 

**课程报告**

|  |  |
| --- | --- |
| **课程名称：** | **企业软件项目实训** |
| **学生姓名：** | **陈思源** |
| **学生学号：** | **201630664086** |
| **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

[(二) 摘要： 1](#_Toc13574436)

[(三) 区块链技术原理： 2](#_Toc13574437)

[一、 区块链技术概览： 2](#_Toc13574438)

[二、 哈希算法： 4](#_Toc13574439)

[三、 加解密算法： 4](#_Toc13574440)

[四、 消息认证码与数字签名： 5](#_Toc13574441)

[五、 数字证书： 6](#_Toc13574442)

[(四) 联盟链和公有链的异同 6](#_Toc13574443)

[(五) Gas在智能合约中的作用 8](#_Toc13574444)

[(六) 分布式存储有什么优势 9](#_Toc13574445)

[(七) 并行计算 10](#_Toc13574446)

[(八) 当前区块链实施的难度 13](#_Toc13574447)

[一、 激励制度设计有很大难度 14](#_Toc13574448)

[二、 维护非常花费成本 14](#_Toc13574449)

[三、 用户为王 15](#_Toc13574450)

[四、 所有的升级是自发的 15](#_Toc13574451)

[五、 扩容非常困难 15](#_Toc13574452)

[六、 中心化会容易很多 16](#_Toc13574453)

# 摘要：

课程合作企业为webank（微众银行：微众银行是由腾讯公司及百业源、立业集团等知名民营企业发起设立，总部位于深圳，2014年12月经监管机构批准开业，是国内首家民营银行和互联网银行），课程主要涉及区块链相关。课程以一线工程师授课、小组实际项目工作、线上线下答疑为主。主要学习的区块链技术是基于微众银行旗下的金融区块链合作联盟——FISCO金链盟所推行的FISCO BCOS。

关键字:

区块链、密码学、分布式存储、并行计算

# 区块链技术原理：

## 区块链技术概览：

区块链是基于分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用形式。区块链具有去中心化的特征，由于使用了分布式核算和存储，体系不存在中心化的硬件或管理机构，任意节点的权力和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。区块链具有防纂改的特征，一旦信息经过验证并添加至区块链，就会永久地存储起来，除非能够同时控制住系统中超过百分之五十一地节点，否则单个节点上对数据库地修改是无效的，因此区块链地数据稳定性和可靠性极高。区块链具有匿名性，由于其节点之间地交换遵循固定地算法，其数据交互是无需信任地（区块链中的程序规则会自行判断活动是否有效），因此交易对手无需通过公开身份的方式让对方对自己产生信任，对信任的累积非常有帮助。区块链是开放性的，系统是开放的，除了交易各方的私有信息被加密以外，区块链的数据对所有人公开，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。自治性也是区块链的一大特性，区块链采用基于协商一致的规范和协议（比如一套公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

区块链是一个不断增长的记录列表，称为块，使用cryptogrphy（密码学）进行链接和保护。 每个块通常包含前一个块的加密散列，时间戳和事务数据。通过设计，区块链本质上可以抵抗数据的修改。 它是“一个开放的，分布式的分类账，可以有效地记录两个或更多方之间的交易，并且可以在可验证的和永久性的存储纪录”。

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。+如今的区块链技术概括起来是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术。其实，区块链技术并不是一种单一的、全新的技术，而是多种现有技术（如加密算法、P2P文件传输等）整合的结果，这些技术与数据库巧妙地组合在一起，形成了一种新的数据记录、传递、存储与呈现的方式。简单的说，区块链技术就是一种大家共同参与记录信息、存储信息的技术。过去，人们将数据记录、存储的工作交给中心化的机构来完成，而区块链技术则让系统中的每一个人都可以参与数据的记录、存储。区块链技术在没有中央控制点的分布式对等网络下，使用分布式集体运作的方法，构建了一个P2P的自组织网络。通过复杂的校验机制，区块链数据库能够保持完整性、连续性和一致性，即使部分参与人作假也无法改变区块链的完整性，更无法篡改区块链中的数据。区块链技术涉及的关键点包括：去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectively+maintain）、可靠数据库（ReliableDatabase）、时间戳（Time+stamp）、非对称加密（AsymmetricCryptography）等。【1】

区块链技术重新定义了网络中信用的生成方式：在系统中，参与者无需了解其他人的背景资料，也不需要借助第三方机构的担保或保证，区块链技术保障了系统对价值转移的活动进行记录、传输、存储，其最后的结果一定是可信的。+区块链技术原理的来源可归纳为一个数学问题：拜占庭将军问题。拜占庭将军问题延伸到互联网生活中来，其内涵可概括为：在互联网大背景下，当需要与不熟悉的对手方进行价值交换活动时，人们如何才能防止不会被其中的恶意破坏者欺骗、迷惑从而做出错误的决策。进一步将拜占庭将军问题延伸到技术领域中来，其内涵可概括为：在缺少可信任的中央节点和可信任的通道的情况下，分布在网络中的各个节点应如何达成共识。区块链技术解决了闻名已久的拜占庭将军问题——它提供了一种无需信任单个节点、还能创建共识网络的方法。+区块链技术的本质是一种互联网协议。&oq=区块链技术重新定义了网络中信用的生成方式：在系统中，参与者无需了解其他人的背景资料，也不需要借助第三方机构的担保或保证，区块链技术保障了系统对价值转移的活动进行记录、传输、存储，其最后的结果一定是可信的。++区块链技术原理的来源可归纳为一个数学问题：拜占庭将军问题。拜占庭将军问题延伸到互联网生活中来，其内涵可概括为：在互联网大背景下，当需要与不熟悉的对手方进行价值交换活动时，人们如何才能防止不会被其中的恶意破坏者欺骗、迷惑从而做出错误的决策。进一步将拜占庭将军问题延伸到技术领域中来，其内涵可概括为：在缺少可信任的中央节点和可信任的通道的情况下，分布在网络中的各个节点应如何达成共识。区块链技术解决了闻名已久的拜占庭将军问题——它提供了一种无需信任单个节点、还能创建共识网络的方法。

区块链技术的本质是一种互联网协议。

## 哈希算法：

安全散列算法（英语：Secure Hash Algorithm，缩写为SHA）是一个密码散列函数家族，是FIPS所认证的安全散列算法。能计算出一个数字消息所对应到的，长度固定的字符串（又称消息摘要）的算法。且若输入的消息不同，它们对应到不同字符串的机率很高。【2】

|  |  |
| --- | --- |
| 优秀功能 | 描述 |
| 正向快速 | 给明文，有限时间、有限资源，能拿密文。 |
| 逆向困难 | 给密文，基本不能推出明文 |
| 输入敏感 | 原始输入的信息的微小变化，新的Hash值都应该有很大不同 |
| 冲突避免 | 很难找到两段不同的明文，他们的Hash值一致。  发生碰撞：Hash值一致。 |
| 抗碰撞性 | 弱抗碰撞性：  给定明文的前提下，无法找到与之碰撞的其他明文。  即是要给定。  强抗碰撞性：  无法找到任何两个发生碰撞的明文。 |

## 加解密算法：

密钥：加密密钥，揭秘密钥

一般来说密钥按照特定算法在每次加密前随机生成，长度越长，加密强度越大。

加 解 密 算 法 
3 ． 加 解 密 过 程 
加 密 密 刨 
加 密 过 程 ： 通 过 加 密 算 法 和 加 密 密 钥 ， 对 明 文 进 行 加 密 ， 获 得 密 文 · 
解 密 过 程 ： 通 过 解 密 算 法 和 解 密 密 钥 ， 对 密 文 进 行 解 密 ， 获 得 明 ． 乙 

## 消息认证码与数字签名：

消息认证码：

全称：基于Hash的消息认证码

消息验证码是基于对称加密，可以用于对消息完整性进行保护。

数字签名：

数字签名基于非对称加密。既可以用于证实某数字内容的完整性，又可以确认来源。

分类：

盲签名：签名者无法看到原始内容的情况下对信息签名。

实现对签名内容的保护，同时防止追踪。

多重签名：n个签名者中，收集到至少m个（n>=m>=1）的签名，即认为合法。

n：提供的公钥个数

m：需要匹配公钥的对至少个数

可以有效用在需要多个投票共同抉择的场景

群签名：一个成员代表群组进行匿名签名

签名可验证来自于该群，却无法准确追踪到签名者

环签名：签名者首先选定一个临时签名者集合，利用自己的私钥和集合中其他人的公钥，可以独立地产生签名，无需他人帮助。集合中其他成员可能不知道自己被包含在该集合中，保证匿名性。

## 数字证书：

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够被探测出来，从而实现对用户公钥的安全分发。

数字证书的分类：

加密数字证书：保护用于加密信息的公钥

签名验证数字证书：保护用于进行解密签名进行身份验证的公钥

证书认证机构（Certification Authority, CA）

一般情况下，证书需要由CA来进行签发和背书。

DigiCert, GlobalSign, VeriSign等

X.509证书规范

规定证书可以包含什么信息，并且说明记录信息的方法。

证书信任链：

从先信任的根证书，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。

如果信任链上某一证书不可靠，则后继所有证书都会失去信任保障。

PKI体系

CA：证书的颁发和作废，接受来自RA的请求

RA：对用户身份进行验证，校验数据和发行，审核通过就发给CA

证书数据库：存放证书

# 联盟链和公有链的异同

公有链：Public BlockChains

例子：比特币

世界上任何个体或者团体都可以发送交易，且交易都能够获得该区块链的有效认证，任何人都可以参与其共识过程。

联盟链：Consortium BlockChains

（较为核心，本课程所学也是该链的一种）

由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定，其他接入节点可以参与交易，但不能过问记账过程，其他任何人可以通过该区块链开放的API进行限定查询。

“公有链”从 "public blockchain"翻译而来，而"public"直译应为“公众、公共”。之所以会翻译成“公有链”，我想大概是由于早期的public blockchain都有内在的代币机制，使用者即代币持有者，因此也无不妥。但按照今天的眼光看，"public blockchain"理解为“公共链”更为合适，“公共链”无差别的对所有公众提供服务，但公众不一定是“公共链”的所有者。我在讨论中还是沿用“公有链”这个词，但我用它指代的其实是“公众链”。联盟链/私有链在具体实施上有不同的许可链选项：可以是节点许可链、出块许可链或者完全许可链，由此也会有相应的优缺点，在此不再重复。这些不同选项的共同之处是，出块节点都是需要许可的，共识范围有限，牺牲了可靠性换来了更好的性能和隐私。未来联盟链/私有链如果能够以无需许可链作为信任基础，其可靠性和信用也可以提高到与无需许可链接近的程度，实际上会成为无需许可链扩容的助力，这是Nervos CKB团队、Nervos AppChain团队和Cryptape Research在探索的方向。如果在跨链协议的帮助，联盟链/私有链之间可以低成本的进行互操作，联盟链/私有链上资产的流动性也将提高到与无需许可链上的资产流动性接近的程度，这是Nervos AppChain团队和Cryptape CITA团队在探索的方向。【3】

公有许可链：public permissioned blockchain

考虑维度1和维度2之间的关系，很容易发现联盟链和私有链都隐含了对用户以及节点的身份限制，因此必然是许可链。有意思的问题是：公有链一定是无需许可链吗？按照上文对公有链的定义，对公众提供服务并不隐含对用户身份的限制。公有链可以对匿名的公众提供服务，也可以不加选择的对有身份的公众提供服务。公有链中的节点是否需要许可，并不影响一条区块链是否对公众提供服务。因此在我的观念中，一条区块链可以同时是公有链和许可链，这两者之间没有矛盾。我把既是公有链又是许可链的区块链称为公有许可链[4]。我们日常谈到公有链时往往想的是无需许可链，但是实际上不少公有链更接近公有许可链的范畴，最典型的例子是Ripple。公有许可链可能的实现形式很多，前面讨论过的许可链、出块许可链、节点许可链、用户许可链都可以是公有许可链。由于身份的存在，公有许可链既有许可链的优点，其适用的场景又与无需许可链互为补充，相信将在未来的加密经济生态中占有重要的位置。

# 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，那么如何支付？ 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还有许多其他的微妙之处，但这应该给你基本的东西！ 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.【4】

# 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。另一个建立在分布式存储创业公司是Storj，SJCX是Storj网络的代币“燃料”，它允许用户通过 DriveSahre 应用和 MetaDisk 来出租和购买存储空间。

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。总之，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。【5】

# 并行计算

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。【6】

并行计算（Parallel Computing）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。

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：是指流水线技术，比如说工厂生产食品的时候步骤分为：

1． 清洗：将食品冲洗干净。

2． 消毒：将食品进行消毒处理。

3． 切割：将食品切成小块。

4． 包装：将食品装入包装袋。

如果不采用流水线，一个食品完成上述四个步骤后，下一个食品才进行处理，耗时且影响效率。但是采用流水线技术，就可以同时处理四个食品。这就是并行算法中的时间并行，在同一时间启动两个或两个以上的操作，大大提高计算性能。

空间上的并行：是指多个处理机并发的执行计算，即通过网络将两个以上的处理机连接起来，达到同时计算同一个任务的不同部分，或者单个处理机无法解决的大型问题。

比如小李准备在植树节种三棵树，如果小李1个人需要6个小时才能完成任务，植树节当天他叫来了好朋友小红、小王，三个人同时开始挖坑植树，2个小时后每个人都完成了一颗植树任务，这就是并行算法中的空间并行，将一个大任务分割成多个相同的子任务，来加快问题解决速度。

为利用并行计算，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。

并行计算科学中主要研究的是空间上的并行问题。从程序和算法设计人员的角度来看，并行计算又可分为数据并行和任务并行。一般来说，因为数据并行主要是将一个大任务化解成相同的各个子任务，比任务并行要容易处理。

空间上的并行导致了两类并行机的产生，按照Flynn的说法分为：单指令流多数据流（SIMD）和多指令流多数据流（MIMD）。我们常用的串行机也叫做单指令流单数据流（SISD）。MIMD类的机器又可分为以下常见的五类：并行向量处理机（PVP）、对称多处理机（SMP）、大规模并行处理机（MPP）、工作站机群（COW）、分布式共享存储处理机（DSM）。

访存模型

并行计算机有以下五种访存模型：

均匀访存模型（UMA）

非均匀访存模型（NUMA）

全高速缓存访存模型（COMA）

一致性高速缓存非均匀存储访问模型（CC-NUMA）

非远程存储访问模型（NORMA）。

计算模型

不像串行计算机那样，全世界基本上都在使用冯·诺伊曼的计算模型；并行计算机没有一个统一的计算模型。不过，人们已经提出了几种有价值的参考模型：PRAM模型，BSP模型，LogP模型，C^3模型等。

并行计算与云计算

云计算是在并行计算之后产生的概念，是由并行计算发展而来， 两者在很多方面有着共性。学习并行计算对于理解云计算有很大的帮助。并行计算是学习云计算必须要学习的基础课程。

但并行计算不等于云计算，云计算也不等同并行计算。两者区别如下。

（1）云计算萌芽于并行计算

云计算的萌芽应该从计算机的并行化开始，并行机的出现是人们不满足于CPU摩尔定率的增长速度，希望把多个计算机并联起来，从而获得更快的计算速度。这是一种很简单也很朴素的实现高速计算的方法，这种方法后来被证明是相当成功的。

（2）并行计算、网格计算只用于特定的科学领域，专业的用户

并行计算、网格计算的提出主要是为了满足科学和技术领域的专业需要，其应用领域也基本限于科学领域。传统并行计算机的使用是一个相当专业的工作，需要使用者有较高的专业素质，多数是命令行的操作，这是很多专业人士的噩梦，更不用说普通的业余级用户了。

（3）并行计算追求的高性能

在并行计算的时代，人们极力追求的是高速的计算、采用昂贵的服务器，各国不惜代价在计算速度上超越他国，因此，并行计算时代的高性能机群是一个“快速消费品”，世界TOP500高性能计算机地排名不断地在刷新，一台大型机群如果在3年左右不能得到有效的利用就远远的落后了，巨额投资无法收回。

（4）云计算对于单节点的计算能力要求低

而云计算时代我们并不去追求使用昂贵的服务器，我们也不用去考虑TOP500的排名，云中心的计算力和存储力可随着需要逐步增加，云计算的基础架构支持这一动态增加的方式，高性能计算将在云计算时代成为“耐用消费品”。

# 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。【7】

开发过程更加严格也更慢

　　创建一个完全统一的系统并不是简单的任务。很小的失误都会使得整个数据库被破坏，或者导致一些数据库变得和其他的不同。当然，被破坏或者分裂的数据库再也没有任何统一性的保证。并且，所有这类系统都需要设计成从外部来看具有统一性。在区块链中，并没有“快速前进，打破常规）”的说法。如果你打破常规，你就失去了统一性，那么区块链就会变得破坏以及没有价值。

　　那么也许你会想，为什么你不能只是修复这个数据库，或者重新启动再推进了？在中心化的系统中，这很容易解决，但是在去中心化系统中却非常困难。你需要系统中所有参与者的共识或者同意，来对数据库进行修改。区块链应该是开源的，并且不被任何中心化单位所控制。

## 激励制度设计有很大难度

　　增加激励制度，并且保证系统中所有的参与者都不会攻击或者破坏数据库，是非常值得考虑的事情。区块链也许具有一致性，但是如果其中含有很多无用数据的时候，这就不会非常有用，因为将数据输入的成本会非常低。也不会有任何具有一致性的区块链会有用，如果其中不包含任何数据，因为将数据放入的代价非常高。

　　那么如何确保数据最终的准确性？你怎么确保奖励是和网络的目标是一致的呢？为什么节点要去维持或者更新数据，在有冲突的时候，他们为什么要选择其中一个？这些都是关于激励的问题，现在需要解答，而且不止是在开始的时候需要统一好，后续随着公司和技术的变化，也要时刻保持统一。不然区块链就没用了。

　　而且，也许你想知道为什么你不能修改一些有问题的激励模式。再一次强调下，这在中心化系统中很容易实现，但是在去中心化系统中，在没有达成共识的前提下，你不能修改任何东西。除非从每个人那边获得共识，不然你不能修改任何东西。

## 维护非常花费成本

　　传统的中心化数据库只需要写入一次就可以。但是区块链需要写入几千次，传统的中心化数据可以只需要一次性检测数据。区块链需要检查几千次数据。传统中心化数据库需要只需要一次性将数据转移到存储器。区块链则需要将数据转移几千次。

　　维护区块链的成本是数量级增长，而且这部分成本还需要根据使用性能进行更改。大多数应用都在追求之前说的一致性和稳定性等特性，但是如果使用完整性检查，收据和备份，在成本上就会便宜很多。

## 用户为王

　　这样会很好，因为公司不喜欢将用户的数据放在首要责任。但是如果用户做出什么不好的行为，这也非常不好，因为你无法将这个用户踢出，或者指出这样做会影响其他很多的便利性。

　　以上可以说明，激励制度的设计非常非常重要，可以使得用户不想去放弃，特别是如果对这个用户来说有利可图。也许你会想说，你可以简单地拒绝为欺诈者服务，这在中心化服务过程中很容易实现。但是，和中心化服务不同，在区块链上拒绝服务很困难因为没有任何个人有权利去将别人踢出。区块链必须要遵守软件中写下的规则。如果这个规则不能惩罚不好的行为，那么只能说你运气不好。区块链上，没有“法律”的精神，你只能花费很长时间去处理恶意行为。

## 所有的升级是自发的

　　强制升级并不是选项。网络上的其他人员没有义务去更改你的软件。如果他们这样做，那么不如打造更加容易，快速以及便宜的中心化系统。区块链的关键在于它不受控制于单个主体，同时这也和强制升级相违反。

　　但是，所有的升级都要和之前兼容。显然这很困难，特别是当你想添加新的特性时，如果从测试角度来看，就更加困难了。每个版本的软件都会添加很多的测试矩阵，也会花费更多的时间来进行释放。

## 扩容非常困难

　　最后，在扩容性方面至少要比传统中心化系统要难几个数量级。原因很明显。同样的数据需要在成百上千个地方，而不是像中心化那样，在同个地方。传输，验证和存储的开销是很大的，因为区块链上任何数据库的复制都需要花钱，而不像中心化的数据库那样，只需要付费一次就可以。

## 中心化会容易很多

　　如果你发现这个问题，那就是去中心化的系统很难进行运作，维护也很昂贵，很难升级并且不容易扩容。中心化的数据库和区块链比起来，就会更加快速，便宜，容易维护并且升级也比较容易。那么为什么人们还要使用区块链作为解决方案呢？

　　首先，很多想要使用区块链的行业，对于IT底层升级已经完全过时了。医疗行业有众所周知地难用的软件。金融结算还在用70年代的软件。供应链管理软件很难使用，也很难安装。这些行业的很多公司拒绝去更新软件，因为这会带来很多风险。有很多底层更新，花费了数百位美元，但是最后又用回之前的软件。区块链可以帮助这些行业IT底层的更新。

　　其次，区块链让你看起来是在科技的前端。其实很少人真地理解区块链，但是都想要使用这些词汇来让自己听起来显得更加聪明。就好像“云计算”意味着其他人的电脑，“AI”意味着修正算法，“区块链”在这篇文章中的意思就是缓慢，昂贵的数据库。

第三，在某些行业，人们不喜欢政府的监管，所以希望有和缓慢昂贵的法律框架不同的仲裁机制。对他们来说，区块链是避免政府监管很好的方法。这其实也高估了区块链可以做的事情，区块链不可能魔幻版地去除人的影响。我们现在就有些像“皇帝的新衣”。

参考文献

【1】戴晓橙，3分钟看懂区块链，《中国社会组织》2016年20期

【2】Eli Biham, Rafi Chen, Near-Collisions of SHA-0, Cryptology ePrint Archive, Report 2004/146, 2004

【3】秘猿科技，知乎论坛回答，2019-04-29

<https://www.zhihu.com/question/286791282/answer/645889029>

【4】Wesle，<https://www.jianshu.com/p/64c42b692c6b>，简书

【5】奔跑写作，<https://www.jianshu.com/p/9dba1af3734d>，简书

【6】百度百科，并行计算

<https://baike.baidu.com/item/%E5%B9%B6%E8%A1%8C%E8%AE%A1%E7%AE%97/113443?fr=aladdin>