**课程报告**

|  |  |
| --- | --- |
| **课程名称：** | **企业软件项目实训** |
| **学生姓名：** | **黄子凯** |
| **学生学号：** | **201630676744** |
| **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**：经过六周的微众银行区块链实训，我对区块链有了进一步的了解。本报告将对自己在六周内自己所学阐述理解以及对自己在小组分工内所做的工作进行介绍和总结，并发表自己的感想。

1. **区块链介绍**

区块链（blockchain）是在比特币之后提出的一个概念，在中本聪关于比特币的[论文](https://bitcoin.org/bitcoin.pdf)[1]中没有直接引入blockchain的概念，而是以chain of block来描述一种数据结构。

Chain of block是指由多个区块通过哈希（hash）串联成一条链式结构的数据组织方式。区块链则是采用多项技术交叉组合，维护管理这个chain of block数据结构，形成一个不可篡改的分布式账本的综合技术领域。

区块链技术是一种在对等网络环境下，通过透明和可信规则，构建不可伪造、难以篡改和可追溯的块链式数据结构，实现和管理可信数据的产生、存取和使用的模式。技术架构上，区块链是由分布式架构与分布式存储、块链式数据结构、点对点网络、共识算法、密码学算法、博弈论、智能合约等多种信息技术共同组成的整体解决方案。

区块链技术[2]和生态起源于比特币，随着金融、司法、供应链、文化娱乐、社会管理、物联网等更多行业对此领域技术的关注，希望将其技术价值应用到更广泛的分布式协作中，区块链技术和产品模式也在持续进化，FISCO BCOS区块链底层平台在区块链技术基础上，专注提升安全、性能、可用性、易用性、隐私保护、合规监管等方面的能力，和业界生态共同发展，体现多方参与、智能协同、专业分工、价值分享的效能。

1. **联盟链与共有链的异同**

目前来说，根据不同的应用场景以及用户需求，行业里通常将区块链的类型分为公有链（Public Blockchain），联盟链（Consortium Blockchain）[3]，私有链（Private Blockchain）。

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随时随地甚至匿名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。

私有链指一个主体（如一个机构或一个自然人）所有，私有化的管理和使用的链，私有区块链与公有链完全相反，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。

联盟链通常是指多个主体达成一定的协议，或建立了一个业务联盟后，多方共同组建的链，加入联盟链的成员需要经过验证，一般是身份可知的。正因为有准入机制，所以联盟链也通常被称为“许可链”。

因为联盟链从组建、加入、运营、交易等环节有准入和身份管理，在链上的操作可以用权限进行管控，共识方面一般采用PBFT等基于多方多轮验证投票的共识机制，不采用POW挖矿的高能耗机制，网络规模相对可控，在交易时延性、事务一致性和确定性、并发和容量方面都可以进行大幅的优化。

联盟链在继承区块链技术的优势的同时，更适合性能容量要求高，强调监管、合规的敏感业务场景，如金融、司法、以及大量和实体经济相关的业务。联盟链的路线，兼顾了业务合规稳定和业务创新，也是国家和行业鼓励发展的方向。

1. **信任链是如何建立的？**

传统物联网已经不能满足用户的隐私和信息安全，访问控制和数据也受到外界威胁。在隐私保护方面，个人隐私通过标 签嵌入等行为被暴露；射频识别的跟踪破坏用户隐私；信息在服务器传输过程容易受到攻击和泄露；另外，传统信道已经不 能满足隐私保护的需求，感应器和定位系统等设备无法保证完全保护用户隐私数据。

进行互联网交易时，人们通常无法确认交易是否安全，对方是否值得信任。不完善的金融体制，导致人与人之间的信任也变得脆弱。安全性是个很大的话题，尤其是构建在分布式网络上多方参与的区块链系统。[4]在系统层面，需要关注网络攻击、系统渗透、数据破坏和泄漏的问题，在业务层面需要关注越权操作、逻辑错误、系统稳定性造成的资产损失、隐私被侵害等问题。安全性的保障要关注”木桶的短板“，需要有综合性的防护策略，提供多层面，全面的安全防护，满足高要求的安全标准，并提供安全方面的最佳实践，对齐所有参与者的安全级别，保障全网安全。而区块链去中心化、不可篡改，通过以下的技术基础解决信任问题：

**3.1共识机制**

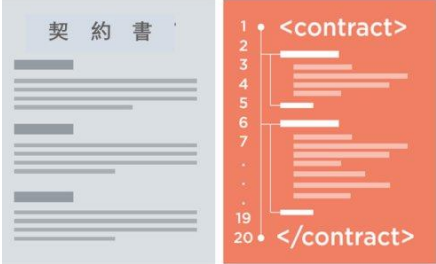
共识机制其实就是构建机器信任的保证，是区块链领域的核心概念，无共识，不区块链。区块链作为一个分布式系统，可以由不同的节点共同参与计算、共同见证交易的执行过程，并确认最终计算结果。协同这些松散耦合、互不信任的参与者达成信任关系，并保障一致性，持续性协作的过程，可以抽象为“共识”过程，所牵涉的算法和策略统称为共识机制。

共识算法需要解决的几个核心问题是：选出在整个系统中具有记账权的角色，做为leader发起一次记账；参与者采用不可否认和不能篡改的算法，进行多层面验证后，采纳Leader给出的记账；通过数据同步和分布式一致性协作，保证所有参与者最终收到的结果都是一致的，无错的。

**3.2智能合约**

智能合约概念于1995年由Nick Szabo首次提出，指以数字形式定义的能自动执行条款的合约，数字形式意味着合约必须用计算机代码实现，因为只要参与方达成协定，智能合约建立的权利和义务，就会被自动执行，且结果不能被否认。

与传统合约相比，智能合约有以下优点：



图一 智能合约

**3.2.1 智能判断，提高合约执行效率**

从自动化方面来看，交易双方一旦有其中一方或两方触发了交易的条件，智能合约将会通过计算机进行快速的智能判断，而传统合约则只能进行人为的认为判断。因此智能合约消除了人为因素产生的错漏，交易双方无需担心执行合约的风险，同时也提高了合约的执行效率。

**3.2.2 客观公正，规避主观因素影响**

从主客观方面来看，智能合约适合客观性请求的场景，而传统合约适合主观性请求的场景。智能合约中的权利、义务和违约的惩罚措施都是提前进行明晰的，一旦触发合约条件程序就会自动执行合约内容。而适用于主观性判断指标的传统合约因主观因素的影响很难被纳入合约自动机中去实行，因此也就很难指导合约事务的及时准确执行。

**3.2.3 代码执行，降低合约履行成本**

从成本方面来看，智能合约中的各项执行条件和相关数据都已经被提前写入了计算机代码中，因此执行的过程中不需要再耗费更多的人力物力即可执行，而传统合约执行的过程中需要花费大量的人力物力去判断交易双方是否违反了合约的条件，并判定交易是否可以继续进行。可以看出智能合约为合约的执行节省了大量的人力物力，因此智能合约的成本也要明显低于传统合约的成本。

**3.2.4 事前编码，节省事务执行时间**

从执行时间方面来看，智能合约是采取的事前预定、预防执行的模式。简单来说，智能合约是一段写在区块链上的代码，通常情况下，在执行智能合约之前，也就是在智能合约构建时，参与制定人员会根据用户的权利和义务科学地不可避免地给交易对方带来损失编写代码，代码中包含的规则可限制行为，当一个事件满足代码中包含的条件，合约才能执行，因此，则可提前防范抵赖、歪曲事实、违约等状况发生。相反的，传统合约属于事后执行、根据状态决定惩罚的模式，在这种模式下，事后再进行判断处理，将会大大延长事件完结的时间。

**3.2.5 数字资产抵押，减少违约纠纷问题**

从惩戒的方式而言，智能合约的“智能”特性赋予了它独特的功能，它可以和数字资产直接挂钩，在合约设立过程中把数字资产被当作抵押品。所以，若有违约行为发生，违约者将不可避免地遭受资产损失。但是传统合约则不同，如果一方违反了合约规定，纠纷问题也会随之而来，在双方无法有效沟通解决的情况下，然后最终就只能通过法律进行裁剪。

**3.2.6 合作全球化，扩大合约使用范围**

从适用范围来看，智能合约的使用不会局限于单个地区，它可以在全球范围内进行推广并投入使用，不论你在任何国家，都可以 达成一项合作，不存在任何束缚。但传统合约则因文化、习俗、具体法律法规的不同而有特定的使用范围，达成合作往往会存在障碍，和智能合约相比，灵活性、便捷性较弱。

**3.3图灵完备**

图灵机和图灵完备是计算机领域的经典概念，由数学家艾伦·麦席森·图灵（1912～1954）提出的一种抽象计算模型，引申到区块链领域，主要指合约支持判断、跳转、循环、递归等逻辑运算，支持多种数据类型如整形、字符串、结构体的数据处理能力，甚至有一定的面向对象特性如继承、派生、接口等，这样才能支持复杂的业务逻辑和完备的契约执行，与只支持栈操作的简单脚本进行区分。

2014年后出现的区块链大多支持图灵完备的智能合约，使得区块链系统具备更高的可编程性，在区块链既有的基本特性（如多方共识，难以篡改，可追溯等，安全性等）基础上，还可以实现具有一定业务逻辑的业务契约，如李嘉图合约（The Ricardian Contract），也可以使用智能合约来实现。

合约的执行还需要处理“停机问题”，即判断程序是否会在有限的时间之内解决输入的问题，并结束执行，释放资源。想象一下，一个合约在全网部署，在被调用时在每个节点上都会执行，如果这个合约是个无限循环，就意味着可能会耗尽整个体系的资源。所以停机问题的处理也是区块链领域里图灵完备计算体系的一个重要关注点。

**3.4安全性技术**

**3.4.1 准入机制**

准入机制指在无论是机构还是个人组建和加入链之前，需要满足身份可知、资质可信，技术可靠的标准，主体信息由多方共同审核后，才会启动联盟链组建工作，然后将经过审核的主体的节点加入到网络，为经过审核的人员分配可发送交易的公私钥。在准入完成后，机构、节点、人员的信息都会登记到链上或可靠的信息服务里，链上的一切行为都可以追溯到机构和人。

**3.4.2 权限控制**

联盟链上权限控制即不同人员对各种敏感级别的数据读写的控制，细分可以罗列出如合约部署、合约内数据访问、区块数据同步、系统参数访问和修改、节点启停等不同的权限，根据业务需要，还可以加入更多的权限控制点。

权限是分配给角色的，可沿用典型的基于角色的权限访问控制（Role-Based Access Control）设计，一个参考设计是将角色分为运营管理者，交易操作员，应用开发者，运维管理者，监管方，每个角色还可以根据需要细分层级，完备的模型可能会很庞大复杂，可以根据场景需要进行适当的设计，能达到业务安全可控的程度即可。

**3.4.3 隐私保护**

基于区块链架构的业务场景要求各参与方都输出和共享相关数据，以共同计算和验证，在复杂的商业环境中，机构希望自己的商业数据受控，在越来越被重视的个人数据隐私保护的形势下，个人对隐私保护的诉求也日益增强。如何对共享的数据牵涉隐私的部分进行保护，以及在避免运作过程泄漏隐私，是一个很重要的问题。

隐私保护首先是个管理问题，要求在构建系统开展业务时，把握“最小授权，明示同意的原则”，对数据的收集、存储、应用、披露、删除、恢复全生命周期进行管理，建立日常管理和应急管理制度，在高敏感业务场景设定监管角色，引入第三方检视和审计，从事先事中事后全环节进行管控。

在技术上，可以采用数据脱敏，业务隔离或者系统物理隔离等方式控制数据分发范围，同时也可以引入密码学方法如零知识证明、安全多方计算、环签名、群签名、盲签名等，对数据进行高强度的加密保护。

**3.4.4 物理隔离**

这个概念主要用于隐私保护领域，“物理隔离”是避免隐私数据泄露的彻底手段，物理隔离指只有共享数据的参与者在网络通信层互通，不参与共享数据的参与者在网络互相都不能通信，不交换哪怕一个字节的数据。

相对而言的是逻辑隔离，参与者可以接收到和自己无关的数据，但数据本身带上权限控制或加密保护，使得没有授权或密钥的参与者不能访问和修改。但随着技术的发展，所受到的权限受控数据或加密数据在若干年后依旧有可能被破解。

对极高敏感性的数据，可以采用“物理隔离”的策略，从根源上杜绝被破解的可能性。相应的成本是需要仔细甄别数据的敏感级别，对隔离策略进行周密的规划，并分配足够的硬件资源承载不同的数据。

1. **链式存储和MPT存储**

**4.1链式存储**

链式存储结构不像顺序存储结构，不需要划分一整块物理存储区域，数据元素可以分别存储在不同位置，通过指针的形式将数据元素的位置进行标识，即在存储数据元素的同时，存储相邻数据元素的物理地址，可以根据物理地址找到下一个（或上一个）数据元素，这样就可以知道不同数据元素之间的逻辑关系。

在区块链中，区块就是链式存储结构中的数据元素，区块是按时间次序构建的数据结构，区块链的第一个区块称为“创世块”（genesis block），后续生成的区块用“高度”标识，每个区块高度逐一递增，新区块都会引入前一个区块的hash信息，再用hash算法和本区块的数据生成唯一的数据指纹，从而形成环环相扣的块链状结构，称为“Blockchain”也即区块链。精巧的数据结构设计，使得链上数据按发生时间保存，可追溯可验证，如果修改任何一个区块里的任意一个数据，都会导致整个块链验证不通过，从而篡改的成本会很高。一个区块的基本数据结构是区块头和区块体，区块头包含区块高度，hash、出块者签名、状态树根等一些基本信息，区块体里包含一批交易数据列表已经相关的回执信息，根据交易列表的大小，整个区块的大小会有所不同，考虑到网络传播等因素，一般不会太大，在1M到几M字节之间。

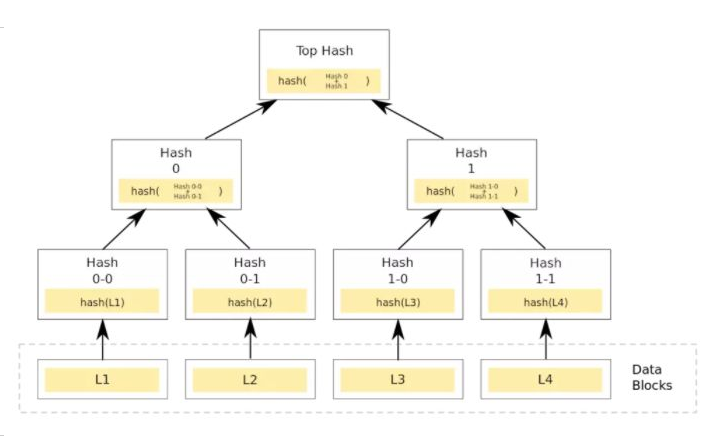
**4.2 MPT存储**

FISCO BCOS采用“账户模型”的设计，即除了区块和交易的存储空间外，还会有一块保存智能合约运行结果的存储空间。智能合约执行过程产生的状态数据，经过共识机制确认，分布式的保存在各节点上，数据全局一致，可验证难篡改，所以称为“世界状态”。状态存储空间的存在，使得区块链上可以保存各种丰富的数据，包括用户账户信息如余额等，智能合约二进制码，智能合约运行结果等相关的各种数据，智能合约执行过程中会从状态存储中获取一些数据参与运算，为实现复杂的合约逻辑提供了基础。另一方面，维护状态数据需要付出不少存储成本，随着链的持续运行，状态数据会持续膨胀，如采用复杂的数据结构如帕特里夏树（Patricia Tree），状态数据的的容量会进一步扩大，根据不同的场景需要，可对状态数据进行裁剪优化，或采用分布式数据仓库等方案存储，以支持更海量的状态数据容量。

以太坊的世界状态便是通过MPT树(Merkle Patricia Tries)实现的。MPT树是由 Merkle Tree 和 Patricia Tree 结合的一种树形结构，理解 MPT 有助于我们更好的理解以太坊的数据存储。

**4.2.1 Merkle树**

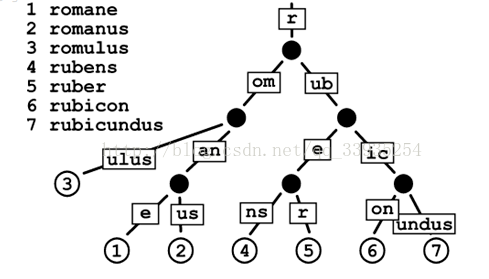
Merkle树[5]，也被称为 Hash Tree，中文名称：默克尔树，主要用于数据集较大时的文件校验。其主要特点为：叶节点存储着数据块的 Hash（如：文件块、一段数据集）；非叶子节点 (包括中间节点和根节点) 存储着对应子节点 Hash 值串联字符串之后的 Hash 值，如图二。



图二 Merkle树

**4.2.2 Patricia树**

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，如图三。

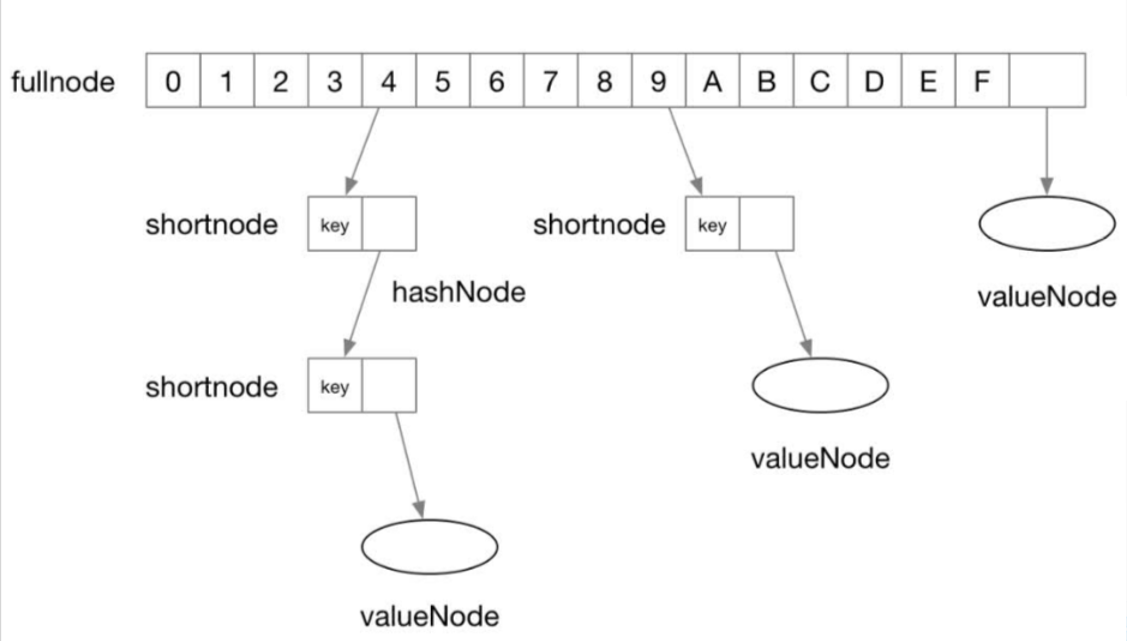


图三 Patricia树

**4.2.3 MPT树**

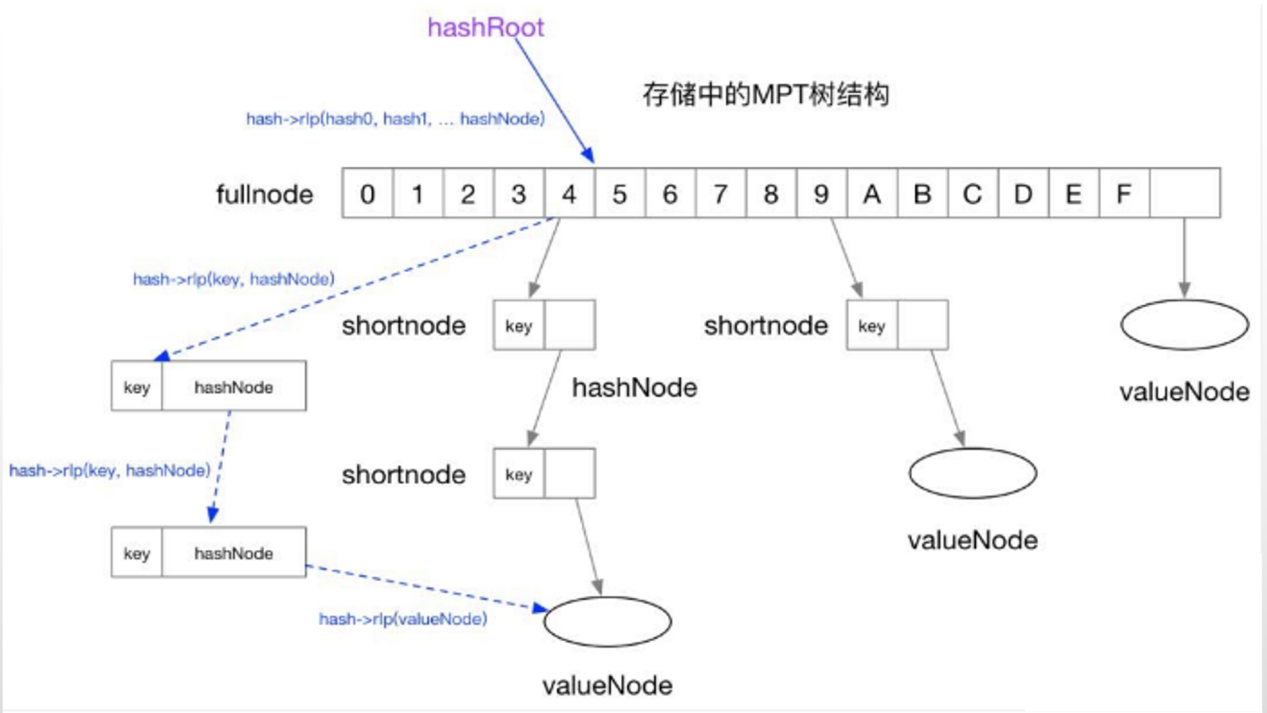
MPT树是Merkle树和Patricia树的结合，在以太坊中, 对于交易树来说，二叉Merkle Tree是非常好的数据结构。因为一旦树已经建立，花多少时间来编辑这棵树并不重要，它就会永远存在并且不会改变。

MPT树的内存结构如图五。一颗MPT树由4种节点连接组成：fullnode是分支节点，shortnode代表扩展节点或者叶子节点（取决于value是hashNode还是valueNode）。需要指出的是：MPT的叶子节点（账户信息）是按照账户的地址（Address）的字典排序形成。也就是说，MPT树上的一个叶子节点路径上的所有的key组成的是账户地址。



图四 内存中的MPT树结构

在内存中，节点和节点的连接关系可以通过“指针”完成。为了将连接关系持久化，需要将节点内容生成对应的，唯一的“地址”。其他引用节点内容的节点，只需要记录引用节点的地址即可，示意如图六中的蓝色部分。



图五 MPT树物理存储

以太坊中，节点内容的地址就是节点内容的hash。比如一个由“key”以及一个“hashNode”组成的节点，节点内容是rlp（key，hashNode），对应的地址是内容的hash。在存储中，存储的是hash到rlp的KV对。其他引用节点的“连接”用hash值代替，从而隐性的实现“连接”。

从上述可见，一个叶子节点的改变，导致节点内容的改变，节点的“地址”也会发生变化。也就是说，父亲节点和该节点的“连接”地址发生变化。因为父亲节点的内容包括“连接”地址，所以父亲节点的内容也发生变化，父亲节点的“地址”也随着变化。随即，父亲的父亲也发生变化，一直变化到MPT的树根。

总的来说，一个账户的改变，导致MPT树，从叶子到树根，整条路径上的所有节点的KV对都发生变化，需要更新到存储中。以太坊中的节点间的“连接”关系用hash来代替，主要原因，hash结果唯一。还有个原因，有关账户中的Storage数据的MPT树。在Storage的数据构建的MPT树，节点排序是通过Storage数据内容的hash，这样保证MPT树的最大高度，避免攻击者通过构造Storage创建深度很高的MPT树。MPT树中的分支节点的分支个数设置为16，而不是更大的原因，可能是怕分支节点内容变的太大，在节点内容大小和树高之间的一个平衡。

**5.Gas在智能合约中的作用**

“gas”是以太坊使用的特殊单位的名称。它衡量一个动作或一系列动作需要执行多少“工作”：例如，计算一个Keccak256密码散列，每计算一次散列需要30个气体，每256位数据被哈希。 Ethereum平台上的一项交易或合同可以执行的每项操作都会花费一定数量的gas，其运营所需的计算资源比计算资源要求较少的运算需要更多的gas。

gas的重要性在于它有助于确保提交给网络的交易支付适当的费用。通过要求交易支付每个操作的执行（或导致合同执行），我们确保网络不会因为执行大量对任何人无价值的密集工作而陷入困境。这与比特币交易费用不同，它仅基于交易的千字节大小。由于以太坊允许运行任意复杂的计算机代码，所以短的代码实际上可能导致大量计算工作的完成。所以衡量直接完成的工作非常重要，而不是仅仅根据交易或合同的长度选择费用。

所以，如果gas基本上是交易费用，如何支付是一个棘手的地方。 虽然gas是一个可以测量物质的单位，但gas并没有任何实际的标志。也就是说，你不能拥有1000gas。相反，gas只存在于以太坊虚拟机内部，作为正在执行多少工作的计数。在实际支付gas时，交易费用是ether的一定数量，以太坊网络上的内置令牌和矿工奖励生产块的令牌。 不直接用ether衡量成本是因为，就像比特币一样，以太网的市场价格可能会迅速变化！但是计算的代价并不是因为以太的价格变化而上升或下降的。所以将计算价格与以太币的价格区分开来是很有用的，这样每次市场走势就不需要改变操作成本。EVM中的操作具有gas成本，但gas本身也具有以ether的gas价格。每笔交易都规定了每个gas单位愿意支付的gas价格，从而使市场能够决定gas价格和计算成本（以gas计量）之间的关系。这是两者的总和，即所用gas总量乘以gas price，得到交易支付的全部费用。

如果我在我的交易中设定的gas price太低，那么没有人会在第一时间去管理我的交易。它不会被矿工包括在区块链中。但如果我提供一个可以接受的天然气价格，那么我的交易就会产生如此多的计算工作，以至于合并后的gas成本超过了我所附加的费用数额，那么这个天然气就会被计算为“花费”，我不会收回。 矿工将停止处理交易，恢复所做的任何更改，但仍将其作为“失败的交易”包含在区块链中，收取费用。这看起来可能很苛刻，但是当你意识到矿工真正的工作是在执行计算的时候，你可以看到他们永远也不会获得这些资源。 所以，即使你设计糟糕的交易用完了，你付给他们的工作也是公平的。

提供太多的费用也不同于提供太多的ether。如果你设置了一个非常高的gas price，那么你只需要付出很少的代价，就像在比特币中设置超高的交易费用一样。你肯定会被排在最前面，但你的钱已经没有了。但是，如果您提供了正常的gas price，并且只需要支付比您购买gas所需的更多的ether，那么超额部分将退还给您。 矿工只收取你实际工作的费用。你可以把gas价格看作矿工的小时工资，把gas成本看作是工作时间表。

gas是使以太坊中的复杂计算“安全”的关键机制，因为任何失控的程序只会在请求运行的人提供的资金的情况下持续下去。当资金停止时，矿工们就停止工作。而你在程序中犯的错误只会影响付费使用它的人，网络的其他部分不会因为你的错误而遭受性能问题。当性能问题消耗掉所有的ether时，他们只会得到一个大的薪水！如果没有这个关键技术，通用区块链的想法将是完全不可能的。

**6.群组架构的好处**

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。该版本在可扩展性、性能、易用性、隐私隔离等方面均取得突破性进展，其新增的群组架构方案，可以让企业间像拉微信群一样快速组链，大大降低维护难度和管理成本。支持区块链节点启动多个群组，群组间交易处理、数据存储、区块共识相互隔离，保障区块链系统隐私性的同时，降低了系统的运维复杂度。群组架构也是FISCO BCOS 2.0新增的，用于克服系统吞吐能力的瓶颈。

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。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](http://www.elecfans.com/tags/%E8%80%A6%E5%90%88/" \t "http://www.elecfans.com/blockchain/_blank)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。

**7.分布式存储**

分布式存储是一种数据存储技术[6]，通过网络使用每台机器上的磁盘空间，并将这些分散的存储资源构成一个虚拟的存储设备，数据分散的存储在网络中的各个角落。所以，分布式存储技术并不是每台电脑都存放完整的数据，而是把数据切割后存放在不同的电脑里。

对于比特币来说，它的交易记录必须要有地方存放，不然没人知道今天有哪些人做了交易，同时根据去中心化的思想，这些交易记录不能够只存在一台电脑里面，那么就只能存放在世界上所有的电脑里面。这样做的好处是：虽然每个人的电脑硬盘容量有限，但是所有人的电脑硬盘加起来容量几乎是无限的，而且就算你通过黑客手段修改了自己计算机里面的交易记录，但是你没法修改全世界每台电脑的交易记录。

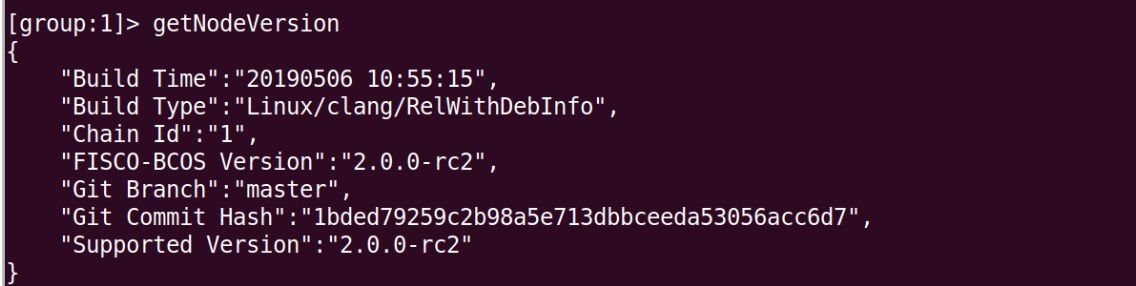
去中心化的分布式存储数据可以说是区块链的特色之一，它可以在所有节点上完成分布式的数据存储，并完好保存下来；而区块链去中心化的特色也使得员工工资、数据中心租金等存储本钱有所下降，这都有力说明了去中心化的分布式数据存储的优势所在，且在区块链范畴的运用非常广泛。[7]

当谈到分散账本技术（DLT）和数据存储之间的互惠关系时，区块链最常见的用方法就是激励。这意味着数据不会存储在区块链本身，但是手头的网络能够利用区块链作为自动支付和价值交换的分类帐本，使用户能够为存储或访问文件付费。在这种情况下，使用区块链优于其他技术的优势是显而易见的。这些包括更快的结算时间，更低的交易费用（实现微交易），更高的隐私性以及保持透明和不变的记录的能力。区块链没有被用于数据存储，它为构建分散网络提供了基础，使其无需任何中央管理机构。

**8.完成的工作**

六周的实训，在微众银行的老师教导下，总算是步入区块链的大门。尽管在完成任务中遇到很多难关，所幸都和小组成员一起克服了。

一开始在老师的教导下，了解了区块链的联盟链，区块链技术架构和原理，还自己动手搭建了FISCO-BCOS区块链网络，启用控制台使用控制台命令调用合约，在完成作业，理解build\_chain脚本情况下，也自己尝试了控制台其他命令行的使用，见图七。



图六 命令行使用

随后完成僵尸游戏教程后，熟悉了solidity语言之后，开始动手编写智能合约。发现完成起来也是比较简单，也特别有成就感。小作业是一个关于书店的积分合约，部署的合约实现了积分初始化，查询（balanceOf），转账（transfer），总积分查询（getTotalSupply）的功能，同时将合约用spring-boot-starter部署，这一步还是有点难度的，自己也看了好多spring-boot-starter教程，终于在同学的帮助下完成了部署。  
 在最后的大作业中，我们选择了宠物商店项目，在经过全体成员的讨论，我们将智能合约分别交给四个人写（包括我），最后由我来整合合约，再由我进行后端开发，用spring-boot-starter进行部署。为了完成和前端的交接，需要查看有关Spring boot 开发API接口的方法。经过尝试完成了最终任务，并且还顺利拿到了金链盟区块链技术认证证书，我心情是非常的高兴，能学有所获是一件令人兴奋的事。

**9.总结**  
 六个星期的实训，不仅让我熟知了区块链的前沿知识，更是让我以前遭人诟病的代码能力有了飞速提升。

目前区块链应用的情景以金融业最多，同时也不少政府部门表示对区块链的运作感兴趣，另外像是医疗界也能够妥善运用区块链技术，医院中病人的数据、病历等等都需要隐私，同时区块链的不可窜改性也让病患资料可以被保障，甚至未来能够结合人工智慧，将病历更进一步的导向智能咨询、智能抓药等功能，行动机器人医生的需求就是大量的、可靠的安全资料，这样的需求可以透过区块联技术来满足，在医疗费用越来越高的此刻，远端医疗的低成本市场、结合人工智慧区块链的医疗保健服务值得我们期待。也希望自己的所学能为社会做出贡献。

**参考文献**

[1]Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008

[2]袁勇，王飞跃 区块链技术发展现状与展望[J] 自动化学报，2016.4

[3]朱立,俞欢,詹士潇 高性能联盟区块链技术研究[J] 软件学报，2019

[4]杨菊英，刘燚，罗佳．一种高效隐私的区块链认知物联网框架[J/OL]．计算机应用研究,2019

[5]何蒲，于戈，张岩峰 区块链技术与前瞻综述[A] 计算机科学，2017.4

[6]方诗虹，彭习羽 基于区块链技术的物联网信息记录安全存储[N] 西南民族大学学报,2019.6

[7]唐萌萌 浅析区块链分布式记账技术下的会计发展现状[N] 山西农经，2019