1. 區塊鏈是一個分散式的帳本，以最後的活頁夾做為基準，有更厚的會複製別人的，可避免雙重花費，提出點對點網路，無須第三方信任的單位來檢驗交易是否成立，會把交易紀錄記錄下來，並放入區塊中，每個區塊都會有一個雜湊值，將每個區塊串接在一起便可形成區塊鏈，依最長的為主鏈。
2. 區塊鏈的特性為去中心化、匿名性、不可沒滅性，每一筆交易都會產生一個新的位址，也需要公鑰與私鑰，而交易紀錄會廣播到網路上，並收到區塊內，區塊至少需要串接六個才算是交易成功，每個交易紀錄的區塊都有一組由數字與英文所產生的雜湊值，當某個區塊在內容上有做任何更改也會產生一個新的雜湊值(鑰匙)，雜湊值計算很花時間也很難驗算。

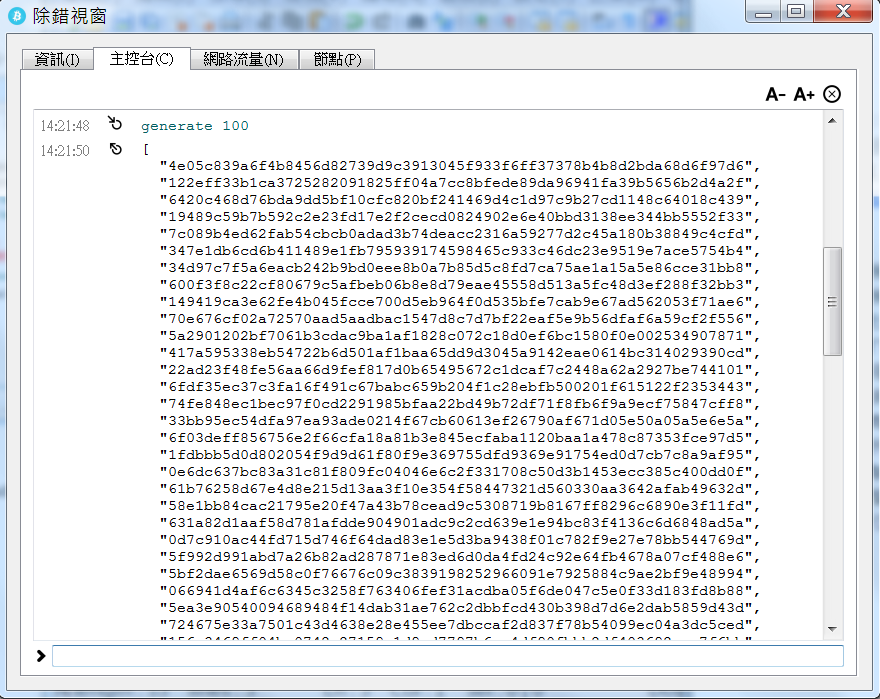
3.

比特幣：使用挖礦的方式來發行，使用私鑰做為數位簽章，允許直接支付給他人，不須經過第三方機構，避免了高手續費、繁瑣流程與受監控的問題。

以太坊手續費：使用以太幣來支付手續費，為私有鏈，區塊鏈不是每個人都可以看到，使用者使用以太幣來分配和支付電腦的使用權，以太幣可在許多加密貨幣的外匯市場上交易，但是對其他實體貨幣的匯率可能會在短時間有大幅度變化，透過智慧合約，可協助驗證合約的談判與執行，需要執行程式的人支付手續費。

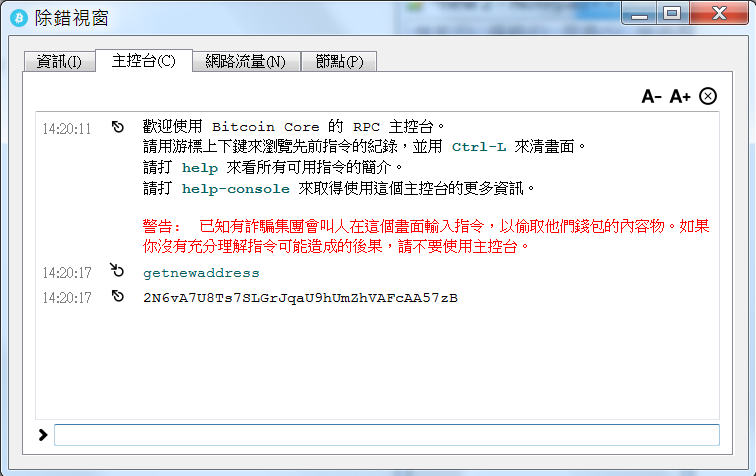
4.

**generate 100**



**getnewaddress**

2MuE8VNbHwa1byaqaiUCMU9CTyeGBhfZFPi



**sendtoaddress 2MuE8VNbHwa1byaqaiUCMU9CTyeGBhfZFPi 10**

付錢





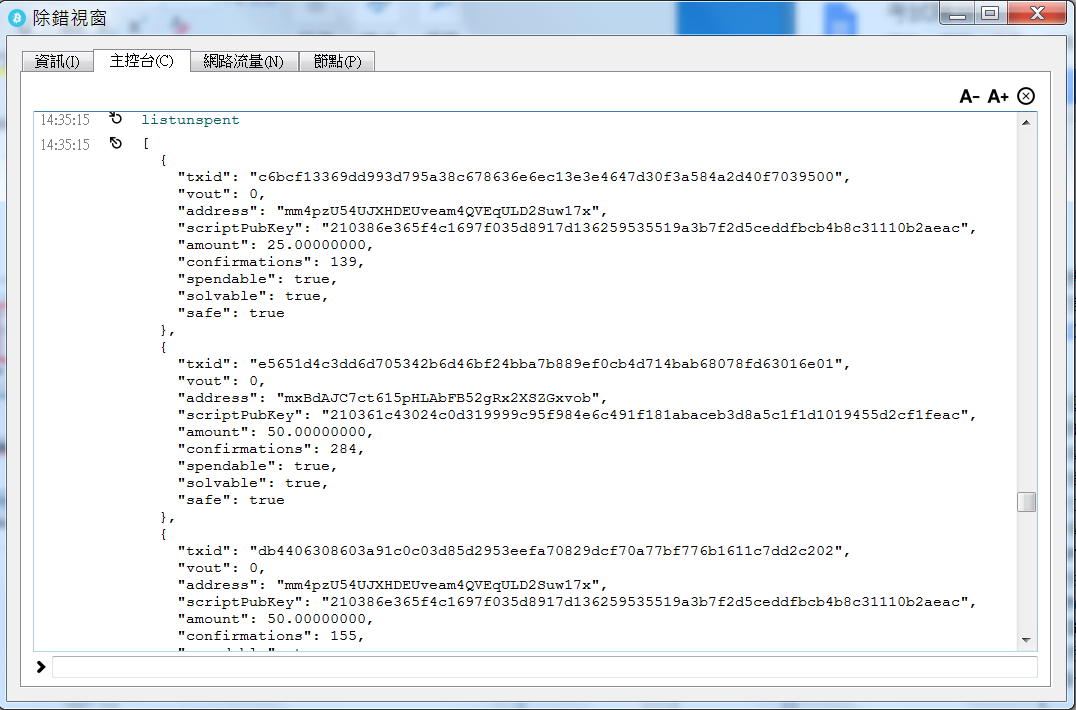
**generate 1**

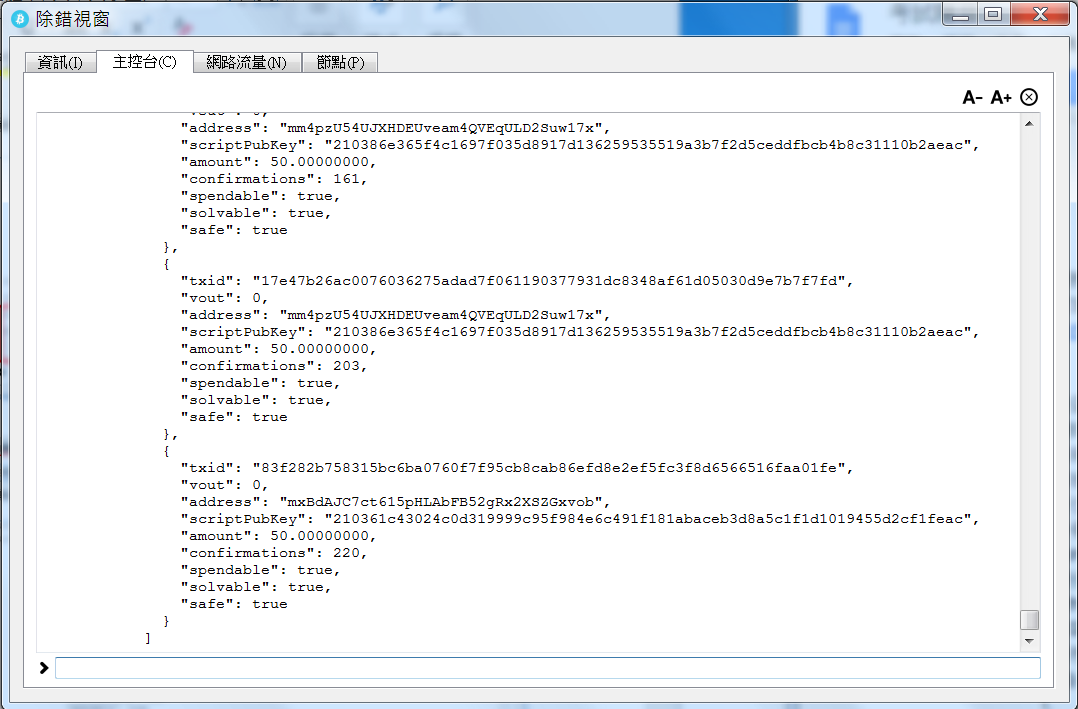
收款





**listunspent**





5.

**one.js**

//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 = "cPAQ1xTHtbXBSzuHzK3nXZzLWc16pNdRctU43h7h9q2ZncD9ALas";

//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('c3acac43c6f0e83538fb5c82ed01379349f5dccf43a8af7bb5d8f0c60fb1fcfc', 0);

//用getnewaddress取得新的位址

txb.addOutput('2MuE8VNbHwa1byaqaiUCMU9CTyeGBhfZFPi', 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);

**# nodejs one**

