华南理工大学

课程报告

课程名称：	企业软件项目实训
学生姓名：	邹鹏宇
学生学号：	201630666653
学生专业：	软件工程
开课学期：	2018-2019 第二学期

软件学院

2019 年 6 月

目录

概述

过去的六周时间里，我们学院开展了与微众银行合作的实训课程，在软件学院和微

众银行的老师们的教授和指导之下，我们有幸接触了区块链这一领域及其相关的知识和技术。区块链这个专业术语对我个人来说常有耳闻，但一直没能够对其架构和设计有所了解，这一次实训课程中，在老师的指导下，我不但收获了很多干货，而且还亲身接触了 FISCO-BCOS，这个在业界享有很大知名度的区块链底层平台。微众银行的老师们不但就该平台的技术、算法细节进行了讲解，还提供了非常宝贵的实操机会给我们。在 FISCO-BCOS 这一区块链底层平台的技术支持下，我们尝试了在自己本地搭链并通过通过控制台对智能合约进行部署、调用等操作。最后，我们将所学所见融汇贯通，根据实训大作业的要求，开发了一个宠物市场的虚拟购物平台，虽然我们并没有在老师给出的题目上有所创新，作为小组组长，我认为我们小组更希望在需求已经比较明确的条件下，将注意力更多地放在我们项目的实现，以及对我们课程内容的实践上面，最终我们的大作业成果还是得到了学院、微众银行的老师们的肯定，这是所有组员分工明确、共同付出的结果。

以下是就区块链相关的几个问题做出的回答：

1. 区块链技术原理

现在互联网上的交易，几乎都需要借助可资信赖的第三方信用机构来处理电子支付信息，比如说支付宝和微信，这类支付方式极大程度上地依赖于第三方机构，用户的隐私信息和个人资产的相关信息都存储在一个中心机构内，安全得不到保证，导致该中心机构的权利过大，通常中心化的系统，会有一个中央服务器来存储数据，通常这个服务器就是一个数据库，如 MySQL、Oracle 等。而去中心化的系统，不再将数据存储于中央服务器，而是存储于比特币网络的每个节点中，将每个节点比作电脑的话，这个记账数据会存在于每个电脑里。但是由于像支付宝和微信这样的可信赖中心机构不可能在国内或者世界上广泛存在，因此去中心化的思想就变得非常重要。运营机构保留一定的权利，但是用户所有的信息和操作记录都以一种不可篡改的方式记录着，因此，区块链的技术和思想应运而生。

一说到区块链技术，让人最容易想到的就是比特币。区块链技术是构建比特币网络与交易信息加密传输的基础技术。它基于密码学原理而不是基于信用，使得任何达成一致的双方直接支付，从而不需要第三方中介的参与区块链（Blockchain）是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术，区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。区块链技术正是比特币技术的基础，简单地说，区块链是一个分布式账本，一个通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案。

从数据的角度来看，区块链是一种几乎不可能被更改的分布式数据库。这里的“分

布式”不仅仅体现为数据的分布式存储，也体现为数据的分布式记录（即由系统参与者共同维护）。

从技术的角度看，区块链并不是一种单一的技术，而是多种技术整合的成果。这些技术一新的结构组合在一起，在不同功能方面起着各自重要的作用，形成了一新的数据记录、存储和表达的方式。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。

狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式。

我大致地总结了一下区块链技术中重要的几个知识点：

1.1 分布式账本

分布式账本，就是交易记账由分布在不同地方的多个节点共同完成，而且每一个节点都记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证，从实质上说就是一个可以在多个站点、不同地理位置或者多个机构组成的网络里进行分享的资产数据库。在一个网络里的参与者可以获得一个唯一、真实账本的副本。账本里的任何改动都会在所有的副本中被反映出来，反应时间会在几分钟甚至是几秒内。在这个账本里存储的资产可以是金融、法律定义上的、实体的或是电子的资产。在这个账本里存储的资产的安全性和准确性是通过公私钥以及签名的使用去控制账本的访问权，从而实现密码学基础上的维护。根据网络中达成共识的规则，账本中的记录可以由一个、一些或者是所有参与者共同进行更新。

跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。

没有任何一个节点可以单独记录账本数据，从而避免了单一记账人被控制或者被贿赂而记假账的可能性。也由于记账节点足够多，理论上讲除非所有的节点被破坏，否则账目就不会丢失，从而保证了账目数据的安全性。

1.2 非对称算法

非对称加密和授权技术，存储在区块链上的交易信息是公开的，但是账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问到，从而保证了数据的安全和个人的隐私。

1.3 共识机制

共识机制，就是所有记账节点之间怎么达成共识，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。区块链提出了四种不同的共识机制，适用于不同的应用场景，在效率和安全性之间取得平衡。

区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。以比特币为例，采用的是工作量证明，只有在控制了全网超过 51%的记账节点的情况下，才有可能伪造出一条不存在的记录。当加入区块链的节点足够多的时候，这基本上不可能，从而杜绝了造假的可能

1.4 智能合约

智能合约是基于这些可信的不可篡改的数据，可以自动化的执行一些预先定义好的规则和条款。以保险为例，如果说每个人的信息（包括医疗信息和风险发生的信息）都是真实可信的，那就很容易的在一些标准化的保险产品中，去进行自动化的理赔。

1.5 P2P 技术

点对点传输。点对点技术（peer-to-peer， 简称 P2P）又称对等互联网络技术，是一种网络新技术，依赖网络中参与者的计算能力和带宽，而不是把依赖都聚集在较少的几台服务器上。简单的说，P2P 直接将人们联系起来，让人们通过互联网直接交互。P2P 使得网络上的沟通变得容易、更直接共享和交互，真正地消除中间商。P2P 就是人可以直接连接到其他用户的计算机、交换文件，而不是像过去那样连接到服务器去浏览与下载。P2P 另一个重要特点是改变互联网现在的以大网站为中心的状态、重返“非中心化”，并把权力交还给用户。 P2P 看起来似乎很新，但在现实生活中我们每天都按照 P2P 模式面对面地或者通过电话交流和沟通。

2. 联盟链和公有链的异同

通常，区块链被分为公有链、私有链和联盟链三种。

2.1 公有链

公有链上的各个节点可以自由加入和退出网络，并参加链上数据的读写，读写时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点。公有链是指像比特币区块链这样的完全去中心化的、不受任何第三方机构控制的区块链，是所有人都能参与进来，读取账本数据、参与交易、竞争记账的区块链。

作为中心化或者准中心化信任产品的替代品，公有链受加密经济的保护，加密经济是经济激励和加密图形验证的结合，用类似工作量证明或权益证明的机制，遵循的总原则是人们影响共识形成的程度和他们能够影响的经济资源数量成正比。

目前的应用有：比特币、以太坊。

2.2 联盟链

联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。是指有若干个机构共同参与管理的区块链，每个机构都运行着一个或多个节点，其中的数据只允许系统内不同的机构进行读写和发送交易，并且共同来记录交易数据。联盟链由于存在一定的中心化控制，所以也可以理解为私有链。

比如说，一个有 17 个金融机构的团体，每个机构都操作两个节点，为了使得区块生效，其中的 10 个必须签署那个区块。阅读区块链的权利可能是公开的，或者仅限于参与者，这类区块链被认为是“部分去中心化的”。

3.分布式存储的优势

分布式存储系统，是将数据分散存储在多台独立的设备上。传统的网络存储系统采用集中的存储服务器存放所有数据，存储服务器成为系统性能的瓶颈，也是可靠性和安全性的焦点，不能满足大规模存储应用的需要。分布式网络存储系统采用可扩展的系统结构，利用多台存储服务器分担存储负荷，利用位置服务器定位存储信息，它不但提高了系统的可靠性、可用性和存取效率，还易于扩展将通用硬件引入的不稳定因素降到最低。

分布式存储系统具备如下几个特性：

- 可扩展

分布式系统可以扩展到几百台到几千台的集群规模，而且，随着集群规模的增长，系统整体性能表现为线性增长。

- 低成本

分布式存储系统的自动容错、自动负载均衡机制使其可以构建在普通 PC 机之上。另外，线性扩展能力也使得增加、减少机器非常方便，可以使用较低的成本实现自动运维。

- 高性能

无论是整个集群还是单机服务，都要求分布式系统具备高性能。

- 易用

分布式存储系统需要提供医用的对外接口，另外也要求具备完善的监控、运维工具，并能够方便地与其它系统集成。如 Hadoop 云计算系统导入数据。

综合网络上的观点和一些文章，总结出分布式存储大致有以下几个方面具有优势：

1）性能

一个具有高性能的分布式存户通常能够高效地管理读缓存和写缓存，并且支持自动的分级存储。分布式存储通过将热点区域内数据映射到高速存储中，来提高系统响应速度;一旦这些区域不再是热点，那么存储系统会将它们移出高速存储。而写缓存技术则可使配合高速存储来明显改变整体存储的性能，按照一定的策略，先将数据写入高速存储，再在适当的时间进行同步落盘。

2）分级存储

由于通过网络进行松耦合链接，分布式存储允许高速存储和低速存储分开部署，或者任意比例混布。在不可预测的业务环境或者敏捷应用情况下，分层存储的优势可以发挥到最佳。解决了目前缓存分层存储最大的问题是当性能池读不命中后，从冷池提取数据的粒度太大，导致延迟高，从而给造成整体的性能的抖动的问题。

3) 多副本的一致性

与传统的存储架构使用 RAID 模式来保证数据的可靠性不同,分布式存储采用了多副本备份机制。在存储数据之前，分布式存储对数据进行了分片，分片后的数据按照一定的规则保存在集群节点上。为了保证多个数据副本之间的一致性，分布式存储通常采用的是一个副本写入，多个副本读取的强一致性技术，使用镜像、条带、分布式校验等方式满足租户对于可靠性不同的需求。在读取数据失败的时候，系统可以通过从其他副本读取数据，重新写入该副本进行恢复，从而保证副本的总数固定;当数据长时间处于不一致状态时，系统会自动数据重建恢复，同时租户可设定数据恢复的带宽规则，最小化对业务的影响。

4) 容灾与备份

在分布式存储的容灾中，一个重要的手段就是多时间点快照技术，使得用户生产系统能够实现一定时间间隔下的各版本数据的保存。特别值得一提的是，多时间点快照技术支持同时提取多个时间点样本同时恢复，这对于很多逻辑错误的灾难定位十分有用，如果用户有多台服务器或虚拟机可以用作系统恢复，通过比照和分析，可以快速找到哪个时间点才是需要回复的时间点，降低了故障定位的难度，缩短了定位时间。这个功能还非常有利于进行故障重现，从而进行分析和研究，避免灾难在未来再次发生。多副本技术，数据条带化放置，多时间点快照和周期增量复制等技术为分布式存储的高可靠性提供了保障。

5) 弹性扩展

得益于合理的分布式架构，分布式存储可预估并且弹性扩展计算、存储容量和性能。分布式存储的水平扩展有以下几个特性：

节点扩展后，旧数据会自动迁移到新节点，实现负载均衡，避免单点过热的情况出现。

水平扩展只需要将新节点和原有集群连接到同一网络，整个过程不会对业务造成影响。

当节点被添加到集群，集群系统的整体容量和性能也随之线性扩展，此后新节点的资源就会被管理平台接管，被用于分配或者回收。

6) 存储系统标准化

随着分布式存储的发展，存储行业的标准化进程也不断推进，分布式存储优先采用行业标准接口(SMI-S 或 OpenStack Cinder)进行存储接入。在平台层面，通过将异构存储资源进行抽象化，将传统的存储设备级的操作封装成面向存储资源的操

作，从而简化异构存储基础架构的操作，以实现存储资源的集中管理，并能够自动执行创建、变更、回收等整个存储生命周期流程。基于异构存储整合的功能，用户可以实现跨不同品牌、介质地实现容灾，如用中低端阵列为高端阵列容灾，用不同磁盘阵列为闪存阵列容灾等等，从侧面降低了存储采购和管理成本。

4.信任链是如何建立的

区块链是一个信任的机器，是在完全不信任的节点之间建立信任机制的技术，是利用互联网传递价值的一种价值网络，这是一个把时间当朋友的技术。

信息，指身份、资产、价格、地理位置等自然属性和行为信息，它并不是先天可信任的，因为信息散乱、不完整，可能虚假，甚至可能会有人利用信息的不对称性牟利。把信息整理成结构化数据，通过数据校验的方式，保证其在传播中可保持完整性、全网一致性、可追溯性，不会被恶意篡改；通过冗余存储的方式，保证其公开、共享、可访问，保证数据一直有效。那么，这信息本身就可以被“信任”，从而成为大家的“公共知识”。

区块链体系基于算法而不是人治，有望通过其独特的分布式架构、加密算法、数据结构、共识机制等，把信息固化成大家的信任锚点；有望通过技术手段把各种现实世界的资源转换成可兑付的数字资产，并展开一系列多方商业协作的活动。

以下为信任链建立的技术基础：

1）

区块链是用算法达成信任的，其中最重要的算法之一，就是密码学。区块链中最基本的密码学应用是 HASH 函数、对称加密和非对称加密算法，以及相关的签名验签算法。

HASH 算法的旧版本已经被证明可破解而被抛弃了，目前在用的 SHA256 等算法依旧坚不可破。HASH 算法的特性是把一堆数据单向生成一段定长的数据，基本不会发生碰撞，可起到原始数据的“指纹”作用，其单向性不可逆，推不出原始数据，具有一定的抗量子性，是能隐藏原始数据又能在必要时提供校验凭据的最佳方式。

数字签名一般基于公私钥体系，用私钥签名，公钥验签或者反之。数字签名源自密码学的牢靠性，使得不可能有人能伪造别人的私钥签名，所以一个拥有私钥的人可以通过数字签名，对他的资产签名确权，或者在双方交易时，采用对手方的公钥发起交易，将资产转移给对方，对方用自己的私钥才能验签解开，以获得所有权。

AES、RSA、ECC 椭圆曲线等几种对称和非对称算法广泛地用于数据加解密、安全通信等场景,其安全级别取决于算法本身和密钥长度,当 AES 使用 128~512 位密钥,RSA/ECC 采用 1024 甚至 2048 位密钥时，其保护的数据理论上需要普通计算机上亿年的计算时间才能暴力破解。这些算法在商业、科学、军事领域都经受了考验。

2）

区块链的数据结构，无非是区块+链。新区块将自己的区块高度、交易列表，和上一个区块的 HASH，共同再生成一个 HASH 做为新区块的标识，如此循环，形成了一个环环相扣的数据链。这个链条里的任何一个字节甚至一个 Bit 被修改，都会因为 HASH 算法的特性被校验发现。

同时，区块数据被广播给全网所有参与者，参与者越多，规模效应越强。少数人即使强行修改、删剪自己的区块数据，也很容易被其他人校验出异常并不予采纳，只有多数人认可的数据得以留存和流传。也就是说，数据是大家人盯人的形态盯着的，且存在多份副本，一旦落地，只要链还在，数据就可以永远留存。

3）

博弈论。共识算法是区块链中至关重要的技术方法。共识算法的定义是在一个群体中，用一种机制协调大家共同或轮流记账，得出无争议的、唯一性的结果，且保证这个机制可以持续下去。

POW（工作量证明）采用算力去竞争记账者的席位和获得记账者的奖励。现实生活中，为了构建具有竞争力的算力工厂，矿工通常需要研发或购买大量的新型号矿机，运输到有稳定和便宜电力供应地区，消耗大量的电费、网费以及其他运营费用，在被监管时又得举家搬迁，浪迹全球，实际上投入了大量（现实世界的）资金、精力以及背着巨大的风险。如果要在 POW 竞争中获得稳定可观的收益，投入的资金动辄以亿计，并不亚于办一家企业。

然而，和现实的商业关系对比，POW 和 POS 等共识并没有法律和监管机制兜底，也容易受不断变化的博弈形势所影响。总的来说，人们还是信任区块链上的“自治”，在这种分布式自治里，单个事件（如一笔交易）具有“概率性”,同时全网又追求“最终一致性”（公共账本的一致）。这种短期的概率性和长期的确定性，一定程度上可以达成动态的“纳什均衡”，支撑起链的生态。

联盟链的记账者一般是机构级的角色。联盟链要求记账者身份可知，参与者们经过许可才能接入网络，他们之间是一种合作博弈。在这种环境里，联盟链的参与者一起协作维护网络，共享必要的信息，在平等透明、安全可信的网络里开展交易，只需要防止少量记账者的恶意操作风险，避免系统上的可用性风险。因引入了现实世界里必要的信任背书，即使联盟链业务逻辑非常复杂，而信任模型却更直观。

4）

智能合约是由多产的跨领域法律学者尼克·萨博（Nick Szabo）提出来的。他在发表于自己的网站的几篇文章中提到了智能合约的理念，定义如下：

“一个智能合约是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议”。

简单地说，可以理解为纸质合约的电子版，用代码实现，无差别地运行在区块链网络的每一个节点上，在共识的作用下执行既定的合约规则。智能合约一般基于一个特制的虚拟机，使用沙盒模式运行，屏蔽掉可能导致不一致性的一些功能。比如获取系统时间这个操作，在不同的机器上，时钟都可能不同，这就可能导致依赖时间的业务逻辑出现问题。再比如随机数，以及外部文件系统、外部网站输入等，这些都可能导致虚拟机执行结果不同，都会被虚拟机沙盒环境隔离。

所以，在区块链上执行智能合约，基于沙盒机制控制，凭借区块链的共识算法，达到全网一致、难以篡改、不可否认等特性，运行结果输出就是全网认可的一份合同。智能合约，是有条件的，是要信经过严格测试、长时间稳定运行、万一出错还有办法补救的合约。联盟链里的智能合约一般是经过严格测试的，上线时会执行灰度验证流程，运营中监控运行过程，且根据治理规则设计事后追责、补救等措施，因此是值得信任的。

5.群组架构的好处

FISCO BCOS 2.0新增了群组架构，用于克服系统吞吐能力的瓶颈。

有别于传统区块链平台整个网络维护一个账本，所有节点参与到这个账本的共识和存储的做法，群组架构允许网络中存在多个不同的账本，每个账本是一个独立的小组，节点可以选择加入某些小组，参与到该组账本的共识和存储。该架构的特点是：

各群组独立执行共识流程，由群组内参与者决定如何进行共识，一个群组内的共识不受其他群组影响，各群组拥有独立的账本，维护自己的交易事务和数据，使得各群组之间解除耦合独立运作，可以达成更好的隐私隔离；

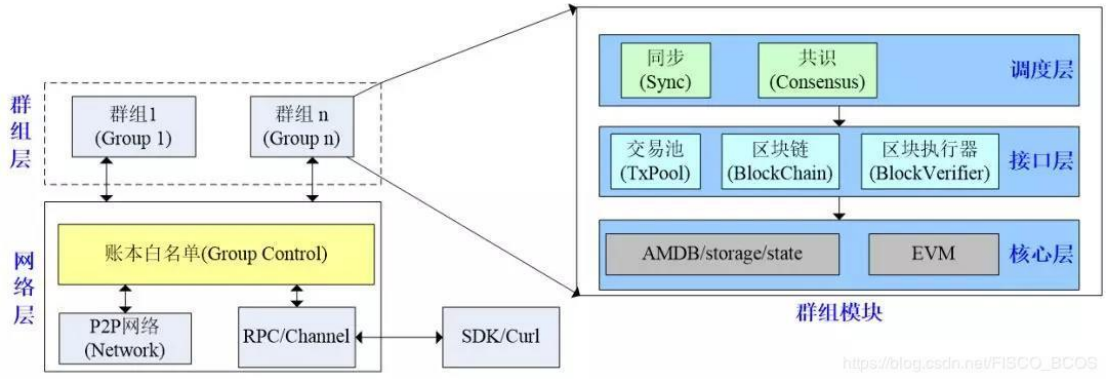
机构的节点只需部署一次，通过群组设置即可参与到不同的多方协作业务中，或将一个业务按用户、时间等维度分到各群组，群组架构可快速地平行扩展，在扩大了业务规模同时，极大简化了运维复杂度，降低管理成本。

群的建立非常灵活，几个人就可以快速拉个主题群进行交流。同一个人可以参与到自己感兴趣的多个群里，并行地收发信息。现有的群也可以继续增加成员。

看回群组架构，采用群组架构的网络中，根据业务场景的不同，可存在多个不同的账本，区块链节点可以根据业务关系选择群组加入，参与到对应账本的数据共享和共识过程中。群组架构具有良好的扩展性，一个机构一旦参与到这样的联盟链里，有机会灵活快速地丰富业务场景和扩大业务规模，而系统的运维复杂度和管理成本也线性下降。

各群组之间解除耦合独立运作。群聊用户都在你的通信录中，都是经过验证才添加的，且不在群里的用户看不到群聊信息。这与联盟链准入机制不谋而合，所有参与者的机构身份可知。

另一方面，群组架构中各群组独立执行共识流程，各组独立维护自己的交易事务和数据，不受其他群组影响。这样的好处是，可以使得各群组之间解除耦合独立运作，从而达成更好的隐私隔离。在跨群组之间的消息互通，则会带上验证信息，是可信和可追溯的。



如图所示，群组架构自底向下主要划分为网络层、群组层，网络层主要负责区块链节点间通信，群组层主要负责处理群组内交易，每个群组均运行着一个独立的账本。

1）网络层

群组架构中，所有群组共享 P2P 网络，群组层传递给网络层的数据包中含有群组 ID 信息，接收节点根据数据包中的群组 ID，将收到的数据包传递给目标节点的相应群组。为了做到群组间通信数据隔离，群组架构引入了账本白名单机制。每个群组均持有一个账本白名单，用于维护该群组的节点列表。为了保证账本白名单群组内一致性，仅可通过发交易共识的方式修改账本白名单。

2）群组层

群组层是群组架构的核心。为了实现群组间账本数据的隔离，每个群组持有单独的账本模块。

群组层自下向上一次分为核心层、接口层和调度层：核心层提供底层存储和交易执行接口；接口层是访问核心层的接口；调度层包括同步和共识模块，负责处理交易、同步交易和区块。

核心层主要包括存储(AMDB/storage/state)和执行(EVM)两大模块。存储负责从底层数据库中存储或读取群组账本的区块数据、区块执行结果、区块信息以及系统表等。执行(EVM)模块主要负责执行交易。

3）接口层

接口层包括交易池(TxPool)、区块链(BlockChain)和区块执行器(BlockVerifier)三个模块。

交易池是客户端与调度层交互的接口，负责从客户端或者其他节点收到的新交易，共识模块会从中取出交易打包处理，同步模块从中取出新交易进行广播。区块链模块是核心层与调度层交互的接口，是调度层访问底层存储和执行模块的唯一入口，调度层可通过该模块提交新区块和区块执行结果，查询历史区块等信息。

区块链模块也是 RPC 模块与核心层的接口，RPC 模块通过区块链模块可获取区块、块高以及交易执行结果等信息。

区块执行器(BlockVerifier)与调度层交互，负责执行从调度层传入的区块，并将区块执行结果返回给调度层。

4）调度层

调度层包括共识模块(Consensus)和同步模块(Sync)。共识模块主要负责执行客户端提交的交易，并对交易执行结果达成共识。考虑到共识过程中，需要尽可能保证每个群组节点拥有全量的交易，FISCO BCOS 2.0 引入了同步模块来保证客户端的交易尽可能发送到每个共识节点。同步模块主要包括交易同步和区块同步。

6.总结

就我个人而言，我感觉之前对区块链的设计理念和实现技术是比较陌生的，只是大概了解过一些和比特币相关的新闻，通过这一次实训课，我觉得我收货最大的方面就是对区块链，或者说是联盟链的整体架构和设计有了自己的概念，老师提出的去中心化、

防篡改的思想让我感觉非常的新奇，我相信这种技术和理念在以后的社会或者金融界一定会起到举足轻重的作用。

另外就是 FISCO-BCOS 的多层证书结构，其实证书的概念在很多年前都有了，在电脑中也有过接触，但对证书的具体实现，公钥、私钥等名词还没有什么概念，在搭链的过程中，我们在虚拟机上对证书的签发和发送有了自己尝试，将老师上课讲的架构理念亲身体会了一次，在实训大作业中，因为要实现一个以 FISCO BCOS 为底层技术平台的应用，所以除了搭链以外还要实现 sdk 与链上数据进行交互的操作，这其中地址和私钥的概念就尤其重要，私钥作为用户的唯一标识在与区块链进行交互的过程中不会暴露，而是以地址、公钥的形式展示，而公钥和私钥之间相互转换的过程已经封装在底层平台中了，且这个过程是不可逆的，这就提供了非常高的安全性以及去中心化的思想。

我主要在大作业实训中负责项目管理和后端开发，在把控项目进度和确保我们的实现和需求一致上，我个人认为我收获很大，不但组织能力得到了锻炼，还收获了宝贵的项目经验。在技术上，后端使用的 spring boot 框架也算是我第一次接触，为了能够有一个更好的后端架构，我请教了一些同学，在网上也查阅了一些知识，对于请求转发、业务处理以及数据相关的操作，在实践之后，我都有了更新的认识。

参考文献

[1] FISCO BCOS 开源社区：FISCO BCOS 2.0 原理解析：群组架构的设计. CSDN,

https://blog.csdn.net/FISCO_BCOS/article/details/89379067

[2]李昊轩，FISCO BCOS 开源社区：区块链底层平台 FISCO BCOS 的证书机制. CSDN，https://blog.csdn.net/FISCO_BCOS/article/details/91897978

[3]区块链技术原理及架构.https://www.chainnode.com/post/163314

[4]FISCO BCOS 平台共识.https://www.cnblogs.com/zhang-qc/p/8688882.html

[5]FISCO BCOS 官方文档：系统设计.
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/design/consensus/

[6]BCOS 平台白皮书：面向分布式商业的区块链基础设施