华南理工大学

课程报告

课程名称：	企业软件项目实训
学生姓名：	吴金泽
学生学号：	**201630665885**
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

企业软件项目实训课程报告

谈及区块链，很多人首先想到的就是比特币。然而，比特币只是基于区块链技术的一种落地实现，两者并不能划等号。那么，什么是区块链呢？本质上，区块链是一种去中心化的分布式数据库。

- 数据库是什么？数据库就是计算机上的一组表格，它可以存放大量的有结构的信息，可以简单地类比为 Excel。比如我们去银行存款、取款、汇款，这些交易信息都是要上传到银行的数据库的。
- 分布式是什么？数据库可以存放在银行的一台超级电脑上，也可以放在多台电脑上。比如工行可能在华北、华中、华东、华南等地区各有一台服务器，每个地区的交易信息发送到本地区的服务器上，各个服务器之间通过银行的内部网络连接。这就叫“分布式数据库”。
- 去中心化是什么？传统的服务器，不管是不是分布式的，都是有“管理员”的。也就是说，有一个银行内部的“超级用户”可以查看所有的交易信息，并且可以随意添加、修改这些信息。这就叫“中心化”。而区块链则是“去中心化”的。也就是说，区块链这个数据库中不存在管理员，所有人都是平等的，都有权查看、添加信息。去中心化是区块链的本质特征。

既然所有人都有权往区块链上添加信息，那么这个“账本”难道不会乱七八糟吗？没有了管理员，人人都可以往里面写入数据，怎么才能保证数据是可信的呢？被坏人改了怎么办？要搞清楚这点，我们需要了解什么是“区块”，什么是“链”。

何为“区块”何为“链”？“区块”是区块链的基本组成。区块就是一个数据块。类比账本的话，区块就相当于账本上的一页，这一页上记录了多条交易信息。而把这些分散在整个互联网上的“页”串成一条链，就可以形成一个完整的“账本”。那么，“区块”是怎么串成“区块链”的呢？

1. 区块链的技术原理

区块链由一个个区块（block）组成。区块很像数据库的记录，每次写入数据，就是创建一个区块。每个区块包含两个部分：区块头和区块体。区块头包含了当前区块的多项特征值：生成时间、实际数据（即区块体）的哈希、上一个区块的哈希等等。

所谓“哈希”就是计算机可以对任意内容，计算出一个长度相同的特征值。区块链的哈希长度是 256 位，这就是说，不管原始内容是什么，最后都会计算出一个 256 位的二进制数字。而且可以保证，只要原始内容不同，对应的哈希一定是不同的。

因此，就有两个重要的推论：

- 每个区块的哈希都是不一样的，可以通过哈希标识区块。
- 如果区块的内容变了，它的哈希一定会改变。

区块与哈希是一一对应的，每个区块的哈希都是针对区块头计算的。也就是说，把区块头的各项特征值，按照顺序连接在一起，组成一个很长的字符串，再对这个字符串计算哈希。

前面说过，区块头包含很多内容，其中有当前区块体的哈希，还有上一个区块的哈希。这意味着，如果当前区块体的内容变了，或者上一个区块的哈希变了，一定会引起当前区块的哈希改变。

这一点对区块链有重大意义。如果有人修改了一个区块，该区块的哈希就变了。为了让后面的区块还能连到它（因为下一个区块包含上一个区块的哈希），该人必须依次修改后面所有的区块，否则被改掉的区块就脱离区块链了。由于哈希的计算很耗时，短时间内修改多个区块几乎不可能发生，除非有人掌握了全网 51%以上的计算能力。

正是通过这种联动机制，区块链保证了自身的可靠性，数据一旦写入，就无法被篡改。这就像历史一样，发生了就是发生了，从此再无法改变。每个区块都连着上一个区块，这也是“区块链”这个名字的由来。

由于必须保证节点之间的同步，所以新区块的添加速度不能太快。试想一下，你刚刚同步了一个区块，准备基于它生成下一个区块，但这时别的节点又有新区块生成，你不得不放弃做了一半的计算，再次去同步。因为每个区块的后面，只能跟着一个区块，你永远只能在最新区块的后面，生成下一个区块。所以，你别无选择，一听到信号，就必须立刻同步。所以，区块链的发明者中本聪故意让添加新区块，变得很困难。他的设计是，平均每 10 分钟，全网才能生成一个新区块，一小时也就六个。

这种产出速度不是通过命令达成的，而是故意设置了海量的计算。也就是说，只有通过极其大量的计算，才能得到当前区块的有效哈希，从而把新区块添加到区块链。由于计算量太大，所以快不起来。这个过程就叫做采矿，因为计算有效哈希的难度，好比在全世界的沙子里面，找到一粒符合条件的沙子。计算哈希的机器就叫做矿机，操作矿机的人就叫做矿工。

理论上，每个可接入区块链的节点都有成为矿工的权利，但是它们不一定有机会成为矿工。挖矿是一种周期性的竞争行为，根据共识算法不同，对

于每个挖矿周期，从矿工中选择“优胜者”的方式也有所不同，通常我们称这些“优胜者”为当前周期“出块者”。这种共识算法通常被理解成为“多数人共识”，而如何在网络中定义“人”这一过程，在不同共识算法中有所不同。挖矿是一种周期性的竞争行为，根据共识算法不同，对于每个挖矿周期，从矿工中选择“优胜者”的方式也有所不同，通常我们称这些“优胜者”为当前周期“出块者”。这种共识算法通常被理解成为“多数人共识”，而如何在网络中定义“人”这一过程，在不同共识算法中有所不同。目前存在很多种共识算法来决定这一过程，如：实用拜占庭容错算法（PBFT）、随机数算法、工作量证明（PoW）等等。

实用拜占庭容错算法刚开始是在 MIT 的 Miguel 和 Barbara Liskov 在 1999 年的学术论文中提出的，他们的本意是为设计一个低延迟存储系统设计系统，将算法复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行，主要是为了应用于不需要大交易量但需要处理许多事件的数字资产平台，每个节点都可以发布公钥，这是被允许的。节点将签名所有通过节点的消息，以验证其准确性。当得到一定数量的签名想用，此交易就被认定为有效。

在“拜占庭将军问题”模型中，拜占庭的 n 个将军围攻一个敌人，n 个将军包围着这个敌人，所以他们是在不同的地方。忠诚的将军希望通过某种协议达成某个命令的一致（比如约定某个时间一起进攻）。但其中一些背叛的将军会通过发送错误的消息阻挠忠诚的将军达成命令上的一致。如果同时发起进攻的将军数量少于 m 个，那么不足以歼灭敌人反而容易被敌人全部歼灭。怎样做才能保证有多于 m 个将军在同一时间一起发起进攻？

Leslie Lamport 在 1982 年提出的虚拟模型，用来解释一致性问题。他证明，当叛徒不超过 1/3 时，存在有效的算法，不论叛徒如何折腾，忠诚的将军们总能达成共识。当叛徒超过三分之一时，则无法保证一定能达成一致性。

拜占庭将军问题之所以难解，在于任何时候系统中都可能存在多个提案（作恶成本很低），并且要完成最终的一致性确认过程十分困难，容易受到干扰。但是一旦确认，即最终确认，概率上是 100%。但比特币采用的方案就不是完全按照 PBFT 来的，比特币的区块链网络采在设计时提出了 PoW（Proof of Work）算法思路，计算高难度的 hash 是为了限制在一段时间内整个网络中出现提案的个数（增加作恶成本），另外一个是放宽对最终一致性确认的需求，是约定好大家都确认并沿着已知最长的链进行延展，系统的最终确认是概率上的确认，不是 100%。这样，有人想作恶，会付出很大的经济代价（超过系统一半的算力）。

后来各种 PoX 的算法，也是沿着这个思路进行改进，采用经济上的惩罚来制约破坏者。

2. 联盟链与公有链的异同

除了区块链之外，相信有人也听说过区块链分为公有链、私有链和联盟链，那么，它们三者有何区别？

- 什么是公有链？公有链上的各个节点可以自由加入和退出网络，并参加链上数据的读写，读写时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点。像大家所熟悉的比特币和以太坊，都是一种公有链。公有链的好处是没有限制，你可以自由参加。

- 什么是私有链？私有链中各个节点的写入权限收归内部控制，而读取权限可视需求有选择性地对外开放。专有链仍具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。其中，R3CEV Corda 平台以及超级账本项目(Hyperledger project)等都是私有链项目，对交易效率、隐私保障和监管控制有着更高要求的场景，私有链的应用是主要方向。
- 什么是联盟链？联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。

三大类型区块链的核心区别，在于访问权限的开放程度，或者叫去中心化程度。本质上，联盟链也属于私有链，只是私有的程度不同。一般来说，去中心化程度越高、信任和安全程度越高，交易效率则越低。

公有链由于其公共开放的特性，所以任何人均可访问同时无法进行篡改等。由于其特性，所以吞吐量较低（TPS），交易过程较为缓慢。例如比特币真实的吞吐量只有 7，也就是每秒仅支持 7 笔交易。所以很难适用到目前的商业场景中。

联盟链是半公开的，只有预先指定的几个节点才能获取到记账权。其他加入的节点仅有交易权利。联盟链的权限设计较之于公有链会更加的复杂。但是由于其无需竞争记账与全网确认账单的特性下，联盟链的 TPS 较之于公有链来说比较好一些。

3. 信任链是如何建立的

信任链，或称数字证书链，是一连串的数字证书，由根证书为起点，透过层层信任，使终端实体证书的持有者可以获得转授的信任，以证明身份。

基于信息安全的考虑，在进行电子商务或使用政府服务时，交易的另一方用户，以根证书为基础，凭借对签发机构的信任，相信当时持有信任链终端的证书持有者确为其人，并透过公开密钥加密确保通信保密、透过数字签名确保内容无误、以及保证对方无法抵赖。

在互联网中，任何机构都可以登记域名以设立服务器，供大众连接沟通并进行电子商务或使用政府服务。虽然公开密钥加密可以确保通信保密、数字签名可以确保内容无误、以及保证对方无法抵赖；但如果数字证书未获得可供信任的数字证书认证机构数字签名（即自签证书），对方的真实身份仍然可疑（除非通信双方早已互相认识并预先透过安全渠道交换数字证书）。数字证书认证机构在公开密钥加密基建担任了非常重要的角色，计算机软件安装并信任了其根证书，根据其私钥签发的下层证书都可（基于数字签名）被自动信任，如果是中介证书，则再下层的终端实体证书也一样被自动信任，此即构成了一条信任链。

4. 分布式存储有什么优势

分布式存储是相对于集中式存储来说的，在介绍分布式存储之前，我们先看看什么是集中式存储。不久之前，企业级的存储设备都是集中式存储。所谓集中式存储，从概念上可以看出来是具有集中性的，也就是整个存储是集中在一个系统中的。注意，集中式存储并不是一个单独的设备，是集中在一套系统当中的多个设备。

分布式存储系统，是将数据分散存储在多台独立的设备上。传统的网络存储系统采用集中的存储服务器存放所有数据，存储服务器成为系统性能的瓶颈，也是可靠性和安全性的焦点，不能满足大规模存储应用的需要。分布

式网络存储系统采用可扩展的系统结构，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。

分布式存储最早是由谷歌提出的，其目的是通过廉价的服务器来提供使用与大规模，高并发场景下的 Web 访问问题。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。优点如下：

- 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。

- 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。

- 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。

- 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。

- 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。

- 弹性扩展

  得益于合理的分布式架构，分布式存储可预估并且弹性扩展计算、存储容量和性能。分布式存储的水平扩展有以下几个特性：

  1）节点扩展后，旧数据会自动迁移到新节点，实现负载均衡，避免单点过热的情况出现;

  2）水平扩展只需要将新节点和原有集群连接到同一网络，整个过程不会对业务造成影响;

  3）当节点被添加到集群，集群系统的整体容量和性能也随之线性扩展，此后新节点的资源就会被管理平台接管，被用于分配或者回收。

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。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：清洗、消毒、切割、包装。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。

空间上的并行导致两类并行机的产生，按照麦克·弗莱因（Michael 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），而常用的串行机也称为单指令流单数据流（SISD）。MIMD 类的机器又可分为常见的五类：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）。

并行计算机有五种访存模型：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）。

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。

至于并行计算与分布式计算的区别，并行计算是相对于串行计算而言，一般可分为时间并行和空间并行。时间并行可以看做是流水线操作，类似 CPU 执行的流水线，而空间并行则是目前大多数研究的问题，例如一台机器拥有多个处理器，在多个 CPU 上执行计算，例如 MPI 技术，通常可分为数据并行和任务并行。而分布式计算则是相对单机计算而言的，利用多台机器，通过网络连接和消息传递协调完成计算。把需要进行大量计算的工程数据分区成小块，由多台计算机分别计算，再上传运算结果后，将结果统一合并得出最终结果。

6. 当前区块链实施的难度

此前，互联网行业都在说，区块链技术是多么多么的好，甚至有人说，区块链可以颠覆世界。然而，区块链应用要想真正的落地，走进老百姓的生活，难度并不小。

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. 群组架构的好处

计算机集群是一组松散或紧密连接在一起工作的计算机。由于这些计算机协同工作，在许多方面它们可以被视为单个系统。与网格计算机不同，计算机集群将每个节点设置为执行相同的任务，由软件控制和调度。集群的组件通常通过快速局域网相互连接，每个节点（用作服务器的计算机）运行自己的操作系统实例。在大多数情况下，所有节点使用相同的硬件和相同的操作系统，尽管在某些设置中（例如使用 OSCAR），可以在每台计算机或不同的硬件上使用不同的操作系统。部署集群通常是为了提高单台计算机的性能和可用性，而集群也通常比速度或可用性相当的单台计算机的成本效益要高。

计算机集群的出现是许多计算趋势汇聚的结果，这些趋势包括低成本微处理器、高速网络以及用于高性能分布式计算软件的广泛使用。集群使用和部署广泛，从小型企业集群到世界上最快超级计算机（如 IBM 的 Sequoia）。在集群出现之前，人们采用具有模块冗余的单元容错主机；但是，集群的前期成本较低，网络结构速度提高，这助推了人们采用集群这种方式。与高可

靠性的大型机集群相比，扩展成本更低，但也增加了错误处理的复杂性，因为在集群中错误模式对于运行的程序是不透明的。

为了通过组合低成本的商用现成计算机，来获得更大的计算能力和更好的可靠性，人们研究提出了各种架构和配置。 计算机集群方法通常通过快速局域网连接许多现成的计算节点（例如用作服务器的个人计算机）。计算节点的活动由“集群中间件”协调，集群中间件是一个位于节点之上的软件层，让用户可以将集群视为一个整体的内聚计算单元（例如通过单系统映像概念）。

计算机集群依赖于一种集中管理方法，该方法把节点用作协调的共享服务器。它不同于其他方法（比如对等计算或网格计算），后者也使用许多节点，但具有更多的分布式特性。计算机集群可能是一个简单的两节点系统，只连接两台个人计算机，也可能是一台速度非常快的超级计算机。构建集群的基本方法是贝奥武夫机群，它可以使用少量个人计算机构建，以产生与传统高性能计算相比经济划算的替代方案。一个展示概念可行性的早期项目是 133 节点的 Stone Supercomputer。开发人员使用 Linux、并行虚拟机工具包和消息传递接口库以相对较低的成本实现高性能。

集群的设计主要考虑性能，但实际使用中还涉及许多其他因素，包括容错（能够容许系统继续使用故障节点）能力、可扩展性、高性能、不需要频繁运行维护程序、资源集成（如 RAID）和集中管理。集群的优点包括在发生灾难时启用数据恢复、提供并行数据处理和高计算能力。在可伸缩性方面，集群提供了水平添加节点的能力。这意味着可以向集群中添加更多的计算机，以提高其性能、冗余和容错。与在集群中扩展单个节点相比，添加节点是一个既节省成本，又可以使集群获得更高的性能的解决方案。计算机集群的这

一大特性允许大量性能较低的计算机执行较大的计算负载。向集群添加新节点时，可靠性也会增加，这是因为进行维护的时候不需要停下整个集群，只需停下单个节点维护，集群的其余节点承担该节点的负载即可。 如果集群包含大量的计算机，那么可以使用分布式文件系统和 RAID，这两种方法可以大大提高集群的可靠性和速度。

8. Gas 在智能合约中的作用

"Gas"就是让以太坊智能合约可以执行下去的“钱”。交易是按照只能合约的规定按部就班的执行下去的，每执行一个命令就会有一定的“钱”被消耗，这个“钱”用 Gas 做为单位，不同命令消耗的 Gas 数量不同。以太坊上的每笔交易都会被收取一定数量的 gas，gas 的目的是限制执行交易所需的工作量，同时为执行支付费用。当 EVM 执行交易时，gas 将按照特定规则被逐渐消耗。如果执行结束还有 gas 剩余，这些 gas 将被返还给发送账户。无论执行到什么位置，一旦 gas 被耗尽（比如降为负值），将会触发一个 out-of-gas 异常。当前调用帧所做的所有状态修改都将被回滚。

Gas 是交易中计算交易费的单位，最终交易费是多少还是用"钱"来表示更直观。交易费 = gasUsed（该交易消耗的总 gas 数量） * gasPrice（该交易中单位 gas 的价格，用 ETH 计算）。如一笔交易的交易费是 0.001ETH，那么这个 0.001ETH 就是 gasPrice。

每笔交易都被要求包括一个 Gas limit（有的时候被称为 startGas）和一个愿为单位 Gas 支付的费用。其中 Gas limit 是这笔交易允许的最大的消耗 Gas 的数量，可以理解为交易服务本身的服务费；而愿为单位 Gas 支付的费用，可以理解为小费。

无论你何时执行智能合约，你必须确定这笔交易允许的最大消耗 Gas 的数量（即 Gas limit 或称 startGas），Gas limit 可以理解为交易时候必要的服务费。除此之外还有一个愿为单位 Gas（可以理解为交易时的小费）当合约执行完成之时，或是达到 Gas 限制之时，都会停止执行该合约。这么做是为了避免智能合约陷入无限循环之中，以防该程序反复执行一组语句，而不继续执行其他合约。

矿工有权利选择先打包哪一笔交易，支付的交易费越多矿工就越快“接单”，交易确认的速度也会越快。Gas limit 是一笔交易最多需要的交易费，交易费一般不会超过这个值，若交易完成后没有用完 Gas limit 数量的 Gas，那么多余的 Gas 会以 ETH 的方式返还给你。如果你想让交易更快的被打包完成，这就涉及到了愿为单位 Gas，也就是交易中多给的小费了。所以想要更快打包的交易所需实际消耗的 Gas（Gas limit+愿为单位 Gas）可能超过 Gas limit（交易的 Gas limit 不一定会都被用光，所以 Gas limit+愿为单位 Gas 可能大于、小于、等于 Gas limit）。

Gas 确保了交易了一定的费用给以太网络。执行的每个交易都被要求支付相应的费用，这样才能确保网络不会因为进行大量密集的工作而陷入瘫痪。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。

参考文献

[1]M.Pilkington, “Blockchain Technology: Principles and Applications,”in Research Handbook on Digital Transformations, 2016.

[2]I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse. “Bitcoin-NG: a scalable blockchain protocol,” in 13th Usenix Conference on Networked Systems Design and Implementation (NSDI'16), Berkeley, CA, USA, 2016, pp. 45-59.

[3]M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1-3.

[4]M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1-3.

[5]M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1-6.

[6] I. C. Lin and T. C. Liao, “A Survey of Blockchain Security Issues and Challenges,” in International Journal of Network Security, vol. 195, no. 5, 2017, pp. 653-659.

[7] M. Conti, C. Lal, and S. Ruj, “A survey on security and privacy issues of bitcoin,” arXiv preprint arXiv:1706.00916, 2017.