# 前言

上周的交谈会，通过网络与各位老师见面，各位老师也相应的给了我们一些相关的学习方向，比如了解一些区块链的比特币，以太坊等，去查看一些相关的参考资料。所以这周我开始去了解一下区块链的相关产物——比特币。这周我很幸运的搜到了一些大学的关于比特币学习的公开课，受益匪浅，并也记录了一些笔记，文章附录我会给出笔记和一些文章的相关链接。

# 1.什么是比特币

## 1.1比特币(Bitcoin)是什么?

Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called bitcoin are used to store and transmit value among participants in the bitcoin network. ------《Master Bitcoin》

“比特币”是一些概念和技术的集合，这些形成了“一种数字货币生态系统”的基础。“比特币”作为货币单位，被用于在比特币网络的参与者之间的存储和转移价值。

其实用通俗的话来讲，比特币就是一种基于密码学的电子货币。它与传统货币不同，比特币完全是虚拟的，从某种意义上，比特币是互联网货币的完美形式，它能够就像普通货币一样，包括买卖商品，汇款提供贷款等，基本上普通货币能做到的，它都能做。并且它更快速，安全，无边界。

## 1.2比特币有哪些组成?

如果说把比特币当成真正的货币，那比特币的组成有哪些成分呢？这些成分有涉及到什么知识呢？《Master Bitcoin》提到了比特币的组成：

比特币包括：

* 一个去中心化的P2P网络 （比特币协议）
* 一个公共交易账本 （区块链）
* 一套规则，用于独立的交易确认和货币发行 （共识规则）
* 一个机制，用于对有效区块链实现全球去中性化共识 （工作量证明算法）

简化来说，1.协议。2.区块链。3.共识规则。4.工作量证明。

其中所涉及到的知识大体包括：**1.密码学基础。2.比特币的数据结构。3.共识协议和系统实现。4.挖矿算法和难度调整。5.比特币脚本。6.软分叉和硬分叉。7.匿名和隐私保护作用**。其中每一部分知识我会在下面慢慢展开。

# 2.比特币的知识

## 2.1密码学基础

由于比特币属于加密货币(crypto-currency)，当然会涉及到密码学的知识，比特币属于一种开源信息的货币，其中的交易记录，交易金额，交易信息都面向全网开放。

比特币中加密涉及到两个内容：1.hash(哈希)。2.签名

1.密码学中用到的哈希函数被称为cryptographic hash function: 它有两个重要的性质:

1. collision(这里指哈希碰撞) resistance
2. hiding 哈希函数的计算过程是单向的，不可逆的。

除了密码学中要求的这两个性质，比特币中用到的哈希函数还有第三个性质：

1. puzzle friendly 指哈希值的预算事先是不可预测的。

比特币中用的哈希函数叫做**SHA-256(secure hash algorithm)**以上三个性质它都是满足的。这里这三个性质其实有详细解释，但是考虑到字数，我会放到附录的链接中。

2.签名又涉及到哪些密码学呢？在比特币系统中创建账户:在本地创立一个公私钥匙对(public key ,private key)，这就是一个账户。其中公私钥匙对是来自于非对称的加密技术(asymmetric encryption algorithm)。非对称密钥是用一对密钥而不是一个，加密用公钥，解密用私钥，加密和解密用的都是接收方的公钥和私钥。公钥是不用保密的，私钥要保密但是私钥只要保存在本地就行，不用传给对方。

通俗来讲，公钥相当于银行账号，别人转账只要知道公钥就行，私钥相当于账户密码，知道私钥可以把账户上钱转走。总体上来讲就是公钥和私钥都是用来签名的。然而这种签名机制就是采用密码学中的非对称加密。

## 2.2比特币的数据结构

比特币所涉及到的数据结构包括：

1. 哈希指针(Hash pointer)
2. 默克尔树(Markle Tree)

1.其实比特币最基本的结构就是区块链，区块链就是一个一个组成的链表，但区块链与普通链表不同的是：区块链采用了哈希指针代替了普通指针。这样的特点是，每个区块都根据自己的区块内容生成自己的哈希值，并且每个区块都要保存前一个区块的哈希值。其实就是有了哈希指针就可以保证该区块的唯一性，并且保证整个区块一旦写入就无法进行篡改。

2.而对于默克尔树Markle Tree，该数据结构类似于我们之前学到的二叉树一样。

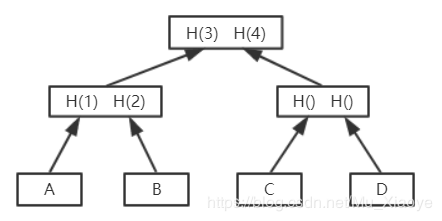


图2-1Markle Tree的示例

这种结构的好处：只要记住哈希值，就能检测出对书中的任何部位的修改。比特币当中各区块之间用哈希指针连接在一起，每个区块所包含的交易组织成一个merkle tree的形式，最下面一行data blocks每个区块实际上是一个交易，每个区块分为两部分，分别是块头和块身(block header ,block body)。块头里面有根哈希值，每个区块所包含的所有交易组成的merkle tree的根哈希值存在于区块的块头里面，但是，块头里没有交易的具体内容，只有一个根哈希值，块身里面是有交易的列表的。利用下面的图可以理解merkle tree的应用场景：

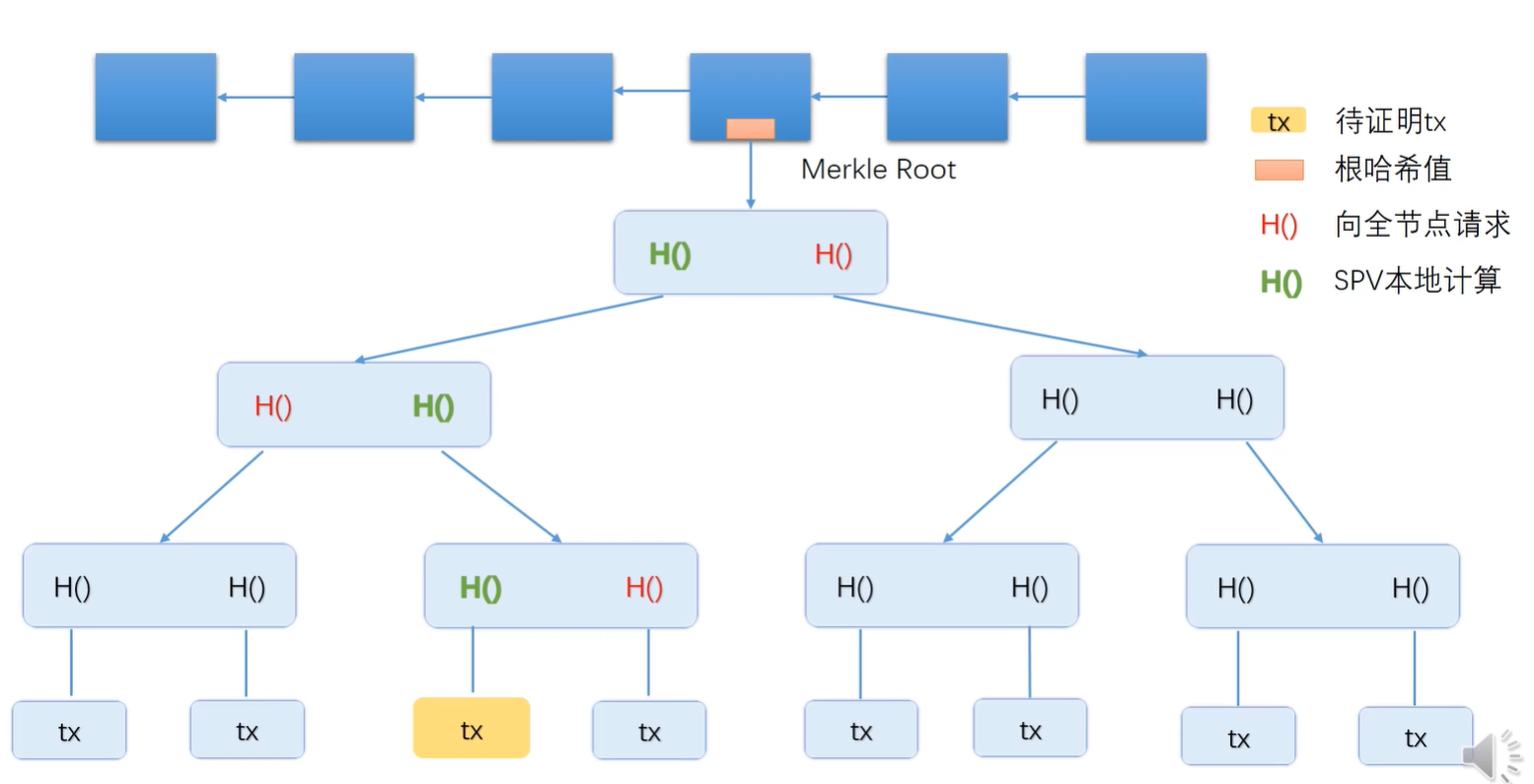


图2-2Markle Tree的应用场景

# 3.本周总结

当然比特币的知识没有在这里总结完全,上面提到的还有几个知识没有给出。毕竟比特币也没有说一周就能够完全掌握的，但是我会在以后的报告中尽可能的总结并完善我对比特币理解，同时也能够把这些理解关联到区块链中。其实这些知识点大部分都是我看网上的信息摘下来，并按照自己的话写下来的，可能会有一些理解的错误，或者解释不对的地方，还希望老师能提出来。同时这周我其实把大部分的时间花在看一些学校的公开课，上面提到的一些知识点有些就是来自我上课的时候听到的一些知识点。总体来说,写这个报告相当于回顾了这周看的课程和查看到的资料，同时这周我也查找到了Master Bitcoin 的中英双文的版本，而且也在CSDN查看了一些关于比特币的文章，我会在附录上给出相关的链接，并会把我的github信息显示出来，也希望各位老师能在其中提出问题。当然如果该报告有一些改进的问题或错误的地方，还望老师提出来，学生加以改正。

# 附录

**1.北京大学肖臻老师《区块链技术与应用》公开课(来自于B站):** <https://www.bilibili.com/video/BV1Vt411X7JF?p=1>

**2. 北京大学肖臻老师《区块链技术与应用》公开课系列笔记:**

<https://blog.csdn.net/Mu_Xiaoye/article/details/104299664>

**3.《Master Bition》github的中英双文版:** <https://github.com/Hello-Afa/MasterBitcoin2ndCn>

**4. 比特币原理详解:** <https://blog.csdn.net/zcg_741454897/article/details/102796022>

**5. 我的github的开源库：** <https://github.com/Hello-Afa/Graduate_career.git>