preface-序章

这书主要介绍的是基于python的一个区块链编程库，通过学习这个库来了解比特币原理，~~进而坚定炒币的信念~~，涉及内容包括数学，计算机科学，少量密码学理论。一个普通计算机学生的知识储备应该是基本足够的

这一档需要不断修正，读完一章修正一章，我相信肯定有很多不甚准确的理解

书1~4章讲应用的数学工具：

1和2讲的是数学基础；

3讲的是加密运算中涉及的椭圆曲线加密算法和有限域问题，后半部分涉及公钥加密解密问题；

4讲的是parsing和serialization，用于验证，解析，存储和传输加密原语

5~8讲的是交易问题，比特币如何设计了一个巧妙的交易系统（本质是一个数据传输系统）

5讲的是交易系统的结构；

6详细介绍比特币的smart contract language 智能合约语言（比特币诞生之初是没有合约的，但经历了2017年的迭代之后就有了合约系统，这个是用于合约交易的语言）；

7是个汇合章，通过学习前4章的基础理论理解椭圆曲线密码学来了解如何创建一个事务（交易事件）

8介绍了pay-to-script-hash（p2sh）系统是如何工作并创立一个比智能合约系统更厉害的东东

9~12讲的区块和网络系统（blocks and networking）

9介绍了block（区块），这里的定义是一组有序事务的集合

10介绍了比特币的网络通信

11~12应该是比特币最出名的部分，分布式&去中心化技术，如何向整个区块链广播和请求数据

13、14章算是拓展内容，讲Segwit以及2017年大更新以后的一些新东西，这书还挺贴心，给了后续学习内容建议。前12章都有同步练习，1314没有

这个书建议的python环境是3.5+jupyternotebook，anaconda直接能一套带走，但是我惯用更新的python，应该影响不大