**课程报告**

|  |  |
| --- | --- |
| **课程名称：** | **企业软件项目实训** |
| **学生姓名：** | **贾学雨** |
| **学生学号：** | **201630676751** |
| **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**

**摘要：**区块链是一种把区块以链的方式组合在一起的数据结构，它适合存储简单的、有先后关系的、能在系统内验证的数据，用密码学保证了数据的不可篡改和不可伪造。它能够使参与者对全网交易记录的事件顺序和当前状态建立共识。区块链技术不是一项新的技术，而是许多技术的组合。主要的核心技术有分布式账本，非对称加密，共识机制，智能合约等。区块链分为私有链，联盟链和公有链，它们的私有化程度由高到低排列。本次实训课程使用的是联盟链，以FISCO BCOS为基础开发平台。本次报告将详细介绍区块链及其原理和部分技术。

**关键词：**区块链、FISCO BCOS、联盟链、分布式、群组架构

1. **介绍**

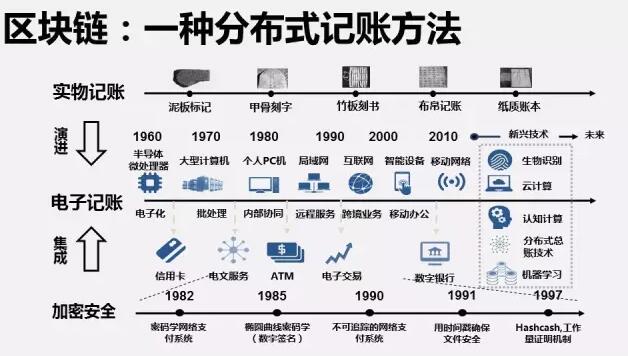
本次企业软件项目实训学院特别荣幸邀请到了微众银行团队的开发成员来担任我们课程的老师，通过一个月的学习与实践，我们从一个对区块链几乎不了解的技术小白，成长为对理论精通，操作娴熟的合格的区块链开发人员。

实训内容是理论与实践并重，理论需要实践去深化，而实践需要理论来做支撑。课程时间的安排上比较自由，每周一次的企业老师授课，剩下的时间让我们自己消化与实践。通过课程，我们深刻地了解了区块链，也通过小组合作，完成了具有区块链技术的应用。区块链[1]由于它独特的优点，让它能在很多场合下具有广泛的应用，比如答辩时候其他小组的宠物商店，保护知识产权的音链，保证可靠性的汽车链等等，都是很好的应用。我相信如果更多的开发与研究人员投入到区块链的研究中，那么区块链将在未来的技术领域中独领风骚。

本次报告将从区块链的技术原理及技术的深入来展开介绍。

1. **区块链技术原理**

区块链是什么？“区块链”技术最初是由一位化名中本聪的人为比特币（一种数字货币）而设计出的一种特殊的数据库技术，它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。但区块链的作用不仅仅局限在比特币上。现在，人们在使用“区块链”这个词时，有的时候是指数据结构，有时是指数据库，有时则是指数据库技术，但无论是哪种含义，都和比特币没有必然的联系。



图一

从数据的角度来看：区块链是一种分布式数据库（或称为分布式共享总账，Distributed Shared Ledger），这里的“分布式”不仅体现为数据的分布式存储，也体现为数据的分布式记录（即由系统参与者来集体维护）。简单的说，区块链能实现全球数据信息的分布式记录（可以由系统参与者集体记录，而非由一个中心化的机构集中记录）与分布式存储（可以存储在所有参与记录数据的节点中，而非集中存储于中心化的机构节点中）。

从效果的角度来看：区块链可以生成一套记录时间先后的、不可篡改的、可信任的数据库，这套数据库是去中心化存储且数据安全能够得到有效保证的。

结论：区块链是一种把区块以链的方式组合在一起的数据结构，它适合存储简单的、有先后关系的、能在系统内验证的数据，用密码学保证了数据的不可篡改和不可伪造。它能够使参与者对全网交易记录的事件顺序和当前状态建立共识。

区块链技术不是一项新的技术，而是许多技术的组合。主要的核心技术有分布式账本，非对称加密，共识机制，智能合约[2]和点对点传输。

1. 分布式账本[3]：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](https://wiki.mbalib.com/wiki/%E6%95%B0%E6%8D%AE%E5%BA%93)。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](https://wiki.mbalib.com/wiki/%E9%87%91%E8%9E%8D)、[法律](https://wiki.mbalib.com/wiki/%E6%B3%95%E5%BE%8B)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。
2. 非对称加密：一种密钥保密方法。在对称加密中加密和解密过程用的是同一把钥匙，而非对称加密中加密和解密过程用的是一对密钥，这对密钥分别称为“公钥”和“私钥”。因为使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。特点：算法强度复杂、安全性强、解密速度较慢。
3. 共识机制：区块链事务达成分布式共识的算法。区块链是一种去中心化的分布式账本系统，它可以用于登记和发行数字化资产、产权凭证、积分等，并以点对点的方式进行转账、支付和交易。区块链系统与传统的中心化账本系统相比，具有完全公开、不可篡改、防止多重支付等优点，并且不依赖于任何的可信第三方。由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序不可能完全一致。因此区块链系统需要设计一种机制对在差不多时间内发生的事务的先后顺序进行共识。这种对一个时间窗口内的事务的先后顺序达成共识的算法被称为“共识机制”。
4. 智能合约：事先制定一个条约，当指定条件被触发时便自动执行相应的操作。智能合约是一套以数字形式定义的承诺，承诺控制着数字资产并包含了合约参与者约定的权利和义务，由计算机系统自动执行。智能合约程序不只是一个可以自动执行的计算机程序，它本身就是一个系统参与者，对接收到的信息进行回应，可以接收和储存价值，也可以向外发送信息和价值。这个程序就像一个可以被信任的人，可以临时保管资产，总是按照事先的规则执行操作。
5. 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。

区块链具有[去中心化](https://baike.baidu.com/item/%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96/8719532)，开放性，独立性，安全性和匿名信等特征。

区块链技术不依赖额外的第三方管理机构或硬件设施，没有中心管制，除了自成一体的区块链本身，通过[分布式](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F/19276232)核算和存储，各个节点实现了信息自我验证、传递和管理。去中心化是区块链最突出最本质的特征。

区块链技术基础是开源的，除了交易各方的私有信息被加密外，区块链的数据对所有人开放，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

基于协商一致的规范和协议(类似[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690)采用的哈希算法等各种数学算法)，整个区块链系统不依赖其他第三方，所有节点能够在系统内自动安全地验证、交换数据，不需要任何人为的干预。

只要不能掌控全部数据节点的51%，就无法肆意操控修改网络数据，这使区块链本身变得相对安全，避免了主观人为的数据变更。

除非有法律规范要求，单从技术上来讲，各区块节点的身份信息不需要公开或验证，信息传递可以匿名进行。

一般说来，区块链系统由[数据层](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%B1%82/20352986)、[网络层](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B1%82/4329439)、[共识层](https://baike.baidu.com/item/%E5%85%B1%E8%AF%86%E5%B1%82/22448420)、[激励层](https://baike.baidu.com/item/%E6%BF%80%E5%8A%B1%E5%B1%82/22447972)、[合约层](https://baike.baidu.com/item/%E5%90%88%E7%BA%A6%E5%B1%82/22469234)和[应用层](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E5%B1%82/16412033)组成。

其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等基础数据和基本算法；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；合约层主要封装各类[脚本](https://baike.baidu.com/item/%E8%84%9A%E6%9C%AC/1697005)、算法和智能合约，是区块链可编程特性的基础；应用层则封装了区块链的各种应用场景和案例。该模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。

1. **联盟链和公有链的异同**

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公有链（Public Blockchain）、私有链（Private Blockchain）以及联盟链（Consortium Blockchain）三大类。

其中去中心化程度最高的是公有链。这种以比特币以及以太坊为代表的公有区块链，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。

私有区块链则完全相反，该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。

而联盟链则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。

总的来说，公有链的进入门槛最低，而私有链以及联盟链则在开放程度上有所限制。

我们课程的实训是通过建立联盟链来开发应用，所以这里我只是比较公有链与联盟链的异同，私有链可以看作私有化程度最高的联盟链。

公有链和联盟链的相同点很多，或者说基本相同，只不过它们面向的群体不同，公有链面向所有群体，而联盟链则只是面向某个群体。联盟链和公链的区别在于使用者、维护者的数量，和业务范围。银行业几个银行间开发的一条区块链可以说就是联盟链；某个项目开发的一条去中心，不限于某个具体的行业，那这条区块链就是公链。公链必须有token，联盟链则可以不用。区块链本质的是通过分布式维护，实现历史记录无法篡改的数据库。而且维护数据库是有成本的，别人为什么要来帮你维护数据库呢？这就需要激励。

公链和联盟链的激励是不一样的。公链面向所有用户开放，要激励普通用户积极参与进来，就需要用代币去激励参与者。联盟链，多用于组织和机构之间的协作，激励是不可篡改特性带来的高效率，高透明度。因为操作在链上都一览无遗，让确权和追责就很容易，可以大幅降低企业之间协作的成本。

而且联盟链与公链的准入门槛不同。公链谁都能参与，谁有能力听谁的，不服的话就分叉，由市场来选择。但是联盟链是有准入门槛的，不是谁都能参与，而且一般也是合作关系。

1. **信任链的建立过程**

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。

那么区块链是如何解决信任问题？它是通过数学和密码学，底层协议和分布式共识来建立信任的。

**来自数学和密码学：**完全随机的随机数生成器，保证了每次都会生成真正不同的随机数。这样，每次使用数字钱包，都能生成唯一不同的公钥和私钥。这样，就不怕账号和私钥和别的用户重了，也不用担心自己的私钥被人偷了，保证了账号的可信。

数学和理论上保证了任何一个内容都会生成出一个唯一的hash值，相同的内容都会生成相同的hash值，不同的内容都会生成出没有冲突的不同hash值。从hash值，不可能推出原来的内容。这样就保证数据的不可窜改和数字签名的可信。

PKI（Public Key Infrastructure/公钥体系）保证了任何公钥加密的内容，只有唯一的对应的私钥，能够解开，保证了私密性和通讯过程中的安全性。任何私钥的数字签名的内容，只有相应的公钥才可以验证通过，保证了数据的integrity，传输的过程中不可能被窜改。拿到的内容，只可能是持有公钥对应的私钥的用户产生的。保证了对数据来源的信任。

从数学和密码学上，保证了区块链上数据的所有权的正确和数据的可信。也就是说，一个用户的私钥签名的数据，只可能是他的，因为别人没法模拟，没法窜改。

**底层协议：**区块链的技术价值在于改变传统互联网的底层协议，使得其能够解决现有社会存在的信任不足、交易安全无法保障的问题。在区块链的世界里，现实世界的规则都被代码重新编译，利用智能合约来执行，因此人们不必再去信任与他发生交易的人，因为算法是可信的。这样发生在互不信任的双方之间的交易就有可能实现。

区块链的去中心化、自信任、分布式账本、数据不可篡改、可溯源的特点使得基于互联网的价值传输可以实现。这样就能够从本质上改变现有市场的信任模式，降低欺诈风险。

传统互联网的数据一般都是统一保存在中心化的服务器中，并且这一些对于用户来说都是一个黑匣子，用户数据、隐私遭泄露的事常有发生，这也是传统互联网出现信任危机的一个重要原因。而区块链利用加密技术可以将数据上链，任何人都无法改变链上数据，也可以追溯数据的流转，加上是分布式存储在区块链中，即便是黑客也无法窃取数据，这样用户就不必再担心自己的个人隐私发生泄露了。

**信任从分布式共识而来：**区块链的分布式共识，解决的是在有不诚实的节点的情况下，如果诚实的节点足够多，是能达成共识的，达成一致性的可信结果。这就是常说的拜占庭将军问题。

基本的原则，就像社会生活中的民主投票，当一个提议被多数人（超过50%）同意通过，那么这个提议就是大家公认的结果、正确的结果，因为大部分人认为是对的。

比如，POW（Proof of work/工作量证明）就是解一道hash难题，谁先解出来的结果，就是这次的提议；然后，其他的节点去验证，当大多数节点都验证正确的话，那么就是这次投票的正确结果，大家以后必须认同和遵守。对多数民主的信任，就是对分布式共识的信任，也就是对区块链的信任。

这个系统分布在全球各个角落，部分系统宕机，其他所有节点依然记录了每一笔账目，所以不会影响整个系统的运作。每个节点的账本数据一模一样，避免了篡改数据，数据造假。

1. **分布式存储[4]的优点**

分布式存储往往采用分布式的系统结构，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。这里列举分布式存储的五个优点。

1. 高性能：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. 支持分级存储：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. 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。
6. **链式存储和MPT存储**

提起链式存储结构，其与数组是两个非常基础的数据结构，每当提到链式存储结构时，一般情况下我们都会将其与数组放到一块儿来比较。

对于数组与链表，从结构上来看，数组是需要一块连续的内存空间来存储数据，对内存的要求非常高，比如说我们申请一个100M大小的数组，而如果我们的内存可用空间大于100M，但是没有连续的100M可用空间，那即便是我们的内存空间充足，在申请空间时也会申请失败。

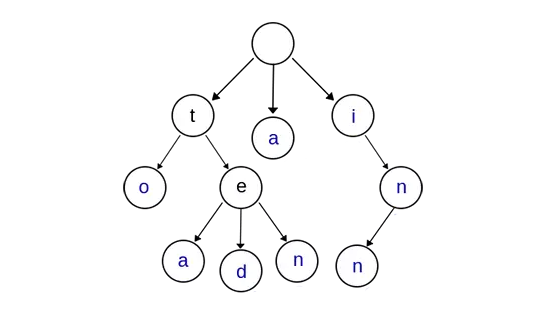
而对于链表来说，他对内存空间的要求就不会有那么高，它并不需要一块连续的内存空间，只要内存空间充足，即使内存空间存在碎片，只要碎片的大小足够存储一个链表节点的数据，该碎片的空间都有可能被分配，链表通过指针或者引用的方式将一组零散的空间串联起来使用。所以如果一个链表需要100M的空间，但是如果内存空间充足，但是没有一个连续的空间大于100M，也不会影响链表的空间分配。

对于链式存储结构，一般情况下我们遇到最多且最常用的大概有单向链表，双向链表，循环链表三种。

链表是通过指针或者引用将分散的内存块链接在一起，我们把串联在链表上的每一个内存块称为链表的节点。

介绍MPT前先介绍Trie树，Patricia树[5]和Merkle树[6]。

Trie 树，又称前缀树或字典树，是一种有序树，用于保存关联数组，其中的键通常是字符串。一个节点的所有子孙都有相同的前缀，也就是这个节点对应的字符串，而根节点对应空字符串。

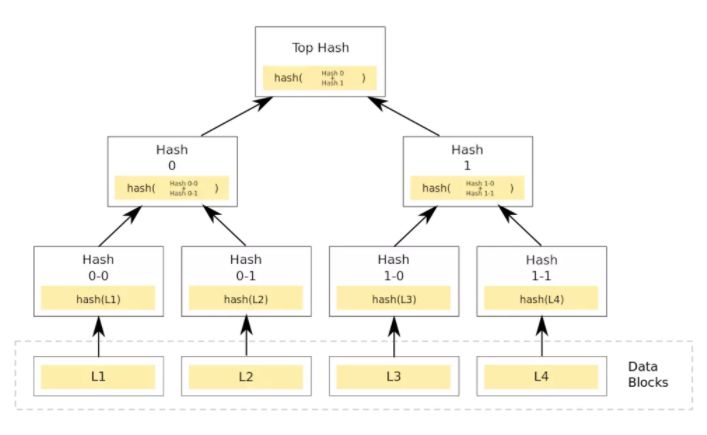


图二

* 根节点不包含字符，除根节点外的每一个子节点都包含一个字符。
* 从根节点到某一个节点，路径上经过的字符连接起来，为该节点对应的字符串。
* 每个节点的所有子节点包含的字符互不相同。

Merkle树，也被称为 Hash Tree，中文名称：默克尔树，主要用于数据集较大时的文件校验。其主要特点为：

* 叶节点存储着数据块的 Hash（如：文件块、一段数据集）
* 非叶子节点 (包括中间节点和根节点) 存储着对应子节点 Hash 值串联字符串之后的 Hash 值。



图三

从上图中可以看出：

* 在最底层，和哈希列表一样，我们把数据分成小的数据块，有相应地哈希和它对应；
* 往上走，并不是直接去运算根哈希，而是把相邻的两个哈希合并成一个字符串，然后运算这个字符串的哈希，这样每两个哈希就结婚生子，得到了一个”子哈希“。如果最底层的哈希总数是单数，那到最后必然出现一个单身哈希，这种情况就直接对它进行哈希运算，所以也能得到它的子哈希再往上推，依然是一样的方式，可以得到数目更少的新一级哈希；
* 最终必然形成一棵倒挂的树，到了树根的这个位置，这一代就剩下一个根哈希了，我们把它叫做 Merkle Root。

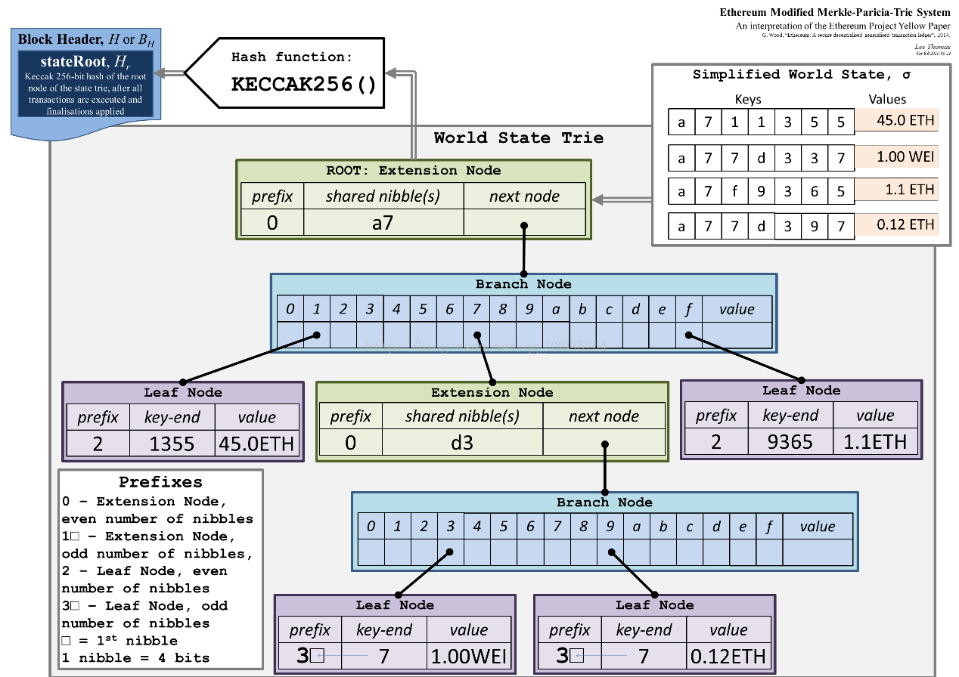
Patricia 树，或称 Patricia trie，或 crit bit tree，压缩前缀树，是一种更节省空间的Trie。对于基数树的每个节点，如果该节点是唯一的儿子的话，就和父节点合并。

上面我们介绍了Merkle Tree和Patricia Tree，而MPT（Merkle Patricia Tree），顾名思义就是这两者的结合。MTP树种的节点包含空节点、叶子节点、扩展节点和分支节点。

* 空节点，简单的表示空，在代码中是一个空串。
* 叶子节点（leaf），表示为[key, value]的一个键值对，其中key是key的一种特殊十六进制编码，value是value的RLP编码。
* 扩展节点（extension），也是[key，value]的一个键值对，但是这里的value是其他节点的hash值，这个hash可以被用来查询数据库中的节点。也就是说通过hash链接到其他节点。
* 分支节点（branch），因为MPT树中的key被编码成一种特殊的16进制的表示，再加上最后的value，所以分支节点是一个长度为17的list，前16个元素对应着key中的16个可能的十六进制字符，如果有一个[key, value]对在这个分支节点终止，最后一个元素代表一个值，即分支节点既可以搜索路径的终止也可以是路径的中间节点。

MPT树中另外一个重要的概念是一个特殊的十六进制前缀(hex-prefix, HP)编码，用来对key进行编码。因为字母表是16进制的，所以每个节点可能有16个孩子。因为有两种[key, value]节点(叶节点和扩展节点)，引进一种特殊的终止符标识来标识key所对应的是值是真实的值，还是其他节点的hash。如果终止符标记被打开，那么key对应的是叶节点，对应的值是真实的value。如果终止符标记被关闭，那么值就是用于在数据块中查询对应的节点的hash。无论key奇数长度还是偶数长度，HP都可以对其进行编码。最后我们注意到一个单独的hex字符或者4bit二进制数字，即一个nibble。

HP编码很简单。一个nibble被加到key前（下图中的prefix），对终止符的状态和奇偶性进行编码。最低位表示奇偶性，第二低位编码终止符状态。如果key是偶数长度，那么加上另外一个nibble，值为0来保持整体的偶特性。



图四

1. **群组架构**

我们实践使用的平台是FISCO BCOS，所以我用FISCO BCOS为例介绍群组架构的优点。

群组架构是FISCO BCOS 2.0众多新特性中的主线，创造灵感来源于人人都熟悉的群聊模式——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。

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。

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](http://www.elecfans.com/tags/%E8%80%A6%E5%90%88/)独立运作，可以达成更好的隐私隔离。

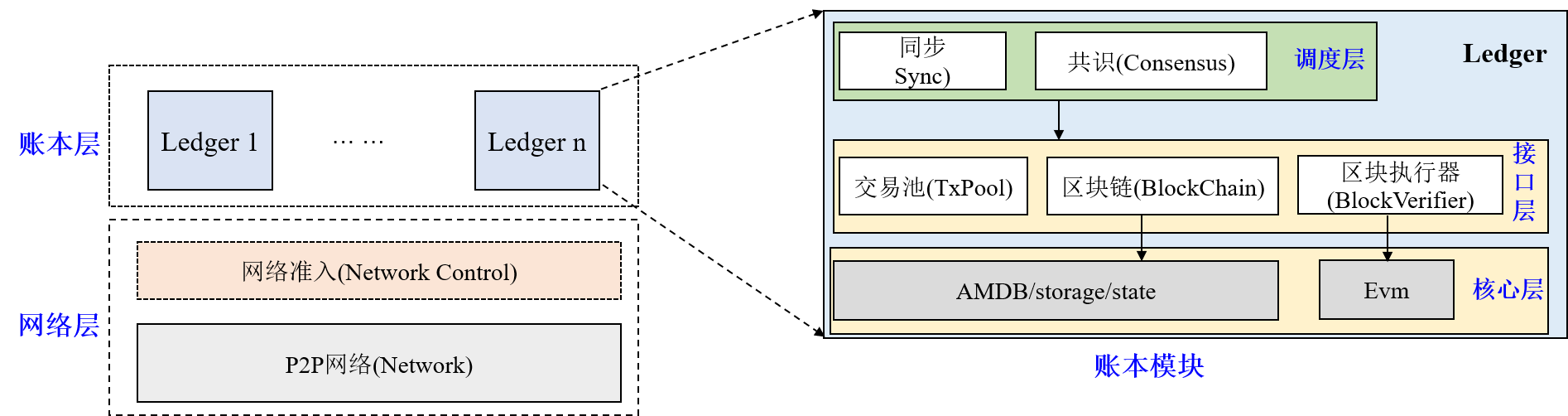
机构的节点只需部署一次，通过群组设置即可参与到不同的多方协作业务中，或将一个业务按用户、时间等维度分到各群组，群组架构可快速地平行扩展，在扩大了业务规模同时，极大简化了运维复杂度，降低管理成本。

举个例子:机构A、B、C所有节点构成一个区块链网络，运行业务1；一段时间后，机构A、B启动业务2，且不希望该业务相关数据、交易处理被机构C感知，有何解？

* 1.3系列FISCO BCOS系统 ：机构A和机构B重新搭一条链运行业务2；运维管理员需要运维两条链，维护两套端口
* FISCO BCOS 2.0 ：机构A和机构B新建一个群组运行业务2；运维管理员仅需维护一条链

显然在达到相同隐私保护需求基础上，FISCO BCOS 2.0具有更好的扩展性、可运维性和灵活性。

多群组架构中，群组间共享网络，通过[网络准入和账本白名单](https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/design/security_control/node_management.html)实现各账本间网络消息隔离。



图五

群组间数据隔离，每个群组独立运行各自的共识算法，不同群组可使用不同的共识算法。每个账本模块自底向上主要包括核心层、接口层和调度层三层，这三层相互协作，FISCO BCOS可保证单个群组独立健壮地运行。

1. **并行计算[7]**

简单来讲，并行计算就是同时使用多个计算资源来解决一个计算问题：

* 一个问题被分解成为一系列可以并发执行的离散部分；
* 每个部分可以进一步被分解成为一系列离散指令；
* 来自每个部分的指令可以在不同的处理器上被同时执行；
* 需要一个总体的控制/协作机制来负责对不同部分的执行情况进行调度。

这里的计算问题需要具有如下特点：

* 能够被分解成为并发执行离散片段；
* 不同的离散片段能够被在任意时刻执行；
* 采用多个计算资源的花费时间要小于采用单个计算资源所花费的时间。

这里的计算资源通常包括：

* 具有多处理器/多核(multiple processors/cores)的计算机；
* 任意数量的被连接在一起的计算机。

为什么要并行计算？主要理由是：

* 节约时间和成本：1）理论上来讲，在一个任务上投入更多的资源有利于缩短其完成时间，从而降低成本；2）并行计算机可以由大量廉价的单机构成，从而节约成本。
* 解决更大规模更复杂的问题：1）很多问题的规模和复杂度使得其难以在一个单机上面完成；2）一个有趣的例子：([Grand Challenge Problems](https://blog.csdn.net/magicbean2/article/details/en.wikipedia.org/wiki/Grand_Challenge))。3）网页搜索引擎/数据库每秒处理百万级别的吞吐量。
* 提供并发性：1）单个计算资源某个时间段只能做一件事情，而多计算资源则可以同时做多件事情；2）协同网络可以使得来自世界不同地区的人同时虚拟地沟通。
* 利用非局部的资源：1）可以利用更广范围中的网络资源；2）SETI@home的例子；以及3）Folding@home的例子。
* 更好地利用并行硬件：1）现代计算机甚至笔记本电脑在架构上都属于多处理器/多核的；2）并行软件已经适用于多核的并行硬件条件，例如线程等；3）在大多数情况下，运行在现代计算机上的串行程序实际上浪费了大量的计算资源。

1. **当前区块链实施的难度**

首先，就是基础设施还相对不够完善。目前来看区块链已经是在各个行业都有所涉及，但对于区块链技术的基础设施来讲还是不够完善，其兼容性还没有达到特定的理想状态，去中心化以及安全隐私性做的还不够好，想要把区块链项目应用到实体经济体系当中就要把这些基础问题解决掉。

其次，新兴的区块链技术还是存在一定的技术缺陷的。在说到区块链技术的缺陷，明眼人心里都清楚，其交易的处理速度以及对资源利益的效率这些都是作为公链发展的阻碍，另外就是互联网的网速问题，再出现大量交易的时候会出现网络堵塞的问题。

再者，就是群龙无首。以区块链发展的趋势来看，其势头是有着不可阻挡的发展前景，区块链技术以其去中心化，数据信息不可篡改性以及溯源性让其成为了新兴技术中的老大。可是对于区块链技术想要在更多的行业生根发芽就需要行业的大佬以及大型企业的照顾，结合区块链技术对原有的营销模式进行升级改造，创造出一个全新的商业体系模式。只有有一个知名度高的企业应用区块链技术来打开市场，这样才有可能让区块链落地实施。

而且，要获得监管部门和市场的认可也面临不少困难。受到现行观念、制度、法律制约。区块链[去中心化](https://baike.baidu.com/item/%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96/8719532)、自我管理、集体维护的特性颠覆了人们生产生活方式，淡化了国家、监管概念，冲击了现行法律安排。对于这些，整个世界完全缺少理论准备和制度探讨。即使是区块链应用最成熟的比特币，不同国家持有态度也不相同，不可避免阻碍了区块链技术的应用与发展。解决这类问题，显然还有很长的路要走。在技术层面，区块链尚需突破性进展。区块链应用尚在实验室初创开发阶段，没有直观可用的成熟产品。比之于互联网技术，人们可以用[浏览器](https://baike.baidu.com/item/%E6%B5%8F%E8%A7%88%E5%99%A8/213911)、[APP](https://baike.baidu.com/item/APP/6133292)等具体应用程序，实现信息的浏览、传递、交换和应用，但区块链明显缺乏这类突破性的应用程序，面临高技术门槛障碍。再比如，区块容量问题，由于区块链需要承载复制之前产生的全部信息，下一个区块信息量要大于之前区块信息量，这样传递下去，区块写入信息会无限增大，带来的信息存储、验证、容量问题有待解决。竞争性技术挑战。虽然有很多人看好区块链技术，但也要看到推动人类发展的技术有很多种，哪种技术更方便更高效，人们就会应用该技术。比如，如果在[通信](https://baike.baidu.com/item/%E9%80%9A%E4%BF%A1/300982)领域应用区块链技术，通过发信息的方式是每次发给全网的所有人，但是只有那个有私钥的人才能解密打开信件，这样[信息传递](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E4%BC%A0%E9%80%92/8232801)的安全性会大大增加。同样，量子技术也可以做到，[量子通信](https://baike.baidu.com/item/%E9%87%8F%E5%AD%90%E9%80%9A%E4%BF%A1/6909117)——利用量子纠缠效应进行信息传递——同样具有高效安全的特点，近年来更是取得了不小的进展，这对于区块链技术来说，就具有很强的竞争优势。

1. **总结**

区块链技术在网络安全领域，影响也是相当巨大的。区块链技术融合了分布式架构、P2P网络协议、加密算法、数据验证、共识算法、身份认证、智能合约等技术，利用基于时间顺序的区块形成链进行数据存储，利用共识机制实现各节点之间数据的一致性，利用密码学体制保证数据的存储和传输安全，利用自动化的脚本建立智能合约而实现交易的自动判断和处理，解决了中心化模式存在的安全性低、可靠性差、成本高等问题。而除了这些特点，它本身的安全特性让人更多的关注使用区块链来提升网络的安全。区块链技术可以在管理和保护用户认证数据、提高网络数据安全、有效阻止DDoS攻击以及增强物联网安全等领域发挥作用。

由于区块链的透明传输和只能按照时间轴读取和写入，不能修改和删除，在应用层面，区块链的安全、透明、高效3大优势，使其特别有助于规范互联网金融的发展，以及促进物联网和共享经济的普及与创新；在资本市场，采用分布式数据库和智能合约还可以大幅减少人工核对工作，为金融机构节省成本。目前，不管是区块链1.0还是2.0或者其他的版本，区块链的应用场景都十分广泛，有包括金融，网络安全，选举等等数十上百个行业的应用，区块链能为这些应用提供安全高效透明的传输方式和安全保障。而每一个应用，对应的都是基于区块链的独特网络管理的系统。虽说区块链本身的特殊的网络交互方式，已经称得上是一种良好的网络管理的方式，而且它的其他应用，也是利用了这一特点，但是其实反过来，利用区块链的思想，也能实现一种新型网络管理方式，这种在点对点的网络传输的基础上，将主机分散化的思想、将数据传输利用hash等数据加密的方式、以及每个区块的特殊的数据结构，可以构成以后一种新的网络管理的方式------去中心化的网络管理方式。

不过到现在为止，从我知道区块链之后，虽然又发展了一年的，但是由于技术还尚未成熟，肯定还是存在很多潜在的漏洞。不过我相信，很快的区块链将在银行业[8]、汽车、预测等等很多领域得到应用并且快速发展。比如教授我们课程的微众银行的老师们，他们就很顺利地在金融领域应用区块链。未来在区块链的领域上，需要我们更多人去参与去完善，只有这样，才能让区块链早日成熟地应用到各个领域。

**REFERENCE**

[1] Marc P. Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing, 2015.

[2] 王春宇, 张守坤. 智能合约与金融合约[J]. 商, 2016(6):198-198.

[3] 黎江, 何京汉. 区块链的“进击”——区块链、分布式账本技术解读[J]. 金融电子化, 2016(3):55-58.

[4] 赵艳妮, 郭华磊, 马晓荣. 大型企业分布式数据存储模式[J]. 硅谷, 2010(16):107-107.

[5] Devroye L. A note on the probabilistic analysis of patricia trees[J]. Random Structures & Algorithms, 2010, 3(2):203-214.

[6] Michael S. Merkle tree traversal in log space and time[J]. Lecture Notes in Computer Science, 2004, 3027:541-554.

[7] 陈国良, 孙广中, 徐云,等. 并行计算的一体化研究现状与发展趋势[J]. 科学通报, 2009(8):1043-1049.

[8] 金檀顺子, 雷霆. 银行应用区块链的前景、挑战和对策建议[J]. 新金融, 2017(7):36-40.