# 西夏普山寨币简介

## 简介



西夏普山寨币是基本原理是山寨比特币，交易基于UTXO，支持P2SH，个人的密钥可以自由创建（理论上可以创建无数个），至于挖矿机制，西夏普山寨币主要是为了学习区块链技术，挖矿太费电脑资源影响其他工作，所以挖矿机制改为计算24点，上一个block在创建时会随机生成4个数字，只要输入正确的计算表达式就可以创建block，没有时间限制。

Block数据是按json格式存储的，日志中也会记录生成的block，可以很方便的查看block数据（日志保存路径为“C:\Users\*{username}*\Documents\XXPClient\log”，日志中最长的那行就是block数据了）以下为高度69的block数据，只有两笔交易。

*{*

*"Header": {*

*"Puzzle": [6, 8, 9, 9],*

*"nonce": "(9\*(7-5))+6",*

*"Version": "0.0.0.4",*

*"PreHash": "C89ACC217B54F071A95312F3DFB1095A2BB39E50D05B314AB8B0372A54F160D4",*

*"Height": 69,*

*"HashMerkleRoot": "00222686549E011D626C63B136F73654168040F6B2FCAF44BDCC2E68BB6EC8D9",*

*"TimeStamp": "20181231160841499"*

*},*

*"listTransactions": [{*

*"TxHash": "05C3D531C132B8161F6EAC2694B23D1752538BCC831B98661D8AE0F5ADDBAEA7",*

*"Version": "0.0.0.4",*

*"inputCount": 1,*

*"listInputs": [{*

*"PreTxHash": "2B001E401103B22BEEC3CB89B12D86E390B086C61878575448E9EFB0567817B6",*

*"OutputIndex": 1,*

*"ScriptSig": {*

*"Signature

*"PubKey": "-----BEGIN RSA PUBLIC KEY-----\r\nMIIBCAKCAQEAyx7hWZiY/kPnEvdbegkyxOR7Wz7PdAWEYuMUsqoLbTa6ZSOD96qJ\r\njgQXwJ3I07LTLQiq5nYmHV7sIZ4KDwg2Pb7ovqVNK4y7y7uaB9fnFJ+8KVHATz7B\r\nmTzi5t4hHiu912GJHia6A3jRq77CaUyUaqjI8+RC7AwKLIhx9DEKKCgTOu6SMLm4\r\nCjm5Aq31+85vNUZBJfG6GWoO3+0+bhMzH3XLrzEIaMy110fxFgvkzXycXPzxTYCG\r\nCi3Pke9vPuesdyllHvUxZuw82b4lRPkn26aEsA6HHlZX5qZhHB474/8i8yLg5jE2\r\n+BAuA7y+XoPnLuiMJP7Wiq2A/Wz/3CKawQIBAw==\r\n-----END RSA PUBLIC KEY-----\r\n"*

*}*

*}],*

*"outputCount": 2,*

*"listOutputs": [{*

*"value": 10.0,*

*"scriptPubKey": "OP\_DUP OP\_HASH160 98F13297C3B4FD23D913040A2AE99CE61DD40FC34A0F433023C4D24D1301C25D OP\_EQUALVERIFY OP\_CHECKSIG"*

*}, {*

*"value": 9.0,*

*"scriptPubKey": "OP\_DUP OP\_HASH160 01314092DF4A3BDBA944E458CED99ED34A88ED4F0B9F179A5AEFC62017BB990D OP\_EQUALVERIFY OP\_CHECKSIG"*

*}]*

*}, {*

*"TxHash": "26CF22D8DD83AFC7036D70DDC6BF8BD2ABF68623A5516DF996EF44808DC557CD",*

*"Version": "0.0.0.4",*

*"inputCount": 1,*

*"listInputs": [{*

*"PreTxHash": "0000000000000000000000000000000000000000000000000000000000000000",*

*"OutputIndex": -1,*

*"ScriptSig": {*

*"Signature": "9336ADD444702644578C3A2E6A8B2B203587103F46D8B60C354EA11092DA6F54",*

*"PubKey": "CE0A475A72D9A497099226F82F1B78E0F78275FA53BAF51E57535ADE6A03FC3B"*

*}*

*}],*

*"outputCount": 1,*

*"listOutputs": [{*

*"value": 24.0,*

*"scriptPubKey": "OP\_DUP OP\_HASH160 01314092DF4A3BDBA944E458CED99ED34A88ED4F0B9F179A5AEFC62017BB990D OP\_EQUALVERIFY OP\_CHECKSIG"*

*}]*

*}],*

*"Hash": "24A9AD586C5272D0A4A696E07DF2CD06E600E0469B5B03DB7853F0BACCB8C37F",*

*"Magic": "xi-xia-pu",*

*"Size": 200,*

*"TransCount": 2*

*}*

加密是用C++封装调用OPENSSL，非对称算法使用的是RSA1024（这个算法比较熟悉，所以就用它了），另外主要使用的就是SHA256.

数据库使用的是开源LevelDB，自己编译了个lib库，然后C++封装成dll C#调用，数据库目前保存的是所有block的数据，UTXO暂时是保存在一个dictionary里，程序每次起来时遍历数据库生成UTXO Pool。

关于数据同步，目前只支持局域网数据同步，可以自动同步block、同步transaction、发现广播新的节点。种子节点配置在配置文件中（其实就是我的局域网IP，没有固定IP，也不是一直在线，找不到了，就只能自己配置一个在线的节点IP凑活玩了），配置文件“Bitcoiner.exe.config”



## 依赖环境

1. .Net Frame Work 4.5.2及以上，下载地址：https://www.microsoft.com/en-us/download/details.aspx?id=42642

2. Vs2013、vs2015 运行库，下载地址：

x86：

<https://aka.ms/highdpimfc2013x86chs> [<https://download.microsoft.com/download/6/A/A/6AA4EDFF-645B-48C5-81CC-ED5963AEAD48/vc_redist.x86.exe>](http://download.microsoft.com/download/1/8/0/180FA2CE-506D-4032-AAD1-9D7636F85179/vcredist_x64.exe)

X64：

<https://aka.ms/highdpimfc2013x64chs>

<https://download.microsoft.com/download/6/A/A/6AA4EDFF-645B-48C5-81CC-ED5963AEAD48/vc_redist.x64.exe>

## 使用说明

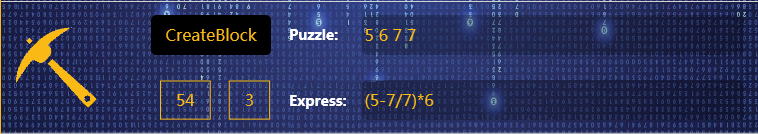


### 3.1 Create key



点击CreateKey 程序会创建一对RSA公私钥，该对密钥会以文件的形式保存在本地，同时后面的显示框计数会加1。

### 3.2 CreateBlock



Puzzle 显示的上一个block随机生成的24点题目。

显示的是上一个block 在链上的高度，创建Block或者收到新的Block时会自动跟新。

 显示的是当前有多少Transaction等待写入Block，在收到新的Transaction时会自动更新。

Express 是输入框，挖矿时输入24点计算表达式，验证通过后就可以成功创建Block，并且会自动推送给其他节点。

### 3.3 Balance



Balance显示的属于你的密钥的余额，它是和密钥关联的，选择不同的密钥会自动显示不同的余额，所以密钥如果丢了，那余额也就没办法找回了。

Un-Balance 显示的还没有写入block 的Transaction属于你的密钥的余额，也是和密钥相关。

最右侧那一串数字是公钥的Hash值，当比人给你转账时其实也就是转向这个公钥的Hash值。

下拉框是用来选择密钥，选择All对应的balance及Un-balance显示的是所有密钥拥有的余额，右侧公钥的hash是第一个公钥的hash值，选择其他密钥Balance、Un-balance、Hash都是和密钥对应。

Nodes显示的是已连接的节点数量。

### 3.4 Transfer



Amount 是要转账的金额

Account 是对方的公钥Hash值，也就Balance栏最右侧显示的。