A104222031 資科四甲 李幸容

(有多傳一份pdf檔，如果版面亂掉請老師直接看pdf檔案)

1. 請解釋什麼是區塊鏈:

是一個利用點對點網路建立的交易，所以無需第三方信任單位即可對交易進行檢驗。

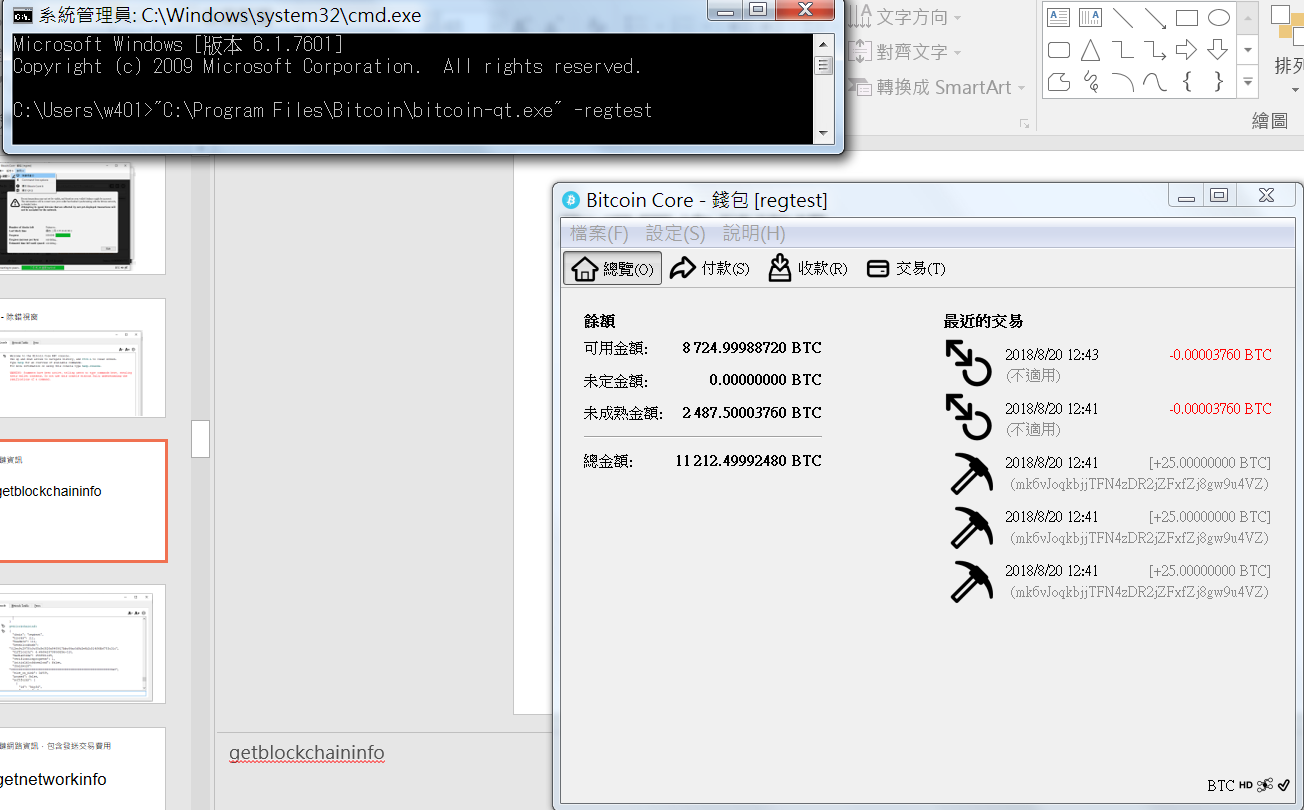
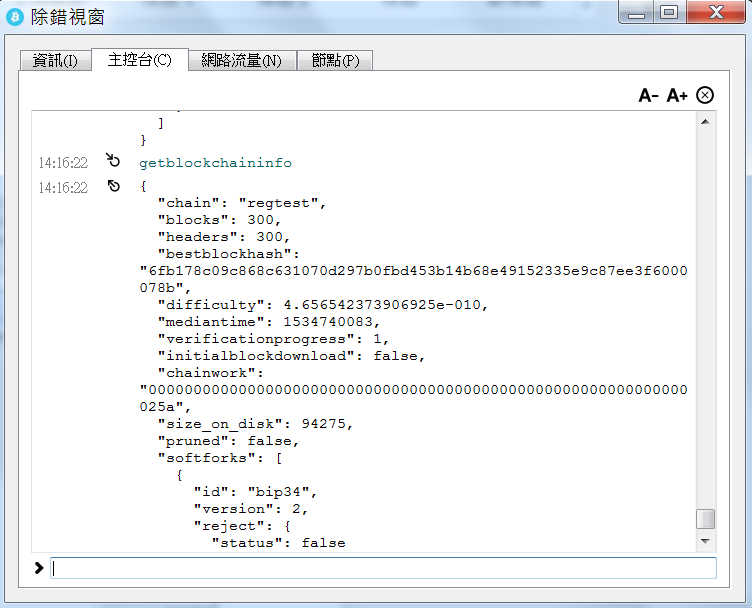
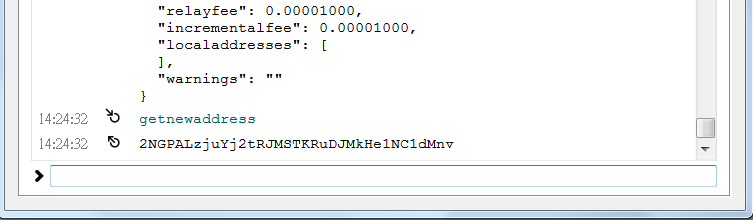
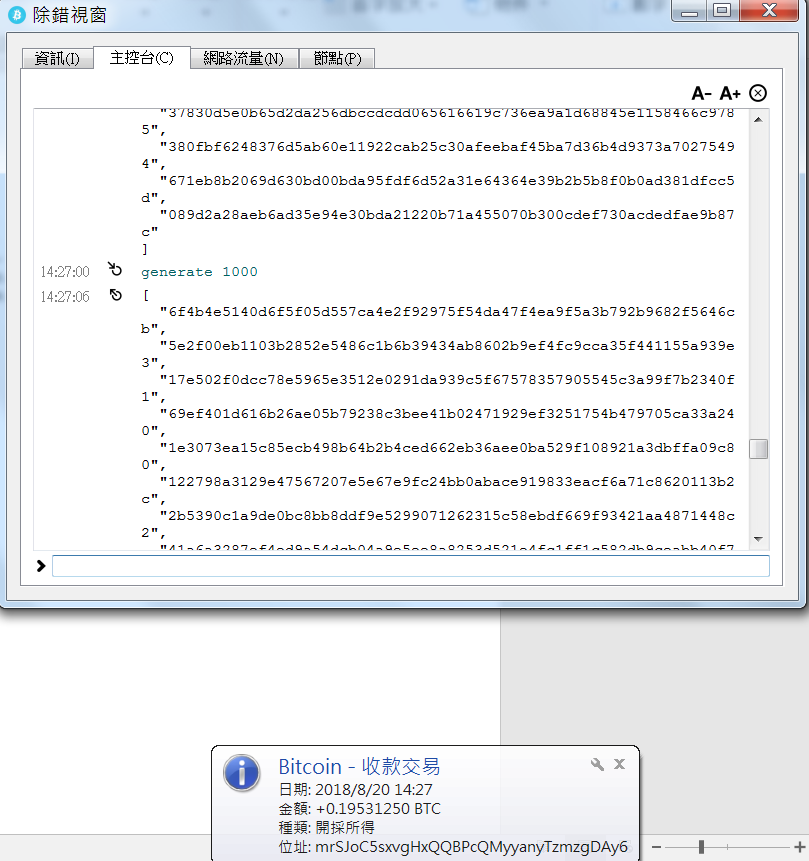
區塊鏈將每一次的虛擬貨幣的交易放入區塊當中，當完成產生區塊所需要的計算過程之後，將區塊與其他區塊串接一起的，成為區塊鏈（Blockerchain）一部分。因此區塊鏈就是用來儲存比特幣交易紀錄的帳本，同時也是防衛竄改交易紀錄的防衛系統。

1. 請解釋區塊鏈的交易為何可以避免被竄改:

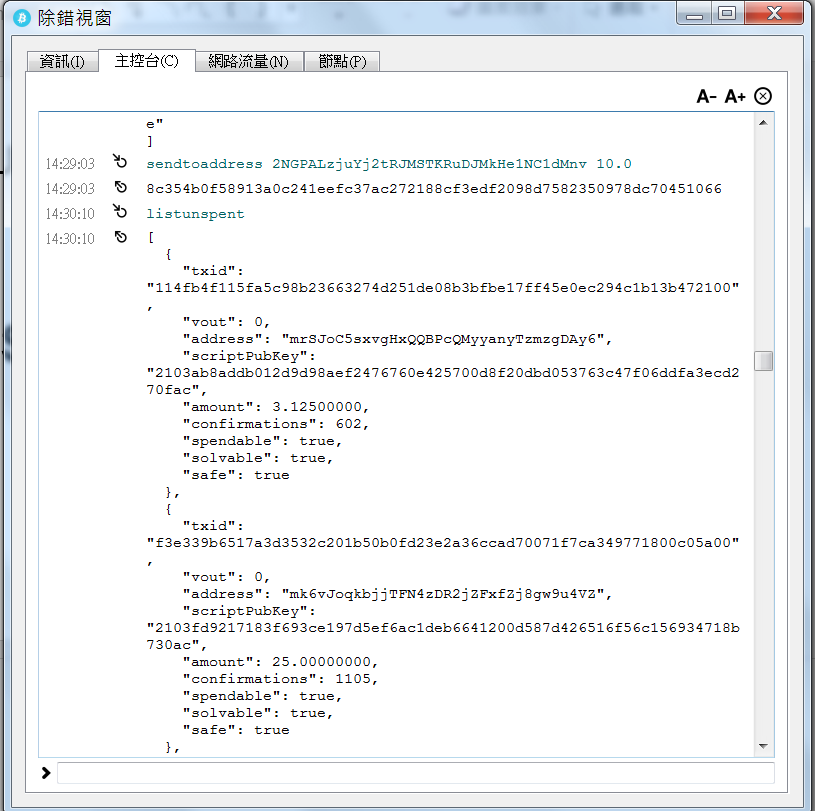
因為區塊鏈交易會將每次的交易記錄在區塊上，而每筆交易後都會產生一個僅限當筆交易的亂數碼，利用這筆亂碼即可判斷交易資料有沒有經過竄改。

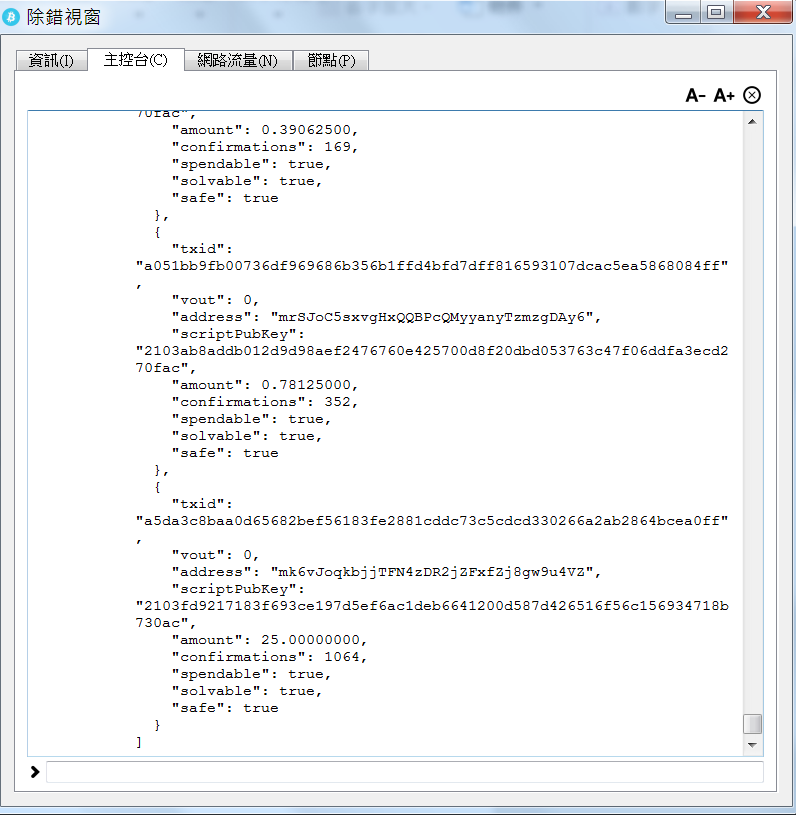
1. 請比較比特幣與以太坊手續費的差異:

比特幣交易由越高手續費者越快速完成交易，以太坊則根據交易價格調整手續費，因此比特幣只要花大錢提高手續費就可以享有不壅擠的網路交易速度，而相反以太坊無法提高手續費，就有可能因為過多垃圾交易造成交易堵塞。

1.  用regtest模式進入比特幣錢包
2. 取得區塊鏈資訊
3. 取得區塊鏈網路資訊及發送交易費用
4. 取得新位址
5. 獲取錢幣
6. 轉給自己10塊



1. 列出交易紀錄



(因為中間有測試所以有很多筆記錄，只截了最前面和最後面)

//引入bitcoin模組

const bitcoin = require("bitcoinjs-lib");

//選用regtest網路

const regtest = bitcoin.networks.testnet

//https://github.com/bitcoinjs/bip65

const bip65 = require('bip65')

//輸入私鑰，教學用，請勿隨意公開私鑰

var privateKey = "cNcvQphXWjAJ365Y8Tuhti5a6fCh9ftpR3GScZs5vdidBwQqpxT4";

//產生公鑰跟私鑰

const keyPair = bitcoin.ECPair.fromWIF(privateKey,regtest);

//產生付款位址

const { address } = bitcoin.payments.p2pkh({ pubkey: keyPair.publicKey });

console.log(bitcoin.payments.p2pkh({ pubkey: keyPair.publicKey }));

const txb = new bitcoin.TransactionBuilder(regtest);

//用listunspent 取出最後一筆資料的txid

txb.addInput('a5da3c8baa0d65682bef56183fe2881cddc73c5cdcd330266a2ab2864bcea0ff', 0);

//用getnewaddress取得新的位址

txb.addOutput('2NGPALzjuYj2tRJMSTKRuDJMkHe1NC1dMnv', 25)

//交易簽名

txb.sign(0, keyPair); //第一個位置的是上一筆交易中的第一個支出，第二個欄位是我們的公鑰與私鑰

//取得交易序號

const transaction\_01 = txb.build().toHex();

console.log(transaction\_01);

