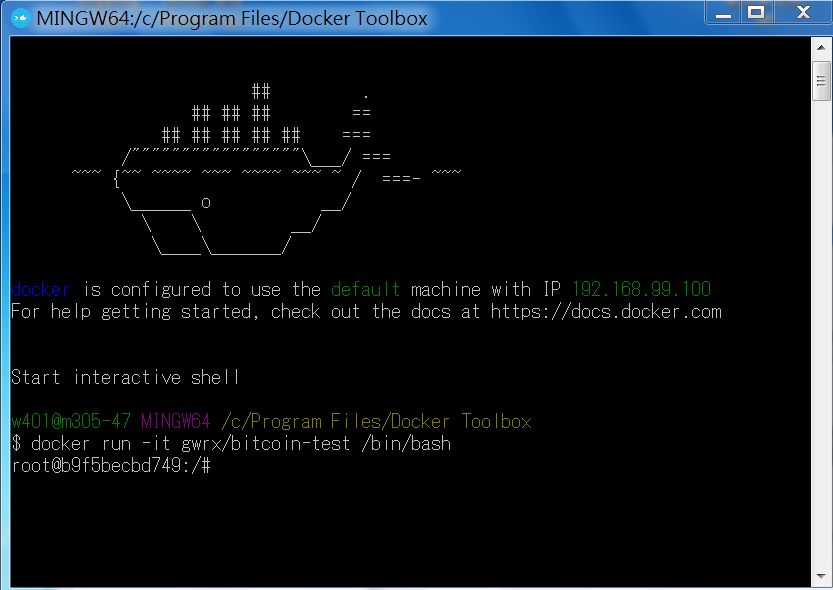
3.請比較比特幣與以太坊手續費的差異。(15分)

比特幣的設計使消費者可以輕鬆指定要支付多少的費用，而接收者指定費用更難且效率低，以太坊的手續費計算是，Gas Price(計算單位是Gwei) \* Gas Limit(交易上限)，手續費不夠交易會失敗，且付出去的手續費是無法回收的。

4.請下載比特幣錢包(<https://bitcoin.org/en/bitcoin-core/>)，進入regtest模式。先產生錢幣，接著是產生新位址，並且轉10塊錢給該位址，最後列出該交易的紀錄。每一步驟都需要寫出執行的命令與截圖，截圖方式請參考(http://esupport.trendmicro.com/solution/zh-TW/1114506.aspx)。(30分)

打開

輸入docker run -it gwrx/bitcoin-test /bin/bash



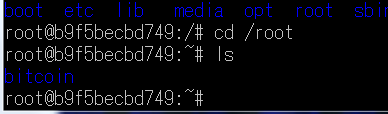
輸入ls指令會顯示<bin> <dev> <home>...



輸入cd /root回到root區



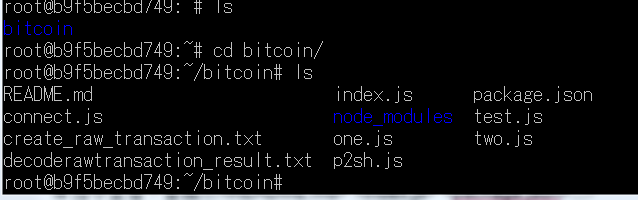
輸入ls指令會顯示只有一個<bitcoin>



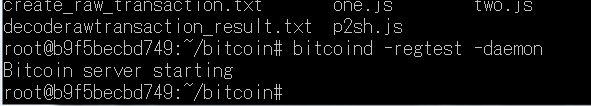
輸入cd bitcoin/進入bitcoin



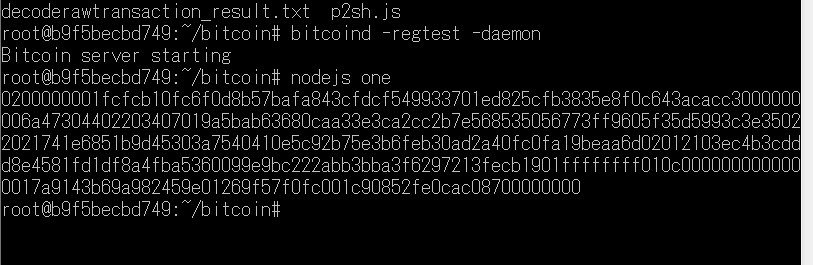
ls指令查看，會顯示<README.md> <index.js> <package.json>...



輸入bitcoind -regtest -daemon，會顯示Bitcoin server starting



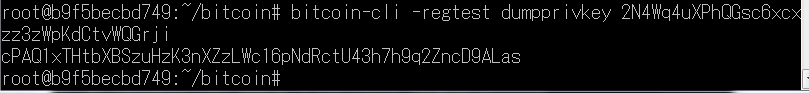
輸入nodejs one



輸入bitcoin-cli -regtest getnewaddress取得帳戶



輸入bitcoin-cli -regtest dumpprivkey + 剛剛的帳戶



增一個區塊bitcoin-cli -regtest generate <數字(10)>



輸入bitcoin-cli -regtest listunspent



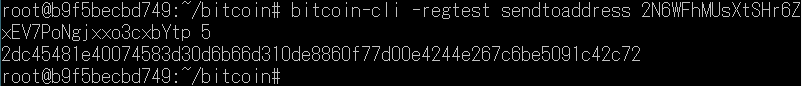




創建新位址



送錢爽一下bitcoin-cli -regtest sendtoaddress <帳戶> <數字>



5. 請利用老師提供的docker，然後請參考https://raw.githubusercontent.com/gwrxuk/bitcoin-core-test/master/one.js，自己撰寫一個js檔案，利用Github將程式碼放到docker當中。利用程式交易25塊錢給上一題當中產生的新位址。請將程式碼貼在答題的Word檔案當中，同時將執行結果截圖。(25分)

a.參考指令：

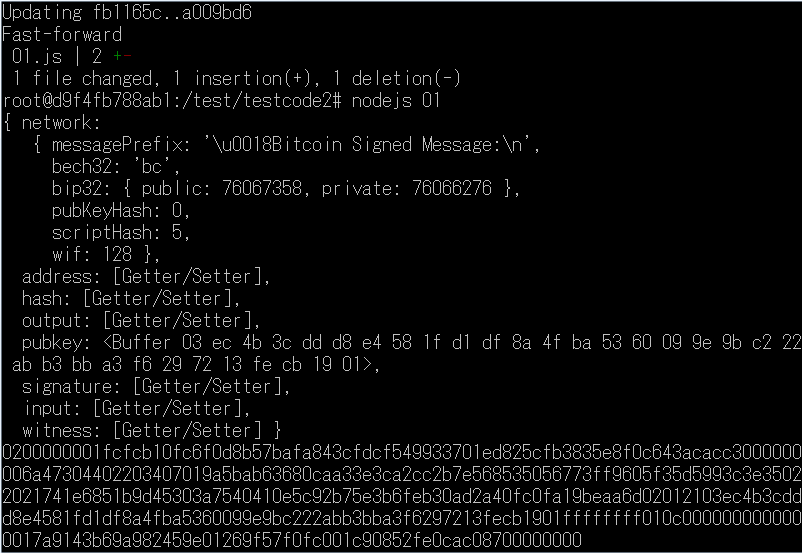
i.將Github的檔案下載到docker: git clone <github專案>

ii.如果Github的檔案有更新，重新下載到docker: git pull

iii.安裝 bitcoin函式庫: npm install --save  bitcoinjs-lib

iv.安裝bip65函式庫：npm install --save bip65

(我被斷網了，到底要斷我幾次，2次都要重來，什麼地址資料通通都不見。。。)



你在斷網阿!!!!!!!!!!!!!!!!!!!!!!!!

