1. 請解釋什麼是區塊鏈?

**簡單來說，區塊鏈是一種以分散式的架構來儲存資料的一種模式，每一個區塊內會存入一筆交易內容，在眾多的區塊前後互相連結則形成所謂的區塊鏈，而區塊鏈中，所產生的區塊，也就是每一筆的交易內容，不會透過第三方去做管理與認證的動作，所以區塊鏈技術又有項特點稱為「去中心化、不可竄改性」。**

1. 請解釋區塊鏈的交易為何可以避免被竄改。

**有鑑於區塊鏈是以去中心化的方式進行資料的驗證，我們可以清楚知道，其驗證的方式是透過多人驗證(5人以上)一筆資料，當這一筆資料被5人驗證過後，這筆資料才會真正的被寫入一個區塊之中，所以若是想要竄改資料，幾乎是不可能發生的。**

1. 請比較比特幣與以太坊手續費的差異。

**比特幣：手續費是根據交易的數據量來計價，而往往高單價的手續費就會吸引人去做處理，以至於高單價的手續費會越快被登記。當然，進行交易的人可以根據每一筆交易的時效性，將手上的手續費進行是當的調整。**

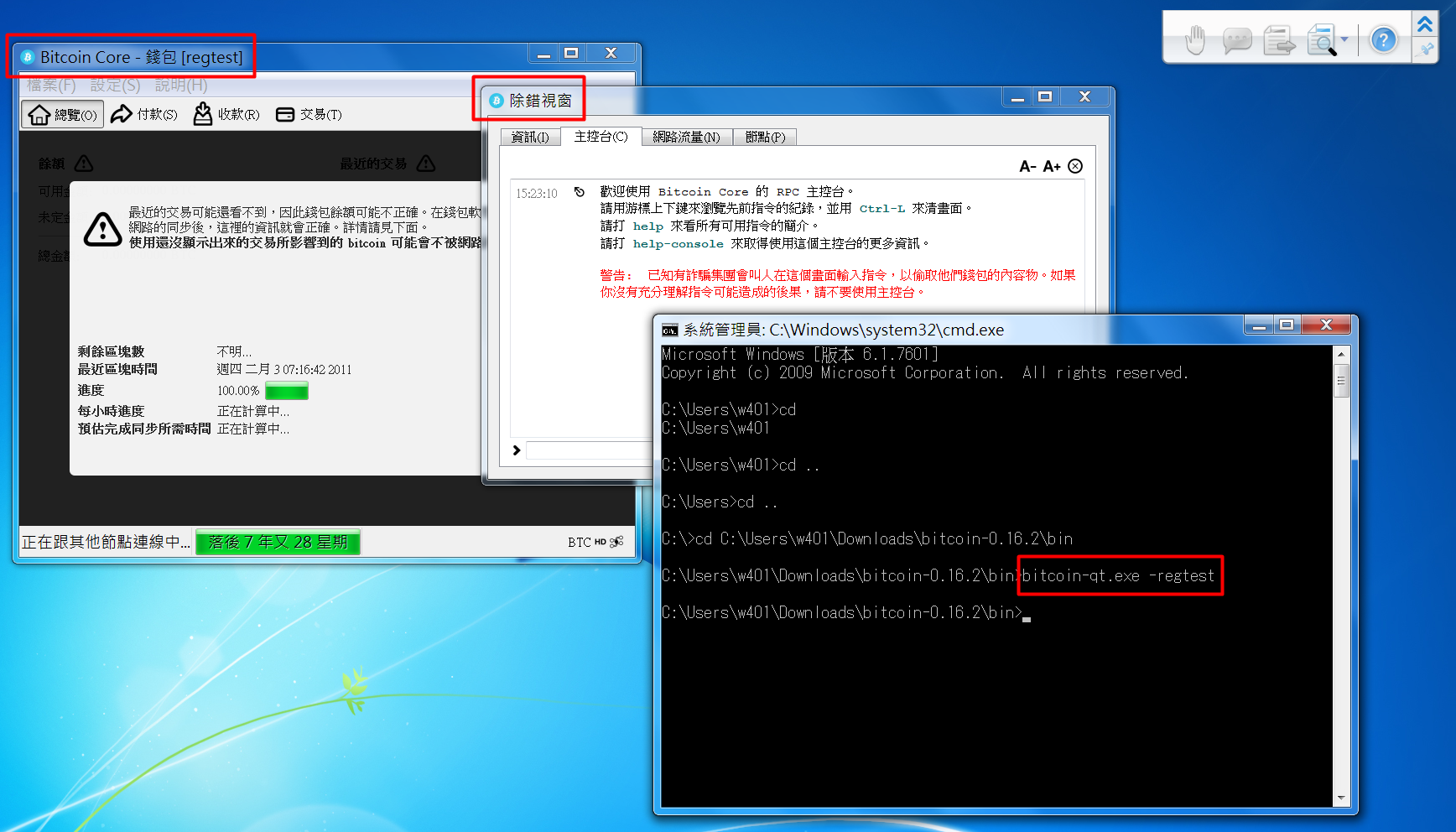
**以太坊：Gas為以太坊的手續費單位，而Gas Price其計算單位是Gwei，**

**Gas Limit則是交易上限，其手續費的計算方式= Gas Price\*Gas Limit。**

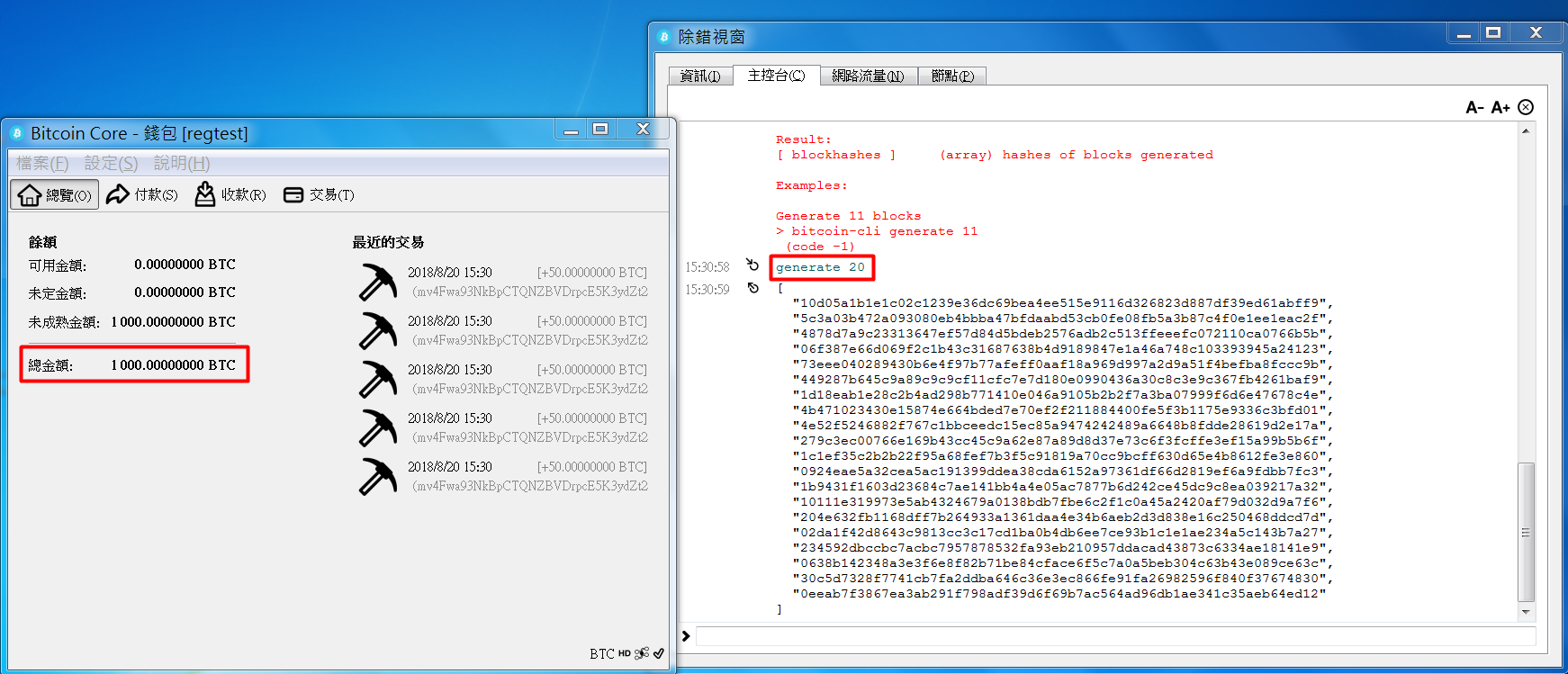
**當手續費不夠支付時，交易會失敗；若是已經付出去的手續費則無法進行回收，而以太坊的區塊大小會受限於每個區塊的Gas Limit(由挖礦者投票決定)**

1. 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)

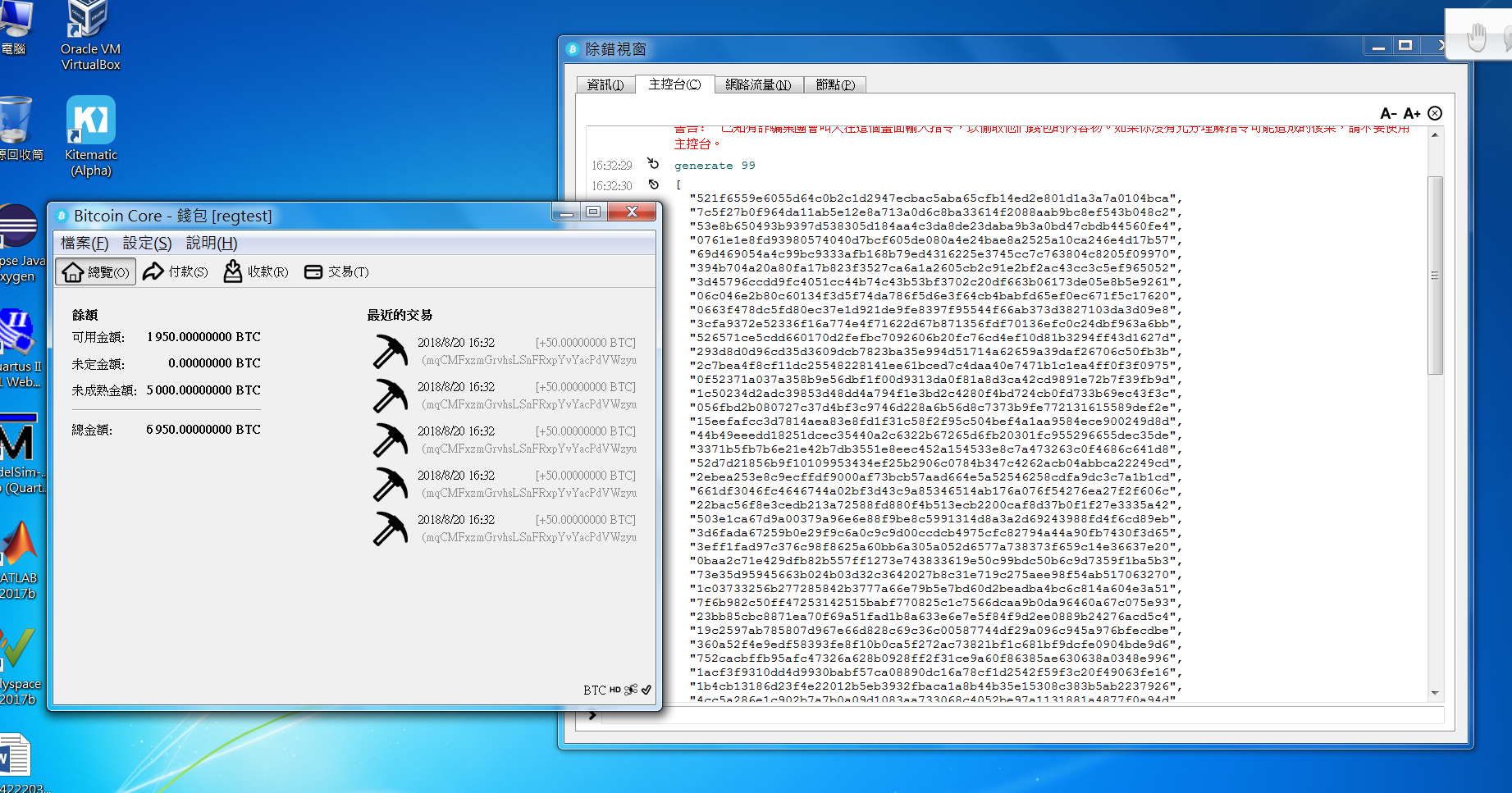
**>> 進入regtest模式 (bitcoin-qt.exe -regtest)**



**>> 產生錢幣 (generate 20)**



**>> 產生錢幣 (generate 99)**



**>> 產生新地址 (getnewaddress)**

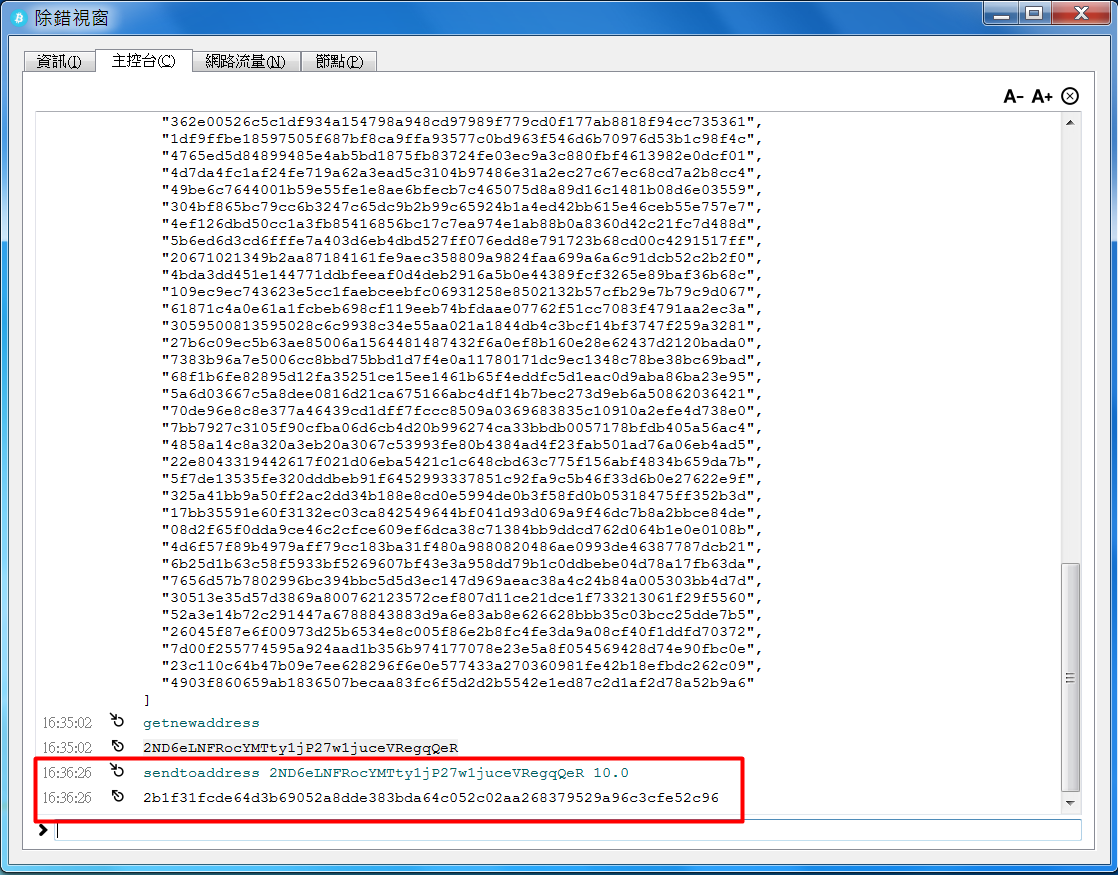
**Address🡪 2ND6eLNFRocYMTty1jP27w1juceVRegqQeR**



**//下一頁**

**>> 轉10塊錢給該位址**

**sendtoaddress 2MtkUkHc5F7sprtAcq3z4bkcLjzyKKWuxgc 10.0**



**>> 列出該交易的紀錄**

**listunspent**



1. 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)
2. 參考指令：
3. 將Github的檔案下載到docker: git clone <github專案>
4. 如果Github的檔案有更新，重新下載到docker: git pull
5. 安裝 bitcoin函式庫: npm install --save  bitcoinjs-lib
6. 安裝bip65函式庫：npm install --save bip65

**# bitcoind –regtest -daemon(啟動bitcoin server)**

**#nodejs one (開啟one.js)**

