**《课程综合实践Ⅱ》实验报告二**

**区块链原理初识及数字币模拟器操作**

**姓名\_张天逸 \_ 专业 计算机科学与技术**

**学号 3220106424 联系方式 15901797658**

## 一、实验目的

1. 在ubuntu系统上配置python环境。

2. 学习scp等文件远程拷贝命令，在宿主机和虚拟机之间传输文件。

3. 了解区块链原理，部署并操作simchain数字币模拟器。

## 二、实验内容及要求

## 三、实验感受及记录

* 1. **实验感受（本次实验遇到的问题、主要收获等内容）**

学习了scp远程文件传输，以后可以使用命令行的方式替代，避免用鼠标拖动文件这一比较麻烦的方式。我在找自己的ip端口时碰到了一些问题，开始传输失败了好几次。

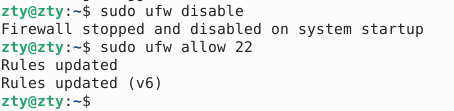
配置simchain的时候我开始使用的是ubuntu22.04，一直没有办法成功，切换了python版本，最后选择切换回了ubuntu20.04

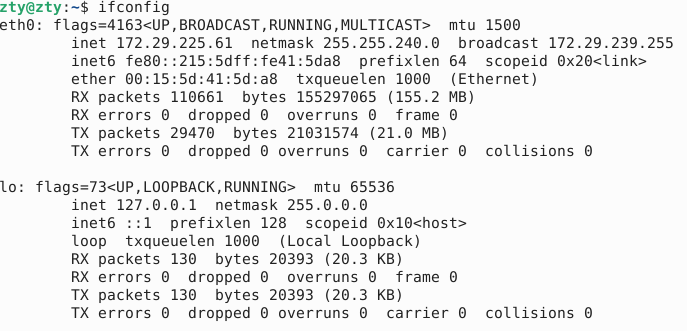
另外，在使用python命令时候应当注意空格，避免不必要的问题

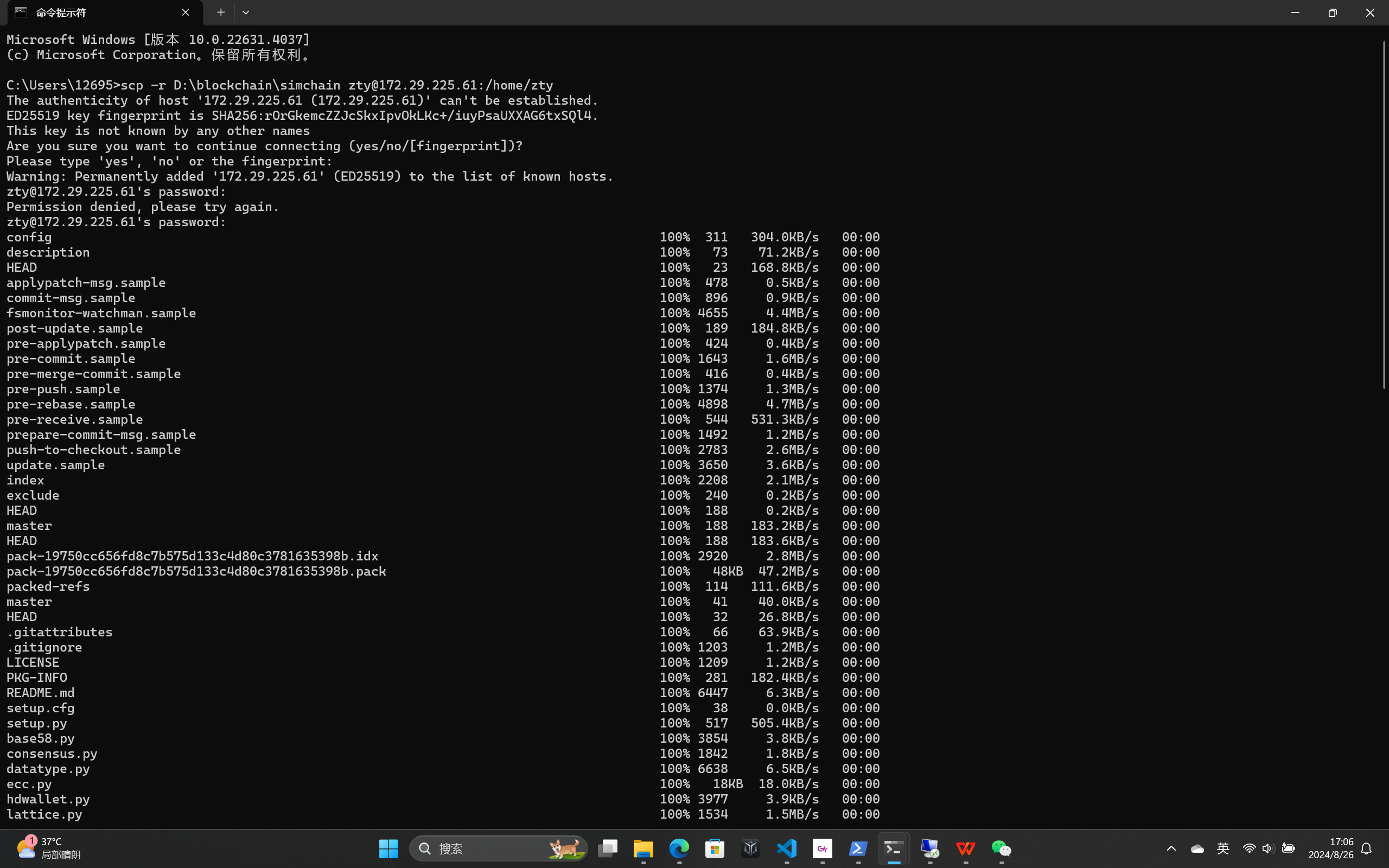
* 1. **实验记录（实验过程中关键步骤截图记录及文字描述）**

1. Scp远程传输

在ubuntu中安装ssh工具，开放22号端口作为ssh服务器的默认运行端口，查看ip，并使用scp命令完成传输。

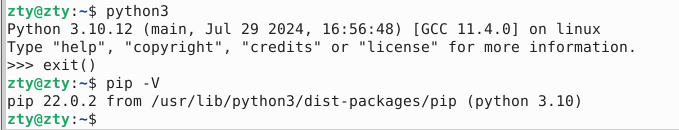






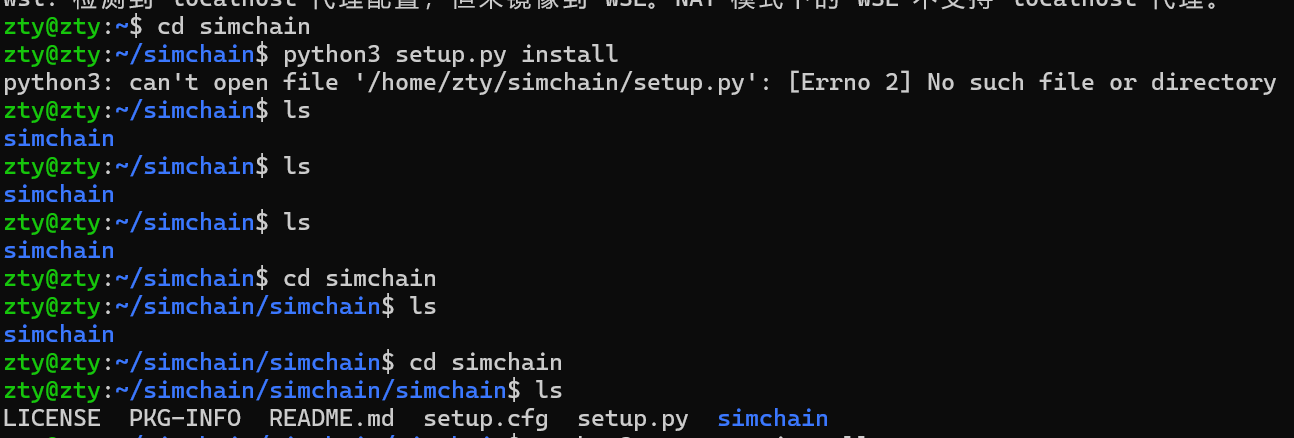
1. python配置

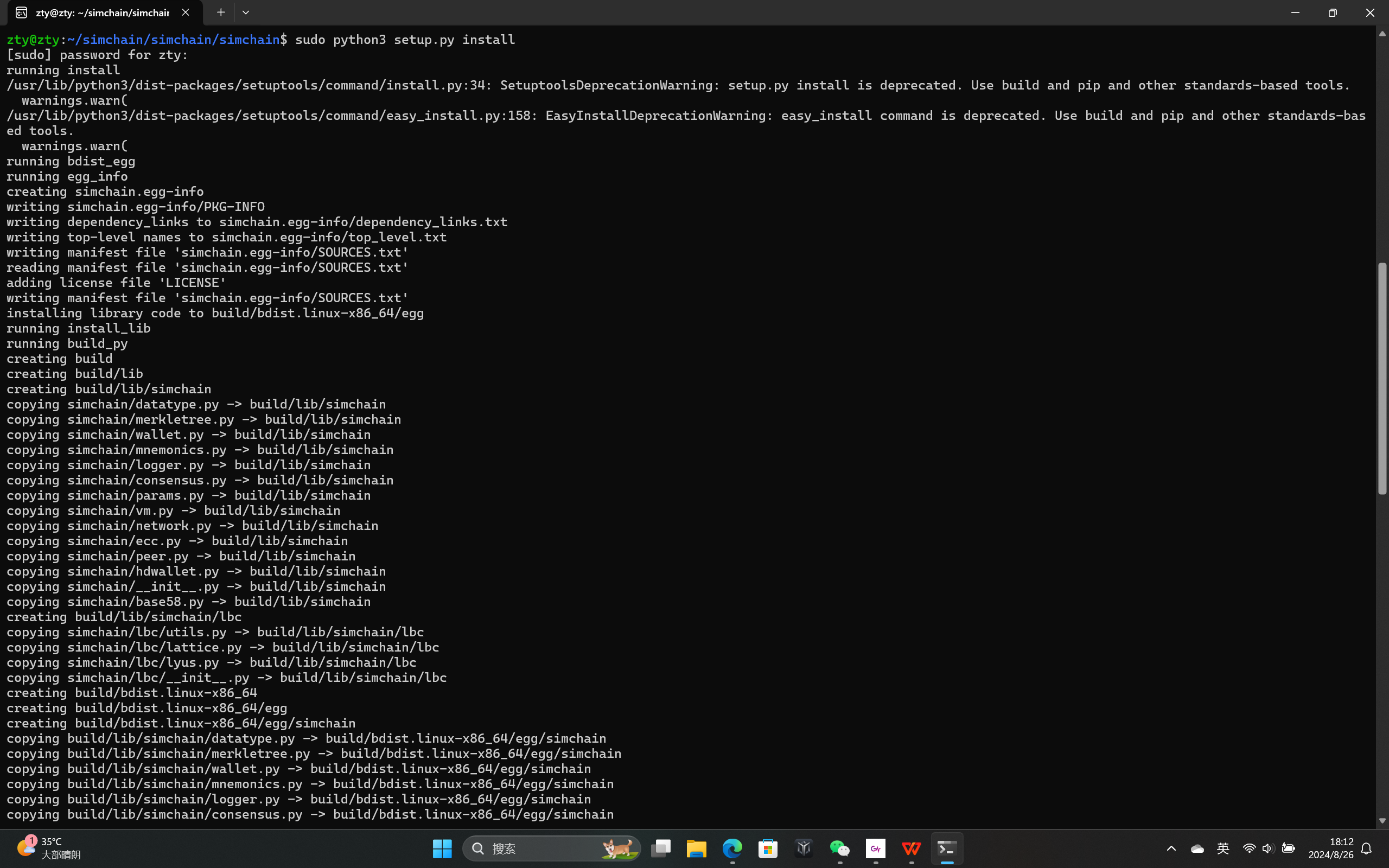
在虚拟机中打开终端，输入命令python3，进入命令行，然后退出。安装pip并查看版本



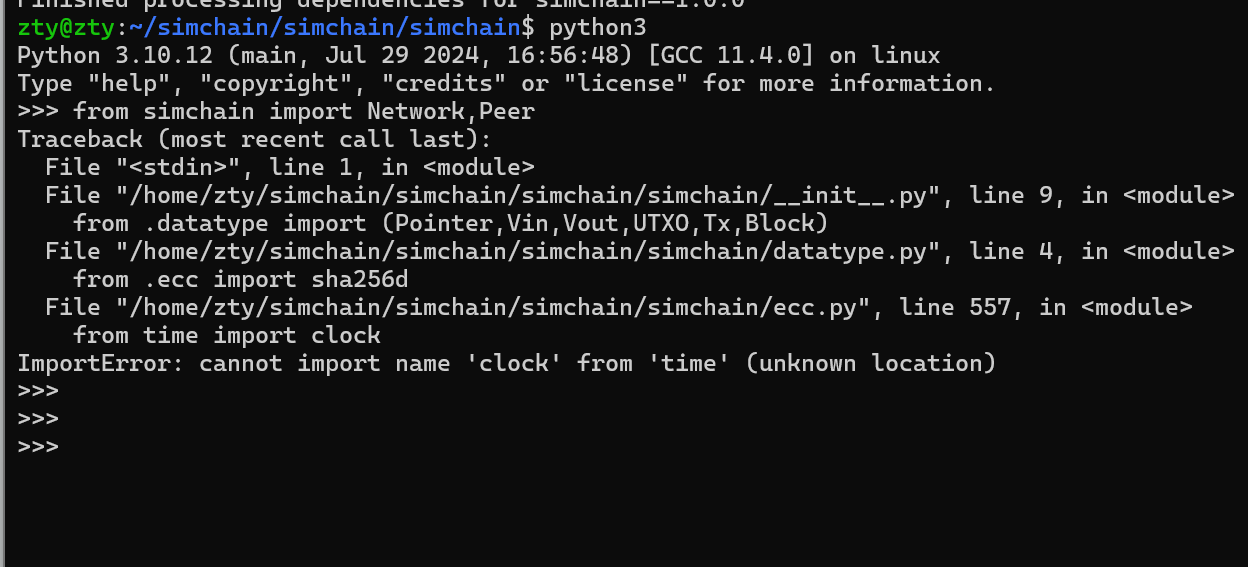
1. Simchain

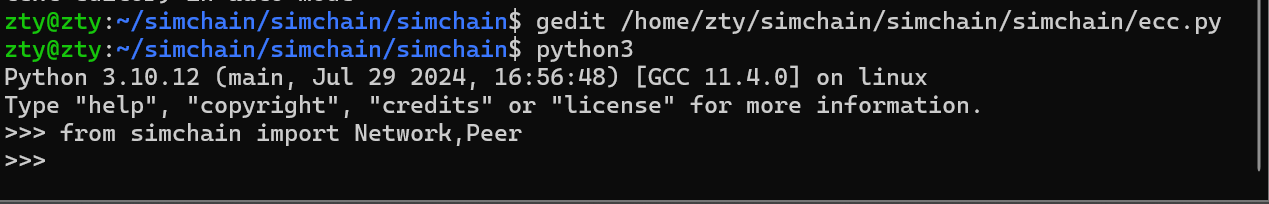
打开终端，使用cd命令进入到刚刚传输的simchain目录内，使用ls命令查看该目录下包含的文件(需进到包含setup.py文件的那层目录)，输入命令配置simchain



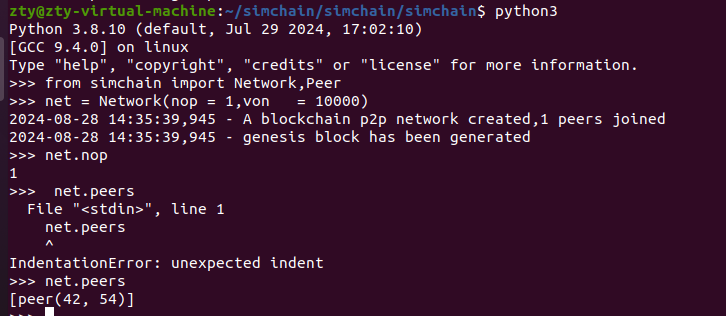


开始会失败，需要修改ecc.py

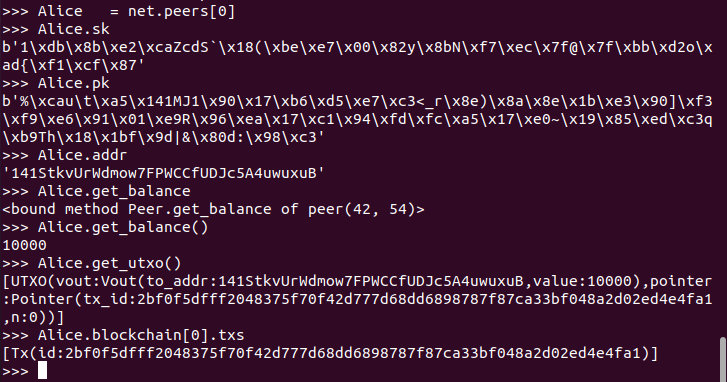




构建一个名为net的区块链网络，并假设网络中只有一位数字货币用户，并给自己写了一笔10000分的交易。输入代码查看网络具体信息



将第一位用户命名为Alice,输入命令查看Alice的相关身份信息，账户相关信息，UTXO集



添加一位新的用户，并将其命名为Bob查看该用户的公钥、私钥、地址和账户余额，查看同一区块链网络内的两者的UTXO集和区块链是否相同，

模拟一种现实比特币交易的情况，创建交易,产生了两个交易输出，一个归属于接收转账方Bob且金额100，另一个归属于发送转账方且金额为9890,查看两位用户的余额,为了让交易继续正常进行，Alice需要将该交易广播到所有区块链节点，再次输入命令查看两位用户的余额,输入命令来获取Alice还未确认的UTXO,为了让交易最终完成，输入命令让整个区块链网络就这次交易达成共识,查看获胜节点的账户余额,查看Alice和Bob的未确认UTXO,查看区块链高度



1. Simchain数字币模拟器——钱包和密钥概念

构建一个12个节点的区块链网络,输入命令查看Alice公钥-私钥-地址对，获取Bob的钱包信息，验证用户与钥匙对之间的一对多关系，查看新生成的公私钥的字节串编码以及地址，获取Bob最新创建的交易，并将其命名为Tx，查看交易输入，为了验证只需知道数字签名和公钥在区块链网络中能唯一确定交易有效性即可，控制变量：不修改本次交易的交易输入，交由Alice做有效性判断，修改本次交易的交易输入中的数字签名(Signature)项，交由Alice做有效性判断，修改本次交易的交易输入中的公钥(pubkey)项，交由Alice做有效性判断，修改本次交易的交易输入中的UTXO来源(to\_spend)项，交由Alice做有效性判断，通过以上实验，我们不难发现只有当数字签名、公钥、to\_spend完全匹配才能被证明为是有效交易。

