前言

“区块链”一词起源于中本聪发明的一种点对点电子货币系统中[1]，这电子货币系统称为比特币。作为比特币的底 层技术，本质上是一个去中心化的数据库。是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方 案。 从科技层面来看，区块链是一门涉及数学、密码学、互联网和计算机编程等很多科学技术综合交叉学问。 从应用视角来看，区块链是一种新兴技术，它是一个分布式的共享账本和数据库；这门技术从特点上分析，具有去 中心化、不可篡改、全程留痕、可以追溯、集体维护、公开透明等特点。 从计算机技术应用模式的视角来看，它具备分布式数据存储、点对点传输、共识机制、加密算法等技术模式。 中国信通院在2018年发布的区块链安全白皮书的序言，可以看出区块链安全在逐渐变得重要。

同时区块链已经上升为国家战略，未来在这一块的资源也会相应倾斜。 想要入坑区块链安全的话，是需要一些密码学基础，掌握了解诸多知识概念，Solidity编程语言。

知识概念

首先，我们需要简单的了解区块链的历史，区块链是什么，大致集成了那些技术？ 此处推荐慢雾科技入门系列的文章 -- https://paper.seebug.org/973/ 这能够帮助我们了解区块链的相关名词，一些基本的概念。对于文章中提到的攻击如果在这个阶段想要尝试复现， 难度会比较大，在后面的学习中我们也会有机会接触的。在这种学习工程中，尽量将文章中的解释进行简化，变成 自己的知识。 接下去我们可以学习区块链的数据结构，这一方面需要搜索多篇文章对比学习。

密码学基础

- 哈希算法
- ECC椭圆曲线算法

主要了解上述密码算法基本的原理以及在区块链中的应用场景。

学有余力可以尝试了解一些针对这些密码算法的攻击

Solidity

这是一门主流的编写智能合约的编程语言

加密僵尸 -- https://cryptozombies.io/zh/

这是一个学习Solidity的编程游戏，完整的学习，会让你加深对Solidity语言的了解，同时也会了解到一些代币标 准。 翻阅官方文档也是一种不错的学习方式

一些工具

- Remix 在线的编写Solidity的IDE
- MetaMask 以太坊钱包
- 以太坊浏览器

一些建议

在学习过程中肯定会遇到阻碍，但是多做尝试，善用google，百度等搜索引擎。不要局限于中文网站，国外的文章 写的也还不错的

写在最后

上述这些只是个人的学习经验，不必完全按照，只是提供一个参考。在学习完上面的内容之后，可以参照CTF-Wiki 进行学习。当然有任何对这个方向感兴趣的同学可以来和我交流。QQ:2384417651