**实验报告**

一、需求分析

对一个交易，实现找到其所有输入使用的输出并验证其脚本的功能

二、设计思想

从键盘取得需要验证的交易——遍历交易的所有输出——对每个输出找到对应输入并合成完整脚本——验证脚本

基于以上流程实现了如下函数原型：

int isvalid(Inputptr ip, Blockptr chain)//将需要验证的输入配对输出并合成脚本

int isscriptvalid(char \*fullscript)//验证脚本

三、调试分析

1.遇到OP\_CHECKSIG操作时会有Expression: b!=(BigInt::Zero)这一报错，经检查是对栈的后进先出理解不够透彻，将先出栈的字符串当作了签名，后经调整报错消失

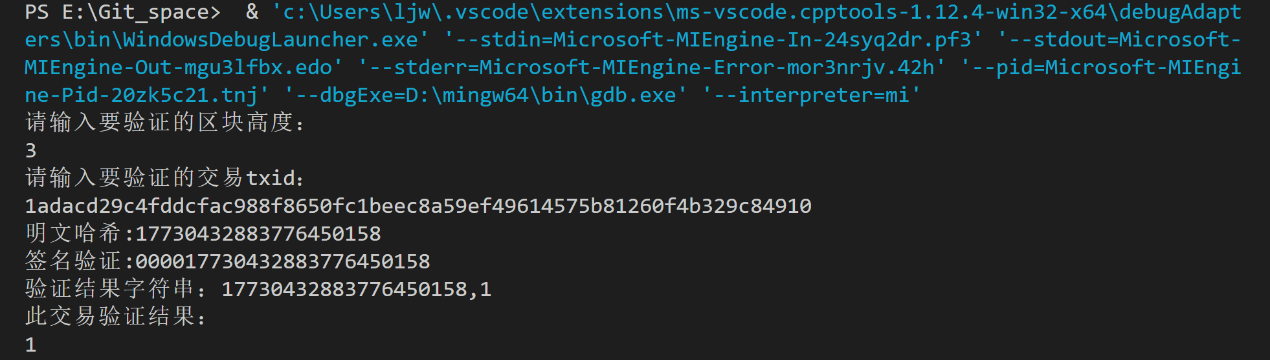
2.在读取csv文件时尾部会有\n进入脚本，需要注意去除

四、测试

测试用例：

用第3个区块的1adacd29c4fddcfac988f8650fc1beec8a59ef49614575b81260f4b329c84910做测试，完整脚本为"22308B989987AEE01DED1BAC4C84497F 20221009 OP\_DUP OP\_HASH160 17730432883776450158 OP\_EQUALVERIFY OP\_CHECKSIG "

测试结果截图：



五、实验总结/心得

经过本次实验，我深化了对栈的认识，也对比特币交易系统有了更深入的了解