**63 | 区块链技术的本质**

陈皓 2018-05-08



C:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\88FEA3B4.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\EE6827E2.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\D8A0F240.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\9768524E.tmp



去年专栏一开始更新的时候，就有读者留言让我发表一下对区块链技术的看法。当时我觉得区块链相关的技术相对比较简单，没什么好说的。并且，“左耳听风”专栏的主要目标是帮助大家学习更为主流的关键技术，所以那会我就把区块链相关的技术文章降级处理了。

那为什么现在我又要写这个主题呢？

2010 年，我在浏览国外技术网站时，看到好多人在讨论一个叫 bitcoin 的东西，还看到有人说用几万个这个东西换了个披萨。随后，我看了一下它的[白皮书](https://bitcoin.org/bitcoin.pdf)，这篇不到 10 页的文档读起来还是很容易的，所以建议你读一读。

然后，我在一台电脑上尝试安装了一下，就像用 BT 或电驴下载一样，连入了这个没有服务器的 P2P 网络，下载了账本，还尝试了一下“挖矿”。

花了不少的时间，我收到了来自系统奖励的 50 个比特币。当时，我默默地看着这个又耗硬盘空间，又非常吃 CPU 的家伙，心里想，这什么破软件，太难用了，就删除了。（是的，这 50 个比特币也就不知道去哪了。）

记得比特币开始有价值的时候，像维基解密这样的机构为了避开被政府控制的银行，会接受比特币的捐款。2012 年的时候，比特币已经看涨了，到了 2013 年，比特币的市值已经比较高了，突破了 1000 美金。

那个时候，中国有好多人在挖矿。记得最厉害的是李笑来，他持有的比特币数量很可观，如果没有卖的话，现在就更为“恐怖”了。

在 2016 年的时候，我听说了个叫以太坊的东西。嗯，是区块链 + 代码的组合，又被叫作智能合约，这的确给予了区块链有更多的想像空间。还听说了这个项目是被 ICO 出来的，然后我就了解了下 ICO。同年，我有一个高中同学，搞了个创业项目，据说是中国第一个 ICO 项目。当时筹到了 1000 万人民币，然后发币上了二级市场。

再然后，2017 年的一天有人带我去见薛蛮子。听他说他在很短的一段时间内出手投了好多个和区块链相关的创业项目。见薛蛮子一周后，中国政府出台政策定性 ICO 非法，开始治理市场，清除所有一切和 ICO 相关的东西。

似乎市场应该就此冷静下来了。

2018 年 1 月 9 日，真格基金创始人徐小平在一个微信群里对他投资公司的 CEO 们说，区块链是一场伟大的技术革命。他要求大家“对区块链不要有怀疑，不要有迟疑，立即动员全体员工，学习如何拥抱这场革命”。

随着徐小平这个微信截图的流出又把区块链推到了风口浪尖。我几个关系不错的做技术的朋友也跟着入坑了……各种人，认识我的，不认识我的，全都来找我，问我区块链的事，我不想关注都不成了……

所以，我想我还是在这里写上几篇文章吧。一方面，我会很客观地把区块链的技术解释出来（不是那种天马行空完全不知所云的比喻，是实实在在的技术，我保证非技术人员都一定能看得懂），包括区块链、非对称加密、挖矿、共识机制等。

另一方面，我会结合现有的一些金融上的交易撮合的中心化标准玩法来让你来比较一下中心化和去中心化的不同。最后，我会谈一些我的观点，可能会上升到哲学层面。当然，最后还是由你自己来做判断。

下面是这几篇文章要回答的关键问题。

1. **为什么区块链技术会成为热点技术？它解决了什么问题？**
2. **区块链（blockchain）究竟是个什么技术？这里，我会带你抽丝剥茧看看区块链技术，看看区块链是如何做到不可篡改的。同时，我还会解释什么是“挖矿”，以及为什么要 " 挖矿 "，全是技术干货。**
3. **去中心意味着没有一个公司，没有公司就意味着没有服务器，没有服务器的软件是怎样提供服务的？这里主要会讲一下无中心化的系统是怎么运作的，是怎么达成一致的？**
4. **智能合约是个什么鬼？它有什么意思？**
5. **简单地谈一谈金融，你可以自行思考一下，区块链虚拟货币是否有可能取代现有的金融服务？并重组整个社会架构？**
6. **最后，我会提出几个逻辑问题来让你独立思考一下“去中心化”的优劣，以及相关的逻辑和哲学问题。**

闲言少叙，我们开始。

## 区块链技术的革命性

你一定看过太多的文章用各式各样的比喻来讲区块链技术是什么，以及为什么它是未来。在这里，我尝试用我的话来说明一下区块链技术的革命性。

说区块链必然要谈比特币，比特币是一种数字货币。但最令人叫绝的是，比特币号称有下面几个特性。

1. **去中心化**。这意味着没有中心的服务器，不受某个人的控制，整个系统直接由用户端的电脑构成。这样的技术难度是非常大的，并不像手机 App 或是小网站一样，你想发布就发布，这需要有人来跟你一起玩。
2. **数据防篡改**。所有交易记录全量保存，并公开给所有的人，而且还被加密和校验。并不是数据不能被篡改，而是数据被篡改的成本非常大。（有人借此说区块链的不可篡改可以解决人类的信任问题，这个并不一定。）
3. **固定的发行量**。不会像国家中央银行那样乱印钞票，造成通货膨胀。

这几个东西加在一起，就可以让那些想作弊的人，尤其是那些有权有势有钱的大公司大组织很难作恶。因为“去中心化”这个事，从本质上来说，造就了整个系统不再需要这些个大的公司和组织，人民可以达到真正意义上的自治，这些大公司都会倒闭。

简单说来，相信区块链的人都相信，可以通过区块链这个技术来改变整个社会的组织形成——不再需要银行、中介机构、电商平台、支付宝等中间机构，人们可以通过一个不受任何人控制和操作的 P2P 金融系统，进行完全自由和可信的交易。

当然，反区块链的人的观点也很明确。他们认为，所谓的去中心化看似很美好，但实则不可能。而且从目前的区块链的应用来看，也没有颠覆什么，连迹象都没有。反而，大家都在疯狂地炒作概念，没有实质的价值。像 ICO 和交易所这样的东西里面充满了大量的投机主义，泡沫非常大。

于是，这种巨大无比的争议性，把人们分割成了两种阵营，把区块链推向了火热。对此，我这几篇文章会把区块链这个技术一点一点讲解清楚，让你自己判断。

其实，对于投资机构来说，在逻辑上，我觉得他们应该感到恐慌才对，因为他们也是被革命的对象啊。如果某个事不再需要公司，人们自治，那么投资人怎么投资啊？投资的实体都没了啊，怎样有回报？

如果说，投资机构想扶植一个小公司用区块链技术把大公司干掉，那在逻辑上也说不通啊，因为如果你投资的公司也可能被别人很容易地颠覆掉，那么你怎么可能会投资呢？

相关的逻辑问题，我们会放在最后来讨论，还是先看一下区块链的技术。下面会有非常详细的技术细节，如果你不关心技术细节，那么可以只看“”技术概要”一节。

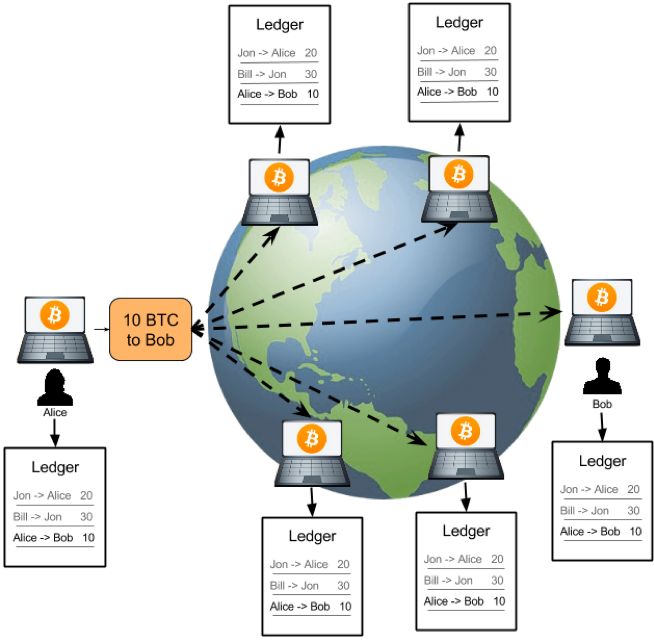
## 技术概要

首先，我们先看一下中心化和去中心化的业务流是什么样的。

下面的图给出了“传统中心化”和“去中心化”的对比。



中心化结构



去中心化的交易

去中心化的比特币交易处理流程如下。

* 首先，需要交易的用户把交易传到网络中。
* 然后，网络上有些机器叫记账结点，它们通过比拼计算力的方式竞争记账权。这也叫“挖矿”。
* 获得记账权的结点，会把待记账的交易进行计算打包，并向全网广播。收到新的记账包的结点会对其进行验证，验证通过后加入自己的区块。

注意，整个比特币的世界是没有服务器的，其完全是靠大家用自己的电脑拼出来的一个分布式系统。既然这些电脑都是大家自己的，所以这种 P2P 的去中心化网络有一个前提假设——**“网络中的任何结点都是不能信任的，它们中的任何一个都可能会作恶”**。

基于这个前提假设，这个分布式的账本系统就需要有如下的设计：**任何人都可以拿到所有的数据。所以，数据要能很容易被验证是合法的没有被修改过的，而且也要是很难被人修改的。**

基于这个设计，比特币使用了两个比较大的技术：**“区块链技术”和“工作量证明共识机制”**。

### 区块链

第一个技术就是区块链，区块链又叫 blockchain，其中有一个一个的区块，每个区块中包括着一组交易信息，然后，每一个区块都会有一个 ID（或是一个地址），这些区块通过记录前一个区块的 ID 来形成一条链。下面的图有助于你形象地理解这一概念，感兴趣可以看看。



但需要注意下面这几个方面。

* **每个块的 ID 都是通过其内容生成的**，所以，只要是内容有一丁点儿的变化，这个 ID 都会完全不一样。
* 而生成 ID 的内容中还包括上一个块的 ID。于是只要上一个块的内容变了，其 ID 也要跟着变（不然就不合法了），那么后面指向这个块的 ID 也要变。于是，后面指向这个块的 ID 也要重新计算，而变成另一个，这样就会形成一个连锁效应——一个块被修改，后续的所有块都要跟着一起改。于是导致了修改成本的提升。
* 这种一处改，处处改的方式，并不代表不能篡改，而只是让修改面比较大，让你的改动麻烦一点。
* 越旧的区块的篡改会造成越大面积的修改，于是越旧的区块就不容易篡改，就越安全。反之，越新的区块就越不安全。

而真正让区块链做到非常难篡改的是工作量证明的共识机制。

### 工作量证明共识机制

我们知道，分布式网络的数据一致性是最难的问题了，在这种去中心化的网络集群下就更难了。其中最大的本质差别是，**一个公司内的分布式系统中的结点是被假设成可信任的，而在去中心化的网络下，结点要被假设成不可信任的。** 想象一下，在一堆不可信的结点上做一致性是不是一件很难的事？

这里，需要解决几个与“数据一致性”相关的问题。

* **以谁的数据为准？** 任何结点都可以修改自己所下载的账本，也就是任何一个人都可以伪造账本。那么，谁的数据才是对的？**在去中心化的网络下，我们只能认为，大多数人认识的数据是对的。**只要我控制了一半以上的结点，我让这“大多数人”伪造同一份账本，那么相当于整个账本都被我修改过来了。**因为在没有服务器的去中心化的网络下，所谓的真理只不过是大多数人同意的东西。**
* **“大多数人”的问题。** 是人数吗？在网络世界里，我可以用程序模拟出无穷多的“人”出来投票，所以，用人数来解决去中心化的问题，在分不清是人还是狗，是生物还是程序的计算机世界里，是一件很愚蠢的事。
* **意见分歧问题。** 如果在同一个时刻，有多个人都在告诉其他人，这账应该这么记。比如说，有人说，左耳朵转了 10 块钱给了耗子叔，有人说，左耳朵转了 20 元给了耗子叔，还有人说，左耳朵没有花钱，是陈皓花的钱。而且，他们的数据都合法，那么，整个网络应该听谁的？

是的，这种没有人组织的玩法真是乱啊。

为了解决这几个问题，比特币使用了 Proof-of-Work 工作量证明机制，也就是“挖矿”。所谓的“挖矿”其实就是用大规模的计算来找到一个符合系统要求的区块 ID。要找到符合条件的区块 ID 只能通过暴力穷举的方式，所以要付出大量的系统计算资源和电力。

这样一来，我们用这种“极度消耗计算力”的方式来提高成本，从而有效地遏制或解决下面几个问题。

1. **修改几乎变得不可能**。试想，如果生成一个区块需要大量的长时间的计算力。也就是在世界上最好的电脑集群下计算 10 分钟才能打好一个包。那么，当我们要去修改数据内容的时候，这个过程也是一样的。前面说过，如果你要伪造一个块，那么你就要修改后面所有的块，修改一个块的成本如此之高，那么修改整个链的成本也就非常之高了。
2. **能掌握 51% 的算力的人变得几乎不可能**。除了伪造一条链的成本很高，还要控制大多数人的算力，这意味着需要巨额的资金投入。这两个难度加起来，几乎不太可能。
3. **解决分歧**。一方面，这么大的工作量找出来的区块 ID，已经有效地降低了大家有意见冲突的概率。另一方面，就算是出现了合法冲突的区块（同时出现了多个合理的区块，即区块链出现分支 / 分叉），**也就是多个合法的账本**。而因为挖矿的成本太高，导致要同时跟进多个账本是不可能的，所以矿工们只能赌跟其中一个。大多数人所选择的那一个分支的链就会越来越多，于是另外一边也就无人问津，从而作废了。

你别看 Proof-of-Work 成本这么高，还这么耗电不环保，但是，这是目前去中心化系统中最安全的玩法。（其中的相关细节可以查看后面的挖矿和去中心化的共识机制）

好了，上面就是区块链的相关技术概要。如果想了解相关的技术细节，你可以继续阅读后面的内容，我会一一给你解析。

**64 | 区块链技术细节：哈希算法**

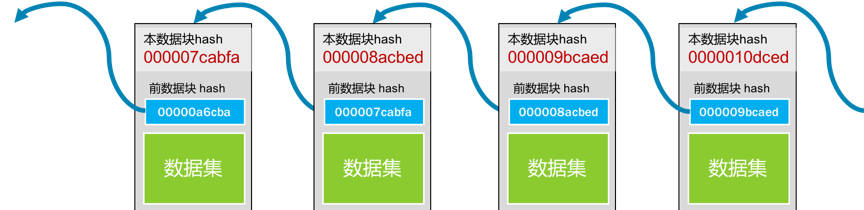


C:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\B973E398.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\84A54566.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\4E74DE64.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\6D0C2612.tmp

对于计算机来说，区块链就像一个单向链表，一个数据块中保存着三个信息。

* 真正的数据。
* 自己的地址（或是 ID）。
* 前一个数据块的地址。

这样，通过追溯前一个块的地址，把所有的数据块存成了一条链。所以，我们叫其 BlockChain。如下图所示。



每个数据块的“地址”的编码使用了计算机上的一个算法，计算机圈内人士把这个算法叫 Secure Hash。有人音译为“安全哈希”，也有人意译为“安全散列”。在计算机应用中，hash 算法主要有几个功能。

* 用来生成唯一标识一个数据块的 ID（身份证），这个 ID 几乎不能重复。
* 用来做数据的特征码。只要数据中一个 bit 的数据出现更改，那么整个 hash 值就完全不一样了。而且数据学上保证了，我们无法通过 hash 值反推回原数据。

于是，很多公司在互联网上发布信息或软件的时候，都会带上一个 Checksum（校验码）。你只要把整个文件的数据传入到那个特定的 hash 算法中，就会得到一串很长的字符串。如果和官方发布的 Checksum 字符串不一样，那么就说明信息或文件内容被人更改或是信息残缺了。因此，也被应用在“数字签名”中。

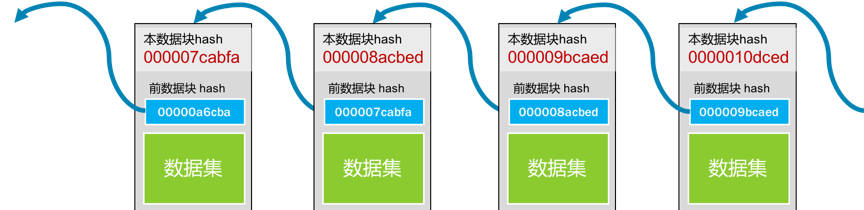
在计算机世界里，有两个很著名的 hash 算法，一个叫 MD5（[Wikipedia 链接](https://en.wikipedia.org/wiki/MD5)），一个叫 SHA-2（[Wikipedia 链接](https://en.wikipedia.org/wiki/SHA-2)）， 区块链用的是 SHA-256 这个算法。

下面是一个示例。

* 对 "chen hao" 这个信息计算 MD5 值得到 9824df83b2d35172ef5eb63a47a878eb（一个 16 进制数）。
* 如果对 “chen hao" 做一个字符的修改，将字母 "o" 改成数字 "0”，即 “chen ha0”，计算出来的 MD5 值就成了 d521ce0616359df7e16b20486b78d2a8。可以看到，这和之前的 MD5 值完全不一样了。

于是，我们就可以利用 hash 算法的这个特性来对数据做 " 数字签名 "。也就是说，我将 " 数据 " 和其 " 签名 "（hash 计算值）一起发布，这样可以让收到方来验证数据有没有被修改。

我们再来看上面那个区块链的图。



对于第一块数据，我们把其“数据集”和“前数据块的 hash 值 00000a6cba”一起做 hash 值，得到本区块的地址 000007cabfa。然后，下一个区块会把自己的数据和 000007cabfa 一起做 hash，得到 000008acbed 这个哈希值……如此往复下去。

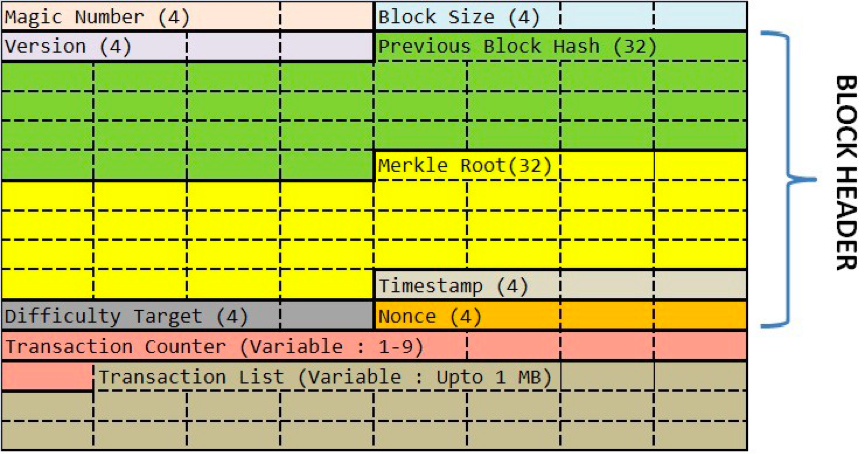
根据“被 hash 的数据中有一个 bit 被修改了，整个 hash 就完全不一样了”这个特性，我们知道：

* 如果前置数据块中的数据改了，那么其 hash 就会完全不一样了，也就是说你的 ID 或地址就变了，于是别人就找不到这个数据块了；
* 所以，你还要去修改别人数据块中指向你的地址，但是别人数据块中指向你的地址（ID/hash）变了，也会导致他自己的地址（ID/hash）随之变化。因为他用你的地址生成了自己的地址，这样一来，你就需要把其他人的地址全部改掉。

在这样的连锁反应下，你想要偷偷修改一个 bit 的难度一下就提高很多。所以，在区块链的世界里，越老的区块越安全也越不容易被人篡改，越新的区块越不安全也越容易被人篡改。

## 比特币的 hash 算法

下面我来简单介绍一下，比特币中区块链的一些细节。下图是区块链的协议格式。



其中 Version，Previous Block Hash，Merkle Root，Timestamp，Difficulty Target 和 Nonce 这六个数据字段是区块链的区块数据协议头。后面的数据是交易数据，分别是：本块中的交易笔数 H 和交易列表（最多不能超过 1MB，为什么是 1MB，后面会说）。

下面我来说一下区块头中的那六个字段的含义。

* Version：当前区块链协议的版本号，4 个字节。如果升级了，这个版本号会变。
* Previous Block Hash：前面那个区块的 hash 地址。32 个字节。
* Merkle Root：这个字段可以简单理解为是后面交易信息的 hash 值（后面具体说明一下） 。32 个字节。
* Timestamp：区块生成的时间。这个时间不能早于前面 11 个区块的中位时间，不能晚于 " 网络协调时间 "——你所连接的所有结点时间的中位数。4 个字节。
* Bits：也就是上图中的 Difficulty Tagrget，表明了当前的 hash 生成的难度（后面会说）。4 个字节。
* Nonce：一个随机值，用于找到满足某个条件的 hash 值。4 字节。

对这六字段进行 hash 计算，就可以得到本区块的 hash 值，也就是其 ID 或是地址。其 hash 方式如下（对区块头做两次 SHA-256 的 hash 求值）：

|  |  |
| --- | --- |
|  | SHA-256(SHA-256 (Block Header)) |
|  |  |

复制代码

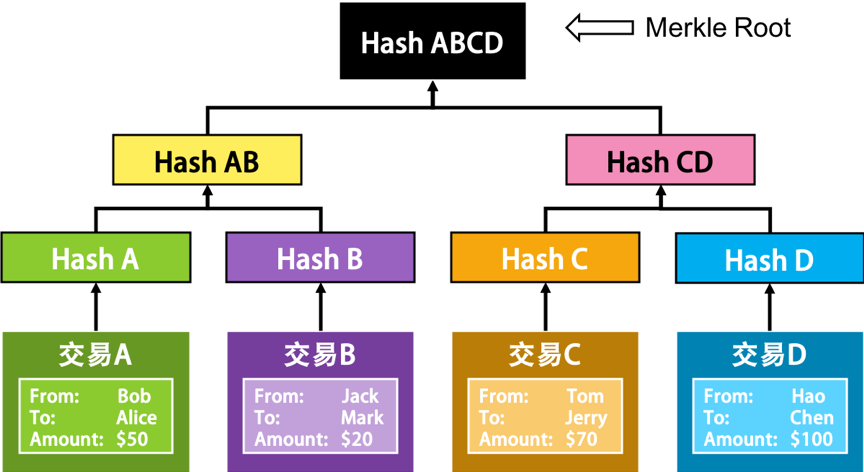
当然，事情并没有这么简单。比特币对这个 hash 值是有要求的，其要求是那个 Bits 字段控制的，然后你可以调整 Nonce 这个 32 位整型的值来找到符合条件的 hash 值。我们把这个事情叫做“挖矿”（在下一篇中，我们会详细讲一下这个事）。

## 关于 Merkle Root

前面说到过，可以简单地将 Merkle Root 理解为交易的 hash 值。这里，我们具体说一下，比特币的 Merkle Root 是怎么计算出来的。

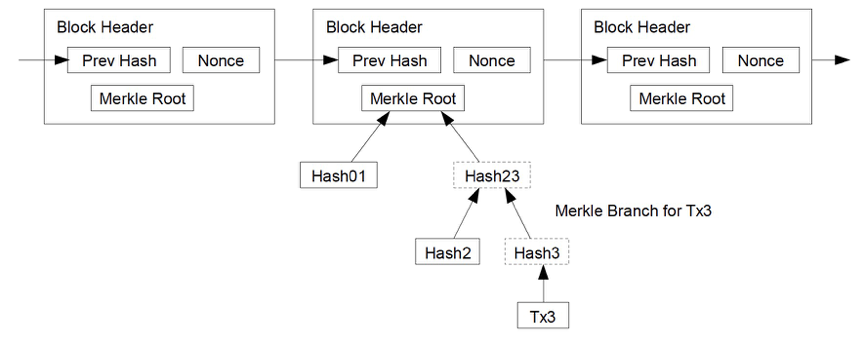
首先，我们知道，比特币的每一笔交易会有三个字段，一个是转出方，一个是转入方，还有一个是金额。那么，我们会对每个交易的这三个字段求 hash，然后把交易的 hash 做两两合并，再求其 hash，直到算出最后一个 hash 值，这就是我们的 Merkle Root。

我画了一个图展示一下这个过程。



上面的示意图中有四笔交易，A 和 B 的 hash 成了 Hash-AB， C 和 D 的 hash 成了 Hash-CD，然后再做 Hash-AB + Hash-CD 的 hash，得到了 Hash-ABCD，这就是 Merkle Root。整个过程就像一个二叉树一样。

下图是一个区块链的示意图，来自[比特币的白皮书](https://bitcoin.org/bitcoin.pdf)。



为什么要这样做呢？为什么不是把所有的交易都放在一起做一次 hash 呢？这不也可以让人无法篡改吗？这样做的好处是——我们把交易数据分成了若干个组。就像上面那个二叉树所表示的一样，我们可以不断地把这个树分成左边的分支和右边的分支，因为它们都被计算过 hash 值，所以可以很快地校验其中的内容有没有被修改过。

这至少带来三个好处。

1. 大量的交易数据可以被分成各种尺寸的小组，这样有利于我们整合数据和校验数据。
2. 这样的开销在存储和内存上并不大，然而我们可以提高校验一组数据的难易程度。
3. 在 P2P 的无中心化网络上，我们可以把大量数据拆成一个一个小数据片传输，可以提高网络的传输速度。

最后，需要说一下的是，以太坊有三个不同的 Merkle Root 树。因为以太坊要玩智能合约，所以需要更多的 Merkle Root。

* 一个是用来做交易 hash 的 Merkle Root。
* 一个是用来表示状态 State 的。因为一个智能合同从初始状态走到最终状态需要有若干步（也就是若干笔交易），每一步都会让合同的状态发生变化，所以需要保存合同的状态。
* 还有一个是用来做交易收据的。主要是用来记录一个智能合约中最终发生的交易信息。在 StackExchange 上的问题 "[Relationship between Transaction Trie and Receipts Trie](https://ethereum.stackexchange.com/questions/5888/relationship-between-transaction-trie-and-receipts-trie)" 中有相应的说明，你可以前往一看。

以太坊称其为 Merkle Patricia Tree（具体细节可参看其[官方的 Wiki](https://github.com/ethereum/wiki/wiki/Patricia-Tree)）。

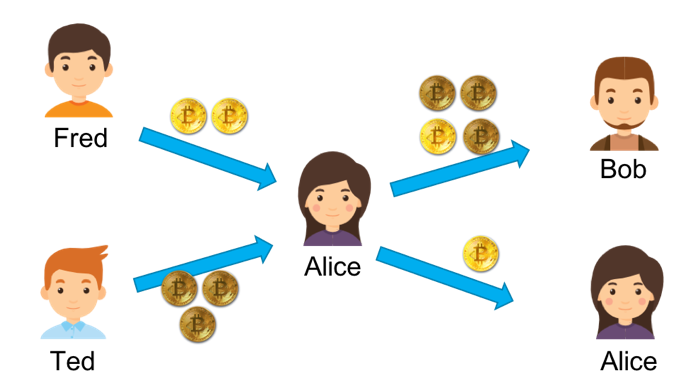
## 比特币的交易模型

比特币区块中的交易数据，其实也是一个链。为了讲清楚这个链，我们需要了解一下比特币交易中的两个术语，一个是 input，一个是 output，也就是交易的支出方（input）和收入方（output）。

在比特币中，一个交易可以有多个 output，也就是说我可以把一笔钱汇给多个人，但一个 output 只能对应一个源的 input，还有一个条件就是，output 跟 input 的总数要吻合。

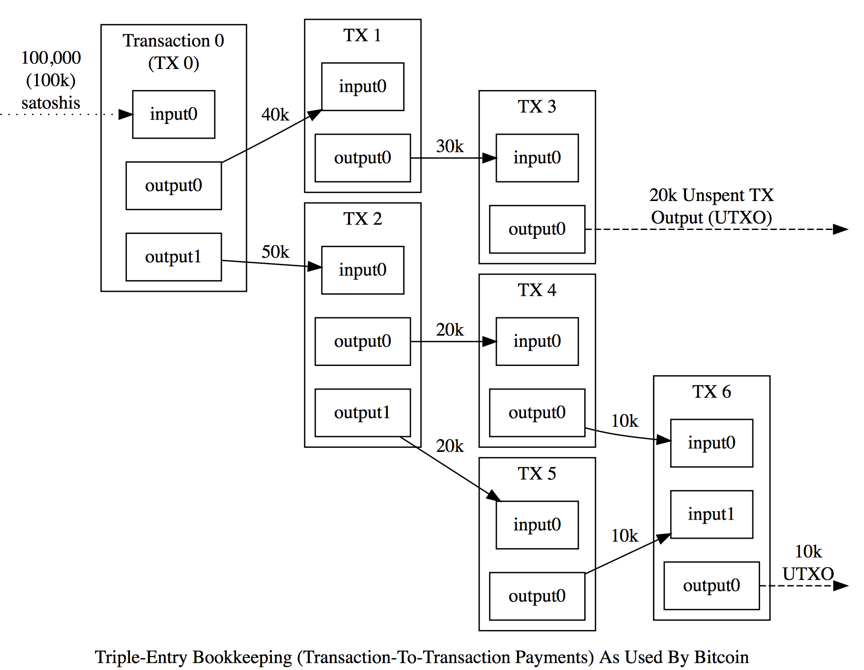
这里举个例子。假设，Fred 给了 Alice 2 个比特币，Ted 给了 Alice 3 个比特币，这个时候，Alice 有 5 个比特币。然而，大比特币的世界里是没有余额的，所以，对于 Alice 来说，她只有两个没有花出去的交易，一个是 2 个比特币，一个是 3 个比特币。这在比特币中叫 UTXO（Unspent Transaction Output）。

此时，如果 Alice 想要转给 Bob 4 个比特币，她发现自己的两个交易中都不够，也不能拆开之前的那两个比特币交易，那么她只能把交易 2 和交易 3 当成 input，然后把自己和 Bob 当成 output，Bob 分得 4 个，她自己分 1 个。这样的交易才平衡。



于是，一笔交易可能会包含大量的 Input 和 Output。因为比特币没有“余额”的概念，所以需要通过多个 input 来凑，然后 output 这边还需要给自己找零，给矿工小费。

这样一来，在比特币交易中，你把钱给了我，我又给了张三，张三给了李四……就这样传递下去，形成了一个交易链。因为还没有花出去，所以就成了 UTXO，而系统计算你有没有钱可以汇出去时，只需要查看一下你的 UTXO 就可以了。

  
(图片来源：<https://bitcoin.org/en/developer-guide> )

UTXO 因为没有账户和余额的概念，所以可以并行进行多笔交易。假如你有多个 UTXO，你可以进行多笔交易而不需要并行锁。然后其还有匿名性的特征，你可以隐藏自己的交易目的地（通过设置的多个 output），而且没有余额意味着是没有状态的。要知道你有多少个比特币，只需要把 UTXO 的交易记录统计一下就可以知道了。但这也让人比较费解，而且也不利于应用上的开发。以太坊则使用了余额的方式。

在这篇文章中，我先讲述了什么是区块链以及它的核心原理是什么。随后分享了比特币的 hash 算法，以及 Merkle Root 是如何计算出来的。最后，介绍了比特币的交易模型。希望对你有帮助。（**这篇文章中图片很多，很难用音频体现出来，所以没有录制音频，还望谅解。**）

**66 | 区块链技术细节：去中心化的共识机制**

陈皓 2018-05-17



C:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\E441A748.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\574EB496.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\E6C48514.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\E0087042.tmp



其实，去中心化的共识机制也是要解决拜占庭将军问题（[The Byzantine Generals Problem](https://web.archive.org/web/20170205142845/http:/lamport.azurewebsites.net/pubs/byz.pdf)），它是莱斯利·兰伯特（Leslie Lamport）于 1982 年提出来的，用来解释一致性问题的一个虚构模型。同时，它也是分布式领域中最复杂、最严格的容错模型。

## 分布式一致性算法

拜占庭的将军们没有一个中心化的领导机构，所以，如果他们需要攻击某个城市，所有将军需要对任何将军可能提出的攻击时间达成共识。也就是说，只有所有的将军都达成了共识，在同一个攻击时间攻击，就有非常大的胜率。但是，问题来了。这时，可能会有多个将军同时发出不同的攻击计划，而且这些将军中还有叛徒。那么，将军们怎样达成共识呢？

莱斯利·兰伯特证明，当叛变者不超过 1/3 时，存在有效的算法。不论叛变者如何折腾，忠诚的将军们总能达成一致的结果。如果叛变者过多，则无法保证一定能达到一致性。

拜占庭问题之所以难解，在于任何时候系统中都可能存在多个提案（因为提案成本很低），并且要完成最终的一致性确认过程十分困难，容易受干扰。但一旦确认，即为最终确认。

比特币的区块链网络在设计时使用的 PoW（Proof of Work） 算法思路。一个是限制一段时间内整个网络中出现提案的个数（增加提案成本），另外一个是放宽对最终一致性确认的需求，约定好大家都确认并沿着已知最长的链进行拓宽。

也就是说，如果比特币系统在某一个时刻同时出现了两个都合法的区块，那么两个都承认。于是，区块链上会出现两个合法的分支（术语叫 " 分叉 "）。此时矿工可以选择任何一个分支继续，在某个分支的长度超过了另一个分支时，短的那个分支马上作废。

如果你看过我之前写的《分布式系统架构的本质》系列文章，那么一定知道 Paxos 协议，这也是一种分布式一致性的共识算法。但为什么不用 Paxos 和 Raft 来做区块链的一致性算法的协议呢？这两个算法对资源的消耗比 PoW 要小得多呢。

如果你熟悉这几个算法，那么你就知道 PoW 和 Paxos/Raft 的算法在本质上有下面这些不同。

* 对于 Paxos/Raft，其需要 Leader 选举，而对于比特币或者以太坊这样的无中心化的方式是没有 leader 的。
* 对于 Paxos/Raft，加入其网络（集群）的结点前提假设都是受信的。然而，对于比特币 / 以太坊来说，其前提假设都是不受信的，它们只相信，超过一半的结点所同意的东西。
* 对于 Paxos/Raft，需要事先对整个集群中的结点数有定义，而无中心化的比特币和以太坊中的结点是想来就来，想走就走，来去自由。如果 Paxos/Raft 在这样的环境下，其会处于一个非常尴尬的境地——要能随时进行伸缩。而且，Paxos/Raft 并不适合在一个非常大的网络中玩（比如上百万的结点）。

但是它们有一些是相同的。

* 它们都是一致性的算法。
* 对系统的修改总是需要一个人来干（区块链用 PoW 消耗资源，让提案变得困难，Paxos/Raft 用领导选举）。
* 系统中暂时的不一致是可以被修正的（区块链会考虑最长链，牺牲了强一致性，保证了可用性，Paxos/Raft 如果没有超过半数的结点在线，会停止工作，牺牲了可用性，保证了强一性）。

总之，区块链所面对的无中心化的 P2P 网络要比 Paxos/Raft 所面对的相对中心式分布式网络要复杂多得多。所以，不太可能使用 Paxos/Raft 协议来替代 PoW 协议。除非，你想干一个相对中心化的区块链，然而这就成了区块链的一个悖论了。

无论你是搞区块链，还是搞分布式，你都需要知道拜占庭容错系统研究中的三个重要理论：CAP、FLP 和 DLS。

* CAP 理论 - “在网络发生阻断（partition）时，你只能选择数据的一致性（consistency）或可用性（availability），无法两者兼得”。论点比较直观：如果网络因阻断而分隔为二，在其中一边我送出一笔交易：“将我的十元给 A”；在另一半我送出另一笔交易：“将我的十元给 B ”。此时系统要么是，a）无可用性，即这两笔交易至少会有一笔交易不会被接受；要么就是，b）无一致性，一半看到的是 A 多了十元而另一半则看到 B 多了十元。要注意的是，CAP 理论和扩展性（scalability）是无关的，在分片（sharded）或非分片的系统皆适用。
* [FLP impossibility](http://the-paper-trail.org/blog/a-brief-tour-of-flp-impossibility/)- 在异步环境中，如果节点间的网络延迟没有上限，只要有一个恶意节点存在，就没有算法能在有限的时间内达成共识。但值得注意的是， [“Las Vegas” algorithms](https://en.wikipedia.org/wiki/Las_Vegas_algorithm)（这个算法又叫撞大运算法，其保证结果正确，只是在运算时所用资源上进行赌博。一个简单的例子是随机快速排序，它的 pivot 是随机选的，但排序结果永远一致）在每一轮皆有一定机率达成共识，随着时间增加，机率会越趋近于 1。而这也是许多成功的共识演算法会采用的解决办法。
* 容错的上限 - 由[DLS 论文](http://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf)我们可以得到以下结论。
* 在部分同步（partially synchronous）的网络环境中（即网络延迟有一定的上限，但我们无法事先知道上限是多少），协议可以容忍最多 1/3 的拜占庭故障（Byzantine fault）。
* 在异步（asynchronous）网络环境中，具确定性质的协议无法容忍任何错误，但这篇论文并没有提及 [randomized algorithms](http://link.springer.com/chapter/10.1007%2F978-3-540-77444-0_7) 在这种情况可以容忍最多 1/3 的拜占庭故障。
* 在同步（synchronous）网络环境中（网络延迟有上限且上限是已知的），协议可以容忍 100% 的拜占庭故障。但当超过 1/2 的节点为恶意节点时，会有一些限制条件。要注意的是，我们考虑的是“具认证特性的拜占庭模型（authenticated Byzantine）”，而不是“一般的拜占庭模型”。具认证特性指的是将如今已经过大量研究且成本低廉的公私钥加密机制应用在我们的算法中。

## 工作量证明

比特币的挖矿算法并不是比特币开创的，其原型叫 [Hashcash](https://en.wikipedia.org/wiki/Hashcash)。这个想法最初是由哈佛大学的女计算机科学家辛西娅·德沃克 (Cynthia Dwork)、加州伯克立大学的 Moni Naor 和 Eli Ponyatovski 于 1992 年的 "[Pricing via Processing or Combatting Junk Mail](http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp_abs.html)" 论文中提出来的。是的，一开始这个算法是用来限制垃圾邮件的。

简单说来，Hashcash 一开始要求邮件发送方对邮件头（其中包括时间和收件人地址）计算一个 160bit 的 SHA-1 哈希值。其前面需要有 5 个零，也就是 20bit 的 0。接收端会检查这个事。

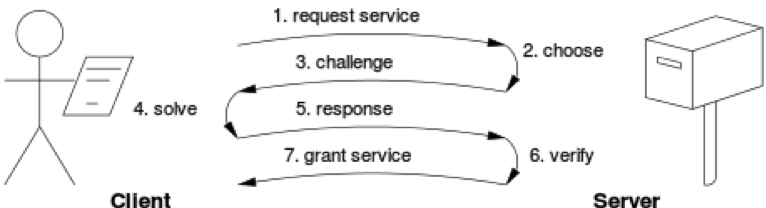
为什么要设计成这个样子？因为如果我们发垃圾邮件，这点算力对于发送方来说，没有什么。但对于需要大量发送垃圾邮件的人来说，这就是一个很大的成本了。就算是那些控制着用户的僵尸网络的黑客来说，发送垃圾邮件时，导致 CPU 使用率过高，会马上引起电脑所有者的警觉，而且还很容易定位相应的恶意程序。

对于一些受信的邮件服务器，我们可以把其放进白名单中，这样，就不需要它们接受 Hashcash 挑战，它们也不用为之付出成本。

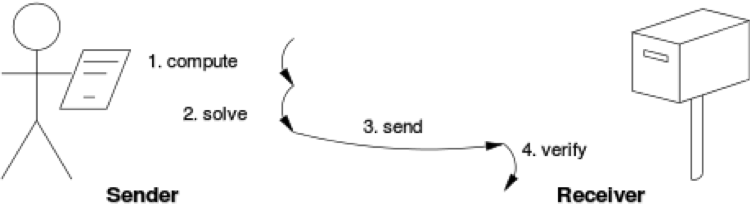
于是，这种玩法叫做 Proof-of-Work，简称为 PoW，工作量证明。我们用这种消耗对手能源的手段来阻止一些恶意的攻击或是像垃圾邮件这样的对服务的滥用。

PoW 有两种协议。

* 一种叫 Challenge-Response 协议，用于 Client-Server。如图所示，如果 Client 需要使用服务，那么需要被 Challenge 去花费一些资源。如果证明自己的资源已被花费了，则通过认证，授权使用。

  
（图片来源：[Wikipedia](https://en.wikipedia.org/wiki/Proof-of-work_system)）

* 另一种叫 Solution-Verification 协议，用于验证使用。Hashcash 就是这种协议。下图可以帮助你更形象地理解。

  
（图片来源：[Wikipedia](https://en.wikipedia.org/wiki/Proof-of-work_system)）

通过前面的描述，可以得知，我们需要为用户记录的交易是不能被修改的，所以使用 hash 方法为每个账本做了“签名”，还把其不断地打包再 hash 形成 merkle root，然后再形成一个串链。于是，修改一个地方就会导致所有地方的“签名（hash 值）”都需要跟着一起修改，于是形成了复杂度。

然而，这样的复杂度对于计算机来说并不高，找上一台或是几台主流点的电脑，分分钟就破解掉了。因为 hash 运维这个事对于计算机来说，是一件非常高效根本不费事的事。

于是乎，我们通过挖矿——PoW 这样的协议来大幅度地提高修改成本，使得有恶意的人要改一个地方，需要花很大很大的成本来修改。这几乎是一件不可能的事情。

因为比特币是去中心化的 P2P 系统，任何人都可以方便地获得所有的数据，所以为了防止有恶意的人修改数据，使用 PoW 的 " 挖矿 " 机制，可以大幅度提高想要通过修改和攻击这个系统的人的成本。

当然，PoW 的初衷是通过消耗资源的方式来阻止一些恶意攻击。然而在区块链的去中心化的世界里，PoW 还有另一个功能，那就是让这些不受控制的分布式 P2P 网络里的结点统一思想。也就是说我们常说的，分布式一致性。这对分布式系统中的交易系统来说是一件非常重要的事。

总结一下，工作量证明就是为了下面几件事。

1. **提高对数据篡改的成本**。让你修改数据需要付出大量的算力，而区块链的数据相互依赖，导致 " 一处改处处改 "，因此你要完全修改就需要付出大量的算力。
2. **提高网络中有不同声音的成本**。试想，如果一个网络有不同的人给出来了不同的账本，而且都合法，你会信谁的？所以，挖矿可以解决这个事。让你要做一个伪造账本的成本极其地大，而校验账本的成本很小。
3. **解决分歧**。当有不同声音的时候，即区块链出现分叉时，所有的矿工只能选择其中一个分支（因为没人有算力可以同时发出两个不同的声音)。于是，大多数人选择的那个分支就会成为事实，少数人选的那头就被遗忘了。**这让整个去中心化系统的一致性，不再以人数多认可的数据为准，而是以算力多的人认可的数据为准**。

只要网络越来越大，能掌握半数以上算力的人基本上是不可能的。是这样的吗？我表示怀疑。

PoW 解决这种无中心化网络的作弊、分歧这样的问题是目前最有效的，其他不用 PoW 这样的玩法的都存在很大的安全问题。但是，现在的 PoW 也有几个非常严重的问题。

1. **越来越中心化地记账**。本来是要大众一起参与去中心化的事，现在因为算力的问题，因为 GPU 的出现，导致一般人几乎无法参与其中了。
2. **越来越跑不动**。比特币今天的链越来越长，导致要验证数据是否正确的成本越来越高，一般人的电脑基本都快要跑不起来了。

所以，比特币社区也开始分裂成好几个衍生品，用不同的手段在解决这个问题。但是，目前为止，我没有看到什么比较好的方式。因为这世界上不存在完美的解决方案，你要一头，另一头就没了。

## 股权证明协议

PoW 这个机制，要找到符合条件的 Hash 值，在目前来看，其耗费的电力和时间成本是越来越大了。所以，为了每个 Block 更快的生成，出现了 PoS （Proof of Stake）协议，中文翻译为股权证明协议。

在 PoS 机制下，矿工不在叫矿工，而是叫 Validator（校验者）。假设现在有一个区域需要被生成，而现在有 4 个 Validator，每一个 Validator 需要以 " 交押金 " 的方式来取得记账权。假如，A 交的押金占了 38%，B 占 25%，C 点 21%，D 占 16%。那么，他们按照股权的比权来获得记账权。比如，A 有 38% 的概率可以获得记账权（不是由系统随机分配，还是要算 hash 值，只不过是财富越多的人挖矿的难度越小）。而如果你发起恶意攻击的话，你的钱就会被系统没收充公。而 Validator 记账后没有奖金，只有手续费。

也就是说，在 PoS 机制下，记账权不再像 PoW 那样由谁的算力大谁就越有机会来记账，而是由谁的财富多，谁就越有可能来记账。于是，记账权按大家财富的比例来分配。

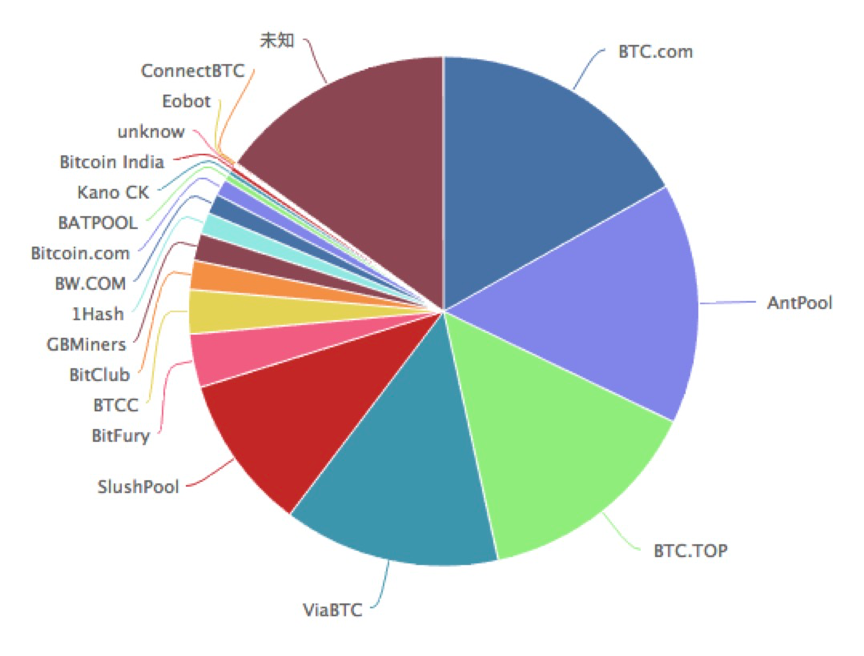
**PoW 好像是 " 多劳多得 " 的社会，而 PoS 更像是 " 资本主义 " 社会，钱越多的人越有话语权。这其实也没有什么不对的。从博弈论的角度上来说，钱越多的人越有动力维护社会的稳定，因为如果社会不稳定了，他是损失最为惨重的人。**

（**这里有一个逻辑问题：如果钱越多的人越有动力维护社会稳定，那么，是不是中心化的机构也越有动力维护整个系统的健康度？如果是这样的话，我们为什么要去中心化呢？**更多的逻辑问题会在本文最后提出。）

在以太坊下，是根据拥有以太币的总量，来决定成为 Validator 的机率。

PoS 宣称至少有如下的几个好处。

1. 第一个好处很明显。不需要那么费劲的挖矿了。那样浪费电力不环保地挖矿的确有点太糟糕了。PoS 很明显地解决了这个问题。
2. 在 P2P 这种无中心化的网络下，如果你要控制整个网络，就需要超过半数以上的能力。在 PoW 下，你需要 51% 的算力。在今天，这会是一个非常大的成本。但是我们看一下，下面的全球比特币的算力图，我们发现只要前四家公司联合起来作弊，就可以完成对比特币的攻击（据说中国有 60% 左右的算力，看来只要中国政府愿意，要拿下比特币也不是什么难事，呵呵）。而在 PoS 下，你需要有 51% 的财富，你才可以发起攻击，这相对于算力而言需要更多的成本。设想一下，你得拥有 51% 的比特币，你才能黑了比特币，然而，如果你有 51% 的财富，你为什么要黑了这个系统，自己把自己干死呢？这就是博弈论。

  
（图片来自：<http://qukuai.com/pools> ）

## PoS 机制潜在的问题

世界上没有免费的午餐，也没有绝对完美的事，所以 PoS 也有其潜在的问题。最明显的一个问题就是，当不需要太多算力的时候，如果账本出现分叉的情况，也就是系统出现两个冲突且合法的区块的时候，在比特币这种算力密集的 PoW 机制下，所有的矿工必需赌其中一个分支往下走。

因为算力的问题，所以基本上来说不太可能同时在两个分支上发展。而其中一个分支如果长于另一个分支，较短的那个分支就会被孤立出去，其上的账本就都不作数了，而矿工的奖励也没有了。这是 PoW 机制的好处。

而在 PoS 这种不需要算力的机制下，就可以让记账人们在两个分支上同时进行，以争取实现利益的最大化（无论哪个分支最终胜出，我都可以有利）。这样一来，攻击者就可以利用这种情况来发起 Nothin-At-Stake 攻击。

也就是说，如果绝大多数人都在发展两个分支，假设有 99% 的人发展 A 分支，99% 的人也同时发展 B 分支，而有 1% 股份的人在分支 A 中写一笔交易，然后在 B 分支没有这笔交易，当其在 A 分支上达成合约后（比如，收到商品），加入 B 分支，然后 B 分支胜出，导致其没有交易。

另外，两个分支发展还可以发起双重支付。就是说，Bob 把他的 10 元钱借给了 Alice，也给了 Marry，在不同的分支上。这就是所谓的 " 双重支付 " 问题（Double Spend Problem）。

在 CAP 理论中，如果出现网络分区的情况（Partition），你要么选择数据的一致性（Consistency）, 那么你就得让整个系统不可用（Availability）；要么选择系统的可用性（Availability），那么你就得牺牲数据的一致性（Consistency）。所以，在无中心化下，我们通过分叉来牺牲数据的一致性，于是，在一个分叉上，Bob 把 10 元给了 Alice，另一个分叉上，Bob 把 10 元给了 Marry。

甚至可以发起 " 贿赂攻击（Bribe Attack）"，攻击者可以在一个分支上声称购买了某个商品。然后，收到货后，以提高手续费的方式只养另一个没有购买这个商品交易的分支，然后把没有这个交易的链养得足够长，长到系统最终选择了没有交易的这条链。

在 PoW 机制下，这种 " 分叉攻击 " 的玩法基本上来说不可能，但在 PoS 的玩法下，这种攻击就很有可能。在以太坊下，如果发现有人玩同时养分叉的玩法，就会予以惩罚。然而，如果这个攻击者有多个账户呢？我用多个马甲来玩不同的分叉……

另外，PoS 这种通过财富的占比来决定记账概率的玩法，可以让结点进行预计算，也就是可以计算下一个的 hash 值，这样一来，相当于我可以偷偷养分叉。

看来，PoS 的问题也很多，所以有人又提出来了一个进化版，叫 DPoS（Delegated Proof of Stake，委托股权证明）。它是 PoS 的进化方案。

以太坊的官方 Wiki 上有一份[Proof-of-Stake 的 FAQ](https://github.com/ethereum/wiki/blob/master/%5B%E4%B8%AD%E6%96%87%5D-%E6%AC%8A%E7%9B%8A%E8%AD%89%E6%98%8E%E6%A9%9F%E5%88%B6FAQ.md)， 你可以前往一读。

## DPoS 机制

在常规 PoW 和 PoS 中，一大影响效率之处在于任何一个新加入的区块，都需要被整个网络所有节点做确认。DPoS 优化方案在于：通过不同的策略，不定时地选中一小群节点，这一小群节点做新区块的创建、验证、签名和相互监督。这样就大幅度减少了区块创建和确认所需要消耗的时间和算力成本。

这就像选举人团代议制度，和美国选总统一样。DPoS 下每个 token 都是选票，大家票选 20 个选举人团 +1 个随机选举人 =21 个选举人代表网络。然后每隔一段时间，在这 21 个人中挑选一个出来维护账本并获得收益。

近日，推崇 DPoS 的 EOS 开始了其 21 个超级节点的选举。作为超级节点，他们将获得 EOS 每年增发 5% 的收益中的大部分，大约每一个节点每年可以获得 238 万个 EOS 的收益，按照当前价格（EOS/RMB ￥34），一个节点每年可以分到 1 亿元人民币的奖励。

（注明一下，EOS 是以准备颠覆以及坊以及整个区块链生态的姿态，打着提高交易吞吐量到百万级 TPS 的技术口号，的进入这个世界的，本文成稿时，EOS 还没有正式发布，相关细节，你可以看看 [EOS 白皮书的中文版翻译](https://www.jianshu.com/p/f65bf7691482) 。）

比较有趣的是，在这次超级节点的竞选上，主要竞选节点来自中国、美国和韩国。这三方的优势是，韩国人拥有最大的 EOS 交易量，而中国人拥有更多的 EOS 之外的资本，而美国人则有规则制定权。看起来就是，美国有政治权力，韩国有经济权力，中国这边有外围经济权。看上去是比较完美的制衡，就像三国演义一样。

为了赢得选举，中国竞选人开始进行了我们熟悉的套路——贿选。所谓贿选，就是指将上文提到的当选超级节点后每年应分得的「巨额工资」返还给每一位投自己票的人。通过这样的贿选就可以破坏上述看起来比较制衡的政治局面。这样搞下去，很有可能，那 21 超级个节点就会成为一家公司所控制。

所以，很快，创始人 BM（Dan Larimer）就现身表示，不支持节点对投票人实行分红的做法。然后，Thomas Cox 也在社区内发帖《为什么付费投票是坏的》来谴责贿选，并在开始陆续发布 EOS.IO 的 0.1 版本「宪法」的第一条款《不说谎》…… （相关的报道可参看《[EOS 超级节点投票：「千亿」利润下的币圈国家战争](https://mp.weixin.qq.com/s/qtbyvpcEmN06V_p-QtCJ7A)》。）

顺便八卦一下，EOS 创建人 BM 在 2014 年的时候，创建比特股时打出超级比特币的概念，然后，因为 Bug 大多，体验非常地差，后面他和公司不合离开了比特股。2016 年，他创建了社交平台 Steemit，想颠覆传统媒体，结果也失败了，并于 2017 年创建 EOS，瞄准以太坊，想做区块链接基础设施（包括并行运算、数据库、账户系统等等）。老实说，我觉得这个对他来说更难。

在我看来，有两点让这区块链这个技术开始有些变味了。

* DPoS 已经开始把区块链的去中心化的初衷开始向中心化的地方演进了。
* 政治在未来区块链的世界里是一个必不可少的技能，这意味着不可控的复杂性。我感觉这些技术宅是一定 Hold 不住的。

## 小结

对我来说，目前为止，PoW 还是一个比较稳健的共识方式，PoS/DPoS 还需要更多的实践和改进，当然，也许混合 PoW 和 PoS/DPoS 也不错呢。" 去中心化 " 和 " 高吞吐 " 这两个事，我觉得是很难协调的。

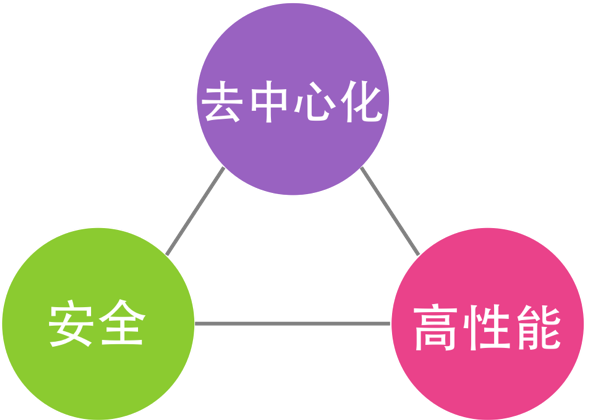
总结一下。

1. PoW 就是蛮荒社会。谁的拳头大谁说话。是真正意义上的无政府的去中心化的社会。
2. PoS 就是资本主义社会。谁的钱多谁说话，还是无政府的社会，但是资本家控制的。
3. DPoS 就是政治主义社会。谁的选票多谁说话，我也不知道怎么个选举，竞选活动吗？有电视辩论吗？还是投票玩玩？但是感觉又回到了中心化架构中的 Leader 选举。

无论怎么样，人类社会进化的影子在去中心化的社会中又开始出现了。那么，另一个逻辑问题来了，如果这种 " 去中心化的社会 " 本质上是在重复一遍 " 中心化 " 的演进过程，那么，还有什么意义？

上面的这个逻辑问题我们留到最后，这里还是看一下技术方面的事儿。

我们都知道，分布式系统的 CAP 原则，在一致性、可用性和分区容忍性上只能三选两。在区块链的 P2P 网络下也是很类似的，在去中心化、安全和高性能中，我们也只能选两个。



* 如果我们想要一个既安全，性能也很高的系统，那么得放弃去中心化的架构，如 DPoS 这样的中心化系统，直接放弃区块链走传统的中心化架构。
* 如果我们想要一个去中心化和安全的系统，主要去挖矿，那么放弃高性能。这就是目前的比特币架构。
* 如果我们想要一个去中心化和高性能的系统，那么就得放弃安全。没有安全的系统，基本上来说是不会有人用的。

**67 | 区块链技术细节：智能合约**

陈皓 2018-05-22



C:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\49ADA3FD.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\A5019413.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\9882FA99.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\5117D10F.tmp



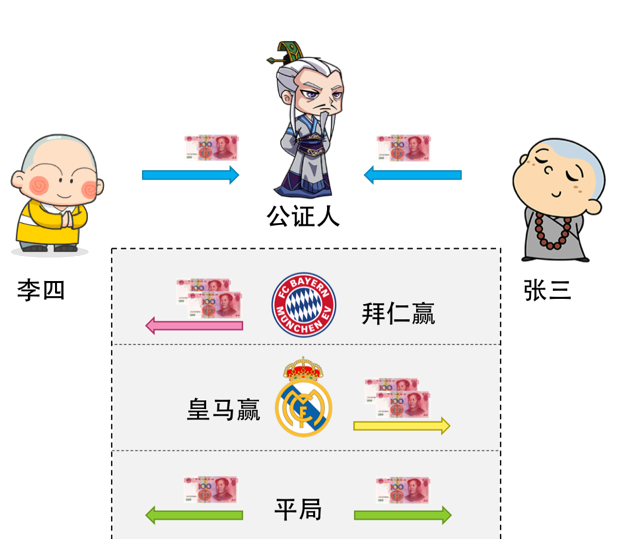
00:00

10:07

讲述：柴巍 大小：9.28M

要讲清楚智能合约，我先给你看几个案例。第一个案例是打赌。比如，张三和李四打赌，周末拜仁和皇马的足球比赛谁会赢。如果拜仁赢了，张三给李四 100 元；如果反过来，李四给张三 100 元；如果打成平局，则不赢不输。

张三和李四都怕对方不认账，所以，他们需要找一个他们都信得过的人来做公证，两人都把 100 元钱给这个公证人。然后，如果拜仁赢了，公证人把全部 200 元给李四；如果皇马赢了，则全部给张三；如果是平局，则分别退还 100 元。



上面这个模型什么都好，就是有一个问题，这个“公证人”跑路了怎么办？因为他们只赌 100 元，公证人犯不着为了 200 元跑路。但是，如果有一万人把赌金交给公证人呢？如果张三李四赌金是 100 万呢？公证人的人性会受到极大的挑战，他还有那么可信吗？

## 银行的资金托管业务

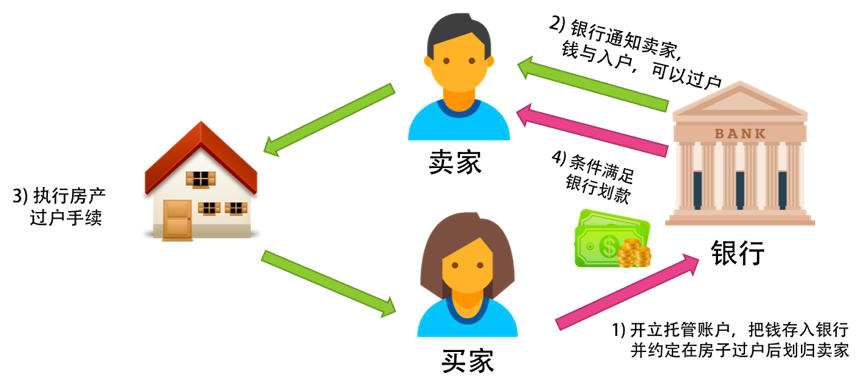
也就是说，当业务大到一定程度的时候，个人的信用是不足以来当中间公证人这个角色了。这时，你要找更为靠谱的机构，这个机构叫银行，银行的信用等级至少在这几方面上要比个人高。

* 银行是机构，所以受政府监管，受法律约束；
* 银行的钱很多，就算是里面有员工作案，银行也赔得起；
* 银行里有比较安全的资金管理流程和措施；

因此，银行的受信程度很高，可以来做担保。

下面，我们来看一个示例，银行在二手房交易中的“资金托管”业务。因为房屋交易时涉及到的资金数目太大，买家怕交了钱后，卖家不过户，卖家也怕过了户后，买家不给钱。而一般像“链家”或是“我爱我家”这样的房屋中介是没有能力来做大额交易的担保的（政府也不会让它们来做）。

于是银行就出来了。买家先到银行开个户，把购房款全额存进去。这个账户和一般的账户不一样，这叫资金托管账户，钱一旦进入后，你就取不出来了，除非满足了某个条件。在开户时，房屋的买卖方和银行三方约定，一旦房产证从卖家过户到买家 30 天后没有纠纷，钱就划给卖家了。



这其实跟在淘宝上买东西差不多，买家把钱转给支付宝，然后买家确认收到货后，在支付宝上点确认，钱就划给商家了。唯一不一样的是，支付宝没有资格担保像房屋交易这么大的交易金额。这是国家为了防范相关的金融风险所采取的措施。

## 以太坊的智能合约

对于以太坊来说，智能合约其实就是一段可执行的程序片段，由发布人使用一种类似于 JavaScript 或是 Python 的编程语言来编写。就像最开始那个民间担保的案例一样，合同的发布可以写成如下形式：

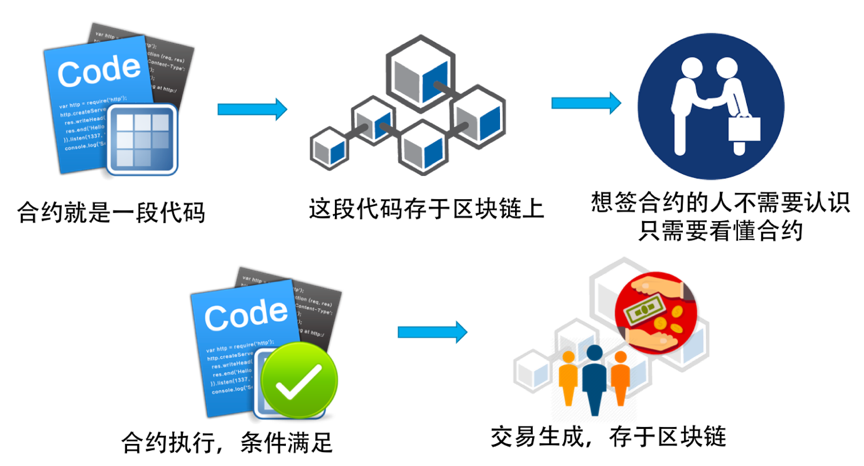
|  |  |
| --- | --- |
|  | Contract MyContract{ |
|  | function transferFrom( address \_from, address \_to, uint256 \_value) { |
|  | if ( isBayernWin ) { |
|  | blanceOf[\_from] += \_value |
|  | blanceOf[\_to] -= value |
|  | }else if ( isRealMadridWin ) { |
|  | blanceOf[\_from] -= \_value |
|  | blanceOf[\_to] += value |
|  | } |
|  | } |
|  | } |
|  |  |

复制代码

嗯，合同都要用代码来写了。看来，我们程序员离统治世界又近了一步。

我们把合约代码在本地编译成功后发布到区块链上，可以理解为一个特殊的交易（包括可执行代码），然后会被矿工打包记录在某一个区块中。当需要调用这个智能合约的方法时，只需要向这个智能合约的地址发送一笔交易即可。

每个节点的电脑都需要安装以太坊客户端，客户端自带了一个和 JVM 类似的一个 EVM。通过交易触发智能合约后，智能合约的代码就会在 EVM 中执行了。这种方式相当于把程序部署到了非常非常多的电脑上，随时都可以通过交易来触发这些智能合约的执行，也从而完成了分布式程序的部署和调用。



这感觉就是 Funciton-as-a-Service 的一种实现啊。

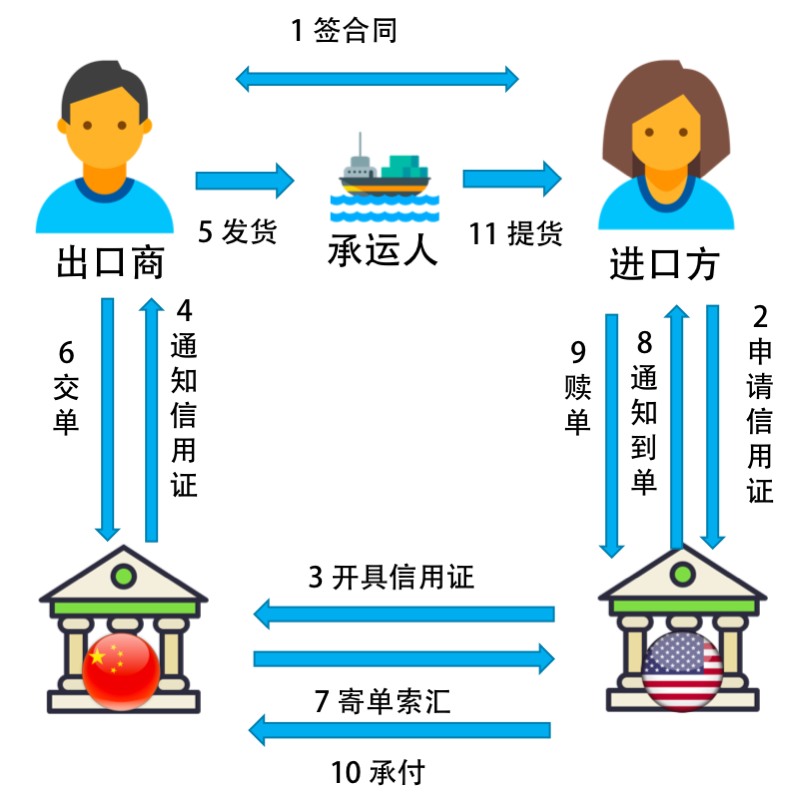
如果人与人之间的交易条件（合约）就像代码一样被严格地执行，你觉得这个世界会变成什么样呢？是不是会少一些无赖，少一些扯皮，多了很多效率，多了很多确定性呢？

## 有银行担保的国际业务

我们再来看一个国际贸易的流程。

假如中国某出口商和美国一个进口方做生意，会遇到货币不一样的问题。如果没有货币兑换，那就只有通过大家都认可的黄金交易了。你给我发一船货，我给你发一船黄金，风险也高，交易的效率非常低下。

如果有银行在中间协调，比如中国的某个银行和美国的某个银行签了互信协议，那么国际贸易的银行担保流程如下。下面是描述这一过程的图片。



1. 首先，出口商和进口商签订买卖合同。
2. 然后，美国的进口方到美国银行那边申请信用证（信用证需要用钱来开的，也是有价格属性的，比如 200 万美金的信用证，就需要用 200 万美金来申请）。
3. 美国的银行向中国银行开具信用证，中国银行根本不关心进口方有没有把钱给了美国银行，反正你开了 200 万美金面额的信用证，我以后要问你要钱的。
4. 中国银行收到信用证后，给出口商发出通知信用证，告之可以发货。
5. 出口商发货，由相关承运人从中国把货运到美国。
6. 然后，中国出口商把提货单交给中国的银行。
7. 中国的银行向美国银行发出“寄单索汇”业务。
8. 美国银行收到提货单后，通知进口方到单。
9. 进口方把货款的钱补完，比如补 300 万美金“赎回”提货单。
10. 然后美国银行向中国银行付款。
11. 美国进口方到承运人提货。

看看，这个过程如此复杂，而且很机械，感觉完全可以用程序来实现。如果用以太坊的智能合约来写一下，这段代码会写成什么样呢？

好像可以写得很简单。

1. 进口方把钱垫到区块链上。
2. 出口方发货方发货。
3. 进口方验货后，钱就到了出口方。

当然，这其上有一些事也需要写在程序中。

1. 一个是进口方的钱垫到区块链上，就需要被冻结掉。
2. 另外还需要物流信息，不然，进口方说没有收到，不好验证。但物流信息要是造假怎么办？
3. 另一个是需要把进口方验货的标准给写进来。代码不知道条件怎么满足，也许需要进口方那边点个确认。如果不点确认，则有个过期时间，时间一到就自动确认。
4. 另外，如果进口方觉得有问题，需要退货，或是需要重新议价，那么需要相关的关联合同。

其中，比较难办的是第 2 步，需要其他方也进入区块链。如果不进来，这事就不好玩了。但是，物流信息怎么才能做到真实可靠的呢？这需要双方选择一个都相信的中心化的物流公司，还是我们搞一个去中心化的物流公司？去中心化的物流公司是个什么形态，你能想像得出来吗？我想象不出来。

## 合同的 Bug

另外，我们要小心智能合同。有程序的地方就会有 Bug，现实生活中会有 Bug，合同也会有 Bug。出现了 Bug 后，大家可以相互协商，给合同打补丁（附加条款，或是重新签合同）。然而，代码合同则不一样，Bug 也会被残酷无情地执行，一旦执行就很难补救了。

最著名的例子就是以太坊一个叫 The DAO 的应用，它是一个去中心化的风险投资基金，以智能合约的形式运行在以太坊区块链上。它也是一个盈利性的去中心化自治组织，它将利用自己掌控的以太币资金通过投资以太坊上的应用为其成员创造价值。在 The DAO 创建期，任何人都可以向它的众筹合约发送以太币，获得 DAO 代币。

因为 The DAO 这个程序写得不好，黑客在其智能合约里找到 Bug，把所有的钱给调走了，大约 7000 多万美刀。这成为有史以来最大宗的数字劫案，而且 FBI 也找不到人。这个项目因为钱被偷走而倒闭以后，引起了以太坊的强行分叉，变成 ETH 和 ETC。关于技术细节可参见其 [漏洞分析文章](http://www.8btc.com/thedao-expolit-analysis)，整个事件的始未可以参见《[彭博社深度还原：The DAO 大劫案始末](https://www.leiphone.com/news/201706/JnNEqj90inEWLTJD.html)》。

还有一个案例，是 2017 年发生的智能钱包（多签名钱包）Parity 被盗事件。它号称自己的智能合约被很多很厉害的安全人员都审查过，都认为没问题。但最后还是被黑客利用了一个叫做 initwallet 的函数，反复调用它，转走了 3000 万美金。

老实说，我觉得任何合同都是会有 Bug 的，无论是在现实生活中，还是在代码中。唯一的不同是，现实生活中的合同出现 Bug，可以自行协商解决，也可以通过法律或仲裁的方式解决。然而，在数字社会中，代码无论好坏都会被计算机残酷无情地严格执行。

有时候，当你是利益方时，你会觉得是好事。但有时候，你是受害方时，你还是会想有挽回的余地。现实生活中可以做到，但我不知道代码世界中的合同如何解决这些 Bug，所以还是不要叫 " 智能合约 "，至少现在还不是。

# 68 | 区块链技术 - 传统金融和虚拟货币

陈皓 2018-05-24



C:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\AF151DE.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\CD64399C.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\3A177E0A.tmpC:\Users\86185\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\AC\INetCache\Content.MSO\431732A8.tmp



00:00

20:34

讲述：柴巍 大小：9.42M

前面我们讲了银行的资金托管业务以及国际贸易业务。我讲这些东西，主要想讲什么呢？

## 金融的本质

我想讲金融的本质。我个人认为金融行业最大的本质就是——**促进交易完成，实现价值提升！** 也就是说，如果整个社会的交易能够更快更高效更安全地完成，那么我们这个社会就会有更好的运作效率，更低的成本，更多的价值。这对于促进整个社会的经济发展是相当关键的。

所以，为了保进交易完成，金融行业需要解决下面几个问题。

1. **交易中的信用问题**。所以，银行会来做中间人来担保。
2. **交易中的资金不足的问题**。通过借贷来让交易完成。
3. **交易中的大额的问题**。把一个大额的金融事件以股份的方式拆碎进行大众投资。

总之，金融行业就是要促进社会的交易，使得这个社会的交易越来越活跃，从而可以产生更多的价值。那么，这个社会的经济就会越来越健康。

下图给出了金融行业的四个重要属性。



* **效率提升**：加快货币、股票、债券的流通性，快速地促成交易。
* **价值提升**：通过金融产品的流通性，让实际价值得到充分地体现，并升值。
* **激励机制**：为实体经济添砖加瓦，并激励社会持续付出和成长。
* **信用评级**：建立信用社会、评估信用等级，从而改善社会。

是不是有银行做担保，有这些金融机构我们就可以高枕无忧了？不是的，我在前面说过，主要是钱不够多，只要钱多到一定数量的时候，什么事都可能发生。因为逐利是人性中非常疯狂的一个特征。只要有利益，人们就会想要更多的利益。这有时候并不是一件好事。

## 经济运作的原理

说到这里，我想先说一下经济是什么。对于经济来说，说白了就是整个社会的交易。每个交易中，对于买方，其需要付出的是货币和信用，对于卖方，其需要支付的是商品、服务或金融资产。而支出方是整个经济的驱动力。也就是说，一个社会的最基本的经济活动是交易，而经济状况好的好坏是受支出方影响的。

所以，一个市场的好坏，和支出方有很大关系。在整个社会运作的过程中，需要有一个“贷款机构”。这些机构把钱贷给想要花钱且有偿还能力的人，然后这会增加整个社会的支出。于是，你的支出成为了别人的收入，别人的收入多了，也会增加他的支出，而如果支出越来越多，某些人的收入就越来越多。

于是这些人的钱花不完，他们就会开始想用钱来生钱。于是就有更多的人借钱给别人。也就是我们所说的投资，而这又增加了更多的支出 。于是，整人个社会就运作起来了。所以说，支出是经济的原动力。

我们知道，经济的价值是可能通过提高“生产率”来提高的。然而，生产率并不是很容易能提高的，这是一个长期的过程。而通过“借贷”我们可以短期的提高经济价值，在借贷发生时，消费超过产出，在还贷时，消费低于产出。

所以，整个人类世界的影响经济波动的东西就是“借贷”，也就是为了购买现在买不起的东西，向未来的自己去借钱，或是由未来的自己去还债。这种未来消费的方式并不一定是坏事。如果能还了，就是良性，如果还不了了，那就成了恶性的。

另外，还有一个问题，**如果整个社会的支出变多，于是就会出现一片繁荣的情况。大多数人都是目光短浅的，所以，大多数人都觉得经济形势很好，于是就出现更多的借贷。人们觉得挣钱好容易，于是就借钱来买其他金融产品，导致金融产品上涨，于是导致大家觉得应该花更多的钱来投资，那样就会借更多的钱……这样一来，就会出现巨大的泡沫……**

关于这个，你可以看一下网易公开课的《[经济机器是怎样运行的](https://open.163.com/movie/2016/6/I/Q/MBPO9ED98_MBPO9S8IQ.html)》。

## 2008 年的次贷危机

2008 年暴发的全球金融次贷危机算是一个银行玩出来的事儿。自 2003 年来，美国人的房价就在不停地上涨，而买房贷款的那些人基本上来说都有比较稳定的工作来每个月偿还房贷。于是，这些人的信用记录，导致房贷成为了比较好的金融产品。

美国房地产贷款系统里面分为三类：优质贷款市场、次优级贷款市场、次级贷款市场。美国把消费者的信用等级分为优级、次优级和次级。

那些能够按时付款的消费者的信用级别被定为优级，那些不能按时付款的消费者的信用级别被定为次级。次级贷款市场就是面向那些收入信誉程度不高的客户，其贷款利率通常比一般抵押贷款高出 2%～3%。尽管美国次级贷款市场所占美国整体房贷市场比重并不大，大约占 7%～8%，但其利润最高，风险最大。

想一想，如果供房人能还款，那是优质贷款，如果不能还了，把房子收回来，也可以卖个高价。毕竟房价一直在涨呢。

贪婪的资本家们觉得，既然房贷的回报如此优秀，为什么不把这些当成债权出售。嗯，债权转让虽然可以让资金快速回来，但是挣得不够多。于是，贪婪的银行家们决定，把这些房贷打包，形成一个优质的金融产品，然后，在二级市场上发行 IPO，让更多的人来投资和炒作，这样就可以挣到一大笔钱。

的确，只要供房人按时供房，这个金融产品就没有问题，所以，房贷打包的二级市场也非常不错。于是，再继续衍生更多的金融产品，各种“杠杆”，然后再加上保险公司为其保险。全世界都疯了。

银行开始乱放贷款，把贷款放给好多根本没有能力还款的人，且相信房价将继续升值的前提下，鼓励了许多次级贷款借款人去取得浮动利率抵押贷款。这些抵押贷款以在预先确定的期限间低于市场利率引诱借款人，期限过后剩下的则是以市场利率计算。

而美国最权威的评级机构也还错误地把风险比较高的金融产品评成最优质的级别。这样在二级甚至三级市场上套更多的人进入。

最终，最底层的越来越多的人不还贷款了，越来越多的房子被拍卖。一方面导致房价下跌，另一方面，导致银行坏账，最终，像多米诺骨牌一样倒了一片……

然而，因为这事玩得太大了，于是美国政府拿出了 7000 亿美金来救那些贪婪的银行，而一些投资机构就此破产，还对国内的经济造成了巨大的打击……

## 金融的监管

上面，我们可以看到金融行业非常积极的本质和作用，也能看到其带来的副作用。金融行业发展成百上千年了，今天，我们还是可以看到其存在很多问题。就像上面说的 2008 年金融危机一样，银行业过于快速地促成交易，加快货币、股票、债券的流通性，导致了各种“杠杆”以及“多杠杆”的出现。

当整个社会为之疯狂的时候，信用评级、风险控制都被抛到脑后了，最终出现投资大大超过和实际价值完全不等价的局面。实际价值无法支撑投资时，风险发生时，整个世界就会出现连锁反应，一发不可收拾。

对于经济活动，这两个事需要平衡，一个是“资”，一个是“债”。如果不平衡了，风险就出现了。无论是对于我们个人，还是对于企业，或是银行，都是一样的。但总是会有人冲昏头脑的，尤其是有财务窟窿或者巨大利诱的时候，所以，才会有监管机构来审查这些金融机构的资和债的风险，并制定相关的政策和条例。

而有时候，监管机构又管得过死，导致经济不能充分发展。于是造成了我们经常听到的“不管就乱，一管就死”的局面。所以，很多时候，政府或央行会通过调节货币利率，以及发行更多货币等手段来引导或调整市场，控制风险 。

于是，出现了各种经济学，比如，主张政府强干预的凯恩斯经济学，以及马克思主义的政治经济学均表示出了对市场经济没有信心，需要用政治干预手段。还有亚当·斯密的以市场为主导的经济学等。

可能这个问题怎么讨论也讨论不清楚。我个人比较认可的是，经济还是需要自由的，而政府应该控制的是风险和保证经济实体的产权。只有自由的市场经济才会回归金融的本质，促进交易提升，激励大众而提升价值。而政府的风控措施可以对整体金融风险进行调节，这是市场经济不能完成的。政府还要保护私人产权，这对于经济活动是非常重要的，产权保护是经济活动的根本基础。

## 虚拟货币

首先，如果虚拟货币想要有货币的特征，那么就需要何持其稳定。这个稳定不仅仅只是不增发（在你看过上述的经济活动的原理，你知道增发货币并不一定是个坏事），其价值最好是稳定的，因为它要代表某种经济体的稳定性。这就好像美金、欧元、英镑，要比非洲某些国家的货币更硬一些。然而，目前的虚拟货币没有一个经济体为其背书，所以远远达不到货币的功能。

于是，虚拟货币开始变成股票一样的，股票是需要后面实体的公司经营情况来背书的，所以流通性比较好的股票，一般来说需要透明公开公司的经营情况，并会受到行情和政策的影响。然而虚拟货币的交易所市场完全在售卖概念，到目前为止还没有一个真正成功的，能够有颠覆性的项目。然而，其靠发布白皮书就可以变成一个几十亿规模的公司。

当然，现在区块链里的经济，是靠二级市场撑着。所以，就像前面说的那个经济规律一样，只要有不停的支出，就会造就一种繁荣的景象。这种繁荣的景象，对于绝大多数不明真相的人来说是很容易让他们心动的，因为人性是想不劳而获且趋利避害的。于是就会引发更多的人进入，于是形成更大的繁荣。

但是，这种后台没有价值体现的玩法，总有一天会达到瓶颈的——就是支出不再能够维持下去的时候。也就是没有新人入场的时候，老人因为钱投进去了，也不会再有更多的钱投入的时候。那个时候就是泡沫破灭的时候。

我在这里讲了这些东西，我想说，就算是虚拟货币，数字货币，其本质也是一样的。如果不能提高效率，降低成本，没有风控和评级，这样完全自由地发展，我认为风险是非常大的。说白了，这就是一个高级赌场罢了，人类历史上已经有过无数这样的案例了……

## 虚拟货币其他的一些问题

### 比特币的几个问题

我们先来看几个比特币的问题，了解了这些问题后，我们才能独立思考后面的几个逻辑问题。

1. **交易成本上升**。由于工作量证明需要消耗大量的算力，同时比特币大约 10 分钟才会产生一个区块，区块的大小只有 1MB，仅仅能够包含三四千笔交易，平均下来每秒只能够处理 5~7（个位数）笔交易，所以比特币网络的拥堵状况非常严重。有时候，一笔交易确认的小费已经很高了（并不见得比银行便宜），另一方面，确认时间很长，在拥塞的时候需要好几天。
2. **个人无法参与**。一条链已经非常长了，所以个人电脑已经跑不动了。也就是说，如果你想玩比特币，你电脑的算力都很难校验账本了。另外，记账的人也越来越趋于巨大的大公司。本来是一个全民参与的去中心化的事儿，而现在成了大众无法参与的事了。那么，这还是去中心化吗？
3. **社区的利益纷争**。上述两个比特币的技术问题必需急待解决，比特币才能玩下去，不然，也就是这一两年比特币也就快玩完了。所以，社区内也很迫切地想解决这两个技术问题。然而，自从中本聪把所有的工作交给比特币的核心团队（core team）并消失之后，比特币社区中就这些技术问题如何解决，核心团队和矿工的谈判就没有谈好过。你可以看到，其中的利益纷争和中心化的组织结构没什么两样。（具体你可以参看这篇文章《[金融史上的神奇怪胎：比特币扩容大战的前世今生](https://mp.weixin.qq.com/s/WfOL1IfEFfa-7zBwNuy76Q) 》。）

作为标杆数字货币，比特币姑且这样，何况其他数据货币呢？但是你要解决这个问题，就会像前面那样所说的那样，你就需要适当去中心化了。

### 几个功能的问题

我认为，下面这几个问题如果不解决好，同样虚拟货币也是有很大风险的。

* **交易时的身份验证**。银行对于网上交易的验权是相当复杂的，不同的金额会有不同的验证。而虚拟代币只关心私钥，而不关心是不是这个人。
* **资金归属权保护**。对于银行，如果我的卡丢了，密码丢了，U 盾丢了，我可以申请冻结账户，并能通过到银行柜面把我的财产声明回来。虚拟代币如果你的密码和私钥丢了，那就真的丢了。
* **损失赔偿问题**。我有个表妹在英国生活，有次在 ATM 机上取款时，突然接了一个公司打来的电话，说有急事需要处理，于是，忘了取卡就走了。被后面的人取了 2000 英镑。后面发现了，报了警，银行方面向警方确认后把失窃的钱全部赔给了我的表妹。

也许，第一个问题还好解决，第二个问题，我觉得在匹块链上是没有解的，而想解决第三个问题，我认为需要一整套的社会运行机制，区块链这个技术更显得无能为力。

### 几个逻辑问题

最后，我们再来思考几个逻辑问题。

* **技术驾驭能力问题**。这种去中心化的技术难题并不是什么人都能 Hold，一方面是结点是不可信任的假设，另一方面，其中有太多的政治上的博弈问题不是技术能解的。所以，那些说用区块链来解决各种业务问题并颠覆现有大公司的人或公司，我觉得他们无论是在业务上还是技术上的水份都很大，更别说颠覆了。思考问题：这是不是一个概念炒作远远大于实际能力的乌托邦？
* **比特币颠覆了什么？** 有人说：“比特币本来应该要证明一个真正的自由市场力量，结果却充满了诈骗者、投机者和小偷，而且对真实世界的交易没有帮助，还消耗了这么多的社会资源”。本来，中本聪想通过比特币来建立一个可以避开政府、银行家和企业的支付系统，从而避免通货膨胀或金融腐败。但相反的是，比特币现在是一堆快速膨胀的投机泡沫，其创造了另一个和传流世界一样的金融体系。思考问题：数字货币是在颠覆现有的传统金融体系，还是建立另外一个一模一样，但充满更多泡沫和投机的体系？
* **是否消除了中间商？** 如今比特币已有各种不同类型的中间商，像是能帮用户把零碎比特币存储成账户的钱包服务等。这些中间商的存在却也破坏了比特币的隐私特性，像 Coinbase 这种中间商就会搜集跟用户有关的大量信息。这并不能怪罪中间商的贪婪，而是因为比特币本身的设计让交易变得非常复杂。对非技术背景的使用者来说，如果没有中间商或应用程序简化，使用比特币还是不太便利。思考问题：比特币的原意是建立一种无需银行和中间商，不会有交易费用的交易系统，但现在比特币的进展却反过来复制了原本想破坏的体系。
* **大公司参与的区块链？** 看到像投资银行高盛或是中介机构蚂蚁金融这样的公司参与到区块链这个事来？你有没有觉得，有点奇怪？我还看到有些人评论到：“区块链就是需要大公司来参与”。看到这，我不知道中本聪会怎么想？反正我感觉有很强烈的喜感。思考问题：区块链本质上是要颠覆这些银行和中间商的，代表了先进的生产关系，而这些传统的落后的生产力来玩这个事，是不是有点像，我造了一列火车，而要用这些马车来拉……
* **投资人投资去中心化的公司？** 我有点不明白，为什么投资人或是投资公司会关注这个事？如果投资人看到了去中心化这个事可以颠覆现有的大公司，所以看好这个事。于是把钱投给了去颠覆中心化的大公司的这些公司，而这些公司又会成为中心化的大公司。这看起来好奇怪啊。因为真正的去中心化是完全找不到主体的。思考问题：**去中心化需要有公司吗？有公司的话，还能叫是去中心化吗？投资人并不傻，那么，他们想来这里面干点什么呢？是投机吗？**
* 有挣大钱的机会，你会共享出来？传销组织的三个阶段：第一，让你觉得你很穷困，告诉你致富的捷径。第二，模糊掉具体细节，用各种高大上的类比和比喻来取得你的信任。第三，通过发展下线来制造虚假繁荣，让你信以为真。所以，虚拟货币中绝大多数都是这样的特征。他们和骗子们所有的技巧如出一辙——“我有一个挣大钱的机会，但是我想和你共享出来，只需要你对我投资一点钱，未来你可以得到百倍的分红”。我靠，可能挣大钱的事，你愿意分享给这么多人？思考问题：在区块链中你有没有发现这样的身影？为什么他们要把这样超级革命性的可以挣大钱的项目在这么早的时候就分享给这么多人？

## 最后一个哲学问题

当一个社会出现问题的时候，在民众开始抱怨和发泄不满的时候，需要一个目标。这是一件很自然的事。于是有人就满足大众，告诉大家，你们今天之所以穷，之所以苦，之所以不公，是因为那些中间商玩弄了你们，是因为政府不可信，是因为有坏人……因为这是最好被民众所理解的，因为有明确的目标，简单粗暴。这也是人们容易被煽动的原因。

然而，整个社会的运作其实是一种协同，由多方带着不同的利益或诉求而形成的。也就是说，问题的出现是多方造成的，或是社会协同出了问题造成的，是机制造成的。并不是其中的某个实体造成的。

而且，无论你制定出什么样的机制或是规则，都会有好的一面和不好的一面，这一面有多好另一面就有多不好。所以，如果一件事完全只有好的，而没有不好的，那么，你有绝大可能是在被人在忽悠中。

去中心化就是好吗？我们不需要权威机构了吗？技术可以解决信任问题吗？

我是要继续改善我们现在这个社会，还是直接毁了再建一个？是“破坏性的建设（Disruptive Construction）”，还是“建设性的破坏（Constructive Disruption）”？

我不知道你喜欢哪个，而我喜欢后者。