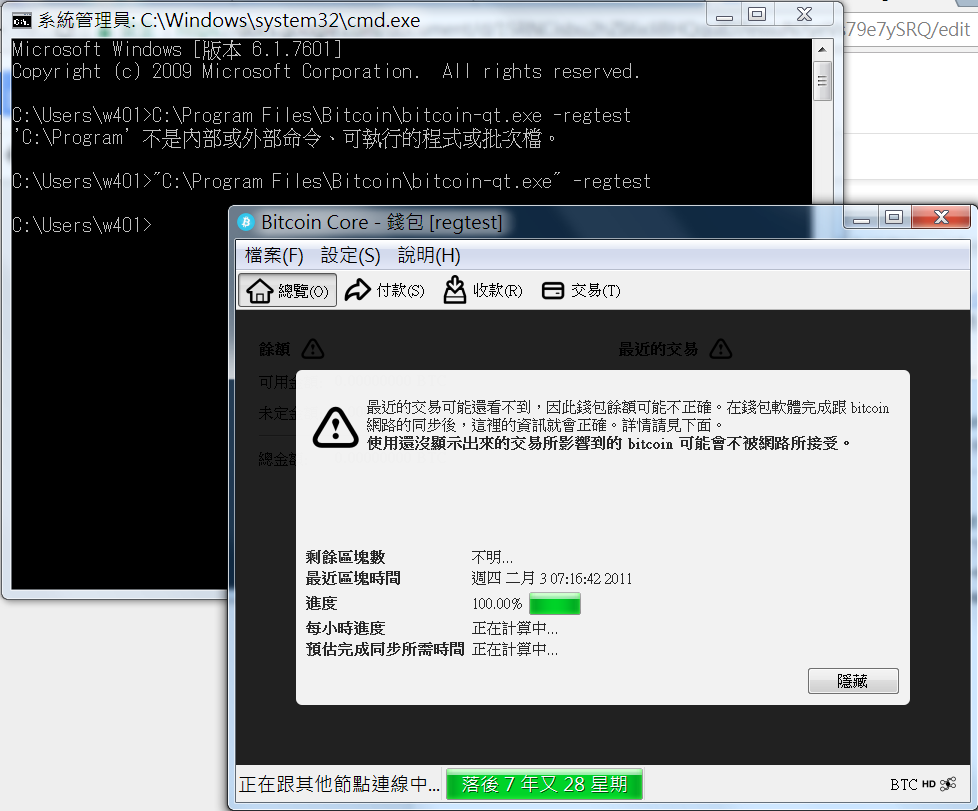
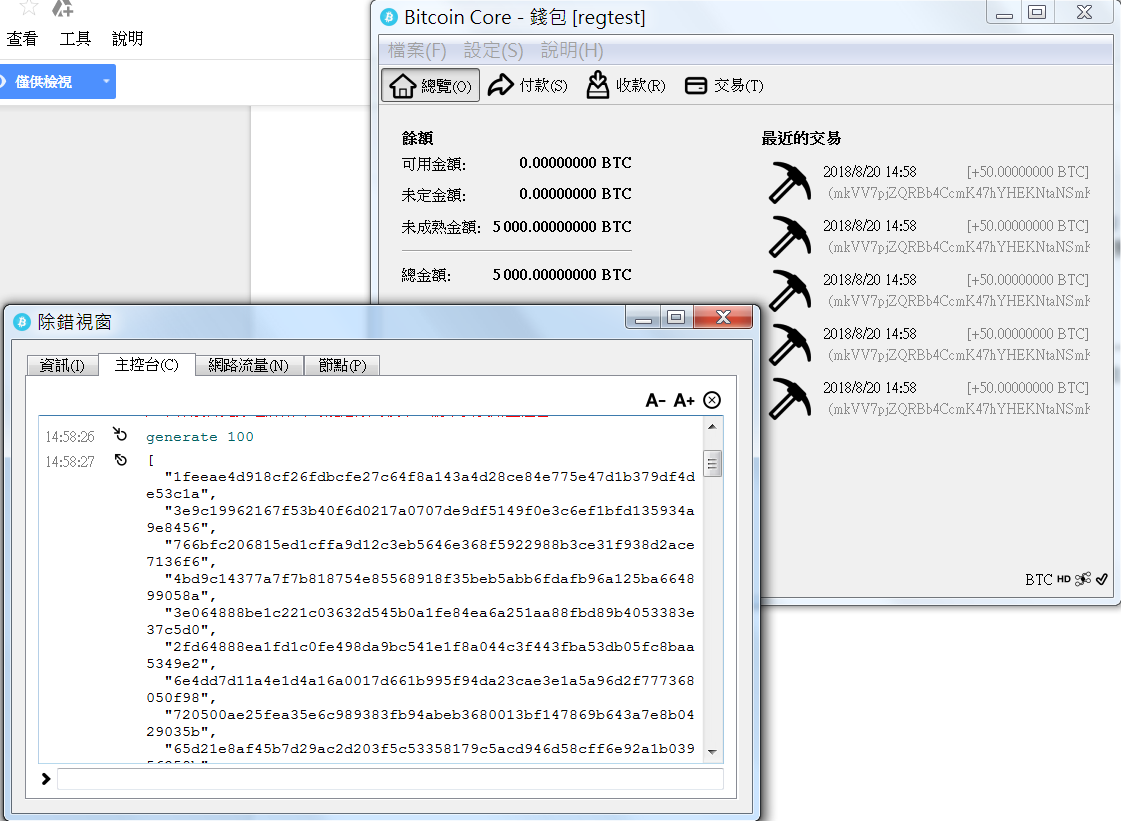
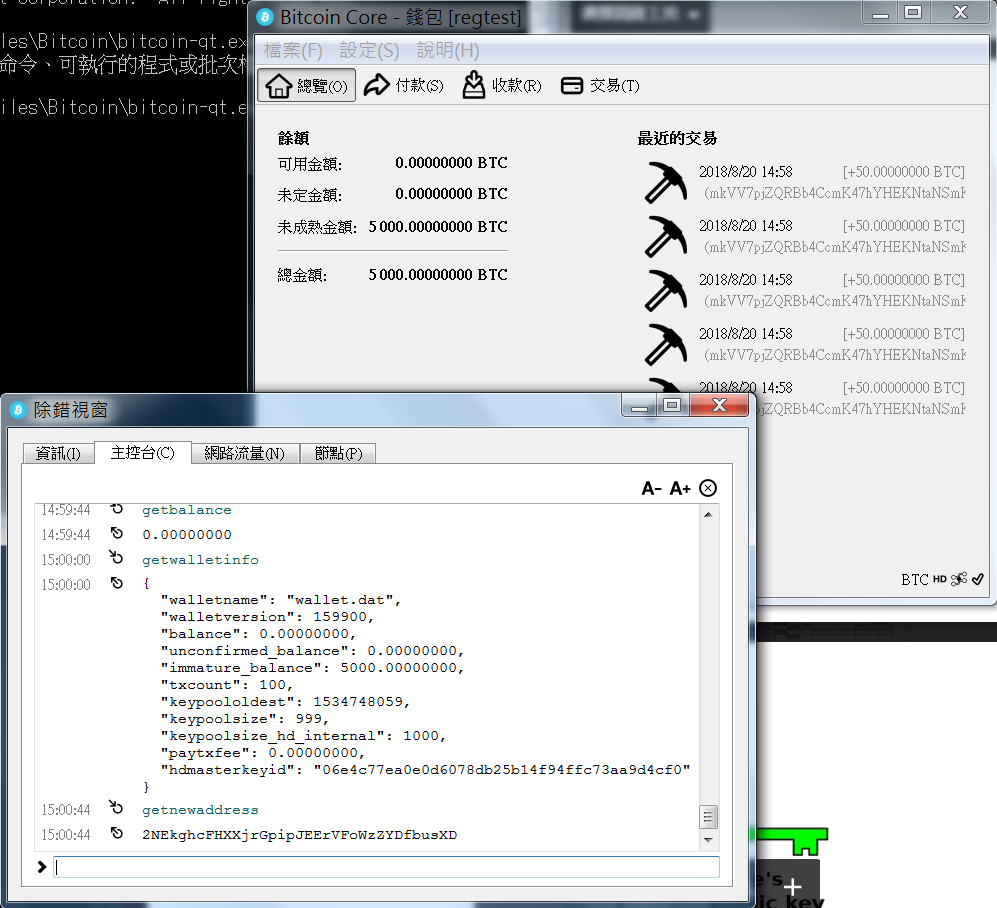
1. 區塊鏈是交易紀錄的資料庫：交易紀錄放入區塊後，再由區塊構成區塊鏈，並為所有節點共享。
2. 每一個區塊都包含前一段的加密雜湊值，這樣的設計使區塊內容在被更動時能夠被發現，具有難以竄改的特性。
3. 比特幣區塊鏈專為比特幣服務，用途較窄。而以太幣（ether）是用來在乙太坊付款的代幣。也就是說，以太幣是為了服務以太坊而存在，兩者關係與比特幣恰恰相反。
4. 進入regtest模式 命令：” C:\Program Files\Bitcoin\bitcoin-qt.exe” -regtest



產生錢幣 命令：generate 100

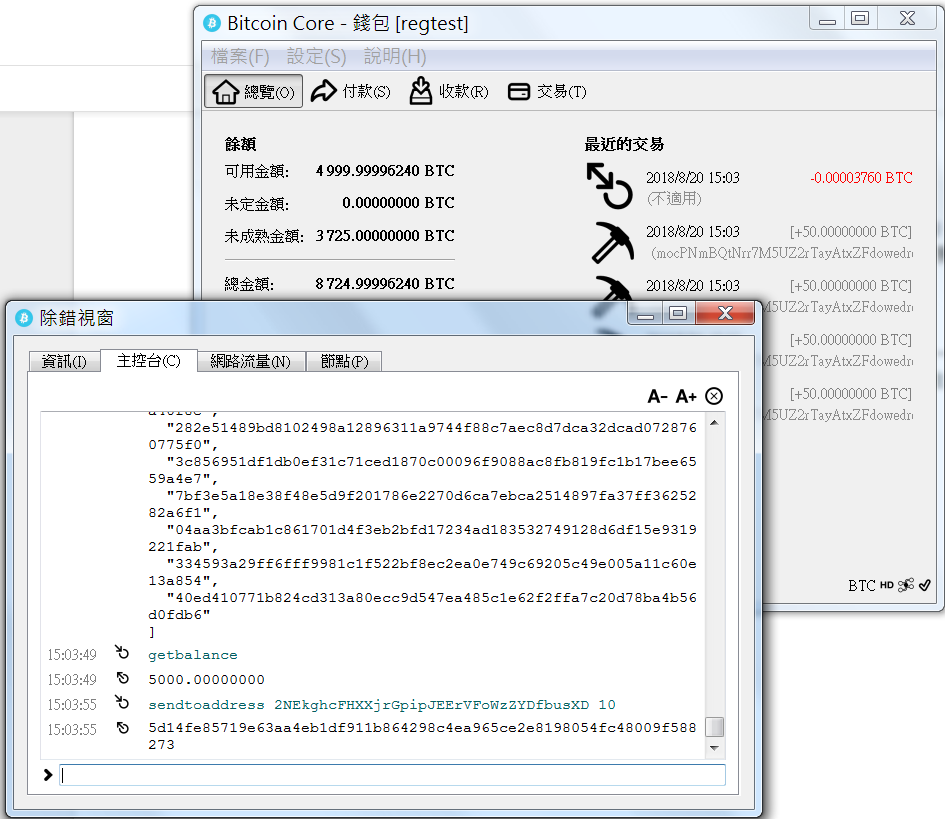


產生新位址 命令：getnewaddress

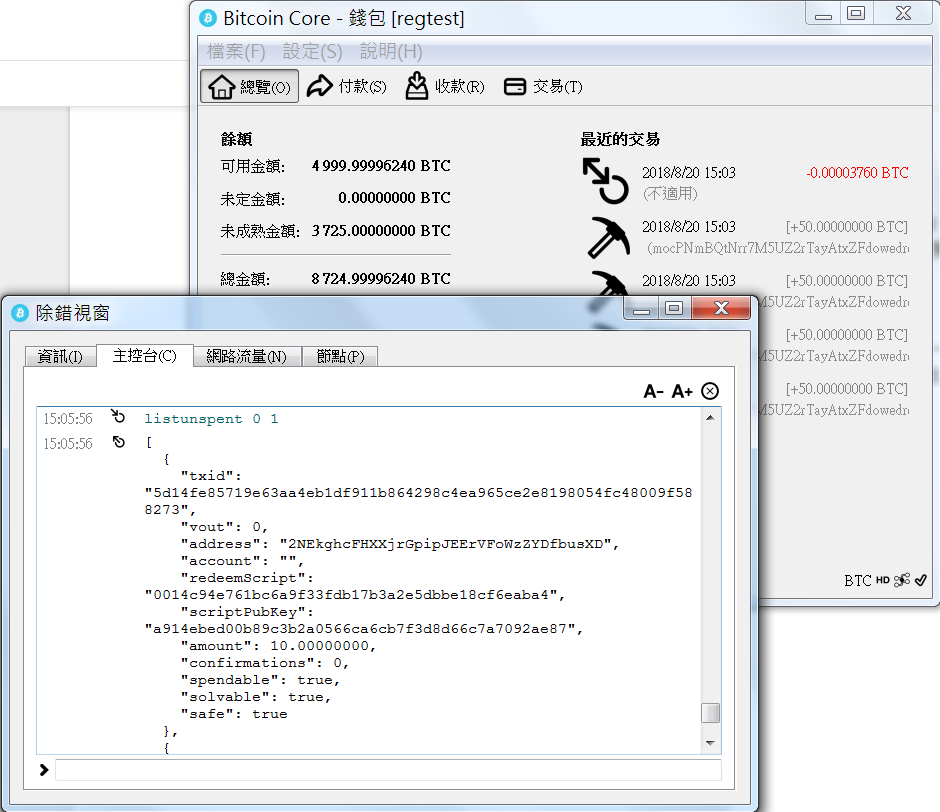


轉10塊錢給該位址

命令：sendtoaddress 2NEkghcFHXXjrGpipJEErVFoWzZYDfbusXD 10



列出該交易的紀錄 命令：listunspent 0 1



//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 = "cN4aXkbu3baz53RyZRHg41Ga87WrYoF6oiUExcjmtQTnaKELCLKG";

//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('5d14fe85719e63aa4eb1df911b864298c4ea965ce2e8198054fc48009f588273', 0);

//用getnewaddress取得新的位址

txb.addOutput('2MxfNS8sB1GcCo3GBLmX2PUw277H9zvrn2L', 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);

