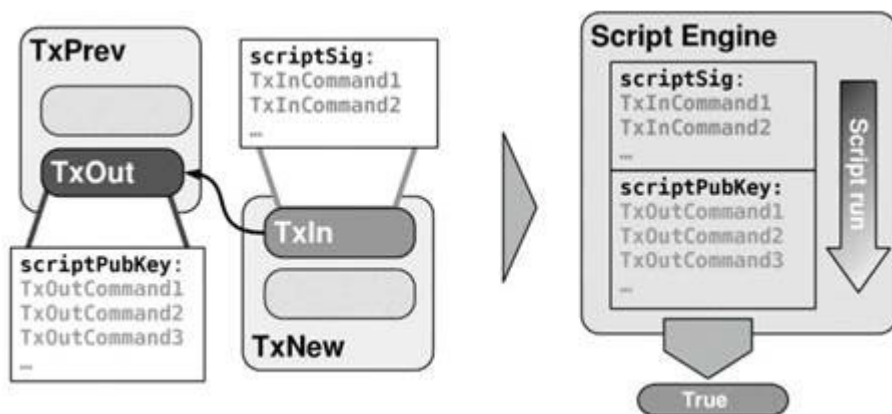


## 编程任务 3

在本次作业中，你将创建多个交易，并将其发布到比特币测试网。我们将使用 `python bitcoinlib` 提供启动代码，`python bitcoinlib` 是一个用于操纵比特币交易的 `python3` 库。



### 练习

(a) 生成可通过以下两个线性方程组的解  $(x, y)$  赎回的交易：

$$x+y = (\text{StudentID 前 4 位}) \text{ 和 } x-y = (\text{StudentID 后 3 位})$$

[为确保存在整数解，请必要时调整（顺序减 1）你的 StudentID 后 3 位，使 StudentID 前 4 位和 StudentID 后 3 位奇偶性相同]。

(b) 赎回交易。赎回脚本应尽可能小。也就是说，一个有效的 `scriptSig` 应该是简单地将两个整数  $x$  和  $y$  发送到堆栈中。确保在 `scriptPubKey` 中使用了 `OP_ADD` 和 `OP_SUB`。

### 推荐阅读

1. 比特币脚本：<https://en.bitcoin.it/wiki/Script>
2. 比特币交易格式：<https://en.bitcoin.it/wiki/Transaction>
3. <https://privatekeys.org/2018/04/17/analytic-of-a-bitcoin-transaction/>