# 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。

技术上加密是用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。

依赖环境：

1. .Net Frame Work 4.5.2及以上。

2. Vs2015 运行库，下载地址：x86： <https://www.microsoft.com/en-us/download/details.aspx?id=53587>

X64：[https://download.microsoft.com/download/6/A/A/6AA4EDFF-645B-48C5-81CC-ED5963AEAD48/vc\_redist.x64.exe](https://download.microsoft.com/download/6/A/A/6AA4EDFF-645B-48C5-81CC-ED5963AEAD48/vc_redist.x64.exe" \t "_blank)

## 界面



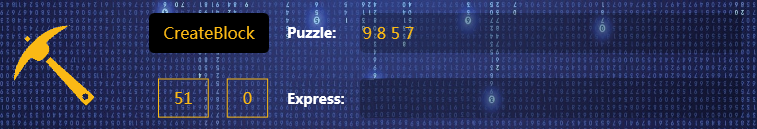
## 使用说明

### 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。