目录

[要求 1](#_Toc15789)

[使用加密函数和密钥 2](#_Toc10095)

[原有交易和输出交易 2](#_Toc18296)

[密钥管理 3](#_Toc14624)

[生成新的交易 3](#_Toc29132)

[新交易的输入 4](#_Toc22029)

[交易类 5](#_Toc6383)

**运行gen\_jiaoyi.py 文件即可**

# 要求

SM2系统参数：

素数：

8542D69E 4C044F18 E8B92435 BF6FF7DE 45728391 5C45517D 722EDB8B 08F1DFC3

系数：

787968B4 FA32C3FD 2417842E 73BBFEFF 2F3C848B 6831D7E0 EC65228B 3937E498

系数：

63E4C6D3 B23B0C84 9CF84241 484BFE48 F61D59A5 B16BA06E 6E12D1DA 27C5249A

基点，其阶记为。

坐标：

421DEBD6 1B62EAB6 746434EB C3CC315E 32220B3B ADD50BDC 4C4E6C14 7FEDD43D

坐标：

0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2

阶：

8542D69E 4C044F18 E8B92435 BF6FF7DD 29772063 0485628D 5AE74EE7 C32E79B7

Locking script：

() 0AE4C779 8AA0F119 471BEE11 825BE462 02BB79E2 A5844495 E97C04FF 4DF2548A 7C0240F8 8F1CD4E1 6352A73C 17B7F16F 07353E53 A176D684 A9FE0C6B B798E857

对应的：

128B2FA8 BD433C6C 068C8D80 3DFF7979 2A519A55 171B1B65 0C23661D 15897263

交易id（哈希值）：请使用SM3哈希函数

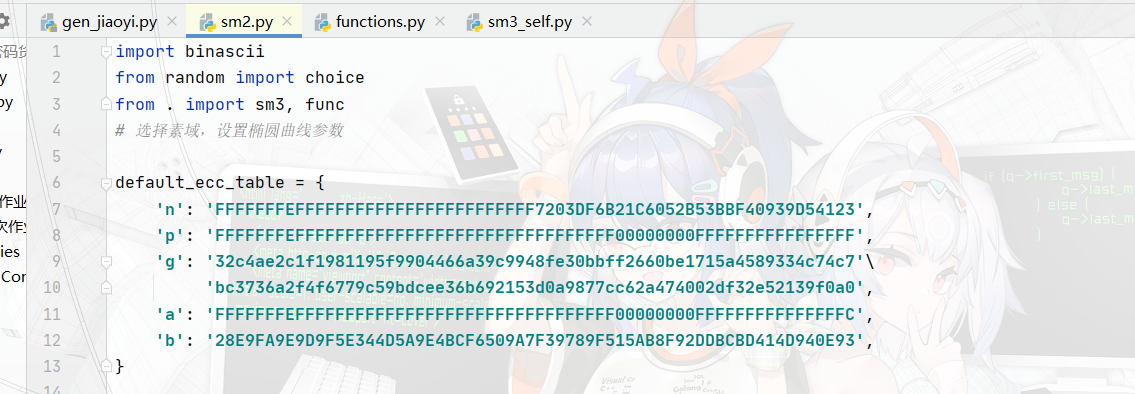
F4A38489 E32B45B6 F876E3AC 2168CA39 2362DC8F 23459C1D 1146FC3D BFB7BC9A

依据以上数据，实现交易生成算法。交易支持多个输入和多个输出。输入包含来源和解锁脚本，输出包含金额和锁定脚本。所使用的数字签名算法是SM2，所使用的哈希函数是SM3。

# 使用加密函数和密钥

使用gmssl 函数库

调用sm2,sm3函数



原本默认加密参数

可以更改，但是找不到以上数据对应的密钥，就别改了

# 原有交易和输出交易

旧的交易

标识已加粗

000000012180B9C9A6E04E9C91F7BA880429273747D7EF5DDEB0BB2FF6317EB00BEF331A83081A6994B8993F3F5D6EADDDB81872266C87C018FB4162F5AF347B483E2462020764280B9C9A6E04E9C91F7BA880429273747D7EF5DDEB0BB2FF6317EB00BEF331A83081A6994B8993F3F5D6EADDDB81872266C87C018FB4162F5AF347B483E24620207c840F4A38489E32B45B6F876E3AC2168CA392362DC8F23459C1D1146FC3DBFB7BC9A1180B9C9A6E04E9C91F7BA880429273747D7EF5DDEB0BB2FF6317EB00BEF331A83081A6994B8993F3F5D6EADDDB81872266C87C018FB4162F5AF347B483E246202075a

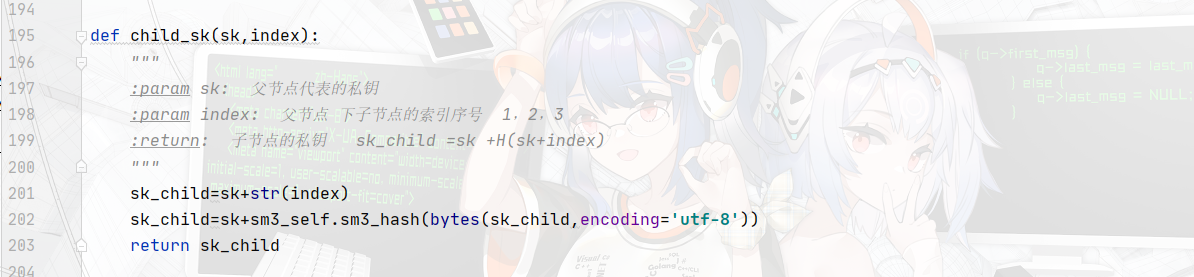
依次为：

**版本号，来源数量，来源index1,公钥长度，公钥，金额，来源index2,公钥长度，金额，前一个输出的hash的长度,前一个输出的hash,输出的数量，输出index1,输出公钥长度，输出公钥，金额**

新的交易

000000011180B9C9A6E04E9C91F7BA880429273747D7EF5DDEB0BB2FF6317EB00BEF331A83081A6994B8993F3F5D6EADDDB81872266C87C018FB4162F5AF347B483E246202076440F4A38489E32B45B6F876E3AC2168CA392362DC8F23459C1D1146FC3DBFB7BC9A117f0AE4C7798AA0F119471BEE11825BE46202BB79E2A5844495E97C04FF4DF25487C0240F88F1CD4E16352A73C17B7F16F07353E53A176D684A9FE0C6BB798E85764

# 密钥管理



没什么用，就写了一个函数

# 生成新的交易

主要函数



## 新交易的输入

***gen\_tx(sk, inputs, output)***

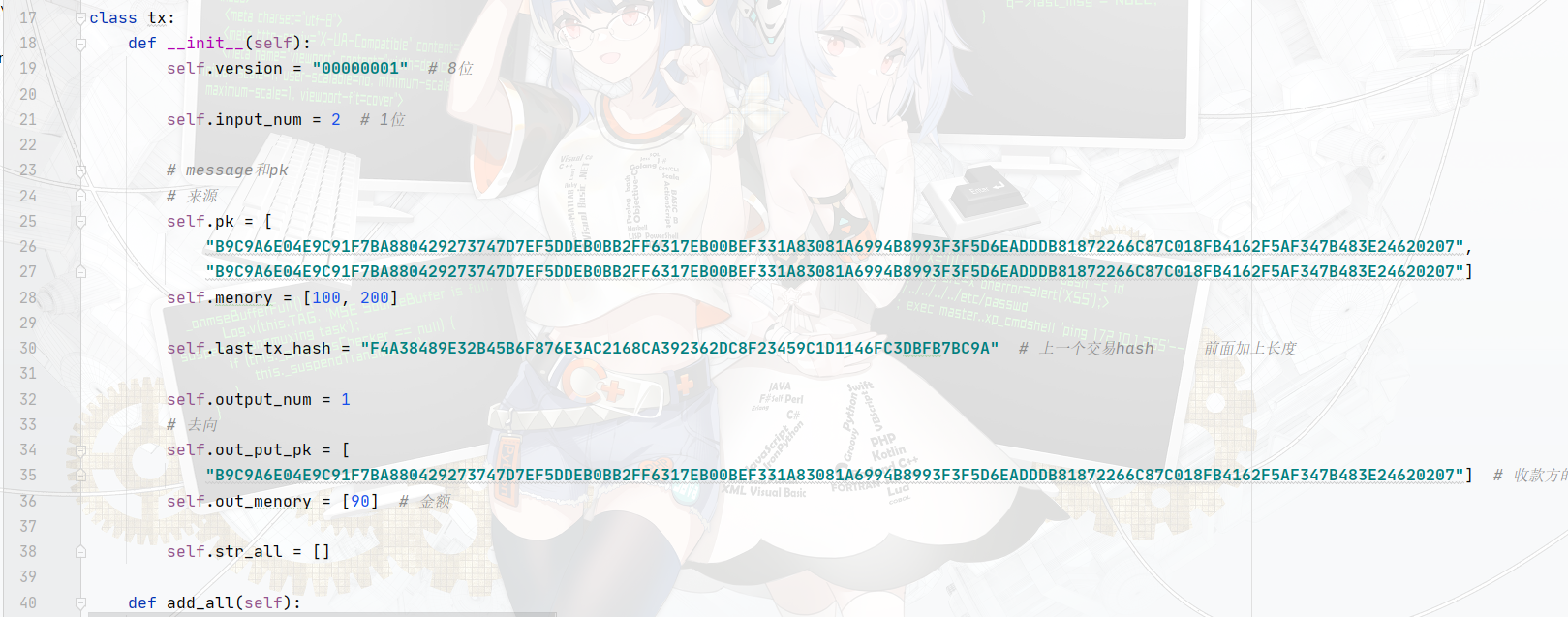
Sk 和原有交易的公钥对应

sk = **'00B9AB0B828FF68872F21A837FC303668428DEA11DCD1B24429D0C99E24EED83D5'**

output = {  
 **"num"**:1,  
 **"pk"**:[**"0AE4C7798AA0F119471BEE11825BE46202BB79E2A5844495E97C04FF4DF25487C0240F88F1CD4E16352A73C17B7F16F07353E53A176D684A9FE0C6BB798E857"**],  
 **"money"**:[100]  
}

# 交易类

包含交易的属性，交易的编码，交易的解码



由list 实现多个输入和输出