对比特币与区块链的基本认知

17343023 董宸宇

近年来比特币这个词越来越多的走进了大家的视野，比特币是互联网发展的产物，它是一种虚拟货币，不像我们平时所用的人民币，而区块链则相当于比特币的“地基“，区块链技术是基础，比特币则是在区块链的基础上衍生出来的应用。

随着互联网的发展，线上交易逐渐变得多了起来，这确实大大方便了我们的生活，因为很多东西，可能我们在线下很难买到，但是网络扩大了我们的市场。不过线上交易也有他自己的问题，其中最显著的就是信任问题，在传统的线下交易中，我们奉行的原则是“一手交钱，一手交货”但是在线上交易中，信任问题被放大了，因为我们在交易时“看不见”对方，可能买方交了钱，卖家拿钱跑路了，也有可能卖家发了货，买家不交钱了，而最常见的解决问题的方法是引入一个可信赖的第三方平台进行监督，如我们日常使用的淘宝，京东等等，这样虽然能保证诚信问题，但是第三方平台往往是提供收费服务的，所以最好的办法是提供一个既可以保证信任问题，又不需要第三方平台介入的机制，在这种机制下，买卖双方进行线上的点对点交易，而中本聪创造的比特币系统，正好能够满足这样一种机制

整个比特币系统大概可以分为三层，最上面一层是比特币，即应用层，中间层是比特币协议，即协议层，最下面一层是通用协议层，区块链就是在这一层。这种分层方式与我们在计算机网络中学习的协议层有点类似。

区块链是比特币的底层技术，而关于区块链的定义，在论文中写的很严谨，但对于不了解相关知识的人来说不太好懂，通俗的解释就是每个人都拥有一份“账本”，账本的内容是所有人共享的，每个人都可以在上面添加记录，然后把它展示给系统中的所有人，我们可以把整个系统看成一张用节点和线连起来的一张大网，每个用户都是其中的一个结点，而在这个系统中的每个人都希望自己的交易是安全的，这里就用到了密码学的原理，每个用户都有自己的公钥和私钥，在交易过程中，很大程度上靠的是密钥，举个例子，在一次交易中，A 应该向 B 支付 3 个比特币，那么 A 就使用他自己的私钥，从他自己的账户里面取出 3 个比特币转给 B（这一步的具体操作是把 A 把 3 个比特币的地址改成 B 的地址），若是 B 想拿出这三个比特币，就只有通过 B 自己的私钥，这样的好处是安全，通俗点理解就是每个人记录的信息都很庞大，如果有黑客想要攻击，难度就会大大增加，关于安全问题，在下面会更详细的说明

了解区块链，就需要了解区块链基本的数据结构，从名字上可以看出来区块链=区块+链，其数据结构跟链表很类似，只不过每个结点多了一个哈希值，这个哈希值由上个结点中的数据所确定，这样在一定程度上也增加了整个系统的安全性，毕竟若是想更改某个节点的话，会产生类似“多米诺骨牌”式的效应，需要将剩下的所有结点全部更改，这样就给黑客的攻击带来了很大的难度，而每个区块中的数据则是这个区块所进行的交易的记录，这些记录的存储也采用了一种二叉树数据结构，叫梅克尔树，它所起的作用跟上面所提到的哈希值类似，都是防止数据被篡改的措施。

前面说到每个人都拥有一份账本，且账本上的信息所有人共享，这就又带来一个新的问题，假设有甲乙丙丁 4 个人，甲和乙在同一时间分别在系统中发布了 A 和 B 消息，但是丙离甲比较近，丁离乙比较近，所以 A 消息很自然的先传播到丙那里，B 消息则会先传播到丁，这样以来丙和丁账本上的信息出现了不同，这样就违背了我们前面所说的机制，所以在这里，区块链系统提出了一种机制:即信任最长的链，最长的链工作量也最大，所以还

需要一个工作量的证明机制，机制在这里摘自中本聪的论文: 我们在区块中补增一个随机数，这个随机数要使得该给定区块的随机散列值出现 了所需的那么多个 0。我们通过反复尝试来找到这个随机数，找到为止。这样我们就构建了一 个工作量证明机制。只要该 CPU 耗费的工作量能够满足该工作量证明机制，那么除非重新完 成相当的工作量，该区块的信息就不可更改。由于之后的区块是链接在该区块之后的，所以想 要更改该区块中的信息，就还需要重新完成之后所有区块的全部工作量。，从安全的角度来说，这种机制也同样有利于维护系统的安全，具体原因参见上面说到的“多米诺骨牌”式效应

对于在互联网上听说过比特币的人来说，“挖矿”应该是一个带有神秘色彩的名次，在比特币系统中的挖矿，实质上就是把一些未认证的交易采用区块使用的梅克尔树结构来组合起来，并创建区块，而比特币系统有奖励机制，每创建出一个区块，就会获得相应的比特币奖励，或者是进行加密哈希计算，计算机与计算机之间进行算力竞争，谁先解决问题，谁就能获得比特币，也就是所谓的“挖出矿”。

关于区块链技术在未来的发展问题，我觉得区块链的技术会逐步的进入各行各业，不断影响着我们生活的各个方面，现在有很多业务已经使用到了区块链的技术，但是至少在目前来看的话，比特币这种电子货币还是很难取代传统货币，今天的货币体系是全世界共同维护出来的体系，具备稳定性，由各国政府部门来进行发行，而基于区块链的比特币技术，若是真正想推广开来的话，还有很长的路要走，也有可能现有的货币体系就是最符合社会主流的体系，这个体系会一直保持下去并占据主导地位

以上内容是我在阅读了老师给出的论文，以及自己在网上查阅的一些有关比特币和区块链的资料之后，根据自己的理解，总结出来的一些关于比特币和区块链的内容，由于自己之前没怎么读过论文，所以在阅读方面还是感到比较吃力，对论文中内容的理解可能也不够深入或准确，不过随着学习的深入，期待自己能对比特币和区块链有更为深入的理解。