**课程报告**

|  |  |
| --- | --- |
| **课程名称：** | **企业软件项目实训** |
| **学生姓名：** | **王松盛** |
| **学生学号：** | **201530612880** |
| **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**

1. **区块链技术原理**

区块链技术并没有发明新的技术，而是成熟技术的一种组合。区块链结合共识机制和智能合约进行协同计算和群体鉴证，具有高确定性和高可信性；区块链的计算，通信，存储均进行加密保护，数字签名的运用导致行为无法抵赖；区块链独特的链式数据容易验证和追查，难以篡改，数据具有高一致性，多方冗余存储不怕数据丢失；区块链采用对等的网络通讯，多中心，无中介，高效率高可用。

区块链的信息传播基于无线网络进行广播，消息无差别的对自己相邻节点进行发送，存在一定的冗余。消息“一传十，十传百，百传千”，通过消息反复的传递，具有极大概率达到全网。

区块链使用基于哈希技术的数字签名。哈希是大量数据的唯一摘要值。原数据少量更改会导致哈希值的大量更改，可以作为数据验证的凭据。哈希算法还具有正向快速，逆向困难的特点。因此适合运用在数据摘要中。信息的发送者使用私钥加密数据，便可以使用公钥验证信息是否由他发送。

在区块链中，每一个区块包含一段时间内的交易数据。将相关数据汇总计算摘要，可以进行汇总的完整性正确性证明。每个区块计算摘要时，把前一个区块计算在内，构成了一个数据链。最新区块包含了所有数据链的完整性证明，整个链条上的任何改动都会破坏数据相关性。

默克尔树是一种二叉树数据结构。它可以为区块链状态，交易列表和交易回执列表提供密码学证明。通过默克尔树根，客户端可以在没有全量数据的情况下验证部分数据。默克尔树最下面的叶节点包含存储数据或其哈希值，非叶子结点是它两个孩子节点内容的哈希值。因为哈希值被逐层记录，底层数据的任何变动都会被传播到父节点。树根的值实际上代表对底层数据的“摘要”。默克尔树可以用于对大量数据的快速比较，快速定位修改，零知识证明等等。

区块链的账户分为外部账户和合约账户两种类型。外部账户使用私钥控制，没有代码关联，可以发起交易；合约账户是合约部署生成，与代码关联，不能发起交易，只能被外部调用。

智能合约希望将现实世界的逻辑在区块链上实现。合约的内容和生命周期被共识，确认，是大家认可的条款。所有节点上都可以保证逻辑的一致性，合约在所有节点上产生和维护一致的数据。但是在现实条件中，合约是可能有bug的。

智能合约开发一般使用solidity语言。Solidity语言是图灵完备的高级语言，支持循环，函数调用等语法。Solidity拥有丰富的数据类型，支持整形，字符串，数组，map等等。Solidity支持继承，库引用等高级用法，拥有大量的参考实现，也拥有广泛的开发者。

共识机制是区块链的核心引擎。它是一种多方协作机制，用于协调多参与方达成共同接受的唯一结果。且保证此过程难以被欺骗，持续稳定运行。在共识模型中，拥有记账权的人更倾向在维护整个体系的过程中获利；使用网络的人需要付出一定成本；少数人作恶的成功几率很低；只有极端势力才有可能不顾一切颠覆这个体系。整个局势不存在确定性，一直在动态的多方博弈。

在PBFT协商过程中，先确认记帐者列表，每一轮选出新的提案人，提案人排序大打包，广播提案；所有记帐者针对提案进行检验，都通过的话发出同意投票，超过三分之二进入下一轮；所有记帐者表示可以收妥提案，如果超过三分之二的人表示收妥，则提交存储，进入下一轮。

然而，区块链并不能“一锤子”解决问题。一方面，区块链与现实世界中存在鸿沟，目前并不能做到物理资产的无缝追溯；另一方面，因为链上存储昂贵，大容量数据需要链外存储；区块链也不能满足高度低时延交易网来需求和高强度计算需求。安全和隐私导致额外的复杂度，而且未必满足金融级安全标准。区块链也不能满足呈现强中心化特质的业务关系。

因此，区块链需要混合架构，由区块链连接多个业务相关机构，而各个机构采用中心化的架构来处理他们需要的业务，这样可以兼顾安全性和效率。

1. **联盟链和公有链的异同**

公有链使用虚拟代币，并使用工作量证明，哈希碰撞的方式“挖矿”，交易双方也是匿名的。目前最知名的公有链莫过于比特币。虽然公有链在应用上取得了一定的成功，但是它具有一定的风险。

一方面，是具有支持暗网交易，洗钱及恐怖主义活动的风险。例如在先前的勒索软件事件中，网络攻击者利用windows系统的漏洞，使用病毒将大量重要数据加密封存起来，并要求受害者用比特币的方式支付赎金来解锁数据。在这一事件中，比特币的私密性被违法者用于暗网交易。

另一方面，公有链的去中心化导致了监管缺位，消费者在市场交易的过程中如果遇到诈骗等情况，无法获得执法组织的帮助。代币的价值也完全由市场决定，浮动比较大，比特币价格的下跌经常使得挖矿者血本无归。如果代币被用于非法活动，造成了部分消费者的损失，也没有一个统一的组织来承担法律责任。

挖矿激励的工作方式虽然保证了代币的价值，但是也造成了电力资源的浪费。大量宝贵的电力资源和计算资源被用于解决哈希碰撞这样本质上没有实际意义的问题。从整个社会的角度讲，造成了电力资源和计算资源的浪费。

代币还具有金融上的不稳定性。由于缺乏组织监管，很多基于公有链的代币会出现“崩溃”的现象。在这种现象中，代币价格下跌，代币拥有者争相出手自己手中的代币，进而导致代币价格进一步下跌，如此恶性循环使得一种代币彻底退出市场。在具有政府背书的实体货币中，这种现象可以通过调整利率，适度的增发或收回货币，以及新闻宣传的方式避免。

另一个重要的问题是，电子货币政策还不成熟。由于这个市场的不成熟，很多问题可能并没有暴露出来。而政策的制定往往是落后于市场现象的。因此，这个领域的相关金融政策不可能是健全完整的。这种情况也会带来一定的金融风险。

目前市场上的公有链，本质上并不是“公众所有”。在比特币中，前十大矿池算力合计超过93%；在以太坊中，前十大矿池算力合计超过了87%；而EOS则是由21个超级节点联合记账。显然，这些都说明公有链具有落入一些大组织掌控的危险。

而“公有链”也并没有服务到“普罗大众”。目前全世界公有链参与者只有大约2000万人，远远低于40亿的互联网用户和76亿的全球人口。公有链目前只是少数人的游戏。与此同时，以太坊上存储的数据量还不到1TB，远远低于全球230亿TB的数据总量和480万TB的腾讯云数据量，并不能承载“数字社会”的使命。

随着技术推动新模式的出现，产业的界限逐渐被打破，新模式创造更多连接机会，企业也迎来了新的发展机会。分布式商业是由多个对等地位的商业利益共同体所建立的新型生产关系，通过预设透明的规则进行组织管理，职能分工，价值交换，共同提供商品与服务共享收益的新型经济活动行为。

区块链可以成为创新互联的基础设施。区块链可以打破机构间或自然人间界限的分布，而不仅仅是服务器，机房，地域的分布。分布式事务通过共识算法在交易发生时就达成一致性确定性，多家机构实时参与到交易的验证和确认中，而不是通过事后处理的方式同步。在验证过程中强调抗欺诈，对抗交易者和记帐者作恶。区块链的计算和存储荣誉，无差别计算和存储，而不是由某一个集中模块计算或有限分片计算，具有极高的容灾能力和系统可用性。接入一个链上的成员采用一致的软件，接口和治理方式韵味方式，可以极大的降低成本提升效率。

使用联盟链，服务于一个分布式商业体系，准入机制严格，不允许联盟外机构进入联盟链，节点可以起到监管的作用，避免公有链中缺乏监管的问题。身份认证透明，避免被不法分子利用，去代币的设计避免挖矿的资源浪费。

在未来，可能各个行业都会形成自己的联盟链。再由这些联盟链接入互联网与使用者交互，这样可以极大增加各个行业企业之间的协同。

1. **信任链是如何建立的？**

消息认证码，全称是“基于Hash的消息认证码”，可以用于对消息完整性的保护。对某个消息利用提前共享的对称密钥和Hash算法进行加密处理，得到HMAC值，该HMAC值持有方可以证明自己拥有共享的对称密钥，也可以利用HMAC确保消息内容未被篡改。

数字签名则类似于在纸质合同上签名确认合同内容和证明身份，基于非对称加密，既可以用于证实某段数字内容的完整性，又可以确认来源。

例如Alice通过信道发送给Bob一份文件，Alice可以先对文件内容进行摘要，然后用自己的私钥对摘要进行签名，同时将文件和签名都发送给Bob。Bob收到文件后用Alice的公钥进行解密，得到数字摘要，与文件进行摘要的结果比对，如果结果一致，则可以确认文件时Alice发过来的，而且没有被修改过。

因此，数字证书机制可以证明某个公钥是某个实体的，并且确保一旦内容被篡改就能被探测出来，从而实现对用户公钥的安全分发。

证书紫红记录了大量信息，其中最重要的包括签发的公开密钥和CA数字签名。使用CA的公钥再次对这个证书进行签名比对，就能证明某个实体的公钥是否是合法的。具体的方法为，通过更上层CA颁发的证书来进行认证。某些根CA可以通过预先分发证书来实现信任基础。

例如，在主流操作系统的浏览器里面，往往会提前预置一些权威CA的证书，之后所有基于这些CA认证过的中间层CA和后继CA都会被验证合法。这样就从预先信任的根证书，经过中间层证书，到最底下的实体证书，构成一条完整的证书信任链。当信任链上任一证书不可靠时，则依赖它的所有后继证书都将失去保障。

1. **链式存储和MPT存储**
   1. **链式存储**

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。

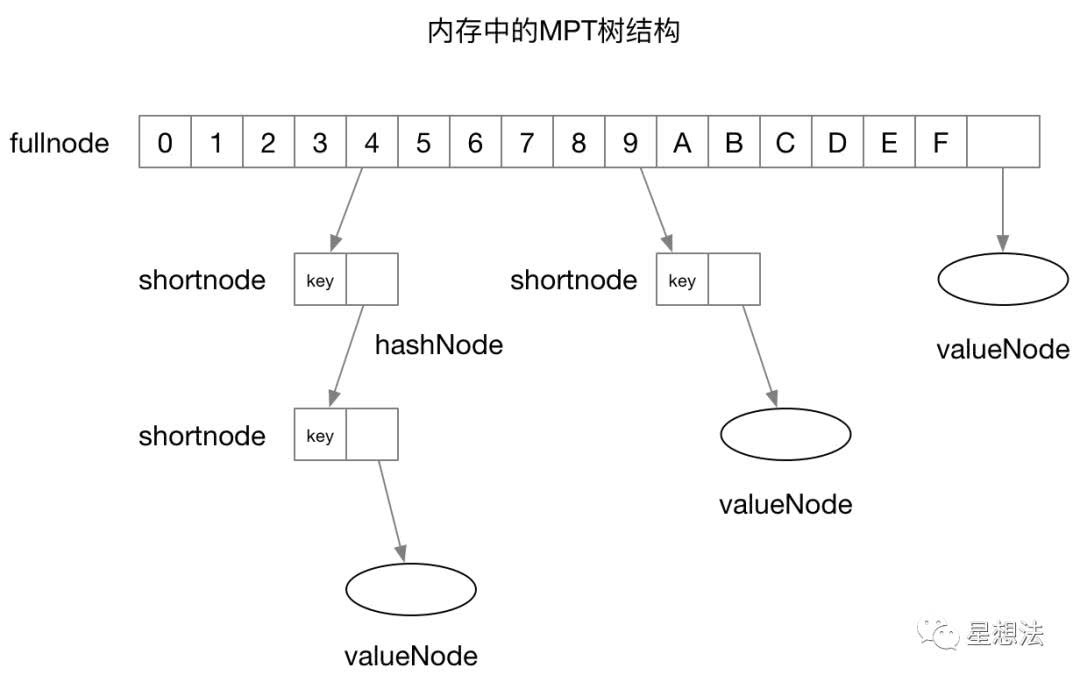
链表是通过指针或者引用将分散的内存块链接在一起，我们把串联在链表上的每一个内存块称为链表的节点。

在单链表结构中，有两个节点比较特殊，那就是第一个节点和最后一个节点。在链式存储结构中，将第一个节点称为头结点，将最后一个节点称为尾节点。头节点记录链表的起始地址，有了这个地址，就可以遍历整个链表。尾节点的后继指针或者引用不是指向一个具体的节点，而是指向一个空地址NULL，从而表示该节点为链表的尾节点。

但是我们都知道，数组在进行数据的插入，删除操作时，为了保证内存数据的连续性，往往需要做大量的数据搬移工作，所以时间复杂度是O(n)。而在链表中插入或删除数据时，因为链表结构中的节点并不需要连续的存储空间，所以在链表中进行数据的插入和删除时并不需要搬移节点。对于链表的删除和插入操作，只需要调整相邻节点的后继指针即可，所以对应的时间复杂度是O(1)。

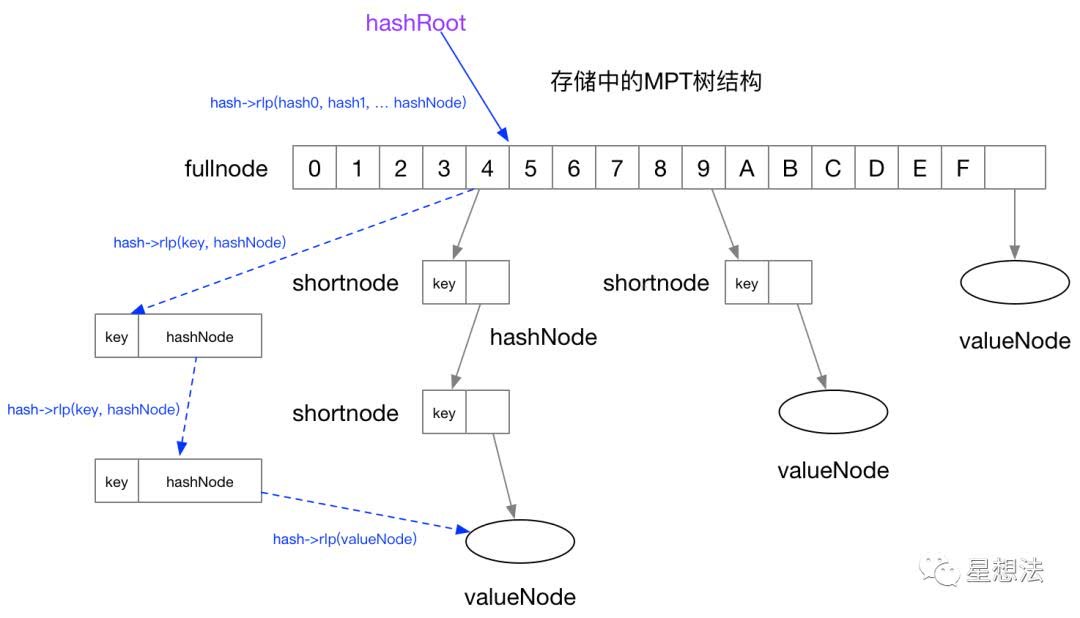
* 1. **MPT存储**

MPT树的内存结构，如下图。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。

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，示意如下图中的蓝色部分。



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”。

再举fullnode的例子，在存储中，fullnode的内容是rlp（hashNode，hashNode ... hashNode, valueNode)组成。

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。

1. **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天然气，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天然气。

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，那么你如何支付？ 这是一个棘手的地方。 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。

起初这可能看起来很奇怪。 为什么不直接用ether衡量成本？ 答案是，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。

这里的术语有点混乱。 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（以天然气计量）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。

尽管这很棘手，但了解这个区别是很重要的，因为这会导致以太坊交易对最初的学习者来说最混乱的一件事情：您的交易没有用完，交易也没有足够高费用。 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，以至于合并后的天然气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。 你可以把煤气价格看作矿工的小时工资，把煤气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。

1. **群组架构的好处**

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。

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。

该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。

群组架构在安全性方面也有足够考虑。群聊用户都在通信录中，都是经过验证才添加的，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。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。

1. **分布式存储有什么优势**

分布式存储是一种数据存储技术，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。就像存放100个鸡蛋，不是放在同一个篮子里，而是分开放在不同的地方，加起来的总和是100个。

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。

从表面上理解，上面说的这种存储方式很粗暴——每台电脑都存放世界上所有人的交易数据。但其实对于比特币来说，只有一些节点才会存放世界上所有人的交易记录，这些节点往往是那些挖矿的矿工，只有他们的电脑才能完整的记录下世界上所有的交易记录，大家不用担心矿工修改记录，因为世界上的矿工有很多，而且几乎相互都不认识。同时他们修改记录需要付出的代价非常大，没有人能承担这个成本。

把亿万用户已有的亿万设备中闲置的空间变成别人数据的储存空间，这会降低世界对服务器的需求。例如，我有5T的数据需要储存，你的设备里有5T的空间空余。那么我可以付钱给你，租你的空间，同时要你保持设备联网以方便我随时取用。

随着存储技术的发展，存储设备的成本越来越小，中心化云服务的成本主要来自于员工工资、法律成本、数据中心租金等，这些固定成本是不变的或逐渐增加，使中心化云服务的价格较高。

而去中心化存储成本只有中心化存储的1/100-1/10，如果去中心化存储系统是完全自动化的，云存储价格最终会降到接近0，中心化云服务的规模优势将败给了去中心化云服务。

分布式存储也是存储技术发展未来一个主要方向。分布式数据存储能提高系统的可靠性、可用性和存取效率，而且易于拓展，在区块链领域应用非常广泛。

1. **并行计算**

对于比特币来说，绝大部分的交易仅仅用于简单转账，如果闪电网络能得到大规模应用，那么拥堵问题应该基本能化解。闪电网络今年3月开始在比特币主网测试，6月底时锁定的比特币有了30多个，7月21日首次突破100个，应该在以一种慢指数的方式增长，所以发展得不错。

但是对于以太坊来说，上面有千千万万的智能合约和token，也有更加丰富多样的交易和操作，即使出块速度已经大大高于比特币，但拥堵问题仍比比特币严重得多，光一个状态通道技术（包括雷电网络），尚不足以完成解决。

于是，提出了另一个解决方案：分片。

在以太坊现在的架构中，所有账户状态构成了以太坊的世界状态，然后世界状态完整地存储在每一个节点中。唯一能导致世界状态变更的，就是交易。每一笔交易都需要所有节点的以太坊虚拟机进行计算处理，计算完毕后，所有节点更新世界状态。从这里可以看出，虽然以太坊有千千万万的节点，但整个以太坊网络的处理能力就等于一个节点的处理能力。

而分片技术，则是将世界状态划分成一个个的小片，可以按照账户地址的前缀来划分，比如a开头的属于分片1，b开头的属于分片2。同时，将所有节点也分成一个个的小组，一个小组负责处理一个分片。这就相当于，原来的以太坊只是一台机器，一笔笔交易，一条条指令，按顺序处理，这是串行处理，但分片后的以太坊，那就是一堆机器，这一堆机器可以各自同时处理不同的指令，由串行处理变成了并行处理，处理能力大大提升。

如果以太坊划成100个分片，那处理能力就是原来的100倍，如果划成1000个分片，那就是1000倍，这种提升是相当恐怖的。所以，V神是把分片当做以太坊的一个重点工作在抓的。

分片的思路其实就这么简单，但实现起来是相当复杂的，而且会带来一些新问题。

首先是安全性的下降，假如以太坊分成100个片，那么每个分片的规模只有原来的百分之一，对于攻击者来说，攻击的成本也大大降低，因为他只要攻击一个分片就可以了。为了安全性考虑，以太坊对于节点的分组并不是固定的，而是随机的，也就是说，对于一个分片，对应哪些节点去处理，是经常变动的。这样，对于攻击者来说，即使他有能力攻击一个分片，但他很大可能压根就找不到攻击的对象，因为他不知道这个分片现在有哪些节点在处理。

另一个问题是，如果两个分片的账户之间要进行交易，该怎么办？

实话说，以太坊的账户状态模型和比特币的UTXO模型相比，并行处理能力是被后者碾压的。对于以太坊来说，一个账户是不能同时发起两笔有效交易的，但比特币可以。这话是什么意思呢？

我们举个例子。

假如以太坊账户A有10个以太币，现在他想转2个给B，转3个给C，表面上看来，这同时转应该没问题，但其实是不行的。因为以太坊节点无法预判你第一笔交易后是否仍有余额支付另一笔交易，所以，在以太坊的账户状态和交易里都有一个序列号字段，一笔交易的序列号与账户状态里的序列号相同，这笔交易才是有效的。所以，以太坊的账户要发起多笔交易，只能按着序列号，排着队，一笔笔处理。

再看比特币。同样，假如比特币账户A有10个比特币，要转2个给B，3个给C。我们知道，一笔UTXO交易，都有自己的“输入”，也就是指明了比特币的来源。这一点，就决定了同一比特币账户的多笔交易是有可能并行处理的，前提条件是，不同的交易对应不同的输入。

比如，如果A的这10个比特币分别来源于三个不同的输入：输入一（2个）、输入二（4个）、输入三（4个），那么他就可以同时发起对B和C的两笔交易，第一笔交易的输入就用“输入一”的那2个比特币，第二笔交易用“输入二”或“输入三”的比特币都可以。

对于比特币节点来说，有可能一部分先收到发给B的交易，那他们就先处理到B的这笔交易，另一部分先收到发给C的交易，那就先处理到C的交易。这两笔交易在比特币网络同时有效，同时被节点处理。

基于此，以太坊在处理跨分片交易时，也引入了更适合并行处理的UTXO模型。

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。

伴随着区块链行业慢慢的发展，其势头已经是有点势不可挡了，众多的科研人员也是马不停蹄的研究解决区块链的诸多疑点难题。小编相信只要解决掉最为基础的区块链技术的设施问题就可以实现区块链行业的落地实施。目前对于行业的发展也是需要区块链这样的技术来带动自己发展，并且满足行业发展的时候还要完善区块链技术的基础设施。

**参考文献**

[1] 区块链分布式存储的优势 https://www.jianshu.com/p/9dba1af3734d

[2] 联盟链架构新解！FISCO BCOS2.0创造群组架构 http://www.donews.com/news/detail/4/3039794.html

[3]FISCO BCOS2.0发布：新增群组架构客服吞吐瓶颈 <https://blog.csdn.net/weixin_33724046/article/details/89190169>

# [4] 区块链：比特币数据存储 <https://blog.csdn.net/chaiyu2002/article/details/82259377>

# [5] 区块链-以太坊MPT存储 <https://cloud.tencent.com/developer/news/305864>

# [6] 细说链式存储结构 <https://blog.csdn.net/zyhlwzy/article/details/83037821>

[7] 分片技术（一）：并行计算 | 以太坊知识普及 https://www.jianshu.com/p/9eef6efbb2a2

[8] 区块链落地实施的难度在哪里？https://www.coingogo.com/news/20436