假期准备学习工作总结——第一周

本周在指导老师的推荐和指引下，阅读了部分与“区块链技术”相关的文献。由于刚刚接触到区块链技术，对于它的原理和应用还不了解，所以这周的主要工作即按照老师的指导搜索相关文献进行初步的了解。

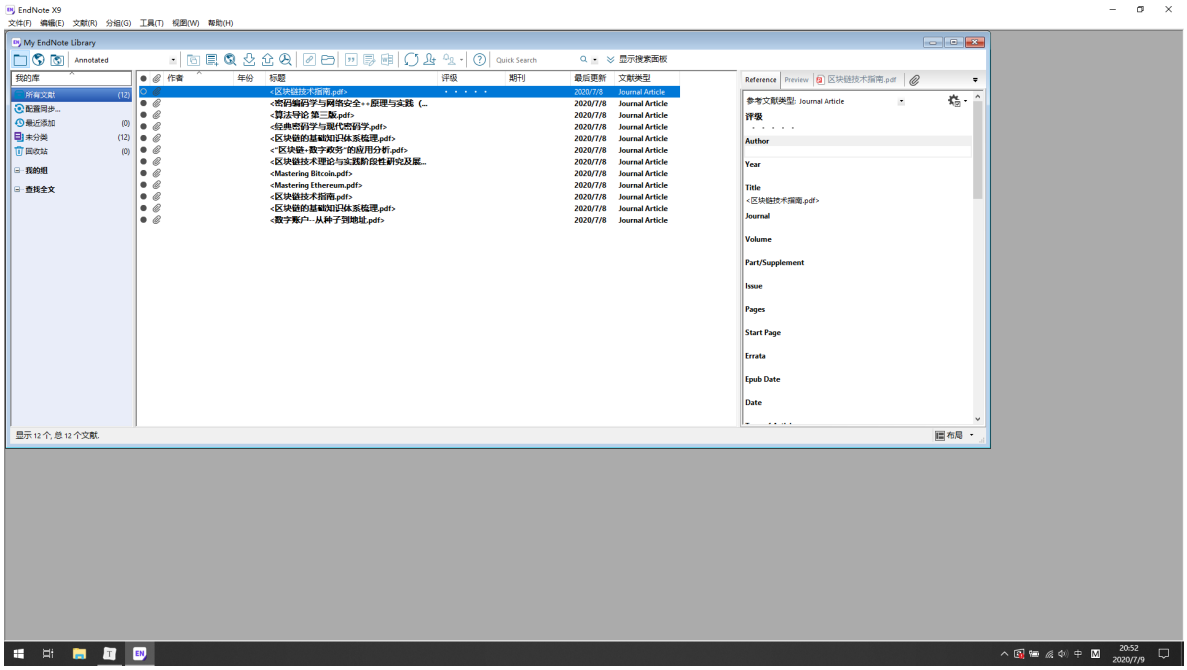
在阅读完“区块链技术理论与实践阶段性研究即展望”这篇论文后，我大致了解了**区块链的背景和意义**。据文献描述，区块链早期是与比特币捆绑出现的，大家对比特币都耳熟能详，但是对于作为比特币底层应用技术之一的区块链却知之甚少。在搜集相关新闻和资料之后了解到，比特币由于其“去中心化”、“匿名性”等特性并不能被当前世界上许多国家的体制和制度所接受，但是区块链技术本身存在着广阔的发展前景。根据我自己的理解来看，区块链是一种利用块链式数据结构来对数据进行验证和存储的技术。其具有去中心化、不可篡改、可追溯性、安全、公开透明等明显优势。然而部分学者对区块链技术具有的优势存在着不同看法，比如说有些学者认为区块链技术存在着“不可能三角”，即“去中心化”、“高效低能”、“安全性”无法同时实现，我认为这也是我学习区块链技术和将其结合具体场景应用的努力方向，目前知识面有限，对其具体实现方式没有认识，希望能够通过学习和实践来证实或者是去解决前辈提出问题。

据资料可知，**区块链技术**并非一种严格意义上的全新技术，而是一种对现有技术的集合创新。 由于在本科学习期间接触到过Hadoop，对于“去中心化”这一特征的认识还算到位，去中心化或者说是多中心化，无需集中的控制而能达成一种共识，实现上则尽量分布式。然而分布式仅是区块链关键技术其中之一，此外还包含了密码学技术、P2P网络技术、哈希算法、数据库和存储系统等。相较于其他技术，对于密码学我比较陌生，所以我规划的第一步工作是先来学习一下密码学，而具体工作的展开是围绕着Richard Spillman所著的《经典密码学与现代密码学》这本书来进行。

通过阅读“区块链技术指南”了解到，为保证存储于区块链中的信息的安全与完整，区块及区块链的定义和构造中使用了包含密码**哈希函数**和**椭圆曲线公钥密码技术**在内的大量的现代密码学技术，同时，这些密码学技术也被用于设计**基于工作量证明（PoW）的共识算法**并识别用户。哈希函数在学习数据结构这门课程时就有所了解，不过本科学习中的hash比较浅显，即给定一个数值，然后通过hash算法计算出hash值。初步了解到目前较为流行的Hash算法包括MD5、SHA-1和SHA-2。

目前所学习到的知识都比较浅显，只是对与区块链有一个认识，对于其中的核心技术以及具体实现仍没接触到。接下来还有很长的路要走，希望可以通过自己的努力，在老师和同学的协助下，学好“区块链技术”这门课程。

以下为我搜集的部分论文和书籍：


EndNote X9
文件(F) 编辑(E) 文献(R) 分组(G) 工具(T) 视图(W) 帮助(H)
My EndNote Library
Annotated
Quick Search
显示搜索面板
我的库
所有文献 (12)
配置同步...
最近添加 (0)
未分类 (12)
回收站 (0)
我的组
查找全文
作者 年份 标题 评级 期刊 最后更新 文献类型
<区块链技术指南.pdf> 2020/7/8 Journal Article
<密码编码学与网络安全++原理与实践（...> 2020/7/8 Journal Article
<算法导论 第三版.pdf> 2020/7/8 Journal Article
<经典密码学与现代密码学.pdf> 2020/7/8 Journal Article
<区块链的基础知识体系梳理.pdf> 2020/7/8 Journal Article
<"区块链+数字政务"的应用分析.pdf> 2020/7/8 Journal Article
<区块链技术理论与实践阶段性研究及展...> 2020/7/8 Journal Article
<Mastering Bitcoin.pdf> 2020/7/8 Journal Article
<Mastering Ethereum.pdf> 2020/7/8 Journal Article
<区块链技术指南.pdf> 2020/7/8 Journal Article
<区块链的基础知识体系梳理.pdf> 2020/7/8 Journal Article
<数字账户--从种子到地址.pdf> 2020/7/8 Journal Article
Reference Preview 区块链技术指南.pdf
参考文献类型: Journal Article
评级
Author
Year
Title
<区块链技术指南.pdf>
Journal
Volume
Part/Supplement
Issue
Pages
Start Page
Errata
Epub Date
Date
显示 12 个, 总 12 个文献.
布局
20:52
2020/7/9


区块链技术指南.pdf
密码编码学与网络安全++原
file:///C:/Users/92394/Desktop/资料/书籍/区块链技术指南.pdf
86 (共 227 页)
引入脚本机制带来了灵活性，但也引入了更多的安全风险。比特币脚本支持的指令集十分简单，基于栈的处理方式，并且非图灵完备，此外还添加了额外的一些限制（大小限制等）。
区块
一个区块将主要包括如下内容：
4 字节的区块大小信息；
80 字节的区块头信息：
版本号：4 字节；
上一个区块头的 SHA256 hash 值：链接到一个合法的块上，32 字节；
包含的所有验证过的交易的 Merkle 树根的哈希值，32 字节；
时间戳：4 字节；
86
原理和设计
难度指标：4 字节；
Nonce：4 字节，PoW 问题的答案；
交易个数计数器：1~9 字节；
所有交易的具体内容，可变长。
设计理念
如何避免作恶
22:13
2020/7/9

- **加密算法**：加密算法对明文进行各种代替和变换。
- **密钥**：密钥也是加密算法的输入。密钥独立于明文和算法。算法根据所用的特定密钥而产生不同的输出。算法所用的确切代替和变换也依靠密钥。
- **密文**：作为算法的输出，看起来完全随机而杂乱的消息，依赖于明文和密钥。对于给定的消息，不同的密钥产生不同的密文，密文看上去是随机的数据流，并且其意义是不可理解的。
- **解密算法**：本质上是加密算法的逆运算。输入密文和密钥，输出原始明文。

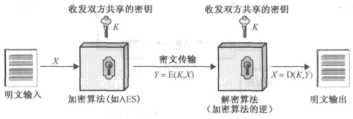


图 2.1　传统密码的简化模型

传统密码的安全使用要满足如下两个要求：

(1) 加密算法必须是足够强的。至少，我们希望这个算法在攻击者知道它并且能够得到一个或者多个密文时，也不能破译密文或计算出密钥。这个要求通常用一种更强的形式表述为：即使攻击者拥有一定数量的密文和产生这些密文的明文，他/她也不能破译密文或发现密钥。

(2) 发送者和接收者必须在某种安全的形式下获得密钥并且必须保证密钥安全。如果有人发现该密钥，而且知道相应的算法，那么就能解读使用该密钥加密的所有通信。

我们假设基于已知密文和已知加密/解密算法而破译消息是不实际的。换句话说，我们并不需要算法保密，仅需要密钥保密。对称密码的这些特点使其能够广泛应用。算法不需要保密这一事实，使得制造商可以开发出低成本的芯片以实现数据加密算法。这些芯片能够广泛地使用，许多产品中都有这种芯片。采用对称密码，首要的安全问题是密钥的保密性。

我们从图 2.2 中可以更清楚地理解对称加密方案的基本成分。发送方产生明文消息 $X=$