BLOCKCHAIN

BLOCKCHAIN TECHNOLOGIES

区块链技术

比特币　以太坊　超级账本

LIBRA

毛德操　◎著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

BLOCKCHAIN

BLOCKCHAIN TECHNOLOGIES

区块链技术

比特币　以太坊　超级账本

毛德操　◎著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

图书在版编目(CIP)数据

区块链技术 / 毛德操著. —杭州：浙江大学出版社，2019.8

ISBN 978-7-308-19283-5

I. ①区… II. ①毛… III. ①电子商务－支付方式 IV. ①F713.361.3

中国版本图书馆 CIP 数据核字(2019)第 131148 号

区块链技术

毛德操 著

策划编辑	吴昌雷
责任编辑	吴昌雷
责任校对	王 波
封面设计	北京春天
出版发行	浙江大学出版社
	(杭州天目山路 148 号 邮政编码 310007)
	(网址：http://www.zjupress.com)
排 版	杭州林智广告有限公司
印 刷	杭州高腾印务有限公司
开 本	787 mm×1092 mm 1/16
印 张	41
字 数	1028 千
版 印 次	2019 年 8 月第 1 版 2019 年 8 月第 1 次印刷
书 号	ISBN 978-7-308-19283-5
定 价	128.00 元

序

在当代，作为现代创新机制重要驱动力，深度信息技术（云、物、社、移、大、智、区……）风行世界，而开源技术是深度信息技术的框架或底层配置。

毛德操老师知识渊博、多才多艺，特别对开源的源代码有透彻分析和深刻理解，他亲力亲为，动手编撰本书，做出重大贡献。毛老师基于开源创作的区块链大作，值得称赞，十分难得！本书不但对区块链技术的开发应用有重大价值，作为开源技术应用的范例，对开源技术的开发应用也意义重大。

中国开源软件推进联盟名誉主席
Linux 基金会推进开源终身成就奖获得者
CNCF 基金会开源领袖国际大奖获得者

陆首辉

2019 年 6 月 10 日

前　言

历时两年半，本书终于脱稿付印。我对区块链技术的研究始于三年以前甚至更早，其间经历了比特币和其它各种代币过山车似的起伏，不过我的注意力一直集中在区块链这个技术，并且深信：泡沫和投机终将过去，但是区块链这个技术必将会沉淀下来并大有作为。

我开始研究区块链技术的时候，比特币的源码已经相对成熟，但别的几种区块链的源码还只是早期版本，后来都有了较大的发展和变化。尤其是“超级账本”即 Hyper Ledger 的源码，更是有了堪称脱胎换骨式的变化，往往是前面的版本还没有充分消化就又出来了后面的版本。一方面这固然给我的研究和写作带来了困难和更大的工作量，另一方面却也迫使我在横向的对比之余还进行纵向的比较而得以加深理解。

尤其值得一提的是，连连支付还为区块链技术的研究和开发组成了一个团队，结合金融业的实际应用进行基于以太坊的联盟链开发，使作为技术指导的我因此而获得了许多直接的体验，这些体验对于本书的写作大有裨益。在那个项目中，我们选用了以太坊的 Java 版源码 EthereumJ；后来的实践证明，Java 版本的选用对于人才的培养很有好处，可以使研发人员很快就切入区块链技术本身，而不是把许多时间花费在 Go 语言上。反过来，一旦对所实现的种种算法有了较为深入和具体的了解，再去读 Go 版本就可事半功倍。所以本书第三章同样也采用了 EthereumJ 的代码。至于第四章对于超级账本则仍采用 Go 版本。这样，比特币的源码是 C++的，以太坊的源码是 Java 的，超级账本的源码是 Go 的，不同语言背景的读者都可从自己比较熟悉的语言开始切入阅读源码，然后举一反三推广到别的语言。

本书的写作仍旧秉承我情景分析的方法和叙述风格，并沿用我在《大数据处理系统：Hadoop 源代码情景分析》一书开始的代码摘要方法。这也是我自己在研究中采用的方法，希望对读者有所帮助和启迪。

书稿虽已准备付印，但我对于本书中可能存在的错误和缺陷却大有诚惶诚恐之感。当然，只要是已经发觉的错误我都已改了过来，但是自知错误之处仍是不可避免，并且可能

也不是一处两处的事，潜在的错误和缺陷可以来自几个方面：

一、文字输入和排印所造成的低级错误，这是最轻的，但是当然也会给读者带来困扰。

二、叙述和修辞方面的缺陷和错误，我尽力把事情说得清楚一些，但是否真的达到了目的，是否真的说清楚了，却很难说。

三、我对源码中某些模块或某些方面的疏漏。我在写作中对于如此庞杂的内容当然要有所取舍，但是我的取舍却未必就是合适的。

四、我对源码和所涉技术的理解错误，这当然是最严重的。

但是，与其无休止地反复推敲，还不如就此付印，起个抛砖引玉的作用。这也使我对常见于国外许多出版物扉页上的那段话有了深刻的认识，那段话的大意是：

出版社和作者均力求本书内容准确无误，但声明对因本书内容所含错误和疏漏给读者带来的种种损失免责，读者须自担风险。

读者对本书内容提出种种商榷和意见，我当然是十分欢迎的；但是因时间和精力所限，我也未必就能够一一作答。不过能就此引起讨论，“抛砖引玉”，也正是我的本意。

就在本书行将付印之际，Facebook 发布了《加密货币 Libra 白皮书》，计划在全球范围内发行数字货币 Libra，并公开了 Libra 区块链的程序源码。鉴于 Libra 潜在的重要性，我又赶写了一个简介，作为附录加在本书的后面。至于更深入的分析，特别是源代码层次的分析，则需要有另一本专著。只要各方面的条件允许，我也有意对 Libra 进行深入研究并撰写这样一本 Libra 专著。

感谢浙江大学出版社领导对本书的重视，更感谢本书责任编辑吴昌雷先生和各位工作人员的辛勤劳动，没有他们的付出，本书的质量是达不到现在这个水平的。

最后，感谢浙大网新和连连支付两个公司对我的支持，没有两个公司为我提供的种种条件，我对区块链技术的研究和本书的写作都不会这样顺利。另外还要感谢我的老友胡希明教授给我的激励；对我来说，和胡老师的闲聊既是休息也是“充电”。

毛德操

2019 年 7 月

目 录

第1章 绪 论

“区块链”这个词的英语原文是“Block Chain”，如果直译就应是“块链”，但是大家都已叫惯了区块链，再说叫着也顺口，在本书中这两个词等价，“区块”与“块”也等价。

本书介绍三种主流的、有代表性和基础性的区块链，即比特币（Bitcoin）、以太坊（Ethereum）、超级账本（Hyper Ledger）。这三种区块链各有特色，也说不上谁比谁好。有人说比特币是第一代区块链，以太坊是第二代，那么超级账本似乎就是第三代。如果是从出现的时间先后上说，这也许有点道理，因为比特币确实出现最早，属于开山之作。但是如果是从技术上、功能上说，这就值得商榷了。事实上，这三种区块链各有千秋、各有利弊，就看用于什么样的环境和目的，所以只能说是三种不同风格、不同特点的区块链，很难笼统地说哪一种更好。这里面并没有“升级换代”所意味的那种截然的好坏强弱之分。

区块链技术的源头在于发明和实施“比特币”的努力。有关比特币的早期故事和近期忽悠，想必本书的读者早已耳熟能详，许多读者的所闻所知比我还多，无需我再来饶舌。而本书的主旨虽然是区块链技术，但技术也并非存在于真空之中；这方面区块链技术还特别典型，可以说很少有像区块链这样的技术，与心理学、经济学、社会学、政治学等学科有那么密切的关系。也许可以说，在人们所见到的各种技术中，区块链是与各国的文化和制度最有密切关系的一项技术。所以，我在本章中着重于结合技术及其存在环境讲述一些本人的理解和带着一些个人见解的话题。

1.1 比特币和区块链技术的发明

比特币（Bitcoin）的起源，毋庸讳言，就是无政府主义。所谓“去中心化（de-centralize）”的“中心”是什么？当然可以说是大公司，可以说是银行，特别是中央银行，但是归根结底还是政府。即使在美国这样的国家，最大的中心无疑还是政府。对于政府的作用，现代左右两派政治学家和经济学家们的争论只是“大政府”和“小政府”之分，但对于政府存在的必要性并无太大异议。而无政府主义者们，则认为政府压根就不应该存在。早期的无政府主义

者还曾经是社会主义者的同路人，后来才分道扬镳并日渐式微。无政府主义在当时还是有相当影响的，中国作家巴金这个笔名就来自巴枯宁和克鲁泡特金这两位早期无政府主义理论家的姓名。然而即便是无政府主义的理论家们也提不出什么可行的措施，所以无政府主义只能是空想而社会主义是科学。当年鲁迅曾嘲笑中国的无政府主义者，说“安那其主义将于四百九十八年后实行”，意思是无政府主义永远都不可能实行。“安那其”是英文无政府主义（Anarchism）的译音。

然而，尽管式微，无政府主义的思想还是有着一定的影响，特别在西方的年轻人中还是相当有市场的。当初聚集在比特币的鼻祖中本聪周围的那一群人，之所以要设法搞出比特币这么个东西，发明出区块链这门技术，其实就是因为他们不承认任何权威，想要绕开任何中心的监管。有了这两条，从这两条出发，后面的那些技术和举措，也包括某些困境，就都是“其来有自”，可以得到完美的解释和理解了。当然，从一种动机出发而发展起来的技术，完全可以被用于不同的目的。诚如 Frederick Brooks 教授所说，Unix 是在失败的废墟上开出的绚丽花朵；那么在无政府主义的土壤上同样也有可能长出丰硕的成果。事实上，许多国家的当局对比特币的态度多少都有点保留，但对于区块链技术却都持鼓励的态度。

回到当年的中本聪们，作为实际上的无政府主义者，或者至少是深受无政府主义思潮影响的人，他们不承认更不信任人世间的任何权威和中心，他们把权利平等的要求推向了极端。既然如此，“去中心”和不受监管就成了他们的自然要求。而自创一种货币，在经济活动中绕开银行，又避开政府的监管，就既是他们孜孜以求的目标，也成了他们的兴趣爱好和热情所在。而互联网技术的发展，又使他们得以群聚在网络论坛上展开各种探讨。当然，也不排除里面有“别有用心”的人，但是应该承认其中大部分人之所以想要摆脱监管倒并非因为想要贩毒走私。中本聪们努力的结果，就是他们自创的货币，即“比特币”，以及相关的一系列技术，统称为（早期的）区块链技术。

要做一个什么事情，总得要满足两个条件：一是“可欲（Desirable）”，就是让人觉得这是个好东西，是值得为此花点代价的；二是“可行（Practicable）”，就是在技术上可以实现，没有什么大的漏洞，不是空想。一般而言，可行性是技术问题，比较客观；而可欲性就比较主观了，不同的人对同一个事情会有不同的主观感受和判断，这个人愿意拿很大代价去换取的东西对那个人可能一文不值。对于中本聪们那样的无政府主义者，或者说极端的自由派人士，自己发行货币的“可欲”是不成问题的。其实，即使对于一般的民众，这里面也有可欲的因素，比方说隐私，比方说如果能更方便，如果能更可靠，那也是好事情。

但是在“可行”方面却有不少障碍，有许多问题需要解决。

我们不妨推理一下他们面临的问题和他们解决这些问题的思路。

要自创一种货币，真要铸币或印刷纸币显然是不现实的，所以这只能是通过网络流通的“数字货币”，或者说“虚拟货币”。但是网络上的流量是可以被拦截监视的，所以只能采用匿名的方式（其实是化名，但是人们已经习惯于说是匿名），从而自然就会使人想到这里面一定会用上加密技术。此外这里还有两个关键性的问题，即如何防止欺诈和重复花费（Double

Spending）的问题。不解决这些问题，自创货币就只是空想。

21 世纪初就已经有了“电子支付”、“数字货币”的概念和实践，但那只限于电子商务、网上银行一类的应用，具体的支付清算仍得要通过银行才能进行，所有的资金往来对于银行都是透明的。那时候也已有了“积分”、“返点”，乃至“游戏币”的使用；但除了那是在“线上”的电子化数字化应用外，与我们在食堂里使用代价券其实并无多大区别。

那些应用，一般而言都只能在特定的条件下使用：如果是在线下，那么一般是面对面使用，并且有某种形式的实体票据，例如食堂里的菜票就是这样。这里的面对面使用解决了真伪的问题；而实体票据的换手则解决了防止重复使用的问题，保证了不能将同一票据花了又花，即“双花”。但如果是在线上就不一样了，由于在线上不能传递实物，真伪和“双花”就成了突出的问题。首先是真伪的验证问题，你所声称的那一部分交换价值，或者虚拟票据，是谁发放的，凭什么发放，又为什么是你的呢？进一步，你究竟是否就是你所声称的你呢？即便这些都对，由于在线上无法传递实物，线上的花费并不引起你手中实体票据的减少，又怎么能保证你不会“双花”呢？还有，支付双方的隐私问题怎么解决？

要解决这些问题，最简单的办法就是由某个机构，特别是银行，替你维护一个“账户”。你每通过这个机构支付一笔钱，它就在你的账户中扣除了这笔钱，下次你还要重复花这笔钱就会被拒绝，这就能很好地解决“双花”的问题。而欺诈的问题，特别是身份证明的问题，如果是到银行柜台上办理，他们可以要求你出示身份证明；而如果是在线上办理（所谓“网银”），则一般都是通过设置登录口令解决的，或者也可以使用密码，可是这意味着所有人都得把密钥交给银行。至于隐私的问题，你从自己的账户中支付一笔钱给另一个账户，这一点对于银行是透明的，并无隐私可言，但是银行有银行的纪律和职业行为规范，一般而言不会有意透露给别人。

显然，这都是银行沿用已久的方法，事实上通过银行进行的“转账”早就不使用实体货币，而只是“额度”的转移。国家发行的货币也有 M1 和 M2 之分，实体的货币即 M1 只是广义货币中的一部分。从这个意义上说，“数字货币”其实早就在使用了。但是，那意味着你的账户，从而你的货币资产，还有你的经济活动，实际上掌握在银行的手里，处于银行的监管之下。显然，这就是个有中心的或者说中心化的模式和秩序。银行就是经济活动的中心。这里说的是银行，但实际上可以是任何金融机构。问题是，你确实信任这些金融机构，这些中心吗？这种信任的根源是什么？

这里主要涉及三个问题：一是其权威性，二是其意向和价值观，三是其技术能力。首先，就银行等金融机构而言，权威性意味着它的可靠性，这种权威性主要来自其实力和后盾。例如美国的银行都是私有的，所以都得由 FDIC（联邦存款保险公司）提供保险，然而 FDIC 只给每个账户提供不超过 10 万美元的保额。中国的银行大多都是国有，由政府提供担保，但即便如此也还是依赖于整个经济环境。至于别的金融机构，其权威性就更是个问题了。其次，金融机构的意向和价值观也是个问题，它们说得当然都很好，但是实际上就难说了，近来有不少 P2P 借贷公司倒闭或潜逃，回过头去看它们的历史，可知有些其实从一开始就是以圈钱为目的。再说，即便这些都没有问题，也还有技术能力的问题，它们的技术能力够不够，能否使你信任？当然，在实际生活中还有政策风险等问题。

然后是用户是否情愿向这些机构袒露隐私的问题，是本来就觉得没什么，还是因为无奈

而只好袒露。那些不情愿袒露的，里面显然有些人是出于不正当的意图，但多数还是属于正当的考虑。固然毒贩也需要支付，他们当然不能袒露支付的目的，然而这并不意味着不情愿袒露隐私就不正当了。

正因为是在中心化的模式和秩序中，你的资金往来实际上就受到监管，银行甚至可以冻结你的账户，也可以限制你的资金往来，你的经济活动还可能受制于他们的效率。在那个中心化的模式和秩序中，你信任也好，不信任也好，反正只能通过这些中心化的机构才能完成支付清算，除非每次都是现金交易。也许你想设法绕过，例如找地下钱庄，其实也只是以一个中心取代另一个中心，这并不改变“中心化”这个模式。同样，你情愿也好，不情愿也罢，那些隐私总归要袒露，你的资金往来乃至经济活动总归要受到监管。对于大多数人而言，这是别无选择，也早已习惯了的事，而且也承认金融机构的权威性，所以也不觉得有多大不妥。

如果说对于一般民众这还可以接受，特别是在别无选择的条件下也只好接受，那么对于中本聪们就是不可接受的了。他们不承认任何权威，崇尚完全彻底的权利平等，追求完全不受政府监管的行动自由。其实这也并非从中本聪这些人才开始，这样的要求早就有了，但是这样的主张和愿望一直都不具备现实的、技术上的可行性。然而互联网技术和密码技术的出现和发展给他们带来了新的鼓励和希望。

人们常说，互联网带来了“扁平化”，使原来金字塔式的层次结构变得相对扁平了，这离无政府主义者们主张的彻底的“平面化”似乎靠近了一些。而密码技术的发展，又为隐私的保护和身份的认证提供了条件。所以，在 21 世纪初，一群人就通过互联网进行热烈的讨论和设计，想要摆脱国家的法币另搞一种数字货币，让人可以不受监管，高度保护隐私，实现“去中心化”的支付。其中的主心骨就是那个号称“中本聪”的人，尽管人们其实并不知道这究竟是一个人还是一个团队。他们要解决的，就是前面所讲的三个具体的问题，即匿名和隐私、防欺诈、防“双花”。

当然，匿名就是为了隐私，但是隐私并不必然意味着逃避监管；有些事情，我可以让“组织上”知道，但是却不愿意让同伴知道，更不愿意让竞争对手知道。其实匿名是早就在用的，互联网上恐怕没有多少是真名。但是那样的化名有两个问题：一是得向某个权威机构登记，说这就是我的化名，这一点当然是中本聪们不能接受的。二是一般的化名碰撞率很高，常有同名出现，尽管规定得有多少个字符，里面要有大写小写，还是免不了会有同名。针对这个问题，中本聪们规定一个化名（他们称为“地址”）必须是 20 字节即 160 位（二进制）长的随机数。160 位的二进制数有多大呢？我们知道 32 位二进制数的表达范围大约是 40 亿，160 位是 5 个 32 位，那就是把 5 个 40 亿连乘在一起，40 亿的 5 次方。取值范围这么大的随机数，碰撞的概率就确实可以忽略不计了。

如果只是停留在这里，那还算不得有多高明，高明之处在于他们还结合用上了非对称加密技术。他们进一步规定：用户自己生成一对非对称密钥，把其中的公钥经 Hash 计算后产生上述的 160 位“地址”，私钥则留在自己手里，以后要发出交易请求/交易说明时就用私钥“签名”，然后把这签名随同原文一起发送。所谓用私钥签名，实际上也是 Hash 计算，只是把你的私钥也一起计算进去，所产生的 Hash 值就是对原文的“签名”。非对称加密技术有个非常好、非常重要的性质，就是根据原文和使用其中一个密钥的签名可以计算出这个密钥的对偶密钥。如果是用私钥签的名，就可以计算出它的公钥，反之亦然。算出了与此私钥配对

的公钥，再用规定的 Hash 算法就可以推算出应有的地址，与你所声称的地址比对。这样，就既解决了匿名的问题，同时也解决了防伪的问题，因为只有你有这个私钥。

说到这里，也许需要对“哈希（Hash）”作点说明。“哈希”这个词是对 Hash 的音译，本书直接采用原文 Hash。所谓 Hash，就是对一块数据进行某种计算，最后得出一个数值，有了这个数值，如果那块原始数据发生了什么变化，再进行一次同样的计算就可察觉。我们小时候练珠算，知道从 1 连加到 100 应该是 5050，这个 5050 就是个（很糟糕的）Hash 值，你把这 100 个数值中改掉任何一个，加起来就不是 5050 了。然而简单相加并不是个好的 Hash 算法，因为你可以交换这些数值的位置，次序变了，但连加起来仍是 5050。所以用加法作为 Hash 的算法可以察觉数据中数值的变化却不能察觉次序的变化。而好的 Hash 算法，就是要保证哪怕你数据再多也能察觉任何一丁点的变化，这是一门专门的学问，要用到高深的数学。

读者也许会问：要是黑客设法伪造一个签名，使计算出来的公钥正好和你的公钥相同，那怎么办？事实是：黑客想要伪造出那样一个签名，是没有办法从你的地址反推的，得要一次一次地反复试算，哪怕用目前世上最强的计算机也平均得算上很多年才行。这就是所谓正向很容易而逆向很难的计算。我有个朋友形容说正向计算势如破竹但逆向计算犹如大海捞针。

事实上，加密技术在中本聪他们那个“比特币”中的应用，就是用来签名，而并未用于加密。所以支付的内容（金额）和对于内容的签名都是公开的，但是你看不出究竟是谁支付给谁，你看到的只是双方的“地址”。而支付内容和签名公开，就谁都可以进行验算，以检验信息的真伪。比特币这东西出来之后，人们常常称之为“加密货币”。其实这个名称有点误导，比特币中没有什么加密的内容，加密技术只是用来签名，应该说是“采用加密技术的货币”。

这样，匿名和防伪的问题就解决了。那怎么防“双花”呢？一般而言只有两种方法：一种就是像银行一样，为每人都建立一个账户，维持一个余额，你每花费一笔钱就在你的账户余额中减去，使你不能超支。另一种就是一笔归一笔，这笔钱是谁给我的，下次要用的时候就拿这笔钱来付账，不够就再添上另外一笔，凑够为止，要是有剩余就找回我一笔钱，放着以后再花。前者相当于转账支付，后者类似于现金支付。比特币所采用的是后者。这就是所谓 UTXO 的方法。UTXO（Unspent Transaction Output）的字面意义是“尚未花费的交易输出”。为什么是“交易输出”呢？很简单，没有人输出，你的钱哪来？用户的资金都来源于某次或某几次交易中的输出，特别是别人的支出，这都有明确的付方和收方，除非是路上捡的。后面会讲到“挖矿”所得，这倒在一定程度上有点像路上捡的，挖矿所得称为“Coinbase（币基，基础币，原发币）”，那是来自比特币的发币机制。总之你的钱只能来自某次或某几次交易的支出，可以是别人的支出，也可以是你自己的支出（自己付给自己，找还给自己）。UTXO 的概念和方法有个鲜明的特点，就是不像银行账户那样汇总成一个账面余额，每个 UTXO 都好像是一个专门制作的“硬币”，只是币值不同，你的财富就是一口袋这样的“硬币”，到使用（花费）的时候再来拼凑和找零，找零就是付给你自己。当然，这里所说的“硬币”其实只是“数字货币”，就是一笔记载。所以 UTXO 其实就是虚拟现金。与我们一般印象中的硬币相比，区别之处在于：一般的硬币都是标准面值的，都是预制的，而 UTXO 则好像是实时打造的非标准面值的硬币。中国古代因没有标准面值的银元，而使用不同大小的银块，与此就有点相似。其实 UTXO 这个概念一点也不新鲜，农村中有些老太太就是这样，她们把收到的每一笔钱都用红纸单独包起，这一包是女儿给的，那一包是卖了鸡蛋的收入，这

样就没有管理账目和计算的问题。到了需要支付的时候，老太太摸出她一包包的钱，从中拿出几包凑够数字，如果有找零就把找回的钱又单独包起。用比特币支付也是这样的模式。

这里又有个问题，实时制作的硬币也好，银块也好，红纸包也好，都是实际拿在持有者手里的，可是在网上怎么办？还是得要把每个 UTXO 的归属记录在一个账本上，就说在这一次的交易中是 A 付款给 B 和 C，所以 B 和 C 就各得一个 UTXO，当然这两个 UTXO 的大小可以不同；而 A 则花去了一个或几个 UTXO。但是 A 首先得要提供证据，说这一个或几个 UTXO 是我 A 的，现在我要花费。账本上确实记着这几个 UTXO 是 A 的，所以 A 要提供的证据是：我就是 A。同样，B 和 C 以后在需要花费他们各自的 UTXO 时，也得提供证据，说我就是 B 或 C。账本上记载着这个 UTXO 是 A 的，那几个 UTXO 是 B 的，哪还有什么隐私？别急，前面讲过，用的是化名，即地址，实际上是持有人的公钥的 Hash 值。而持有人要提供的证据，则是用其私钥对花费（支付）说明签上一个名，连同花费说明一起发送出去。发送给谁呢？原则上是发送给所有的比特币使用者。这里还要强调说明，并非别人说付给你一个 UTXO 的时候就签名把它领过来放着，这里根本就没有“领过来”这一说，因为这不是实物，而只是把说明这个事情的记录留在账本上，到你要花费的时候才提供证据认领，并且立即就把这个 UTXO 付出去，这就是一次“交易（Transaction）”。每一次交易都有资金来源，也有资金去向，而且二者必须相等。交易中可能需要把几个 UTXO 合并成一个 UTXO，也可能需要把一个 UTXO 分割成好几个 UTXO，其中之一也许就是找回给你自己的。对于 UTXO 的合并和分割，读者不妨想想古代使用银块的时候，就常常需要把大块切成小块，或把碎块熔成大块。既然记录在账本上的 UTXO 并不明说这是付给谁的，而只是说凡要花费这笔钱的人必须提供与某个“地址”相符的（对于花费说明的）签名，那我们就可加以推广，用在这里的不一定非得是对花费说明的签名，还可以比方说是对于某一段话的签名。总之，只要把“签名”这一种加密技术用上，就能保证不会被冒领。所以，账本上的每个 UTXO 给定的实质上是一种招领条件，并不非得是收款方的地址。比方说，给定一个句子和一个公钥，对方必须提供用与此公钥配对的私钥对这个句子的签名。而声称要花费这个 UTXO 的人则要提供认领证据，这个证据就是对某种数值或文字信息的签名。而“签名”这种加密技术，则足以保证只有掌握对应私钥的那个人才能认领。这样，对于一次具体的交易，或者说一次 UTXO 的换手，付方可以根据收方的地址及其花费这 UTXO 时的签名确认这收方真实无误；而收方也可以根据付方的公钥及其在花费处于支付链上游的 UTXO 时所作的签名确认付方也真实无误。

至此，这个推理链好像快能闭合成环了，可是实际上还有很大的缺口，就是：谁来保存和维护这个账本，谁来验证认领证据与招领条件是否相符？如果答案是为此成立一个什么机构，或者将其委托给某个组织或公司，那就又回到网上银行的中心化老路上去了，因为这个机构或组织实质上就是权威，就是中心，只是具体的技术和实现有所不同而已。中本聪们哪里能接受这个，他们的目的就是要去中心。

既然不能把账本放在一家手中，也不能接受让独家把持对于认领证据的验证，那就让“公众”来保存、来验证。简而言之，就是“一个账本，多家保存，大家使用”，并且是谁愿意保存就可以自己保存一份，账本是对全社会开放的。至于验证，也是谁都可以验证，因为根据

记入账本中具体 UTXO 的信息和认领者提供的签名，很容易就可以推算出与用来签名的密钥相对应的公钥（这个过程是“势如破竹”的）；而这个公钥，就作为这个 UTXO 的一部分（一般是作为收款人地址）记录在账本中，谁都可以验算比对。众目睽睽之下，谁也做不了假。而且多家保存就保证了账本不会丢失，因为一家两家的账本丢失根本无所谓。当然，这会导致存储账本的总成本飙升，但现在存储信息的成本已经降得很低，以后还会进一步降低，况且又是由多家分摊，这也没有什么。对于中本聪们，这个环节是特别重要的，因为这就朝去中心化的方向又前进了一步。

好，又前进了一步，但是还有问题。前面说了“一个账本，多家保存”，那么这由多家分头保存的账本得要一致，是同一个版本才行。如果版本之间有不同，一来会有以谁的版本为准的争执，二来也就难以保证不会丢失，因为也许这个为准的版本只有一份，但是却丢失了，而别人保存的账本上却没有你讲的那个 UTXO。进一步，“线上”的支付是通过网络进行的，而网络的各个部分各个地域有随机变化着的不同延迟，使得同一交易请求（支付说明）到达网络中不同节点上的时间参差不齐。另外，显然不能为每一个交易请求都发布一次公告，说大家把这笔交易记入账本，而只能成批发布，过一会儿就说大家把这么一些交易请求、按这样的次序记入账本，成为一个“块”（可以想象成一个账页）。可是由于网络的延迟在同一时间点上处于不同地域的节点上积累起来的交易请求却有可能是不一样的，那由谁来决定把哪些交易记入账本并统一加以发布呢？当然，我们可以指定（或协商、推举）由某一家来担当这个重任。可是这不又回到中心化的老路上去了吗？中本聪们不会接受这样的方案。不仅如此，如果固定由某一家发布，且不说对于作弊的担心，至少还须考虑万一这一家的网络节点发生了故障或者被关机了又怎么办。

也许我们可以引入某种选举机制，每过多少时间就举行一次选举，选出下一任的发布者？可是选举只能在一个至少是大致确定的集合中才能进行，否则就无法计票。然而既然是“去中心化”，要面向大众，而不是采用“会员制”，就得允许人家来去自由。然而此进彼出，此起彼伏，这就连个“选民登记”都很难进行，使选举变得不现实了，何况频繁的选举本来也不现实。那，或者由谁每次临时加以点名指定，说这次由谁发布？中本聪们显然会嗤之以鼻，那还叫什么去中心化；须知无政府主义者是极端的民主派，极端的自由派，极端的平等派。还有个可能的办法是轮流（Round-Robin），可是那样就得让公众承担义务，并且也不一定承担得了，本应轮到我的时候正好我的机器坏了呢？这也不现实。

所以，摆在中本聪们面前的挑战是，怎样才能在去中心化的前提下解决由谁发布新块的问题。他们的方案是，每次都由广大群众竞争新块的发布权，但是当然这种竞争必须能在“线上”进行。

怎样竞争呢？办法不止一个。比方说，在公司的董事会中就可以论股权大小，在学术界可以论“影响因子”，对于学生可以有标准化考试。对于普通群众，比较合理的是能力加努力程度的竞争。体育竞技就是一种能力的竞争，比方说看谁跳得高，可是那只能把竞争者和观看（评判）者聚在一起，在公众的注视下进行才行，而在网络上却“谁也不知道你是人还是狗”。再说，由谁来组织这样的比赛呢，组织者不又成了中心？那怎么办。中本聪们想了个办法，称为“工作证明（Proof of Work）”，简称 POW，就是让各个有意发布新块的节点针对自

己所欲发布的那个块进行 Hash 计算和试凑，谁先达到某种预定的要求，当前这个块的发布权就归谁。

说得具体一些，就是大家都认同、并且议定这样一组规则（共识）：

- 各家都把已经到达了你那里，把经过检验认为合规、即提供的认领证据符合所欲花费 UTXO 的认领条件的交易请求集合在一起，在前面加上一个 Coinbase 交易，说这次发放的原发比特币是发给我的；把这些信息合在一起就成为一个“块（Block）”，我们可以把一个块想象成一个账页。这就是你想要发布的新块中固定的那部分信息。注意两个不同网络节点各自所欲发布的块的固定部分是不可能相同的。首先所含的交易请求就可能不同；即使所含的交易请求相同，它们的次序也可能不同；即使连这也相同，Coinbase 中所含的（本节点）地址却一定不同，因为谁也不会愿意为他人做嫁衣裳，把因本次记账而发放的原发比特币让给别人。所以每个节点上 Hash 计算的起点一定是不同的，计算过程的随机性正是由此而来。
- 在这新块中还加有一个不固定的信息，给你留了一个空位，你得在这空位上填上一个数，什么数都可以，这个数值称为 Nounce。
- 然后你就对这个块的固定部分连同你填入的那个数一起进行 Hash 计算，计算所得的结果当然是个数值。然后将这个数值与预定的条件进行比较。
- 预定的条件是：把这个数值按规定的位数写完全，就是不省略前面为 0 的那些数位，看前面有几个 0，是否够上某个预定的值。打个比方，假定采用五位十进制，那么把 123 写全 5 位是 00123，即前面有两个 0。如果预先的规定是至少两个 0，并且你此刻还没有看到别人抢先发布，那么恭喜，你马上就把这个块发出去，你很可能、非常可能赢了。
- 如果你得到的 Hash 值不满足这个条件，那么有点遗憾，不过还有机会，回到上面的第二步，换上一个数，再算。
- 要是看到别人已经抢先发布，那么这次你没戏了，下次再努力。不过你不妨验算一下，看看人家发布的那个块，连同人家填进去的那个数，Hash 计算以后得到的数值是否真的符合要求。

上面用十进制数举了个例，实际使用的当然是二进制数，但道理是一样的。另外，仍以五位十进制数为例，前面至少有两个 0，其实就是说所产生的数值小于 1000。那么五位十进制数（从 00000 到 99999）中有多大比例的数是小于 1000 的呢？那就是 1/100。就是平均算一百次才能命中一次。而中本聪们设计用于比特币的 Hash 值，却是 256 位二进制数，假定要求前面有 32 个二进制的 0，那就是平均计算四十几亿次才能命中一次。但是当然，说不定你运气好，只算了一次就给撞上了。正是这样的随机因素，把各家通过计算得到结果所经历的时间给打散了，使得有两家或更多家恰好同时得到符合条件的计算结果并加以发布的概率降到最低。注意，之所以有这样的随机性，主要是因为如上所述每家在开始 Hash 计算时的起点是不一样的；哪怕别的都一样，也至少还有本身的地址不一样。要不然的话，如果大家都按同样的规律试凑，例如都从 0 开始，然后 1，2，3，这样去试凑，（除机器的运算速度外）就没有什么随机性可言了。

读者也许会想，要是我看到别人发布了一个块，我马上就把它照抄过来，立即发布出去，说是我计算出来我发布的；由于网络中的传输不均匀，不是有好多网点会先收到我这个，从