# 计算机安全导论课程报告

# 关于区块链技术的学习报告

班　　级: 1703011

学　　号: 17069130005

姓　　名: 崔恩博

二零一九年十一月

# 摘　　要

区块链技术在电子加密货币、存证鉴伪、供应链溯源、选举投票、物联网等场景中有广泛应用。从最初的比特币，到后来代表区块链技术 2.0 的以太坊，再到现在的石墨烯技术上建立的去中心化应用，区块链技术在不断的完善着。本文将针对区块链技术及其发展，从数据结构、共识机制等角度探讨自己关于这几代区块链技术的认识和理解，最后再结合一个实例来讨论区块链 3.0 之后的去中心化应用及发展。

**关键词**：区块链；比特币； 数据结构； 共识机制； 去中心化应用

# 第 1 章　绪 论

## 1.1　区块链起源

2008 年中本聪综合前人在加密货币上的成果提出了比特币的概念，并于 2009 年 1 月 3 日挖出了创世区块，实现了数字世界的价值表示与价值转移，也引发了人们对其底层技术--区块链技术的探索。在比特币之前就有很多专家进行过加密货币的研究，并给出了自己方案，如亚当·贝克的哈希现金，哈尔·芬妮的比特黄金，戴伟的 B-Money 等。他们的方案存在着一个共同点，就是要通过计算机的计算来创造电子现金。在这种思想的基础上，中本聪融合前人观点，设计了基于工作量证明的共识机制，使得去中心化成为可能，最终解决了数字现金的问题。

## 1.2　以太坊

以太坊创始人维塔利克分析了比特币系统，在比特币系统的四点不足上建立以太坊。其目标是建立一个新的区块链，内设有成熟的图灵完备的语言，可以利用这种语言来编写代码，创建合约，实现任意的状态转换。

以太坊的突出贡献在于实现了智能合约，使区块链技术从数字货币向数字资产转变。对于由智能合约来控制的实体资产，引用萨博的例子来说明：“例如，为了防止一部车被偷窃，除非确定拥有者完成正确的“挑战响应协议”，否则车是不会启动激活的。 例如，如果车是贷款买的，当拥有者无法偿还贷款时，智能合约将会自动启动扣押令，并将车钥匙的控制权交给银行。一旦拥有者还清贷款，智能合约就移除扣押令。”总而言之，以太坊的出现使得创造通证变得简单。随着物联网技术的发展，越来越多的机器需要通证，基于区块链技术，为机器设计专用的钱包和通证将成为未来物联网发展的又一可能。

## 1.3　EOS

在《区块链革命》中，商业思想家唐·塔普斯科特这样写道：“区块链上运行的所有计算资源可以在整体上视为一台计算机。”。仔细考虑使用一条区块链所需要的资源，包括带宽资源（相当于硬盘）、计算资源（相当于 CPU）、 状态资源（相当于 RAM），确实和一台计算机十分相似。以太坊曾把自己定位为一台“全球分布式计算机”，那么 EOS 就是建立在这台计算机上的软件系统，他代表了区块链应用的一种发展方向，即开发一条通用的基础公链，实现一切去中心化。通过相关资料，我发现 EOS 已经在许多方面大异于比特币和以太坊，比如他的共识机制、区块产生方

式，账户等，并且开创性的提出了基于角色的权限系统。目前来说，区块链技术想要落地应用还有很多问题没有解决，哪条路才是切实有效的也没有定论，未来等着我们去探索。

## 1.4 结构安排

本文共分为三大部分，首先从比特币说起，讲述我学习到的比特币系统，阐述其数据结构、共识机制，分析安全性等。之后，讨论代表区块链 2.0 的以太坊，由于他的共识机制基本与比特币相同，所以主要阐述了以太坊的三种主要的数据结构。第三部分，阐述了区块链应用的可能方向以及一款基于功能类公链的应用实例--Steemit。

# 第 2 章 比特币系统的技术原理及安全分析

在比特币系统中第一次给出了区块链技术的定义：“区块链是数字世界中进行价值表示和价值转移的技术。”而比特币作为区块链硬币，他的一面是表示价值的加密数字货币或通证，另一面是进行价值转移的分布式账本与去中心网络。本章将从分布式账本与去中心网络及数据结构的角度讨论比特币系统，并分析其安全性。

## 2.1 分布式账本与去中心网络

威廉·穆贾雅在《商业区块链》中将比特币总结为四个要点分别是：点对点电子交易；不需要金融机构；加密证据而不是中心化信用；信用存在于网络，而不是某个中心机构。

现如今的数字世界中的货币有三种存在形式，包括中心化的在线支付，如微信、支付宝等；中心化互联网积分，如 Q 币等；去中心化的电子现金。在中心化的在线支付系统中流转的货币是各种法币的映射，这些映射来的“数字货币”本身没有价值，其价值依赖于法币本身的购买力。同样中心化的互联网积分，其价值不与任何法币想关联， 完全由发行公司决定，且只能用于购买这家公司的服务和产品。对于比特币系统的去中心网络比特币的价值由其算法保证，即使整体的算力出现波动，算法也能在至多 2016 个区块后通过调整目标阈值来调整挖矿难度，从而使得比特币系统的平均出块间隔维持在 10 分钟左右，以此保证了比特币系统内部比特币的价值稳定（与法币的汇率不是由比特币系统决定的）。比特币的以上优点很大程度上是得益于其分布式账本和去中心网络。

比特币的去中心网络由由众多轻节点和全结点组成，其中全节点包含所有比特币区块链的区块数据，轻节点仅包含自己相关的数据。并且比特币网络是开放的，任何服务器都可以加入成为全结点，共同维护这个去中心网络。由于网络没有一个类似于“央行”的中心化组织存储信息，所以所有用户持有的比特币信息都存在一个分布式账本中，可以认为同时存储在所有全结点中。

## 2.2 比特币系统的加密体制

比特币与密码学是密不可分的，从比特币“账户”（实际是地址）产生就使用了非对称密码体制，到每次交易签名，再到区块链内部的梅克尔树，以及区块链间的哈希指针都反应了密码学原理。

首先，在生成一个比特币账户时，实际上我们得到的一对公私钥对，其中公钥的哈希值即为比特币地址，作为转账交易的收付款地址；而私钥用于对我支付的每一笔交易进行签名。当我发起一笔交易时，我将用我的私钥对这笔交易记录进行签名， 同时广播出我的公钥以便其他的节点能够验证这笔交易的合法性，同时我还要为这笔交易付一点“小费”。这样操作下来，再等上一段时间，我的交易就会被写入区块链中

成为不可逆的交易。

比特币系统使用的哈希函数是 SHA-256。除了哈希函数本身的抗碰撞性和单向性外，应用于比特币系统的哈希值还有 puzzle friendly 的性质，即要求块头的哈希值小于某个目标阈值。以及难于计算，但易于验证的性质。这些性质一方面保证了区块链上数据的不可篡改性，另一方面也为各个节点达成共识提供了基础保障。

此外，这种密码体制的安全性还建立在一个好的随机源上，这样才能确保有足够大的搜索空间来保证安全性。

## 2.3 比特币区块链的数据结构

比特币区块链是一条通过哈希指针连接起来的链表。后一的区块的哈希指针是通过前一区块的全部内容(包括前一区块的哈希指针)计算出来的。这样从最后一个区块就能知道前面的区块是否被修改，使得系统中的某些节点不需要保存全部区块信息。

每个区块中的数据是被打包进这个区块的一系列交易，这些交易按规则形成一颗梅克尔树。梅克尔树是一颗由哈希指针连接起来的哈希树，其中叶子节点是要打包进区块的交易信息,非叶子节点是由叶子节点计算而来的哈希值。这样设计有很多好处，比如一个轻节点如果想知道自己的交易(位于第 n 层)是否已经被打包进区块链中，那么他只需要向全节点请求他不在的那条路径上非叶子节点的哈希值。之后，它就可以先计算要验证交易的哈希值（这一定是已知的），再将这个哈希与全节点给出的第（n-1）层的哈希值共同计算(n-2)层的哈希值，如此迭代下去，最终可以求得这笔交易所在的梅克尔树的根哈希值。将这个根哈希值与全节点给出的根哈希值比较即可验证交易。这样设计使得更多的节点能够低门槛的连入比特币系统，增加了比特币系统的活跃程度。

此外，区块头部中也包含着很多的重要信息，比如比特币版本协议信息，指向前一个区块的指针，梅克尔树的根哈希值，挖矿的难度目标阈值，随机数等。这些信息对于比特币系统达成共识有着至关重要的作用。

## 2.4 比特币系统的共识机制

所谓共识机制，指的是众多互不相识、互不信任的节点之间就交易的合法性达成一致意见。这对于比特币这样一个去中心化的网络十分重要，只有确保了共识机制，才能保证不同账本节点上数据的一致性和正确性。

比特币系统所采用的策略是工作量证明。简单来说就是通过求解一个随机数来使得块头的哈希值小于一个给定的目标阈值，这个过程也称为挖矿。从概率学的角度来说，每次实验都可以看作是一次伯努利实验。当试验次数很多，而成功概率很小的时候，我们就可以用泊松分布来近似。也就是说，在比特币系统中，想要得到记账权没有任何捷径可走，只能单纯的通过反复尝试不同的随机数来求解。这也就保证了每个挖出区块的节点都是做了大量的工作来维护这条区块链，从而保证了区块链上数据的一致性。

比特币系统在共识机制做出了两点创新。其一是引入了奖励机制，通过比特币奖励使得区块链上节点愿意打包交易，主动维护账本，加快了一致性的达成。其二是引入了随机性的概念,尽管比特币系统不是完全可靠的,但是一般来说经过 6 个区块后，出问题的概率会呈指数级下降。

实际上，共识机制的形成过程是一个投票过程，只不过比特币系统是通过算力进行投票。拥有较大算力的节点能够优先把自己认为合法的交易打包进区块中，即通过算力给这些交易投票。

## 2.5 比特币系统的安全分析

首先通过一个例子来简单的说一下比特币的转账过程。假设现在甲要向乙进行转账，那么甲会发起一个转账交易，并用自己的私钥进行签名，同时将收款人的姓名写为乙的地址，并发布出去。听到这个交易的节点，首先验证 nbits 域的设置是否符合难度要求；验证头的哈希是否小于等于目标阈值。然后验证 body 中的交易是否有甲的合法签名,这笔钱以前是否被花过。第三要验证这个区块是否是连在最长合法链上。假设这个区块已经被打包进了区块链中,那么沿着这个区块继续挖的区块也会来验证这笔交易。一般来说，经过 6 个区块后这笔交易就可以认为是这笔交易不可篡改。针对比特币的转账过程，我探究了以下几种安全问题。

### 2.5.1 伪造转账交易

首先，考虑攻击者能否转走别人账户上的比特币。这是不可能的。第一，因为比特币系统中合法交易需要交易发起方用自己的私钥进行签名，而私钥无法伪造，所以不能成功。第二，如果恶意节点强行将交易写入区块中，那么诚实的节点也不会认可这笔交易，同时攻击者也损失了一笔出块奖励，同样说明这种攻击难以实现。

一般情况下，发起交易的一方要广播自己公钥来让其他节点可以验证自己的签名合法性。假设现在有一个攻击者想要转走 A 账户上的比特币，那么他先伪造一笔 A 转出的转账交易，并用自己的私钥进行签名，同时广播自己的公钥说成是 A 的公钥。这样能否转走 A 账户上的比特币呢？也是不可能的,因为 A 账户上的比特币一定来自之前的某一笔交易，而之前交易的收款人地址正是 A 的公钥的哈希。由于攻击者的公钥哈希与这个收款地址哈希对不上，其他节点就不把他作为合法交易，也不会写进区块链中。

### 2.5.2 回滚交易数据

假设现在 A 要向 B 转账 5 个比特币，A 签名了这个交易并发布到网络上，表面看起来 B 已经得到这笔交易的输出。但是如果攻击者立即发布一笔交易将这 5 个比特币转给自己，由于两笔交易都有 A 的合法签名，所以两者都会被作为合法交易打包进区块链中。同时如果攻击者具有足够多的算力将回滚交易所在的链拓展成最长链，那么交易就会被回滚。这种通过向区块链中间插入某个区块来回滚某个已经发生的交易，又称为分叉攻击。防范这种攻击的简单方式是等待六个区块的确认，这样拓展回滚交易所在的链的难度就会大大增加。

分叉的原因有很多，实际上，即使完全正常运作的比特币系统中也会存在分叉。可能有两个节点几乎同时挖出了新的区块，并把它广播出去。由于网络延迟和节点间距离的差异最终导致不同的节点收到了不同的合法区块。按照比特币协议，一个节点只会接受第一个收到的合法区块，所以最终会导致区块链出现分叉。但这种分叉只是暂时的，随着时间的推移，两条分叉上的算力互相竞争，最终会以一方称为绝对的最长合法链而告终。

### 2.5.3 掌控最长合法链

我们知道，新的区块的内容中包含前一区块的哈希值。也就是说，在正常情况下没有前一个区块就不能产生新的区块。并且比特币系统中，合法的区块应该是位于最长合法链上。现在如果有一个恶意节点想要掌握最长合法链，当他挖出一个区块后，先不广播，而是在这个区块的基础上接着挖下一个。直到自己手里这条链变成绝对的最长合法链再一起发布出去，从而使得其中的非法交易合法化。这种攻击很难奏效，因为比特币系统是基于算力进行投票的，所以攻击者想要将自己的链变成最长合法链有很大难度。

挖出区块而不广播的理由可能还包括盈利目的。假设某个节点挖出了第 n+1 个区块，但是不立即广播，然后接着这个区块继续挖第 n+2 块。当有其他节点挖出第 n+1 块时，他立即广播第 n+1 和 n+2 块。那么由他记账的区块链就变成了最长合法链，同时得到这两个区块的出块奖励，看起来就像是一步领先，步步领先。

但实际上，在比特币系统中，这种行为很难成功。这样做的成功前提是在别的节点挖出一个区块的时间里，他能保证挖出两个以上区块。这样做存在很大风险，有可能一个出块奖励也得不到。

### 2.5.4 比特币的匿名性

比特币系统的匿名性是很难以维护的，因为区块链是公开的，并且区块链具有不可修改性。一旦有一次交易暴露了身份，那么这个影响将是永久性的。并且比特币作

为一种虚拟货币，最终会和法币相关联，一旦与实体世界发生关系，那么就可能在用比特币支付和进行资金转入转出时发生隐私的泄漏。如果先不考虑与实体世界的联系，我们可以每次转账交易都生成一个新的地址，采用多路径转发的方式，使得从交易推理出身份的难度增大，从而加强匿名性。此外，市面上还出现了牺牲性能而增强匿名性的货币，如零币零钞等基于零知识证明的加密货币。但是由于普通用户对匿名性的要求并不高，所以并未被广泛使用。

## 2.6 总结

以上就是我对一些感兴趣的攻击比特币系统的手段分析。上述分析基础是比特币网络中大部分节点都是诚实的，恶意节点只是少数，不会占据 51%以上的算力。然而近些年出现的矿场使得算力更加聚集，历史上就曾经出现过大型矿场占据 51%以上的算力的情况(他们为了防止引起恐慌，自行分解了算力)。这说明比特币系统的安全性是相对的，想要持久的维护比特币系统的安全性就要维持比特币社区的活跃度，使得诚实的节点永远占据大多数。

# 第 3 章 以太坊

维塔利克在分析了比特币系统的缺陷的基础上提出了以太坊。目标是提供一个区块链，内置有成熟的图灵完备的编程语言，用这种语言可以创建合约来编码，实现任意状态转换功能。通过这种语言，按照 ERC 标准，我们可以编写出自己的智能合约，进行区块链上的状态转换，进行链上数字资产的转移。其开创性的智能合约使得区块链技术从数字现金向数字资产转移，为日后的应用奠定了基础。接下来的一部分主要描述一些关于以太坊的数据结构。

## 3.1 以太坊的数据结构

首先，以太坊区别于比特币系统，设置了账户系统。在比特币系统中，每次交易都会把余额转到另一个零钱地址中。而以太坊中为了支持智能合约，就需要参与方有相对稳定的身份，所以改用账户系统，每次交易直接增删余额。以太坊被看作是由交易驱动的状态机，所以在以太坊中要保存状态和交易。因此，以太坊设置了三种树，分别是状态树，交易树，和收据树。

### 3.3.1 状态树、交易树、收据树

建立状态树的目的是要建立一个从账户到状态的映射。其中以太坊账户为 40 位十六进制数，状态中包括余额，交易次数，如果是合约账户还包括代码和存储的变量。同时，要求这颗树上的数据不可篡改，便于查找，增加，删除，同时节省存储空间。此外，应该令轻节点易于验证某个键值对是否存在。于是以太坊在传统的 Trie 树的基础上，压缩路径，增加哈希指针得到了 Modified Merkle Partricia Tree。

首先说 Trie 树，它常被用来存储单词，进行多模式串的模式匹配。在以太坊中，由于账户是由 40 位十六进制数构成，所以每个节点的分支最多有 17 种可能（加一个结束标志）。Trie 树的优点是无需排序，即使插入顺序不一样，得到的结构也是一样的；同时它还具有很好的更新局部性，由于每个区块中涉及发生的交易是少数的，采用这种结构不需要去管其他的分支，增强了修改的性能。

Trie 树的缺点也很明显，它有很大的存储浪费，并且实际的查找效率与树的深度有关。于是进一步的考虑 Partricia tree，一种路径压缩的 trie 树。对于基数树的每个节点，如果该节点是唯一的儿子的话，就和父节点合并。当键值分布较为稀疏的时候，更新时需要打开压缩部分的概率就比较低，性能也就更好。而以太坊的地址就恰好是这种结构。

借鉴比特币系统的思想，将树中指针全部换成哈希指针得到了 Merkle Partricia Tree(MPT)树。而以太坊系统中使用的是略作修改的 MPT 树，本质上没有改变。

以太坊的结构是一颗大的 MPT 树中包含很多小的 MPT 树，每个小的 MPT 就是一个

合约账户。对于全节点来说，他维护的也不是一颗 MPT，而是每产生一个新的区块就新建一颗 MPT，这些树中大部分节点是共享的，只有少数更新的节点可能要新建分支。

我通过与比特币系统的对比，发现比特币系统中不需要保存历史状态，而是通过 UTXO 的输入输出计算得来。但是以太坊不同，由于账户的设计，智能合约的出现，每个交易被打包进区块链的时候，其账户余额也被改变。这样设计的优点是天然的防范了双花攻击。但是如果某个交易所在区块不在最长合法链上，为了保持账户余额和合法链上得到的交易的结果是一致的，就需要对分叉部分进行回滚。我认为这就是需要保存历史状态的原因。

至于交易树和收据树，他们本身也是一颗 MPT 树。每个交易执行完，会形成一颗收据树，记录这个交易的相关信息。交易树和收据树上的节点是一一对应的。但每个区块的交易树和收据树又是相互独立的。他们发布的交易本身也被认为是相互独立的。

### 3.3.2 bloom filter

以太坊为了支持一些复杂的查询的查询操作，比如查询近十天里和某个智能合约相关的交易而设计了这个数据结构。对于这个问题，可能最开始的想法就是遍历这个链将符合规则的区块挑出来，但是对于轻节点来说，他不能保存所有区块的信息，同时也存在查找效率低下的问题。

而 bloom filter 结构可以理解为一个大的向量，称为摘要。是将每个元素取一个哈希，形成的一个向量，其中某位为 1 代表对应该哈希值的元素存在。假如现在要查找过去十天发生的和某个智能合约相关的交易。首先，查找区块块头的 bloom filter，看看哪个块头的 bloom fikter 里有我要的交易类型。如果某个块头里有，再去相应的收据树的 bloom filter 中查找。每一步轻节点都可以向全节点请求少量的信息就可以查询下去，很好的解决了问题。即使考虑哈希碰撞，那么也只会出现误报，而不会出现漏报。而误报情况可以在逐渐细化的查询中被发现。

### 3.3.3 cache 与 DAG

比特币的挖矿设备从最初的 CPU，转向 GPU，再到现在的 ASIC 芯片挖矿，设备趋向于专业化，挖矿门槛越来越高。这样不利于比特币系统的安全稳定，只有当算力足够分散的时候，发动 51%以上算力的攻击才很困难。为了做到杜绝 ASIC 芯片，以太坊在莱特币的基础上改进了挖矿算法，使得求解从纯粹的算力竞争上转向内存竞争。

莱特币曾经是市值仅次于比特币的一种加密货币。他首先将内存引入了挖矿算法。他基于 Scrypt 加密算法，需要用大的内存来保存这个数组，否则每次都要重新计算。简单来说，Scrypt 算法是先通过一个种子取哈希得到数组中的第一个元素，之后再将这个元素取哈希得到第二个，反复迭代得到后面的元素。但是对于轻节点来

说，他只是想验证某个区块的合法性，却需要和矿工等量的计算。这与区块链的基本理念:难于计算，易于验证相悖。考虑到这个原因，莱特币只将这个数组设置为 128K，这显然太小了，对于矿机来说，完全可以通过计算来弥补内存的薄弱。

以太坊在莱特币的基础上进行了改进。他规定了两个数据集，16M 的 cache 和 1G 的 DAG，其中 DAG 是通过 cache 计算得来。轻节点只需要保存 cache 即可验证区块，矿工通过 DAG 来计算随机数使最后的哈希值低于目标阈值。

Cache 的形成与莱特币类似，也是从一个种子节点开始依次取哈希来填充数组。对于 DAG，他首先从 cache 里随机读一个数，然后进行哈希计算，得到下一个要读取的数的位置。然后用 cache 中这个位置的数和当前的哈希值再计算出一个哈希。反复迭代 256 次，将最终得到的数填充到 DAG 的第一个位置。

对于矿工来说，在挖矿的时候，先根据块头和 nonce 值计算一个哈希，这个哈希映射到数组中的某一个位置。通过这个位置和其相邻位置的元素进行运算得到下一个要计算哈希的位置。反复迭代 64 次，最后得到的哈希值与目标阈值比较，看一下是否满足要求，不成功则换下一个 nonce 尝试。

对于轻节点，想要验证一个区块是否符合要求，他需要这个区块的 nonce 以及 cache 数组。验证的过程与挖矿类似，只是轻节点没有保存 DAG 中的元素，所以用到的部分需要从 cache 中重新计算生成。

## 3.2 智能合约

关于智能合约，其智能可以理解为是一段自动执行的代码，无需外界干预，自动自治进行，运行在以太坊虚拟机中；合约可以看作一个管家，一个“自治代理”，它拥有自己的账户，交易发生时自动执行一段代码。借用 V 神的话就是“他们收到交易信息后就相当于被捅了一下，然后自动执行一段代码”。

如果说区块链存储的是状态，那么智能合约就是用于状态转换的方式。它像是一个特别的时钟，把世界从同步转向异步。

智能合约的出现使得创建通证变得简单。Komhar 公司曾给出过 ERC20 通证发行过程，大体可以表述为：一个项目通过智能合约创建通证，这个通证是实体资产或线上资产的价值表示物。投资者（用户）发起交易，向智能合约转入以太币（ETH），智能合约自动运转，在满足一定规则后，它向投资者账户转入相应数量的通证。这里的通证大多对应以太坊区块链之外的资产。因此，以太坊的出现对区块链技术转向数字资产做出了巨大贡献。

## 3.3 以太坊共识机制与 GHOST 协议

在比特币系统中，只有在最长合法链上挖出来的区块才有出块奖励。这使得挖出分叉的节点不甘心放弃自己链，对于大的矿池来说，他很有可能不顾一切的去挖自己的链使他成为最长链。这样做的优点是便于确认区块的合法性，也在一定程度上避免了双花。但是对于以太坊来说，这样做并不合适。以太坊设有账户系统，可以杜绝双花，而且以太坊的平均出块时间设定为 15 秒，分叉也会成为常态。因此，以太坊引入了 GHOST 协议，目的是在出现分叉后及时合并。

GHOST 协议的核心思想是对没有竞争成为最长合法链的区块也发放一定的出块奖励。同时下一“代”区块要包含所有的叔父区块，并得到 1/32 个出块奖励的额外报酬。为了防止在挖矿难度较低的时候产生叔父而不当获利，以太坊规定叔父必须是 7 代以内。并且叔父区块中的交易不执行，因此也不检查交易合法性，只检查这个区块是否符合挖矿难度。

GHOST 协议一方面保证了分叉及时被合并，另一方面也减少了 ASIC 矿机挖矿的必要性，有利于维持分布式账本和区中心化的稳定。在回避 ASIC 的问题的问题上，以太坊另一个做法是每年都宣称自己即将从工作量证明转为权益证明，从而有效的将以太坊挖矿限制在 GPU 挖矿的级别。

# 第 4 章 区块链的应用与 Steemit 博客

## 4.1 区块链的性质

想要将区块链投入应用，首先要明确区块链有什么用。有人总结区块链的性质总结为以下四条。

第一，是不可篡改性。要修改一个区块中的数据，那么就要修改后面所有的所有区块。而共识机制的存在使得修改大量区块的成本极高，因此篡改几乎不可能实现。2018 年 3 月，在网络零售集团京东发布的《区块链技术实践白皮书》中，京东认为，“区块链技术（分布式账本）的三种应用场景是：跨主体协作，需要低成本信任，存在长周期交易链条。这三个应用场景所利用的都是区块链的不可篡改特性。多主体在一个不可篡改的账本上协作，降低了信任成本。区块链账本中存储的是状态，未被涉及的数据的状态不会发生变化，且越早前的数据越难被篡改，这使得它适用于长周期交易。”

第二，是表示价值所需要的唯一性。比特币的出现使得数字世界中出现了一种不可复制的“文件”。腾讯 CEO 马化腾说“区块链确实是一项具有创新性的技术，用数字化表达唯一性，区块链可以模拟现实中的实物唯一性。”百度 CEO 李彦宏说：“区块链到来之后，可以真正使虚拟物品变得唯一，这样的互联网跟以前的互联网会是非常不一样的。”

第三，是智能合约。智能合约的出现使区块链上可以进行更加复杂的交易，并且交易本身也不可篡改。在以太坊白皮书中，维塔利克写道：“（合约）应被看成存在于以太坊执行环境中的“自治代理”，它拥有自己的以太坊账户，收到交易信息，它们就相当于被捅了一下，然后它就自动执行一段代码。”

第四，是去中心自组织。在《去中心化应用》一书中，作者西拉杰·拉瓦尔（Siraj Raval）从两个维度看现有的互联网技术产品：一个维度是，在组织上是中心化的，还是去中心化的；另一个维度是，在逻辑上是中心化的，还是去中心化的。在他看来比特币在组织上是去中心化的，在逻辑上是集中的。

根据这些性质，有人总结了五条区块链通向应用平台的可能路径。分别是通用类基础公链，功能类基础公链，行业类基础公链，联盟类基础公链，基础服务。在我看来，开发专用于某个功能的基础公链更可行，接下来通过 Steemit 来谈一谈区块链的应用。

## 4.2 Steemit

Steemit 是基于 steem 公链平台的社交软件，类似于博客。可以通过发文章，写评论来赚钱，但没人直接付钱。这个平台促进内容生产者发布更加优质的内容，同时屏蔽掉劣质内容。

Steem 链中有三种代币，分别是 steem，steem power, steem dollar。其中，Steem 币是 Steem 链的基础代币。Steem Power 相当于股权，只能持有不能买卖。Steem Dollar 是公链中稳定代币，无论何时，SBD 只能兑换成价值一美元的 Steem 币，维持内部代币价格稳定。

当作者发布一篇文章时，并不马上得到收益。其收益真正来源于持有 SP 用户的点赞，这点类似于 EOS 的权益证明。拥有 SP 越多的用户点赞带来的收益也越多，同时点赞用户也会得到一部分收益，类似于矿工打包交易时的得到的手续费。此外，SP 用户还可点踩，当点踩的人足够多时，Steemit 会隐藏这些内容。

# 总　　结

总的来说，区块链很有可能成为互联网上的新层次，专门用于进行价值表示和价值转移。 在其上可以建立区块链应用，以利用区块链的价值表示和价值转移特性，在链上进行数字资产的转移。同时这些数字资产被映射成链上原生资产，线上资产或线下资产，从而改变目前人类的生成生活方式，影响金融、军事、教育乃至生活的方方面面。

通过本次大作业的机会，我充分学习了关于区块链的内容。区块链的诸多性质中，去中心化的性质尤其吸引我。在中心化的网络中，我们的数据是不安全的，每天倡导安全的组织却能轻易掌握我们的数据；我们的思想可能是被蓄意引导的；努力工作得到的货币也未必是保值的；同时，离开中心我们也是生存不下去的。也许去中心化的系统中存在着混乱，比如区块链中的分叉，但是我认为混乱也是一种自治，或许目前的去中心化的结构还不完善，性能还不够强大，但我相信在不远的将来，我们就可以在生活的方方面面感受到去中心后的便利。