**课程报告**

|  |  |
| --- | --- |
| **课程名称：** | **企业软件项目实训** |
| **学生姓名：** | **祝鹏富** |
| **学生学号：** | **201630666608** |
| **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**

**微众银行区块链实训课程报告**

**摘要：**区块链的概念是在中本聪设计比特币系统的时候首次提出的，也是区块链技术第一次得以落地并且运用得最成功的一次。2008年，中本聪发布了一篇名为《比特币：一种点对点的电子现金系统》论文，他认为传统货币最根本的问题在于信任，银行必须让人信任它能帮我们管好钱财，但是银行却在用货币制造信贷泡沫，通货膨胀使人财富缩水。首先中本聪把比特币定义为一种点对点的电子现金系统，目的很明确：希望这套系统不要依赖任何一个中心，比如中央银行，所以这个系统肯定是分布式系统。

**关键词：**区块链，信任，分布式。

目录

[1 前言 3](#_Toc13604902)

[2 区块链技术原理 3](#_Toc13604903)

[2.1 核心技术一：区块，链 5](#_Toc13604904)

[2.2 核心技术二：分布式、去中心化结构 7](#_Toc13604905)

[2.3 核心技术三：加密算法（非对称） 9](#_Toc13604906)

[2.4 核心技术四：脚本 10](#_Toc13604907)

[3 联盟链和公有链（以及私有链）的异同 10](#_Toc13604908)

[4 分布式存储有什么优势 11](#_Toc13604909)

[5 并行计算 14](#_Toc13604910)

[6 总结 15](#_Toc13604911)

[7 附录 15](#_Toc13604912)

# 1 前言

2008年，一位名为中本聪的神秘人在金融危机的这一年发布了一篇名为《比特币：一种点对点的电子现金系统》的论文。在这篇论文中，中本聪认为，传统货币的最根本的问题在于信任。在现实生活中，我们常常通过银行来保管我们的钱财，我们希望银行是值得我们信任的，但是银行却在用货币制造信贷泡沫，通货膨胀使人财富缩水。而中本聪在论文中提出的比特币，被定义为一种点对点的电子现金系统，目的在于希望这套系统不要依赖任何一个中心（比如银行），而是一个分布式的、去中心化的系统。“区块链”技术在此时诞生。

区块链技术最初是中本聪为了比特币而设计出来的一种特殊的数据库技术，基于密码学中的椭圆曲线数字签名算法（ECDSA）来实现去中心化的P2P系统设计。如今大部分人们听到区块链总会联想到比特币，然而区块链技术的作用绝不仅仅局限在比特币上，区块链技术可以看作一种数据结构、一种数据库技术，但都和比特币没有必然的联系。

区块链，是一种把区块以链的方式结合在一起的数据结构，用密码学相关技术提供了数据的不可伪造和不可篡改的保障。区块链技术，是多种现有技术，如加密算法、P2P等结合的产物，这种技术与区块链数据库巧妙的结合，形成了一种新的数据记录、存储、传递的方式。在过去，人们将数据（如资产）交由一个中心化的机构（如银行）进行管理，而通过区块链技术，可以让系统中的每一个人都参与到数据的管理中，同时还有比中心化系统更强的数据完整性、安全性和一致性。

# 2 区块链技术原理

区块链技术涉及到的关键点较多，基本原理包括三个基本概念：

交易：一次对账本的操作，导致账本状态的一次改变，如添加一条转账记录；

区块：记录一段时间内发生的所有交易和状态结果等，是对当前账本状态的一次共识；

链：由区块按照发生顺序串联而成，是整个账本状态变化的日志记录。

如果把区块链系统作为一个状态机，则每次交易意味着一次状态的改变，生成的区块，就是参与者对其中交易导致状态改变结果的共识。

区块链的本质是一种互联网协议，它的目标是实现一个分布的数据记录账本，这个账本只允许添加、不允许删除。账本底层的基本结构是一个线性的链表。链表由一个个“区块”串联组成，后继区块中记录前导区块的哈希（Hash）值。某个区块（以及块里的交易）是否合法，可通过计算哈希值的方式进行快速检验。网络中节点可以提议添加一个新的区块，但必须经过共识机制来对区块达成确认。

区块链技术原理的来源可以归纳为一个数学问题——拜占庭将军问题：

一组拜占庭将军分别各率领一支军队共同围困一座城市。为了简化问题，将各支军队的行动策略限定为进攻或撤离两种。因为部分军队进攻部分军队撤离可能会造成灾难性后果，因此各位将军必须通过投票来达成一致策略，即所有军队一起进攻或所有军队一起撤离。因为各位将军分处城市不同方向，他们只能通过信使互相联系。在投票过程中每位将军都将自己投票给进攻还是撤退的信息通过信使分别通知其他所有将军，这样一来每位将军根据自己的投票和其他所有将军送来的信息就可以知道共同的投票结果而决定行动策略。

该策略的问题在于，将军中可能出现叛徒，他们不仅可能向较为糟糕的策略投票，还可能选择性地发送投票信息。假设有9位将军投票，其中1名叛徒。8名忠诚的将军中出现了4人投进攻，4人投撤离的情况。这时候叛徒可能故意给4名投进攻的将领送信表示投票进攻，而给4名投撤离的将领送信表示投撤离。这样一来在4名投进攻的将领看来，投票结果是5人投进攻，从而发起进攻；而在4名投撤离的将军看来则是5人投撤离。这样各支军队的一致协同就遭到了破坏。由于将军之间需要通过信使通讯，叛变将军可能通过伪造信件来以其他将军的身份发送假投票。而即使在保证所有将军忠诚的情况下，也不能排除信使被敌人截杀，甚至被敌人间谍替换等情况。因此很难通过保证人员可靠性及通讯可靠性来解决问题。假使那些忠诚（或是没有出错）的将军仍然能通过多数决定来决定他们的战略，便称达到了拜占庭容错。在此，票都会有一个默认值，若消息（票）没有被收到，则使用此默认值来投票。

上述的故事映射到计算机系统里，将军便成了计算机，而信差就是通信系统。虽然上述的问题涉及了电子化的决策支持与信息安全，却没办法单纯的用密码学与数字签名来解决。因为电路错误仍可能影响整个加密过程，这不是密码学与数字签名算法在解决的问题。因此计算机就有可能将错误的结果提交去，亦可能导致错误的决策。在分布式计算中，不同的计算机通过通讯交换信息达成共识而按照同一套协作策略行动。但有时候，系统中的成员计算机可能出错而发送错误的信息，用于传递信息的通讯网络也可能导致信息损坏，使得网络中不同的成员关于全体协作的策略得出不同结论，从而破坏系统一致性。

假如我们要解决计算机世界里的拜占庭将军问题，我们需要考虑三个问题，这也是区块链技术的核心：

问题一：如何建立一个能够存下海量数据并在没有中心化机构存在的体系下保证数据库的完整性和一致性？

问题二：如何保证这样一个数据库在参与数据管理的某些节点崩溃的情况下能够保证数据的完整性？

问题三：如何保证这个数据库值得信任，即在没有中心化管理同时所有用户都能影响到数据的情况下保证数据的可信？

## 2.1 核心技术一：区块，链

为解决问题一，区块链技术对数据库的结构进行了创新，将数据分成了不同的区块，每个区块通过特定的信息链接到上一个区块的后面，通过一条串联的链保存了一套完整的数据，这就是“区块链”的形象表示。

在区块链技术中，数据以电子记录的形式被永久储存下来，存放这些电子记录的文件被称之为“区块（block）”。区块是按时间顺序一个一个先后生成的，每一个区块记录下它在被创建期间发生的所有价值交换活动，所有区块汇总起来形成一个记录合集。

在区块中，会记录区块生成时间段内的交易数据，区块主体实际上就是交易信息的合集。每一种区块链的结构设计可能不完全相同，但大结构上分为区块头（header）和区块身（body）两部分。块头用于链接到前面的块并且为区块链数据库提供完整性的保证，块身则包含了经过验证的、块创建过程中发生的价值交换的所有记录。参考结构如下：



图 区块结构图

其中区块通过区块头里的前驱区块哈希值和后续区块哈希值链接在链上，同时区块头还记录了这个区块的哈希值、交易总数、默克尔根哈希值等信息，区块体里记录了交易列表记录。

可以这样说，每个区块的生成都依赖前一个区块（直到创世块），通过前一个区块的哈希值等信息，以及新区块生成期间产生的信息、时间戳等，生成了这个区块的信息并连接到上一个区块的后面，因此，每个区块严格按照时间顺序连接起来后，就保存了一套完整的数据记录。参考结构如下：

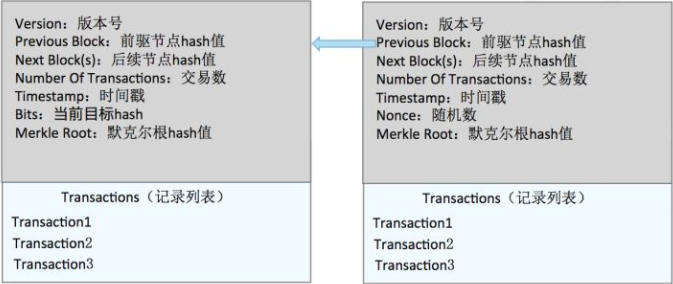


图 链机构图

这就是区块链技术可追溯性的基础，区块链上的每一笔交易数据都可以通过区块链的结构来追溯，同时因为时间戳的存在，提供了不可篡改的特性。

## 2.2 核心技术二：分布式、去中心化结构

当我们解决了数据的存储问题后，接下来就要考虑记录和存储的问题了。我们应该让谁来参与数据的记录，又应该把这些盖了时间戳的数据存储在哪里呢？在现如今中心化的体系中，数据都是集中记录并存储于中央电脑上。但是区块链结构设计精妙的地方就在这里，它并不赞同把数据记录并存储在中心化的一台或几台电脑上，而是让每一个参与数据交易的节点都记录并存储下所有的数据。

问题四：如何让所有节点都能参与数据的记录？

问题五：如何存储下“区块链”这套严谨的数据库？

针对问题四，区块链的办法是：构建一整套协议机制，让全网每一个节点在参与记录的同时也来验证其他节点记录结果的正确性。只有当全网大部分节点（或甚至所有节点）都同时认为这个记录正确时，或者所有参与记录的节点都比对结果一致通过后，记录的真实性才能得到全网认可，记录数据才允许被写入区块中。这也被称作共识。

而对于问题五，区块链的办法是：通过构建一个分布式结构的网络系统，让数据库中的所有数据都实时更新并存放于所有参与记录的网络节点中。这样即使部分节点损坏或被黑客攻击，也不会影响整个数据库的数据记录与信息更新。

区块链根据系统确定的开源的、去中心化的协议，构建了一个分布式的结构体系，让价值交换的信息通过分布式传播发送给全网，通过分布式记账确定信息数据内容，盖上时间戳后生成区块数据，再通过分布式传播发送给各个节点，实现分布式存储。

从硬件的角度讲，区块链的背后是大量的信息记录储存器（如电脑等）组成的网络，这一网络如何记录发生在网络中的所有价值交换活动呢？区块链设计者没有为专业的会计记录者预留一个特定的位置，而是希望通过自愿原则来建立一套人人都可以参与记录信息的分布式记账体系，从而将会计责任分散化，由整个网络的所有参与者来共同记录。

区块链中每一笔新交易的传播都采用分布式的结构，根据P2P网络层协议，消息由单个节点被直接发送给全网其他所有的节点。

区块链技术让数据库中的所有数据均存储于系统所有的电脑节点中，并实时更新。完全去中心化的结构设置使数据能实时记录，并在每一个参与数据存储的网络节点中更新，这就极大的提高了数据库的安全性。

通过分布式记账、分布式传播、分布式存储这三大“分布”我们可以发现，没有人、没有组织、甚至没有哪个国家能够控制这个系统，系统内的数据存储、交易验证、信息传输过程全部都是去中心化的。在没有中心的情况下，大规模的参与者达成共识，共同构建了区块链数据库。可以说，这是人类历史上第一次构建了一个真正意义上的去中心化体系。甚至可以说，区块链技术构建了一套永生不灭的系统——只要不是网络中的所有参与节点在同一时间集体崩溃，数据库系统就可以一直运转下去。

这里再补充一下，为什么我们要那么强调去中心化呢？为了安全和信任。首先来说说安全，这个应该都好理解。比如现在我们用支付宝，所有的转账支付行为都要经过支付宝这个中心，这个中心一旦出问题，所有用户都受影响；这个中心一旦被黑客攻破，数据就非常容易被修改；而分布式系统中，全球每个节点既是客户端也是服务器，除非同时有51%以上节点被篡改，否则所有修改均无效，被“自治”，所有篡改数据难道非常大。安全上的保证也极大解决了信任问题，但是主要的还是数据控制权问题，中心化的系统，被掌握在一个中心中，比如我们的交易数据被掌握在支付宝中，鬼知道有没有被出卖，有没有被利用；而分布式系统中，所有数据透明，不属于任何一个中心；人人都是数据生产者也是拥有者。

## 2.3 核心技术三：加密算法（非对称）

现在，我们有了一套严谨的数据库以及协议，现在我们就来解决核心问题三：如何保证这个数据库值得信任，即在没有中心化管理同时所有用户都能影响到数据的情况下保证数据的可信？

首先我们需要了解，什么是非对称加密？简单来说，它让我们在“加密”和“解密”的过程中分别使用两个密码，两个密码具有非对称的特点：

* + 加密时用到的密码，我们称之为“公钥”，公钥是全网公开可见的，链上的每一个用户都可以用自己的公钥来加密自己的信息；
  + 解密时用到的密码，我们称之为“私钥”，私钥是只有用户自己才知道的，被加密过的信息只有拥有相应私钥的用户才能解密。

因此小结如下：区块链系统内，所有权验证机制的基础是非对称加密算法。常见的非对称加密算法包括RSA、Elgamal、D-H、ECC（椭圆曲线加密算法）等。在非对称加密算法中，如果一个“密钥对”中的两个密钥满足以下两个条件：

* + 对信息用其中一个密钥加密后，只有用另一个密钥才能解开；
  + 其中一个密钥公开后，根据公开的密钥别人也无法算出另一个，那么我们就称这个密钥对为非对称密钥对，公开的密钥称为公钥，不公开的密钥称为私钥。

在区块链系统的交易中，非对称密钥的基本使用场景有两种：

* + 公钥对交易信息加密，私钥对交易信息解密。私钥持有人解密后，可以使用收到的价值。
  + 私钥对信息签名，公钥验证签名。通过公钥签名验证的信息确认为私钥持有人发出。

我们可以看出，从信任的角度来看，区块链实际上是数学方法解决信任问题的产物。过去，人们解决信任问题可能依靠熟人社会的“老乡”，政党社会的“同志”，传统互联网中的交易平台“支付宝”。而区块链技术中，所有的规则事先都以算法程序的形式表述出来，人们完全不需要知道交易的对手方是“君子”还是“小人”，更不需要求助中心化的第三方机构来进行交易背书，而只需要信任数学算法就可以建立互信。区块链技术的背后，实质上是算法在为人们创造信用，达成共识背书

## 2.4 核心技术四：脚本

脚本可以理解为一种可编程的智能合约。如果区块链技术只是为了适应某种特定的交易，那脚本的嵌入就没有必要了，系统可以直接定义完成价值交换活动需要满足的条件。然而，在一个去中心化的环境下，所有的协议都需要提前取得共识，那脚本的引入就显得不可或缺了。有了脚本之后，区块链技术就会使系统有机会去处理一些无法预见到的交易模式，保证了这一技术在未来的应用中不会过时，增加了技术的实用性。

一个脚本本质上是众多指令的列表，这些指令记录在每一次的价值交换活动中，价值交换活动的接收者（价值的持有人）如何获得这些价值，以及花费掉自己曾收到的留存价值需要满足哪些附加条件。通常，发送价值到目标地址的脚本，要求价值的持有人提供以下两个条件，才能使用自己之前收到的价值：一个公钥，以及一个签名（证明价值的持有者拥有与上述公钥相对应的私钥）。

脚本的神奇之处在于，它具有可编程性：

* + 它可以灵活改变花费掉留存价值的条件，例如脚本系统可能会同时要求两个私钥、或几个私钥、或无需任何私钥等；
  + 它可以灵活的在发送价值时附加一些价值再转移的条件，例如脚本系统可以约定这一笔发送出去的价 值以后只能用于支付中信证券的手续费、或支付给政府等。

# 3 联盟链和公有链（以及私有链）的异同

目前来说，根据不同的应用场景以及用户需求，区块链大致可以分为私有链、联盟链和公有链三大类。三种类型的链顾名思义，主要的区别就在于受众范围不一样，其中：

* 私有链：对单独的个人或实体开放，网络的写入权限由某个组织或者机构全权控制，数据读取权限受组织规定，要么对外开放、要么具有一定程度的访问限制。简单来说，可以将其理解为一个弱中心化或者多中心化的系统。由于参与节点具有严格限制且少；与公有链相比，私有链达成共识的时间相对较短、交易速度更快、效率更高、成本更低。不过这种类型的区块链更适合于特定机构内部使用，比如Linux基金会。
* 联盟链：对特定的组织团体开放，是介于公有链以及私有链之间的区块链，可实现“部分去中心化”。链上各个节点通常有与之相对应的实体机构或者组织；参与者通过授权加入网络并组成利益相关联盟，共同维护区块链运行。从某种程度上来说，联盟链也属于私有链的范畴，只是私有化程度有所不同而已。为此其同样具有成本较低、效率较高的特点，适用于不同实体间的交易、结算等B2B交易。
* 公有链：对所有人开放，任何人都可以加入，去中心化程度最高，不受第三方机构控制，世界上所有的人都可读取链上的数据记录、参与交易以及竞争新区块的记账权等。程序开发者无权干涉用户，各参与者（即节点）可自由加入以及退出网络，并按照意愿进行相关操作。

# 4 分布式存储有什么优势

在传统的数据库存储中，使用CS（客户端-服务器）架构，在这种架构中，客户端（用户）可以修改存储在中央服务器中的数据。数据库的控制权保留在获得指定授权的机构处，他们会在用户试图接入数据库前对其身份进行验证。由于授权机构对于数据库的管理负责，如果授权机构的安全性受到损害，则数据面临被修改、甚至被删除的风险。

而在区块链技术中，大多数区块链都是作为去中心化数据库而设计的，且其功能也相当于一个分布式数字账本。而这些区块链账本则以区块的形式记录和存储数据，且其中的区块也都将按照时间顺序排列，并通过密码学证明来相互链接。区块链技术的出现为许多行业都带来了一定的优势，并为缺乏信任的环境提供了更高的安全性。然而，区块链的去中心化特性某些时候也带来了一定的弊端。就比如说，与传统的中心化数据库相比，区块链的效率是有限的，且需要更大的存储容量。

简单来说，区块链技术运用到的分布式存储有以下优势：

1） 分布式：区块链数据库由数个分散的节点组成。每一个节点都会参与数据管理：所有节点都会验证新加入区块链的内容，并将新数据写入数据库。对于加入区块链的新内容，大多数节点必须达成一致才能成功写入。这种共识机制保证了网络安全，让篡改内容变得非常困难。由于区块链数据通常都被存储在分布式节点网络上的数千个设备中，所以系统和数据对于技术故障和恶意攻击都具有很强的抵抗性。其中每个网络节点都可以复制并存储数据的副本，因此单点故障将不会有影响：单个节点的脱机将不会影响到的网络的可用性和安全性。相比之前，许多传统数据库却只依赖于单个或几个服务器，所以更容易受到技术故障和网络攻击的影响。

2） 稳定性：已被确认的区块基本上不可能再被逆转，这就意味着一旦数据被注册到区块链中，则很再难进行删除或更改。而这就使得区块链可以成为存储财务记录或任何其他需要审计追踪的数据的一项优秀的技术，因为区块链中的每个更改都会被分布式公众账本所追踪和永久记录。

3） 去信任机制：在大多数传统的交易支付系统中，交易过程的不仅会存在交易双方，同时还需要依赖于第三方中介机构（例如，银行、信用卡公司或支付方式提供商）。然而，在使用区块链技术时，情况却完全不同，因为分布式节点网络只需通过“挖矿”的过程来核实并验证交易。因此，区块链系统将消除信任单个实体的风险，并减少了整个过程中的成本和交易费用（通过减少中间商）。

区块链技术在拥有上述优势的同时，随着它的不断发展，同时也显露出了一定的劣势：

1） 51%攻击：多年来，保护比特币区块链的工作量证明 共识机制一直都非常有效。然而，却逐渐出现了一些可以影响到区块链网络的潜在攻击，而其中51%攻击则被谈论的最多。当一个实体设法控制了50%以上的网络哈希算力时，此种攻击就会发生，而此种情况最终将会允许攻击者通过故意删除或修改交易的顺序来破坏网络。尽管此种攻击理论上是可行的，但事实上比特币区块链网络上未曾出现过成功的51%攻击。并且，随着网络规模的扩大，安全性也随之提高，同时矿商们不太可能花费大量的资金和资源来攻击比特币，因为他们已经从诚实的挖矿中获得了很好的回报。此外，由于区块之间是通过密码学证明相互链接的（篡改之前的区块则需要巨大的网络算力），所以成功的51%攻击将只能在短时间内对最近期的交易进行修改。并且，比特币区块链也具有极快的适应性，而这将能够迅速的反应并适应各种攻击。

2） 数据修改：区块链系统的另一个缺陷在于，一旦数据被添加到区块链当中，就很难在对其进行修改。虽然难以修改的稳定性是区块链的一大优势，但有些情况下也可能是他的弊端所在。更改区块链的数据或节点一般都是非常困难的，通常都需要硬分叉，也就是使用新链来占用旧链。

3） 私钥丢失：区块链是使用公钥（或不对称）密码学来赋予用户对其加密货币（或任何其他区块链数据）的所有权。每一个区块链账户（或地址）都有两个对应的密钥：公钥（可以共享）和私钥（应该保密）。用户需要使用他们的私钥来访问资金，这就意味着用户充当自己的银行。如果用户丢失了私钥，那么他们实际上就丢失了对资金的控制权（且资金的丢失也无法挽回）。

4） 低效率：区块链，尤其是那些使用工作量证明的区块链，它们通常都是效率极低的。并且，由于挖矿业的激烈竞争且每10分钟只有一位获胜者，所以在此期间其他矿工的工作和时间就浪费了。矿工们正不断的尝试提升他们的算力，以便于自己有更大的机会找出有效的哈希块。并且最近的几年中，比特币网络使用的资源也明显增加，目前它所消耗的能源也已经超过了某些国家使用的能源（如丹麦、爱尔兰和尼日利亚等）。

5） 存储：区块链账本随着时间的推移也逐渐变大。目前比特币区块链就已经需要大约200GB的存储空间。而目前区块链规模的增长也似乎超过了硬盘设备的增长，且如果分类账变得太大以至于个人无法下载和存储，则网络就可能会丢失节点。

总结，与传统的数据库存储，最主要的区别还是在于区块链技术通过分布式存储消除了中心化控制的风险。而尽管存在缺陷，但区块链所呈现出的一些独一无二的特性已经明确表示出了区块链将会继续生存下去。在获得普遍采用的过程中我们还有很长的路要走，而且现在的许多行业也正在逐渐适应区块链系统的优势和劣势。再过几年，企业和政府也许会尝试更多的应用，以此来找出区块链技术可以在哪些方面展现出其最大价值。

# 5 并行计算

在学习研究区块链的过程中，我们不难发现，区块链的运行速度会受到多种因素的影响，包括但不限于加密/解密计算、交易广播、排序、共识算法多阶段提交的协作开销、虚拟机执行速度，以及CPU核心线程主频、磁盘IO、网络带宽等等。

鉴于区块链技术是天然的跨网络的分布式协作系统，而且同时强调安全性、可用性、容错性、一致性、事务性，用较复杂的算法和繁琐的多参与方协作来获得去信任化、数据不可篡改以及交易可追溯等特出的功能优势，根据分布式的CAP原理，在同等的硬件资源投入的前提下，区块链的性能往往低于中心化的系统，其表现就是并发数不高，交易时延较明显。

虽然如 FISCO BCOS 等区块链平台已经对区块链运行的整个流程都做了很高的优化，包括加密解密计算、交易处理流程、共识算法、存储优化等，使得运行速度达到了一个较高的性能水准，已经基本能满足一般的金融业务要求。但是我们也需要考虑到的是，对于用户数、交易量、存量数据较大或可能有显著增长的海量服务场景，对系统提出了更高的容量和扩展性要求，单链架构总是会遇到软件架构或硬件资源方面的瓶颈。而区块链的系统特性决定，在区块链中增加节点，只会增强系统的容错性，增加参与者的授信背书等，而不会增加性能，这就需要通过架构上的调整来应对性能挑战，所以，像 FISCO BCOS 等区块链平台就提出了“并行计算，多链运行”的方案。

并行计算或称平行计算是相对于串行计算来说的。它是一种一次可执行多个指令的算法，目的是提高计算速度，及通过扩大问题求解规模，解决大型而复杂的计算问题。所谓并行计算可分为时间上的并行和空间上的并行。 时间上的并行就是指流水线技术，而空间上的并行则是指用多个处理器并发的执行计算。并行计算是指同时使用多种计算资源解决计算问题的过程，是提高计算机系统计算速度和处理能力的一种有效手段。它的基本思想是用多个处理器来协同求解同一问题，即将被求解的问题分解成若干个部分，各部分均由一个独立的处理机来并行计算。并行计算系统既可以是专门设计的、含有多个处理器的超级计算机，也可以是以某种方式互连的若干台的独立计算机构成的集群。通过并行计算集群完成数据的处理，再将处理的结果返回给用户。

使用并行计算的系统，通常计算问题表现为以下特征：

1） 将工作分离成离散部分，有助于同时解决；

2） 随时并及时地执行多个程序指令；

3） 多计算资源下解决问题的耗时要少于单个计算资源下的耗时。

并行算法是一门还没有发展成熟的学科，虽然人们已经总结出了相当多的经验，但是远远不及串行算法那样丰富。并行算法设计中最常用的的方法是PCAM方法，即划分，通信，组合，映射。首先划分，就是将一个问题平均划分成若干份，并让各个处理器去同时执行；通信阶段，就是要分析执行过程中所要交换的数据和任务的协调情况，而组合则是要求将较小的问题组合到一起以提高性能和减少任务开销，映射则是要将任务分配到每一个处理器上。总之，并行算法还需要相当多完善的地方。并行算法与串行算法最大的不同之处在于，并行算法不仅要考虑问题本身，而且还要考虑所使用的并行模型，网络连接等等。

而在区块链技术上运用并行技术，可以参考 FISCO BCOS 的官方文档，上面有着非常详细的介绍说明和操作步骤。

# 6 总结

通过这次的区块链实训课程，让我从无到有的认识了区块链这门技术，在这个过程中，区块链技术给我的感觉是从完全不清楚，到懵懵懂懂，到最后的“美”，随着学习的深入，能够慢慢地感受到它的潜力。

通过这次学习，不仅让我学到了“区块链”这一门新的技术知识，同时也让我的编程能力有了进一步的提高，感觉受益匪浅。

# 7 附录

**参考文献**

[1] Bitcoin: A Peer-to-Peer Electronic Cash System.中本聪.

[2] 区块链技术指南.yeasy@github.

[3] 区块链原理、设计与应用.杨保华、陈昌.

[4] 区块链入门-概念原理篇.

[5] Decentralizing Privacy: Using Blockchain to Protect Personal Data.

[6] Horizon Scan of Emerging Issues for Global Conservation and Biological Diversity.

[7] Blockchains and Smart Contracts for the Internet of Things.