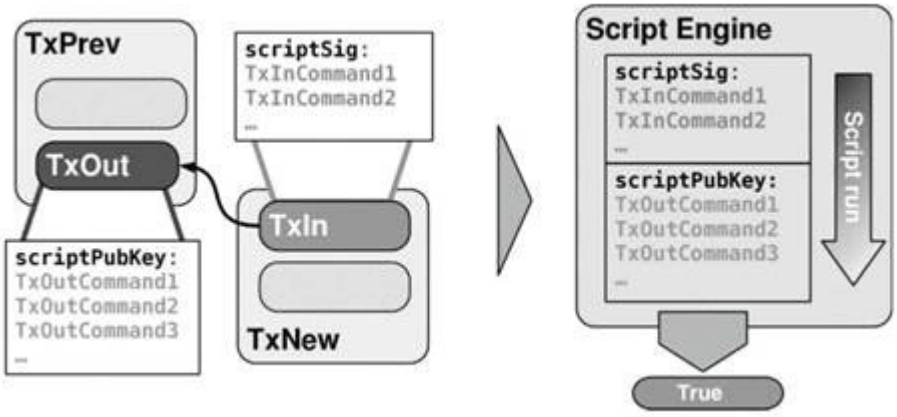
区块链基础及应用 **2022**

编程任务 2

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） 生成一个**涉及四方的多签名交易**，这样交易可以由第一方（银行）与另外三方（客户）中的任何一方（客户）共同赎回，而不仅仅只是客户或银行。对于这个问题，你可以假设是银行的角色，这样银行的私钥就是你的私钥，而银行的公钥就是你的公钥。使用 keygen.py 生成客户密钥并将它们粘贴到 ex2a.py 中。（b）赎回事务并确保 scriptPubKey 尽可能小。可以使用任何合法的签名组合来赎回交易至 faucet 地址，但要确保所有组合都有效。

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/