解码区块链

原理机制、场景案例与通证经济

黄京磊　林大亮　张剑南　著

清華大學出版社
北　京

内 容 简 介

区块链，对于绝大多数人都是崭新的名词。它只有十年的历史，为人所关注也只是近三四年的事。有的人把它当作技术革命，希望借助它的力量实现人们一直渴求的东西；还有人把它视为资本浪潮，是一种虚幻而无意义的妄想。身在其中和置身于外的人都有些迷茫，看不清它到底是什么，会带领我们走向何方。

我们想，有必要写一本书来帮助大家看清前面的路。也许只是一条泥泞不堪的小路，但至少我们要告诉大家前面不是万丈深渊。穿越艰难险阻的勇士们，会得到他们想要的东西。

本书收集了产业发展和技术原理与实战案例，并用最通俗的语言娓娓道来。我们将为您呈现一个用区块链改造社会与技术的崭新世界。本书适用于所有区块链技术爱好者和希望快速而全面地了解区块链行业的企业家以及其他读者朋友。读完本书，您对区块链技术、机制原理与应用领域的了解将如数家珍。

图书在版编目（CIP）数据

解码区块链 : 原理机制、场景案例与通证经济 / 黄京磊 , 林大亮 , 张剑南著 . —北京：清华大学出版社，2020.7

ISBN 978-7-302-54894-2

Ⅰ. ①解…　Ⅱ. ①黄… ②林… ③张…　Ⅲ. ①电子商务－支付方式－研究　Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2020）第 022934 号

责任编辑：杜　星
封面设计：李伯骥
版式设计：方加青
责任校对：王荣静
责任印制：

出版发行：清华大学出版社
网　　址：http：//www.tup.com.cn，http：//www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：
经　　销：全国新华书店
开　　本：170mm×240mm　　**印　　张：**15.75　　**字　　数：**238 千字
版　　次：2020 年 7 月第 1 版　　**印　　次：**2020 年 7 月第 1 次印刷
定　　价：59.00 元

产品编号：081279-01

前　言

从中本聪提出比特币开始，区块链行业已经历经了多次蜕变。区块链技术逐渐在考验中成熟，展现出它强大的生命力。人们开始越来越多地关注共识机制的设计，解决工作量证明机制中的耗能、攻击风险等问题；开始尝试开发扩展技术，利用脱链、分片等解决方案增强区块链的可扩展性和容量。同时，人们也启动了智能合约的研发。在数字化、信息化的社会，智能合约将以更低成本提供更为便捷的服务，使区块链技术覆盖到更广泛的领域，深入人们的生活。

区块链及其背后去中心化的思想不光为技术领域，同时也为其他领域带来了火光。人们思考利用新的技术和思维，改造原本遇到瓶颈的行业。区块链与能源、确权、医疗、金融等领域的结合，都会成为突破行业枷锁的契机。区块链行业也日趋完善，围绕基础设施开发衍生出的安全防护、硬件制造、行业服务等细分领域组合成了区块链产业集群，可为行业健康发展提供便利。

通证经济学是区块链技术为经济学界带来的新分支。通证体系下的经济运转模式有别于经典理论。通证呈现的多种属性和功能是经济学界尚未深入研究过的新金融产品。通证经济学对公共经济学、货币经济学、博弈论与信息经济学理论的延伸为研究者们提供了新的思考角度和思维模式。这些传统经济学理论与通证经济学的互相作用为经济学家和区块链从业者都带来了不小的收获。

也许很多人仍对区块链行业持有疑义，我们认为这再正常不过。经常

性的反思是行业前进进程中必需的，也恰恰说明了人们对区块链行业的关注。当人们学会从批判性思维的角度去审视它时，人们就实际收获了更多。历史总是螺旋式上升，行业也在螺旋式发展。一次次挤掉泡沫，回归价值本身的行业最终一定能为社会带来真正的改变。

目前区块链的发展方向十分多元，每一个细小的分支都有开拓者在前进，这是无比令人振奋的场景。中国希望从技术大国向技术强国发展，正需要更多的区块链技术和为此勤勤恳恳付出的区块链从业者。我们大胆预测，未来的十年区块链将落地现实，创出高于现在数倍的价值。希望现在抓住区块链的人们，届时都能享受胜利的喜悦。

本书创作团队由黄京磊和林大亮领衔，由多位行业从业者和研究者组成，经历数年对区块链行业的观察与调研，深入各大区块链一线企业考察前沿技术与思路创新，并阅读了大量区块链行业一手文献资料，最终创作完成本书。期间作者们获得了许多业内人士的帮助和指导，尤其是某些知名区块链团队和社区的技术人员与开发者的指导。他们在不遗余力地推动区块链技术向前发展之余，在技术宣传上也颇费心血，对本书的创作更是指导良多。本书在此对他们一并表示感谢。希望本书创作团队数年来的体悟能对读者朋友更全面、迅速地了解区块链行业有所裨益。

目　录

第 1 篇　走进区块链

1.1　区块链概览　/　2

1.1.1　什么是区块链　/　2

1.1.2　区块链行业概览　/　5

1.2　去中心化的逻辑　/　8

1.2.1　中央集权制的国度　/　8

1.2.2　中心化的交易　/　9

1.3　去中心化进程　/　10

1.3.1　数字货币 30 年　/　11

1.3.2　比特币　/　20

1.3.3　区块链行业发展　/　55

第 2 篇　区块链实战

2.1　区块链 + 金融　/　88

2.1.1　什么是金融　/　88

2.1.2　保险　/　89

2.1.3 资产交易与登记结算 / 92
2.1.4 供应链金融 / 95
2.1.5 一份来自会计师事务所的报告 / 97

2.2 区块链 + 确权 / 102
2.2.1 无可奈何的盗版 / 102
2.2.2 知识产权的保护 / 105
2.2.3 实战案例 / 106

2.3 区块链 + 医疗 / 107
2.3.1 行业痛点 / 107
2.3.2 区块链能做什么 / 108

2.4 区块链 + 大数据 / 111
2.4.1 大数据时代 / 111
2.4.2 区块链与大数据的融合 / 111

2.5 区块链 + 物流 / 114
2.5.1 区块链物流的崛起 / 114
2.5.2 实战案例 / 115

2.6 区块链 + 公益慈善 / 116
2.6.1 行业现状及问题：谁来守护公益和慈善的净土 / 116
2.6.2 基于区块链的解决方案：“通证”卫士 / 118
2.6.3 “区块链 + 公益”的案例分析 / 119

2.7 区块链 + 溯源 / 120
2.7.1 行业现状及问题 / 120
2.7.2 基于区块链的解决方案 / 124
2.7.3 “区块链 + 溯源”的案例分析 / 129

2.8 区块链 + 人工智能 / 133
2.8.1 行业背景与市场分析 / 133
2.8.2 “区块链 + 人工智能”解决方案和案例 / 135

2.9 区块链 + 数字广告 / 139
2.9.1 行业现状 / 140
2.9.2 数字广告行业存在的问题分析 / 143
2.9.3 基于广告行业的解决方案 / 144

2.10 如何判断区块链与行业的结合 / 146

第 3 篇 未来

3.1 Layer-2 技术与共识机制的新探索 / 150
3.1.1 Layer-2 技术扩展 / 150
3.1.2 共识机制 / 167

3.2 通证经济学 / 190
3.2.1 从经济出发 / 190
3.2.2 通证经济学 / 191

3.3 区块链的未来——向死而生 / 221
3.3.1 区块链必须死? / 222
3.3.2 向死而生 / 225
3.3.3 预言 / 234
3.3.4 再远一点的未来 / 237

参考文献 / 239

结尾鸣谢 / 241

第1篇 走进区块链

区块链，像互联网一样。你不了解它，它自己却走来，以不可阻挡的势头改变你的生活，强迫你最后还是要了解它。我想不如现在主动了解一点的好。

——作者

1.1 区块链概览

如果你不相信我，或者说没有理解我的意思，那么我没有时间尝试去说服你。

——中本聪

1.1.1 什么是区块链

2008 年，是区块链的元年。

2008 年 11 月 1 日，一位名为中本聪（Satoshi Nakamoto）的密码朋克在一个秘密讨论群“密码学邮件组”中发表了一篇题为“比特币：点对点电子现金系统”的署名文章。一次人类历史上最伟大的数字货币实验正式开始。

从此，“比特币”与“区块链”两个概念逐渐进入人们的视野。之后的 10 年，这两个词引发了一场技术革命和思想革命。但当时，人们只是认为：嗯，又一个异想天开的疯子。

为了弄清比特币和后面这场革命的来龙去脉，我们不得不把关于这项发明的详细介绍往后放一放。至少，我们首先需要对几个相关概念进行了解，才能体会到中本聪这次尝试的令人兴奋之处和伟大意义。

严格意义上说，区块链的发展并不是随比特币的出现而开始的，区块链也是完全不同于比特币的一个概念。不过比特币的出现把原来鲜有人关注的区块链推到了世人面前。

1. 技术定义——不可篡改的数据结构

关于区块链的定义，不同的人从不同角度作出过诠释。从技术的狭义角度定义，区块链特指的是一种数据结构：

“区块链是一种数据结构，即通过哈希指针构建的链表。”

“狭义上讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改、不可伪造的分布式账本。”

不同于一般的数据结构，区块链具有两个标志性的特征：单向性和唯一性。

单向性是指在区块链上的数据区块排布具有固定顺序，只能单向延伸。这种顺序往往是按照时间进行排列的，因此每块数据都打有时间戳。处于时间序列后部的人仅能沿区块链对之前的数据进行追溯和查找，但无法进行添加或销毁。

唯一性是指区块链上记录的数据与区块链的数据结构一一对应。链接后一区块与前一区块的哈希指针以哈希函数为基础，而哈希函数具有完美的安全特性：隐秘性和约束性，即任意两个不同的输入不会产生相同的输出，通过输出无法反推输入。利用哈希函数的这两个特性，可以使得一个区块链中的哈希指针仅对此区块链中的数据有效，而对其他区块链毫无价值。另外，对数据进行改动会导致之后区块链上所有的哈希指针发生变动。

拥有这两个特征的区块链因此具有了能应用于现实的重要特性：数据不可篡改。任何企图对数据的改动或增减都会导致区块链的数据结构发生改动。只要保证区块链的头部数据不可篡改，全链的数据就是真实可靠的。

2. 组织形式定义——去中心化的数据共识协议

“区块链是一个去中心化的分布式数据库。”

“区块链是一种新型的去中心化协议。”

去中心化，作为最常被从业者提起的优势，之所以被认为是区块链的核心特征，主要是因为其对组织形式的改造。无论是商事交易中的中介，还是商业组织里的管理层，如果需要多个个体达成一致，都需要这样一个中心化的组织汇总、协调各方意见或者制订统一的策略。因此，一个共识的达成往往依赖于中心化组织的高效率和良好决策。这种组织形式蕴含着较大

的道德风险和个体风险。个体的协同对中心化组织产生过分依赖，同时中心化组织获得了与自己义务不相称的权力。由此产生的分配不均、利益窃取、信息贩卖等问题在互联网这个信息快速流通、利益关系日趋复杂的社会更是层出不穷。

现代社会是个体独立的社会。由于生产力解放、个人意识觉醒，每个个体拥有愈发强烈的发声欲望。人们不满足于中心化机构对共识达成过程中的过分干涉和信息隔离造成的信息不对称。社会有越来越强的意识希望信息的筛选、识别和彼此沟通摆脱中心化机构的桎梏。但是在以往，缺少中心化机构会带来沟通的不便和共识形成的效率低下。而在区块链的帮助下，人们的这一愿景逐步成为现实。通过计算机与互联网，信息之间的交互在纳秒级内发生。人们可以利用电脑程序对信息进行客观检验，自动执行某一过程，实现对一种情形或事实的统一认可。

从组织形式角度定义区块链，区块链正是这样一种无需中心化组织参与的节点间对数据的共识协议。具体而言，是在区块链数据单向延伸的过程中，不同参与者按事先约定规则对延伸方向和延伸速度达成一致意见。

由于这种共识全部依赖于公认的逻辑和程序，所以其需要具有透明性和匿名性这样的特性以保证节点之间的平等。决策仅应该受节点的意志影响而非其现实身份或掌握的更多信息。区块链所做的，就是用技术手段保障透明性、匿名性和沟通效率，使得去中心化的数据共识得以实现的一类协议。

3. 现实应用定义——技术有机整合后的应用模式

“区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。”

“区块链技术不只是单一的技术，而是多种技术整合的结果，包括密码学、数学、经济学、网络科学等。这些技术以特定方式组合在一起，形成了一种新的去中心化数据记录与存储体系，并给存储数据的区块打上时间戳，使其形成一个连续的、前后关联的诚实记录存储结构，最终目的是建立一个保证诚实的数据系统，可将其称为能够保证系统诚实的分布式数据库。”

类似于人们对人工智能、自动驾驶的理解，更多的人对区块链的认知是在其具有现实意义的应用层面。区块链本身并不是一项新出现的技术，而是一个整合了分布式账本、块链式数据、梅克尔树、工作量证明等技术的创

新解决方案，可以用来解决现实生活中的问题和其他行业的痛点。发明比特币的中本聪，就是提供这类解决方案的高手。其以电子现金、工作量证明、非对称加密算法等技术为基础设计出的比特币，可以实现 P2P 电子支付，解决资本流通障碍、跨国转账成本高等现实中的货币流通问题。在此过程中，又会激发新的相关技术出现，提高区块链解决更多现实问题的能力。

从这个意义上，区块链行业指的就不只是数据结构开发和共识机制设计等技术领域，还包括技术转化、应用普及、产品优化、共识建设、辅助功能实现等衍生领域。现在绝大多数公司，包括互联网巨头的区块链研究院、行业区块链开发者、区块链实验室等都是在解决这个定义层面的区块链问题。

对于区块链概念的界定总归是一件仁者见仁、智者见智的事，但对于投身于区块链的人们来说，明晰这一概念有助于对自己的前进方向和发展潜力产生更客观的认识。总体而言，我们认为区块链存在三种维度的界定：技术维度、组织形式维度和现实应用维度。每一维度的定义递进产生了区块链的特征：数据不可篡改、去中心化、透明性、匿名性、技术集合等。因此，区块链就是以哈希链表为数据结构，以去中心化数据共识协议为组织形式，具有现实意义，拥有以上特征的技术集合。

1.1.2 区块链行业概览

区块链作为崭新的行业，一出现就受到了空前的关注。互联网人视之为流量红利耗尽之后的增长点，技术人士视之为苦苦寻觅的技术突破口，政府视之为潜在的经济助推器，民众视之为蕴含无限机遇的朝阳产业。

不过如同所有新生的事物一样，诞生伊始总要经历创痛和非议。有人批评它是骗子与狂妄者的集散地，有人惋惜地称之为又一次“全民疯狂”。投资盛宴，技术狂欢。虚假与夸夸其谈大行其道，笃行的人却总是默默无闻。专家、程序员、公关、写手，有的被指责为炒作与营销的始作俑者，有的被称呼成欺骗与自私的传销头目。流言蜚语、指桑骂槐、明争暗斗、尔虞我诈，为了建立去中心化和信任世界的人们，却在短期利益面前放弃了信仰。真的有必要付出如此惨烈的代价吗？

区块链的乱象仍会持续，但最终胜利的不会是空想和骗术。对于区块链外的人，要做的是看清行业和行业里做实事的人，利用手中的资源帮助他们前进。对于区块链内的人，要做的是了解行业环境和发展方向，通过技术和想法上的创新带给行业与社会一些改变。让区块链内外的人初步了解行业，就是本节的目的。

了解一个行业首先需要了解的是它所涉及的业务和详细划分。广义上的区块链行业范围很广，包括基础设施和平台建设、硬件制造、安全防护、行业服务、区块链应用五大板块。

基础设施和平台建设是区块链产业的核心分支，主要分为公有链、联盟链和 BaaS（blockchain as a service）平台。它涉及共识机制设计、数据结构搭建、经济体系建立、网络通信、工具和接口提供等一系列复杂问题，也是区块链应用赖以存在的基础，所以在整个产业链条中处于底层和核心地位。

硬件制造主要包括芯片制造和算力中心。在区块链延伸过程中，加密的安全性依赖于加入体系的算力保障。高性能的芯片能使得投入最少的电力，进行最多的运算，提供最好的安全支持。算力中心是高效利用分散算力的优化方式，也是联盟链、私有链等项目的算力提供方未来的发展方向。

安全防护是区块链行业特殊的分支领域。由于区块链项目的代码多为开源，所以更易受到恶意攻击。如果出现漏洞，会迅速传播开来，更具危险性。安全防护的主要领域集中在开源代码、加密算法、共识机制、智能合约和数字钱包等方面。目前安全防护公司主要为区块链项目提供技术支持、代码审计等服务。

行业服务主要包括媒体社区、投资机构、行业组织和研究机构等。媒体社区掌握流量，可以扩大区块链项目的影响力、促进行业交流并提升公众认知。区块链项目前期投资多较庞大，投资机构可以有效分担风险并提供资金，帮助区块链早期项目迅速扩大规模、聚拢人才、渡过难关。行业组织提供行业内部交流平台，制定行业规范，减少行业内信息不对称情况。研究机构主要负责区块链行业概况梳理，深度挖掘行业价值和内在规律，为区块链创业者和投资者提供详实的情报。

区块链应用处于区块链产业链最上层，覆盖面较广，涉及金融、医疗、

教育、物流、供应链等诸多领域。绝大多数行业与区块链相结合都能碰撞出火花，产生新的创新点和价值。利用区块链技术造福各行各业，也是发展区块链技术的目的之一。

2018 年年末全世界有统计的成规模区块链项目已达 900 多个。中国更是发展区块链行业的重点国家，知名项目已有数百个，包括民营资本、政府、外资等各方力量均在区块链发展上有所涉足。行业整体还处于发展早期，各项目相对独立，尚未进入横向整合阶段。

区块链行业与制造业不同，它的产业结构属于网状结构，而不存在一个明确的上下游关系。基础设施和平台建设处于相对核心的领域，区块链应用、安全防护与行业服务之间也有千丝万缕的联系。常规产业往往具有产业链，上下游企业之间为供应关系，以中间产品为传递媒介；同级企业之间为竞争关系，不存在商品传递。区块链产业则打破了这一定式。除了硬件设备交付之外，企业间传递的主要是信息和价值。

从互联网到区块链，人们常说是从信息互联到价值互联的过程。实际上这个说法有失公允，因为互联网时代已经出现了价值互联，但还不十分广泛。例如基于开放协议 HTTP 服务的网站、基于 SMTP 协议的电子邮件服务。没有一家网站需要为使用 HTTP 协议支付专利授权费，也没有哪一次电子邮件发送需要出售真实身份。但是进入互联网巨头时期，企业之间彼此成为信息孤岛。由于信息的收集者、储存者和使用者都是互联网企业，它们就相当于拥有了信息的一切所有权、使用权、收益权和处分权。信息的价值垄断在巨头手中，缺少流通以产生新的价值。区块链时代则进一步开放数据的流通。代码、交易记录等数据可以为所有人共享，区块链打开了信息自由流通的大门。个体的信息价值在群体中创造出更大的价值。这就是价值互联的本意。

区块链相关的法律法规尚不完善，部分政府制定了发展报告、产业政策以表明态度，但相关规范性文件鲜有出台。国外也缺少相关经验借鉴。实际上，区块链产业发展的规章制度是全世界监管机构的共同难题。区块链应用中的数字货币被部分国家政府视为打破美元体系的利器，但是实际反响并没有想象中的颠覆性效果。因此很多国家对区块链及其加密货币应用都由积极转向了观望态度。

1.2 去中心化的逻辑

及至始皇，奋六世之余烈，振长策而御宇内，吞二周而亡诸侯，履至尊而制六合，执敲扑而鞭笞天下，威振四海。

——《过秦论》

区块链是去中心化的世界。去中心化的组织形式是区块链有别于其他技术进展给人们带来最大的灵感。无数从业者满怀着对“去中心”这三个字的无限崇敬投身到区块链建设的事业中，想象着“去中心”后世界自由、平等、美好的样子。他们已然是虔诚的信徒，甚至不少人坚定地认为在区块链的发展中任何向中心化妥协的一点点趋势都是对神圣信仰的背叛。在评价这种价值取向是无知的狂热还是坚定的笃诚前，我们有必要先来审视一下中心化的世界，这对我们理解这种“去中心”思潮和比特币的创新都是有好处的。

1.2.1 中央集权制的国度

从秦朝到清末，中国传统社会一直实行的是高度的集权制。皇族通过世袭获得统治天下的名义权力，官僚阶级作为皇帝的代理人对国家进行实际统治。整个社会呈现严密的等级划分，社会关系以从属性关系为主。皇帝有权代理民意，以个人意志作为集体共同目标。所有权力在个体诞生时即被上交到最高的权力者手中，然后经由官僚阶级进行逐级分配。普通个体的基本权利时时受到被剥夺的威胁。国家通过暴力机关（军队、牢狱）保证权力的收集和分配秩序过程。

这种中央集权式的社会结构在中国历经了两千余年。从现在的眼光审视这种高度中心化的结构，其所形成的树状社会未免太过压抑个体的意志，个体权利无法得到充分保护。但如果我们把眼光着眼于当时的社会环境和历史进程，倒是会有一些有趣的发现。

中国是古老的农耕社会。兴修水利、疏通河道、开垦土地、抢种抢收，都需要集体的力量才能完成，因此人们产生了对组织和管理者的需要。农民

需要与铁匠、盐商等其他经济主体进行商品交换，因此产生了对集市这类公共服务的需求。水源、农忙时的劳动力分配不均，产生了对合理规划资源分配的需求。农业生产需要稳定，出于对自身安全和财产的保护，人们产生了对职业军队的需要。一个中心化的社会，可以以强制力集合集体的力量，高效率地实现以上目的。在个体生产力并不发达、竞争环境激烈、个体承担较大风险的时代，中央集权制的中心化社会是当时人们最好的选择。

所有人从一出生就被强制要求服从于中心化的社会管理体系，以极大地割舍个体权利为代价换取了社会关系、政治关系和经济关系的长期稳定。无论是西方的贵族政治还是东方的宗族式家庭，文化习俗和社会秩序莫不如此。

1.2.2 中心化的交易

古往今来所有基于信用的交易都是中心化的。

在原始社会，交易并不需要中心化，因为一笔交易只会牵扯到买卖双方。一手交钱，一手交货，所谓货银对付是也。每个人接触到的社会非常小，人与人之间进行的是重复博弈。一名交易者弄虚作假会立刻影响他的下一次交易，并损害其之后所有交易的利益。

但这样的交易模式阻挠了商品经济的进一步发展。越来越多的交易者和商品进入市场，使得交付货物的同时获得货款变得困难重重。为此，人们开始利用信用交易，原始社会遵循的交易流程发生了转变。由于钱货并不立刻两清，所以出于对债权人的保护，必须要有一定的外部力量保证债务的及时履行。在江湖上可以是规矩，在商业团体中可以是道德，在现代社会里可以是法律。但无一例外，人们对交易信用的破坏必定会遭到制裁和敌对。因为随着人与人之间的社会关系日趋复杂，交易双方的联系越来越淡，找到一个双方都认可的约束力变得愈发困难。因此，人们又产生了对中心化商业机构的需要，以负责维护交易秩序和交易信用。在同一个国家内进行交易的双方并不需要额外寻找一个对双方都拥有强制约束力的第三人，因为国家和其下辖的暴力机关为这种信用交易提供了最高的信用背书。除却国家，类似于淘宝、美团外卖、滴滴出行这样的互联网平台就是网络购物、外卖送餐、交通出行的中心化机构。淘宝可以强制清退商家，美团外卖可

以禁止餐馆或送餐员提供服务，滴滴出行可以排除差评率过高的司机加入备选车辆。即使不是理论上最优的选择，但共同相信这些平台的双方构成了博弈论中的纳什均衡。

伴随着信用社会到来的同时还有博弈方式的改变。由于古代人际关系相对封闭，进行经济活动的双方往往要进行反复博弈，一方失信的成本很高，而且存在经济关系之外的其他联系为交易双方的信用背书。随着商品经济的全球化，交易的地理联系、社会联系都日渐淡化，交易形式逐渐转变为一次性博弈。进行经济决策时，人们更加理性，更加专注于财富层面的积累，导致信用成为越来越廉价的商品。人们苦于无法保障交易的稳定性，执着追求建立规模更大、覆盖面更广的中心化组织，但是事实上信用却越来越难以得到保障。贸易保护主义更为跨越国界之间的商事信用维护蒙上了一层阴影。工业革命到来之后，个体生产力得到解放，每个人可以独立创造的价值在暴发式地增加，人与人之间的经济关系开始突破各种各样束缚。当信息时代悄然而至时，个体被再次赋能，成为信息的广播者和中转站。技术的进步推动人们接触到更多元的信息，形成更加丰富的思想，也产生了更多对隐私和财产权利的要求。人们开始对于中心化机构隐瞒实情、刻意制造信息不对称产生不满，对它们征收过于高昂的中间费用抱怨不公，甚至对于它们存在的价值产生了怀疑。有没有手段能在保证交易信用的同时，尽可能保护交易者的隐私和财产不受侵犯？有没有更低成本的方式促使所有人对交易规范达成共识？中心化的世界真的是一成不变的吗？

“去中心”的思潮在暗流涌动，构建技术信用社会的前奏已经鸣响，一种新型的数字货币呼之欲出。

1.3 去中心化进程

在某些时候，我确信有一种方法可以做到这一点，而不需要任何信任，并且忍不住想到它。更多的工作是设计而不是编码。幸运的是，到目前为止，所提出的所有问题都是我之前考虑和计划的事情。

——中本聪

比特币的本质是，一旦 0.1 版本发布，其核心设计将在其余生中保持稳定。

——中本聪

1.3.1 数字货币 30 年

站在 10 年后的角度评述比特币的诞生，我们称赞其为一次天才的绝妙尝试，堪称货币史上的里程碑，可惜当时的人们并不都这么想。因为在比特币被人们广为接受之前，无数密码学天才已经在数字货币的构建上进行了 30 余年的尝试，但是无一得到大规模应用。

1. 电子支付与盲签——E-cash

1983 年，大卫·乔姆（David Chaum，密码学奠基人之一）首先提出了电子支付手段。从他的论文[①]可以看到，他敏锐地察觉到诸如交通、住房、娱乐等数字化消费信息对个人隐私暗含的威胁。同时他对现有银行体系无力应对政治贿金、黑市交易等灰色现金交易提出了改进方法。在其中，他指出自动支付系统应该具有以下几大特征。

（1）交易的收款人、支付时间和金额完全不受第三方控制。

（2）特殊情况下，交易发起人应当有能力证明支付的发生与收款人的身份。

（3）在支付媒介被盗的情况下，用户有能力阻止账户进行支付。

为此，乔姆提出了盲签技术。对盲签技术的解释常采用选民身份确认的例子。当选民填写完选票后，可以将其与一张复写纸共同封装在信封内，信封外事先打印好选民证书。当这份信封被邮寄给官员（签名者）时，官员在核实选民身份后可以直接在信封上签名，从而在官员不打开信封的情况下完成对选票的签署。签署后，信封会被退还给选民。选民可以将具有官员签名的选票另外转移到新的信封中。整个过程没有向第三方透露除身份外的任何信息，但获得了第三方的信用认证。利用这种思想可以设计出很多种盲签方案，如 RSA 盲签或 ECDSA 盲签。

---

① David Chaum，“Blind Signature for Untraceable Payments”，1983

RSA 盲签是最简单的一种盲签方式。在 RSA 加密模式中，私钥和公钥分别对签名者和公众开放，分别用于信息的签名和身份验证。

假设公钥为 e，签名者手中的私钥为 d，公有模数为 N，A 需要 B 对信息 m 进行签名，同时保持信息不被 B 所知晓。A 可以选择一个与 N 互素的随机数 r[如 gcd （r，N）=1]，利用取模运算得到盲因子 k。

$$k \equiv mr^e \pmod N$$

然后 A 将这个盲因子寄往 B。由于 r 选取过程和 $r^e \pmod N$ 结果的随机性，通过 k 反推 m 是不现实的。因此寄往 B 的盲因子 k 不会泄露任何有关于信息 m 的内容。B 利用私钥完成签名 s' 后，将 s' 回传给 A。A 通过手中掌握的随机数 r 得到 B 对信息的真实签名 s。

$$s' \equiv (m')^d \pmod N$$

$$s \equiv s'r^{-1} \pmod N$$

这是因为有 $r^{ed} \equiv r \pmod N$，所以：

$$s \equiv s'r^{-1} \equiv (m')^d\, r^{-1} \equiv m^d r^{ed} r^{-1} \equiv m^d r r^{-1} \equiv m^d \pmod N$$

s 实际上仍然是对信息 m 的签名。

事实上，一种签名方案还需要满足对一条信息的盲签最多产生一条有效签名信息的性质。上述签名方法就并不满足此种性质。不仅原信息 m 与真实签名 s 是有效的，盲因子 k 与盲签名 s' 也是符合条件的，甚至会有聪明的攻击者构建出其他的组合。针对这种问题的一种解决办法就是对信息的密码散列（cryptographic hash）进行盲签，而非对信息本身。

除了创造性地使用盲签技术保证信息的安全，乔姆还在自己设计的电子支付系统中融入了审计的可能。任何交易付款方都会收到一张电子收据，注明交易的标的和日期，同时生成签名的副本。在特殊情况下，银行（签名者）可以与付款人一起验证收款方的账户真实性。通过查验签名款项的真实流向，可以判断交易中是否出现了欺诈行为。如果黑市上的交易者对交易不满，他可以公布签名的副本实现款项追踪。

在对钱款流出进行控制之外，乔姆还希望这种收据能对流入进行存档。对于税收支付者，支出和支付的收据可以用于税收审计。但是机构纳税者

的支出存档可能会泄露顾客的信息，所以存档不必保留。相较于之前的支付系统，乔姆意在打造一个隐私性和安全性更高、可审计、货币供给确定的不可追查支付手段。

乔姆的设想是电子货币的雏形。他第一次给出了一整套实际解决方案以实现无信息泄露的认证过程。但是对于这种加密方法是否能被攻破、钱款的输入输出记录是否暴露用户身份等困扰当今数字货币世界的问题他没有再做深入的阐述。而且此种设想并没有排除第三方对交易的干涉，银行与清算中心仍扮演着重要的角色，乔姆只是把支付过程数字化了。不过这并不影响乔姆在密码学和数字货币史上的重要地位。利用加密技术设计数字货币的思路，激发了无数人的想象。

尽管乔姆的电子支付设想具有划时代的意义，他直到 1990 年才得以将想法付诸实践。乔姆于 1990 年创立了 DigiCash 公司，以“E-cash”为商标。然而，在美国，只有一家位于密苏里州圣路易斯的马克吐温银行引进了 E-cash，将其作为微支付系统进行测试。可惜效果不佳，长达 3 年的试验期内只有约 5 000 名用户。在马克吐温银行被一家大型信用卡发行商系统收购之后，该系统最终于 1998 年被解散。失败的原因按照乔姆的话来说，就是“随着网络的发展，用户的平均素养在降低。很难再向他们解释隐私的重要性”。实际上，失败的更重要原因在于这种支付手段仍高度依赖于一个中心化的中介机构。[①]

2. 数字货币雏形——B-money

在比特币的创造历程中，B-money 占有重要地位。不只是 B-money 的创造者戴维（Wei Dai）是最早在 2008 年中本聪开发比特币时与其进行接触的人（如果戴维自己不是中本聪的话），B-money 的论文还被比特币白皮书进行了引用，也就说明 B-money 与比特币之间存在很强的联系，至少他们对于“无政府加密状态”的追求都是高度一致的。

戴维对 B-money 的设想十分简略。在 1998 年的论文[②]中，戴维设计了两种协议：第一类协议针对个人，戴维自述为不切实际的，因为要用到大量同步性和不可调的匿名广播通道，但它会推动第二类更为实际的服务器协议出现。这两类协议都假定网络不可追踪，消息发送者和接受者都仅能

① 知乎《比特币是什么》江卓尔

② Wei Dai www.weidai.com/bmoney.txt

识别到公钥这样的假身份。每条消息由发送者签署，并由接受者解密。这类假设基于的正是乔姆设想中盲签的可实现性。

第一类协议里，每个参与者都拥有基于自己假身份（如公钥）的独立数据库，而后所有的账户共同定义拥有者的货币量。第一类协议主要解决每个账户的更新问题，其重要意义在于戴维开创性地设计了很多想法，并成为了工作量证明机制的重要基础。

（1）货币创造

任何人都可以通过广播一个之前未解决的计算问题来创造货币。这就是之后比特币基础共识——工作量证明机制的扼要阐述。判定解决计算问题所耗费的时间和验证需要足够容易。获得的数字货币应该等同于其消耗算力所花费的金额。例如解决一个问题所需要的最少算力约为 100 小时，竞争市场上购买 100 小时算力的价格约为 3 个现实货币单位。那么当有人在广播中公布了解决问题的方案时，所有人都应该在自己的账本上记下解决问题者多拥有了 3 个数字货币。

（2）货币支付

当 A 广播声称自己将 X 单位的数字货币转移给 B 时，所有人都应当在自己的账本上减去 A 账户 X 单位的货币，增加 B 账户 X 单位的货币。但如果 A 账户的余额不足以进行支付，则自动忽略。这里已经出现了分布式账本的基本雏形。

（3）数字合约

戴维在这里设计了一种数字化的合约。一个有效的合约应该包含合约各方违约的最大补偿金额以及合约仲裁方的抵押。当合约各方及仲裁方向网络公布合约和他们的签名时，所有人会在自己的账本内扣除各方的最大补偿金额和抵押，并将总金额转移至一个特殊账户，如图 1-1 所示。

当合约被顺利履行时，所有人从特殊账户返还合约各方最大补偿金额和抵押并记录合约执行结果，如图 1-2 所示。

当合约执行结果出现争议时，合约各方首先申请仲裁方的仲裁。如果仲裁后仍有异议，戴维给出的指导原则是：合约各方分别广播一个合理的赔偿方案和对自己有利的证据，由每名参与者决定赔偿的金额并更改相应的账户。

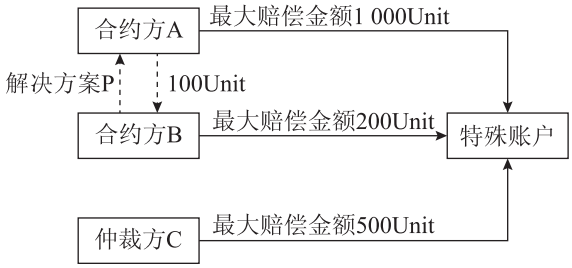

图 1-1　数字化合约（一）

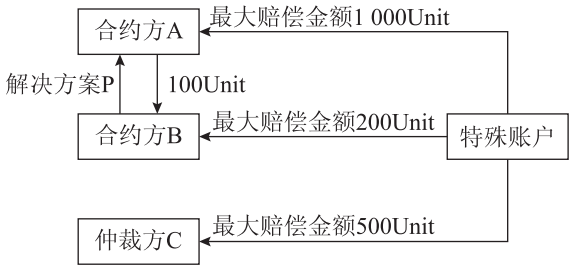

图 1-2　数字化合约（二）

在第二类协议中，每个账户的金额交由参与者的集合们（以下简称“服务器”）决定。每个服务器之间通过 Usenet 式广播通道连接。每个在通道中广播的交易信息格式与第一类协议相同，但每个交易关联方需要确认信息已经被随机选出的一部分服务器成功接收了。

为了服务器能保持诚实，戴维设计了额外的机制。每个服务器都要存储一定数额的货币，以用于潜在的罚款或奖励。此外，每个服务器必须定期公布创造的数字货币和货币所有权的数据库，经由每名货币持有者确认并确保货币总量没有超出创造出来的总货币量。这就避免了服务器之间，甚至全部服务器之间串通，导致无成本地永久增加货币总供给。新的服务器也可以利用公开的数据库及时与其他服务器保持同步。

通过以上两种协议，戴维成功地搭建起一个更具实际应用可能和效率的货币系统与合约执行方案。戴维希望 B-money 能为“无政府加密状态”的实现推波助澜。实际上，他确实做到了。

不光如此，高瞻远瞩的戴维还在论文的附录中附上了一种创造货币的新方法。

他认为受计算能力快速发展的影响，一些秘密的计算技术可能对

B-money 创造货币的公平性和合约的安全性产生威胁。所以戴维设计了一种 B-money 创造的替代方案。他把每次创造分为以下四个步骤。

①计划：货币持有者商讨下一时期货币供给是否增加和计算供给增加量的支持数据。

②竞标：希望创造 B-money 的人对自己希望创造的货币量和待解决计算问题进行广播。

③计算：在竞标完成后，竞标者即开始计算问题并广播答案。

④货币创造：所有人在广播了答案并投标最高的人的账户上增加对应货币量。

这种货币创造方式虽然烦琐，但是保证了货币供给量经过了充分商讨，而不会出现计算能力突飞猛进对 B-money 造成严重的通胀。

B-money 的设计已经把去中心化账本的想法与加密计算结合起来，并考虑到货币创造的公平性与利用 B-money 实现数字合约的可能。尽管 B-money 缺少对去中心化账本结构、服务器间通信、货币创造所需数学运算的复杂度等问题的具体方案，但可以说 B-money 已经基本具有了比特币的雏形。很多人怀疑戴维就是 10 年之后完成整座精美的数字货币体系搭建的设计师，但戴维自己否认了比特币与自己的想法一脉相承。他认为中本聪独立想到了这一点，而把功劳加在了自己身上。

著名密码学家尼克·萨博（Nick Szabo）曾述：

“我，戴维，哈尔·芬尼，是在中本聪出现之前仅有的真心喜欢并追逐这个想法的人。”

但谁知道戴维是不是就是中本聪本人呢？

3. 比特币架构的直接前身——Bit gold

正如尼克·萨博所自述的那样，除去中本聪，在数字货币的研究上最有激情和贡献的三个人就是他、戴维和芬尼了。在戴维发明 B-money 的同时，萨博创造出了 Bit gold[①]，一种听名字就知道与比特币有千丝万缕关联的数字货币。

对 20 世纪恶性通货膨胀的深恶痛绝和对银行深深的不信任促使萨博萌

① Nick Szabo，“An unending variety of topics”，https：//unenumerated.blogspot.com/2005/12/bit-gold.html

生了创设类似于贵金属，具有强保值功能和不依赖于第三方发行的数字货币的思考。贵金属由于其开采的高成本产生了稀缺性。但验证贵金属成色过程的复杂性阻碍了其大规模应用于日常流通，因此往往需要第三方机构将贵金属制成标准的硬币。此外，贵金属的运输成本高，风险大。更为重要的是，贵金属无法数字化转换为网络支付手段。因此，萨博期待能构建一种创造不可伪造的，同时尽可能减少对第三方机构依赖的货币。这种货币可以只通过建立最小化的信任即可安全地存储、转移或验证。

萨博构想出的 Bit gold 基于“用户谜题机制”或“工作量证明机制”。假设现在已有一个公开的字节串，那么新增加字节的用户必须基于已有字节串，通过求解特定函数得到答案以证明自己的工作量。工作量证明利用时间戳进行安全性保障，新增加的字节和工作量证明的时间戳一起被分布式账本记录下来。此后下一个字节又要在新增加的字节后进行延伸。如果用户希望查验另一名账户的余额，他可以验证字节串中记录的工作量证明和时间戳。

萨博认为整套逻辑可以利用软件自动实现，问题的关键在于如何保证账本记录和修改时间戳的过程足够的去中心化。其实，萨博最开创性的贡献在于他把 B-money 中通过计算独立的数学问题证明工作量发展成通过计算与之前存储数据高度相关的数学问题证明算力的付出。再加上时间戳具有的不可逆向生成的特性，数据之间就形成了矢量串，而不是孤立存在。这样的特点还有一个非常显著的好处，即绝大多数用户必须就已有数据达成一致，才能进一步完成数据串的延伸。这为之后比特币的分布式账本在全网达成一致提供了良好的借鉴。B-money 中的账本是很可能相互之间记录出现偏差而需要较长时间才能发现问题的。

作为一位毕业于华盛顿大学的计算机专家，萨博是一位笃定的经济自由主义者。针对数字货币面临的双重支付问题，一般采用的解决方案都是引入一定程度的中心化监管，但对于萨博来说这是不可接受的。

“我试图尽可能地在网络空间中模仿黄金的安全性和信任特征，其中最重要的是它不依赖于值得信赖的中央权威。”①

① Peck，Morgan，“Bitcoin：The Cryptoanarchists’Answer to Cash”，2012

4. 摆脱双重支付——RPOW

哈尔·芬尼与萨博和戴维都是好友。受他们的启发，芬尼决定进一步采用无中心化机构认证的方式解决困扰数字货币的双重支付问题。他认为萨博的“Bit gold”过于烦琐，但是思路是正确的：创造一种自带稀有属性的货币，保证这种货币的可传递性和可验证性。

芬尼设计了一套“可重复使用的工作量证明机制”（RPOW）。他将体系中的货币分为 POW 和 RPOW 两种，其中 POW 基于的是 Adam Back 在 1997 年发明的哈希现金（Hash cash）。①

（1）哈希现金

哈希现金实际上是一串固定格式的字符。它具有一个独特的特性：当经过 SHA-1 哈希运算后，在这种字符串的前 20 ～ 30 位都是 0。基于 SHA-1 的特性，找到这种字符串的概率完全随机。完全不存在一个能提高效率的寻找方式，之前的答案对寻找下一个答案也毫无帮助，唯一的方法就是不断地去试。

芬尼在他的论文中举了一个例子：

1:28:040727:halmail1@finney.org::1c6a5020f5ef5c75:63cca52

这就是一个具有 28 字节价值的哈希现金。因为经过 SHA-1 哈希计算，它得到的结果是：

0000000a86d41df172f177f4e7ec3907d4634b58

它的开头有 7 个 0，在十六进制的表示中就意味着有 28 个字节为 0。

由于每一字节是 0 的概率都是 1/2，所以发现一个前 n 位全都是 0 的哈希值意味着平均要计算 2^n 次。对于一个 20 字节价值的哈希现金，这种计算平均需要 100 万次；对于一个 30 字节价值的哈希现金，这个数字已经涨到了 10 亿。一般来说，每增加 1 字节的要求，时间就会相应增加一倍。也就意味着多 1 个字节价值的哈希现金，哈希现金的稀有度也就增加一倍。一个 30 字节价值的哈希现金应当是一个 20 字节价值哈希现金的 1 024 倍。

哈希现金存在两个显著的好处：其一是它的产生需要消耗大量算力，所以稀有性得到保障；其二是任何人只要将哈希现金代入 SHA-1 函数都可以很轻易地计算出哈希值，并通过对开头的 0 进行计数得到哈希现金的价值。

① Hal Finney，https：//nakamotoinstitute.org/finney/rpow/theory.html，2004

这保证了哈希现金的可验证性。现在距离萨博理想中的数字货币只差一条可流通性，而在这一点上哈希现金做得并不好。

因为哈希现金并不能被良好地重复使用，否则将存在严重的双重支付问题。一名哈希现金的接收者会由于无法判断其收到的哈希现金是否已支付给别人而拒绝接受。为了避免双重支付，哈希现金植入了“资源字符串”，用以标注每个哈希现金的用处，让接收者可以辨识哈希现金是否是创作出来用于该笔交易用途的。例如对于邮件来说，“资源字符串”可以是接收者的邮箱。当接收者确认了邮件发送者支付的哈希现金确实用于寄给自己，他才选择接收邮件。同时，哈希现金的接受者还要保存有最近创造出的全部哈希现金记录，以判断一个哈希现金是否被用于双重支付。为避免记录的保存无限制增加，哈希现金还植入了创造的时间和日期，过于陈旧的哈希现金会被剔除出记录。

很明显，上述的手段过于烦琐，也并不能实质上封锁双重支付的所有漏洞，反而增加了接受者的验证成本。在萨博的“Bit gold”中，双重支付的避免依赖于时间戳和分布式账本。但对于一个存在异步性的网络，账本的统一需要时间，而且存在核对的成本。有没有可能从货币本身入手，保证其不存在双重支付的可能呢？

（2）RPOW 代币

RPOW 代币类似于可以重复使用的哈希现金。当哈希现金被利用 POW 机制创造出来后，它可以在 RPOW 服务器处兑换为等值的 RPOW 代币。RPOW 代币又可以继续兑换成其他 RPOW 代币，也就是说一个 POW 机制产生的哈希现金将作为一连串 RPOW 代币的基础。这些代币与哈希现金一起都可以作为数字货币使用，不过一个代币或哈希现金只能使用一次。当一名用户向其他用户支付哈希现金后，这笔哈希现金将会失效，而获得它的人可以通过将其兑换为 RPOW 代币重新获得货币价值。这样不依赖于账本的记录，数字货币之间的流通既具有了可传递性，又防止了双重支付的可能。

为了防止包括 RPOW 服务器在内的所有人伪造 RPOW 代币，芬尼希望 RPOW 代币的创造也需要必要的成本。不过不同于 POW 机制的是，这种创造的成本较低，而且创造一个新的高价值 RPOW 代币与低价值 RPOW 代币的运算难度没有区别。因为 POW 的价值依靠所耗算力作为支撑，而 RPOW

的价值依赖于其所转换的 POW。这也被称作零通胀原则，即在 RPOW 代币的创造过程中不额外产生价值。

为保证一个哈希现金或 RPOW 代币只被使用一次，RPOW 服务器会保留所有兑换过的 POW 与 RPOW 代币记录。当收到新的兑换请求后，它首先会与自己的数据库进行比对。只有未被兑换过的哈希现金或 RPOW 代币才会被 RPOW 服务器签名，之后数据库也会将这次兑换更新进去。

除了兼顾流通性与不可复制性，RPOW 代币还具有合并与分割的功能。需要储存时，任意价值的代币可以组合成一个大面值的新 RPOW 代币；需要分发给多个人时，大面值的 RPOW 代币可以再分割成小 RPOW 代币。由于每相差一字节，哈希现金的价值相差一倍，所以代币的兑换遵循二进制。假设一个人希望创造 36 字节价值的巨额 RPOW 代币，他完全可以创造 64（2^6）个 30 字节价值的哈希现金，然后将它们组合起来。这种方式相较于直接创造巨额哈希现金而言，产出更加稳定。

尽管整套 RPOW 货币体系理论上解决了萨博对于数字货币所提出的所有要求，对于 RPOW 代币兑换过程中采用的数据结构、签名方式乃至硬件设施，哈尔·芬尼也都作出了规定，但这个体系却也存在致命的缺陷：对 RPOW 服务器的高度依赖。诚然，RPOW 服务器可以尽可能的分散以保证去中心化，但它们彼此之间又产生了对维护统一的代币创造数据库的需求。归根结底，萨博的顾虑依然未能得到解决：**货币的可流通性、潜在的双重支付与去中心化记录之间究竟怎样才能找到平衡呢?**

1.3.2 比特币

从提出去中心化命题的 E-cash、创造货币稀有性的 B-money，到实现去中心化共识的 Bit gold 和允许货币重复使用的 RPOW 代币，数字货币一步步完成了从“无政府加密状态”设想到拥有成熟理论和具体实现方案的蜕变。

我们认为一个可以应用于实际并具有稳定性的数字货币体系应当具有以下特征。

（1）稀有性。稀有性指货币产生需要耗费一定的资源和时间，不存在

以比创造新货币更低成本的手段复制货币且货币不可伪造。稀有性保证了数字货币的固有价值，赋予了其价值尺度和储藏手段的货币职能。

（2）可流通性。可流通性指货币可以用于交易。交易中获得货币的一方可以继承货币的价值并用于新的交易。这要求数字货币能避免双重支付和交易回滚，并具有保值属性。为了方便交易进行，数字货币最好还具有自由分割和组合的功能。

（3）去中心化。为保证数字货币可以在整个体系中被公平创造和公平交易，其产生与流通环节的决定方式应该足够分散。基于公平开放与节点平等原则，数字货币必须立足于为所有节点所承认的共识机制上。共识机制包括对体系价值的认同、历史数据的认可和决策机制的统一。为了达成共识机制，节点放弃部分隐私权利，用以换取其他节点的信任。

之前关于数字货币的尝试已基本实现了稀有性，但是在可流通性和去中心化上总是难以兼顾。直到2008年，天才的中本聪一篇《比特币：一种点对点的电子现金系统》才完美地解决了这一切。

1.3.2.1 稀有性

1.SHA-256与哈希函数

在比特币关于工作量证明的论述中，中本聪提到了自己希望使用的函数：SHA-256。SHA-256可译为安全哈希算法，是一个经典的哈希函数。对于一般的哈希函数而言，它们可以将任意长度的输入在有限的时间内[或$O(n)$的复杂度内]计算得到固定长度的输出结果。但对于应用在安全领域来说，它们还需要具有碰撞阻力、不可逆推和无求解捷径的特性。①

碰撞阻力指的是两个不同的输入无法获得相同的输出；不可逆推指通过输出难以得到输入；无求解捷径指当加入哈希函数的参数满足高阶最小熵分布时，没有方案比单纯一遍遍尝试输入更便捷地得到特定输出。

满足这三类神奇的特性使得哈希函数可以用于加密。因为这意味着加密信息难以复制、难以伪造和难以破解。

SHA-256就是满足以上所有特性的一种函数。它可以将768位固定长度的信息压缩成256位。任意长度的信息可以切分为很多512位的小段。首先将一小段与一个初始的256位向量共同作为SHA-256函数的输入，得

① 阿尔文德·纳拉亚南等：《区块链：技术驱动金融》，2016。

到 256 位的输出后再继续与下一小段信息构成共同输入。通过这种方式，完整的信息都可以被压缩入一个 256 位的输出中。这种变换在密码学中称为 MD（Merkle-Damgard）变换。现在 SHA-256 具有了验证任意长度信息真实性的能力。

2. 哈希函数的安全性

1993 年，美国政府标准机构 NIST（美国国家标准与技术研究所）出版了一套“安全哈希标准”，但于出版后被国家安全局撤回。1995 年，NIST 再次发布了新的修订版 SHA-1，之前的版本即被称作 SHA-0。SHA-1 的固定输出长度是 160 位，曾被用作保护敏感的非机密信息。但是自 2005 年以来，密码学界不断出现了降低 SHA-1 碰撞阻力的方法。2005 年，王小云等密码学家宣称他们能在 2^{69} 次计算之内找到产生哈希碰撞的两个输入。人们不断地寻找使 SHA-1 产生哈希碰撞的方法，并由 CWI[①] 与 Google 于 2017 年宣布实现了破坏攻击。经过大约 $2^{63.1}$ 次 SHA-1 评估，它们找到了两份不同的 PDF 文件对应同一个 SHA-1 哈希值。尽管这种攻击对于普通的单 CPU 计算机意味着 6 500 年连续运算，但在算力发展日新月异的今天，这无异于彻底宣布了 SHA-1 的死刑。其实 NIST 早在 2010 年之前就向各联邦办事机构宣告了 SHA-1 存在碰撞阻力消失的风险，并要求所有依赖于 SHA-1 的应用必须在 2010 年之后应用 SHA-2 函数。[②]

SHA-2 函数共包含 6 个变种：SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256。SHA-256 是最早被公布的 SHA-2 函数，于 2001 年出现在 NIST 对美国联邦标准修订中。它与 SHA-512 分别对应 32 位与 64 位的哈希函数，使用不同的位移量和附加常数，但在结构上是完全相同的。到目前为止，SHA-2 函数还未发现碰撞，但是也已开始受到“中间相遇”[③] 攻击和 Bicliques 伪原像攻击的威胁。[④]

另外，SHA-0、SHA-1、SHA-256 和 SHA-512 函数都无法抵御长度扩展攻击。长度扩展攻击指的是当攻击者掌握有一条消息的哈希值和长度时，

① Centrum Wiskunde & Informatica，荷兰数学与计算机科学中心
② https：//en.wikipedia.org/wiki/SHA-1
③ MITM（Meet-in-the-middle）
④ https：//en.wikipedia.org/wiki/SHA-2

可以控制附带有此条信息的另一条信息。[①] 当 Merkle–Damgard 基础哈希值被误用作消息验证码时，长度扩展攻击可以在当前信息的最后附加额外信息。[②] 此类攻击对 MD5、SHA-1、SHA-2 这类基于抗碰撞加密哈希函数方法建构起来的哈希函数都是有效的。但是对于 SHA-512/224、SHA-512/256、SHA-3 等函数则作用不大。因此，现在人们已经逐渐开始转向使用 SHA-3 函数。不过 SHA-256 函数到现在为止仍然是安全的（至少碰撞阻力还没有消失），并且预计其安全性仍能维持 5 年。从中本聪发明比特币的时代来看，SHA-256 似乎已经是最安全的选择了。

3. 工作量证明机制

戴维与萨博已经将工作量证明机制（proof of work，POW）的框架搭好，差的只是寻找到一个符合要求的函数。SHA-256 的应用使得工作量证明机制真正可以用于创造货币了。利用 SHA-256 对信息进行加密，并对结果加以足够高的限制（在比特币中是要求运算结果必须以不少于特定数目的 0 开头）可以证明加密者付出了相应的算力，由此可以获得奖励。将前一信息与后一信息相关联可以保证每次加密都是独立的过程，当前一信息的加密被完成后，所有人最理智的选择就是投入下一信息的加密过程中。举个例子，如在公路上进行的长跑比赛，在确保所有人没有使用交通工具的前提下，虽然裁判没有看到运动员跑完全程，但当运动员冲过终点线时，他拥有充分的理由判断运动员已经付出了相应的努力。这种长跑比赛只取第一名。下一次比赛会换一条全新的公路。对之前跑道的熟悉和跑步名次对在下一个跑道上奔跑完全没有帮助。

在 2009 年中本聪发布的比特币代码中，他对每一次第一个加密成功的人应该获得多少比特币奖励进行了详细规范。这激励着比特币使用者一遍又一遍地完成枯燥乏味的加密工作。

4. 身份

也许很多人都有过这样的感受：在缺少证件的场合证明自己的身份是多么困难。当没有一份以国家公信力为你开具的身份证明时，其他人没有充分的理由相信你不会伪造一个身份。甚至即使你出具了身份证、户口本

① https：//en.wikipedia.org/wiki/Length_extension_attack

② https：//en.wikipedia.org/wiki/Merkle%E2%80%93Damg%C3%A5rd_construction

和所有的证件之后，办事处的官员还会满脸怀疑地看着你：“你和这上面的照片不太像啊。”这涉及我们社会关系中一个很重要的问题：个体的身份是如何获得的。

从社会的角度而言，一个人的出生是一件可以直接认定的事实，他的父母也是客观确定的。所以天然地，他就应该获得一个身份：他是他父母的孩子。但是这个身份对于社会是没有意义的，因为社会的本质是建立在人与人的沟通交往之上的。一个人真正对社会有意义的身份是他与别人产生交往时，别人对他具有特质的认定。因此这种身份是社会赋予而非自然存在的，是依赖于他人认可而非自我宣告的。例如历史书描写一个出生于中世纪的人，其身份是高贵、富有的伯爵。高贵、富有是社会对他品质的认可。每当这两个词出现在对他身份的描述中，其他人就会对他产生一个模糊的画像。伯爵则是在他所处时代人们对他阶层的定位。一个自称伯爵而无人承认的人只会被大家当作妄想症。从这里我们可以看到，身份分为自然身份和社会身份。一个社会中，重要的是别人认为的“你是谁”，而不是“你自己事实上是谁”。这种身份包含主观判断，人们既可以给予他人身份认可，也可以随时否认或撤销。因此产生了对权威身份认证机构的需求，中心化的民政部门、互联网平台再次应运而生。对于为达成去中心化社会管理的比特币来说，这很不好。

因此，在比特币的体系里只有自然身份。每一名用户就是一个地址，或者说一串固定长度的数字。一个地址的存在对于其他人的意义仅仅是这个体系中多了一分子，正如同仅仅知晓了一个婴儿的出生。对于婴儿的其他信息，别人一无所知。尽管这个地址在未来会参与创造货币，在一定的时间内将一定数额的比特币支付给另外一个比特币地址，并且收到其他人的支付。但仅仅根据这些信息，我们很难对这个人的真实身份和行为模式进行判断（在之后关于“匿名性”的论述中会继续提到），因此社会身份的建立也就无从谈起了。这种纯粹的自然身份对实现比特币体系身份平等的愿景是极为有利的，因为数字与数字间显然不存在什么高低贵贱之分。

也正因如此，比特币体系中的身份与现实社会身份并不是一一对应的关系。一个人可以拥有许多个身份，许多人也可以共用一个身份。这与我们传统的身份认知方式不同。在传统的认知中，虚拟身份与真实身份越对应越好，

因为两个身份的对应可以增加交往的确定性，将真实世界中的权利义务传递到虚拟世界中，把虚拟世界作为真实世界的延伸。比特币的初衷从一开始就与这一观念不同，它就是要打造一个从身份到社会关系都完全重新建造的社会。

在个人的能力被无限放大的时代，人本主义思想改变了我们对于社会的想法。我们与社会发生联系的原因越来越多地在于个人能从社会中获利，而不是天生地就认为自己是社会的一员。社会整体带给成员的效用在逐渐被个体与个体之间的互利行为所代替。层级化的社会不断坍塌，人际信任不断被拉扯。社会的惯性依然强大，而新时代的“三大改造”已悄然而至：身份数字化、结构扁平化、社会碎片化，哪一个将成为第一个碾向我们社会关系的车轮？

现在的社会规则已经很明确，对于新生代的年轻人而言改变的阻力巨大。不过他们手中掌握的技术复苏了一个古老的想法：能不能让社会重新签订一遍契约？

“法律和制度必须与人的思想同时前进。”托马斯·杰斐逊[①]在他对民主的设想中曾产生过这样的思考：能否让全体美国公民每 20 年重新签订一遍社会契约，以保障每个人都拥有参与社会契约制定的权利。这种思想很类似于把社会秩序的搭建交由人的自然身份而非社会身份。因为自然身份下，个体与个体从形式上没有差别。这是最符合罗尔斯的公正原则的。

前面我们已经阐述过“盲签”机制的实现，认证者可以在不接触信息的情况下对信息签名进行认证，这成为比特币创造身份的基础。利用数字签名方案中的 Generate Keys 程序，可以同时生成一对私钥和公钥。在这里中本聪还进行了一个巧妙的设计，就是采用椭圆曲线算法（ECC）来生成私钥和公钥，而非常见的 RSA 算法。尽管后来传出了 RSA 算法留有可降低难度的后门的说法，但 ECC 却一直十分稳固。也许这的确是一点小小的运气成分吧。[②]

比特币将地址设置为公钥的哈希值（其实还需要经过一步 Base58 算法，

① Thomas Jefferson，（1743.4.13—1826.7.4），美利坚合众国第三任总统（1801—1809 年在任），同时也是《美国独立宣言》主要起草人，美国开国元勋之一。

② 阿尔文德·纳拉亚南等：《区块链：技术驱动金融》，2016

但由于这个算法是可逆的，所以可以把地址等同于公钥哈希）。由于哈希函数的特性，人们可以轻而易举地验证地址与公钥的对应关系。“公钥即身份”是一种很形象的说法，人们通过私钥加密自己的信息，再由他人通过公钥确认身份。这种公钥由随机数产生，可能结果足足有 2^{256} 种之多。两个由完全随机数产生的公钥出现相同的可能性微小到完全不必担心此类情况发生。现在有很多比特币钱包，申请人注册时无须提供任何的身份校验信息，唯一需要的是接受私钥的邮箱地址。当申请人收到私钥时，他就正式成为比特币体系中的一员，可以接受、分发和开采比特币，并参与维护比特币共识。需要注意的是，为保证公钥的唯一性，密钥必须随机产生。任何相同的随机来源或可预测的随机都将导致对公钥安全的潜在威胁。

无论一个地址后面藏着多少现实生活中的人，还是一个闲得无聊的人注册了多少比特币的地址，比特币世界对待每个地址都是一视同仁的。地址对地址的信任当且仅当建立在公钥验证成立的条件下。你与我都是一串数字，很平等不是吗？

5. 创造比特币

知晓身份和哈希函数两个概念，我们就可以理解比特币体系中最为精巧的一步：创造比特币。在早期关于比特币的经典著作《区块链：技术驱动金融》原版序言中曾经对这一过程有非常经典的论述：“B-money 和 Bit gold 通过数字计算直接创造货币。任何人都可以解题，答案本身就是货币。但在比特币体系中，解决数学计算并不构成货币，这是确保区块链安全，间接地在有限时间里创造新货币。”

在比特币的世界里，货币创造可以理解为一次没有支付者，只有接受者的交易（关于“交易”的具体细节我们会在之后谈到）。这笔交易的作用是为完成了工作量证明的一个身份增加特定数目的比特币。在中本聪的时代，完成一次工作量证明（或者说打包一个区块，“区块”这个概念将出现在 1.3.2.2 小节“数据结构”中）可以获得 50 个比特币，此后每进行 210 000 次工作量证明衰减一半。工作量证明的难度每 2 016 次进行一次自动调整，使其平均难度接近 10 分钟一次。这样计算下来，每经过大约 4 年，奖励的比特币就会折半。2018 年年末完成一次工作量证明的奖励已经降为 12.5 个，并将于 2020 年进一步衰减为 6.25 个，直到 2140 年，奖励衰减为

50/8 589 934 592 比特币，这个数额已经小于比特币体系中的最小金额一聪（1/100 000 000 比特币），这时创造比特币的过程将全部结束。利用等比数列求和，我们可以轻松地得到那时比特币的总量：2 100 万（实际上是 20 999 999.976 9）。因此比特币的创造是一项越来越缓慢并且有明确截止期限的过程。到 2019 年年末为止，已经有超过 1 800 万枚比特币被创造出来，接近总量的 4/5。

改变这个既定上限从理论上来讲是可能的，只要足够多的用户同意。但问题是增加比特币的供给对所有拥有比特币的人来说无异于一种通货膨胀，理性的他们并没有这样做的激励。只要还有比特币的用户坚持 2 100 万这个上限，在他们的体系中比特币的供给就是确定的。当然完全有可能有足够多的人抛弃了这个上限，而对另一个数字达成共识，但那就是另外一种数字货币的故事了。

哈希函数的特性支撑了工作量证明的有效性，确保创造比特币是一件费时费力且难以伪造的过程。每一次货币创造都关乎一个自然身份，使得每一个比特币本质上都是独一无二的，但在功能和价值上又是完全替代的。这就是比特币作为数字货币所必备的稀有性的来源。

1.3.2.2 可流通性

1. 数据结构

（1）时间戳

人们常常混淆比特币与区块链两个概念，足以见它们关系的密切。区块链，按照我们开头给出的技术定义，正是比特币的数据结构基础。

区块链的理论最早可以追溯到 1991 年哈勃[①]和斯托尔内塔[②]针对音像版权证明设计时间戳的构想。在最早的一篇论文[③]中，他们论证了一种神奇的“盖章”方法——为每份文件生成一个根据文件内容和产生时间创造出来的章，把一份文件的生成日期与文件内容牢固地结合起来。生成章的方法需要满足一个章对应一份文件。敏感的读者此时会联想到我们刚刚提到的一种神奇的加密方法——哈希函数。不错，哈勃和斯托尔内塔的确采用的就是它。

① Stuart Haber，时间戳记录最早的提出者之一。

② W. Scott Stornetta，时间戳记录最早的提出者之一。

③ Stuart Haber，W. Scott Stornetta，“How to Time-Stamp a Digital Document”，1991.

他们一共给出了两种方法：第一种是把需要“盖章”的文件交给 TSS 服务器（time-stamping service），由它们盖章完成后与之前和之后的文件串成链。但这种方法又陷入了中心化的困境。因此他们给出的第二种方法是以文件的哈希值为种子，通过伪随机数生成器选中一个用户池，由用户池对文件进行盖章。由于哈希值完全遵循随机分布，以此种方法选择的用户池也将满足完全随机。文件的“盖章”就实现了彻底的自实现。

哈勃和斯托尔内塔认为这种加盖时间戳的方式甚至可用于生成时间没那么重要，但需要保证不可篡改的文件。他们甚至预测不会有比盖时间戳更具有效力的认证方式了。截至目前，各种数字货币的数据结构基本沿袭了时间戳的想法，说明这种说法可能并不过分。

区块链的数据结构就是把数据按照单向链接的方式连成一串，这与时间戳的设想不谋而合。时间作为矢量非常特殊，它只在一个方向上具有意义，这正是区块链追求的单向性。现在每一个区块链上的文件都包含了三项内容：文件信息、产生时间和指向前项文件的哈希指针，形成了完美的单向延伸结构。

（2）查找方法

不过单向延伸的意义在于阻止伪造文件，而不能阻碍查找。当前的线性哈希链查找的时间复杂度为 O（n），这太长了。在这里有必要介绍一下时间复杂度的概念。时间复杂度是计算机科学中形容算法所花费时间量的计算复杂度。[①] 时间复杂度提高，意味着计算花费的时间要提升一个或几个量级。在这里我们仅涉及一对简单的比较，即 O（log n）远小于 O（n），如图 1-3 所示。

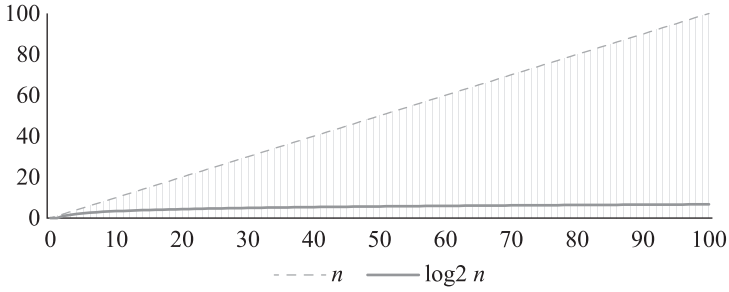

图 1-3　时间复杂度对比

① https：//en.wikipedia.org/wiki/Time_complexity

为了达到降低时间复杂度的目的，我们有两个备选方案：一种是梅克尔树；另一种是跳跃列表。

梅克尔树又称二元哈希树，是一种以根节点为起点，不断二分链接叶节点的非线性数据结构如图 1-4 所示。

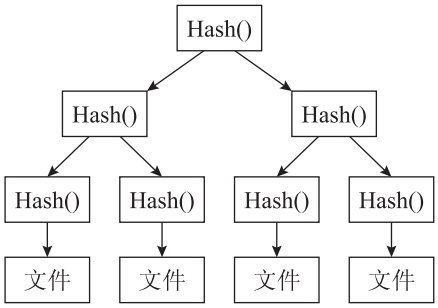

图 1-4 “梅克尔树”

通过这种方式查找数据的复杂度可以直接降为 O（log *n*）。例如对一个具有 1 024 个数据的线性哈希列而言，从末尾向前查找位于第 3 个的数据需要进行 1 021 次计算，而通过梅克尔树组织起来的数据只需要 10（$\log_2 1\ 024=10$）次就够了。随着数据量的进一步增加，这种计算复杂度上的降低会更加明显。

跳跃列表则是按层构建的。底层还是有序的线性哈希链，上层则充当查找的快速通道。每一层的元素在下层出现的概率均为 1/2（或 1/4）。查找方式为从顶部列表的头部元素开始，水平前进查找。如果遇到的元素等于待查找值，则已找到；如果小于待查找值，则自动转入下一层进行查找，然后重复此过程，如图 1-5 所示。

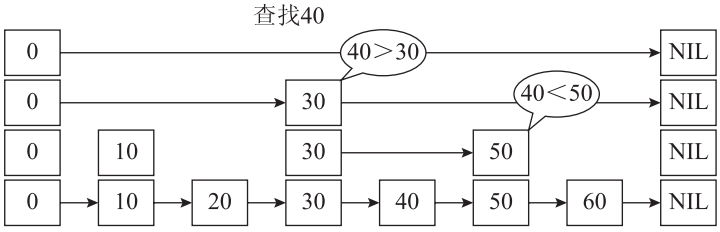

图 1-5 “跳跃列表”图

尽管跳跃列表在实践中更容易实现，但它的缺陷也很明显。底层哈希链的排序必须有一个较强的量化指标以便于比较。而对于我们要建构的数

据结构来说，哈希链的排序依赖的是时间戳。查找一个数据内容是否存在于哈希链上的人很难同时拥有数据产生的确切时间，从而无从查起。

因此，梅克尔树是一种更好的选择。比特币的改造方式是把一部分数据打包成区块，在区块内部运用梅克尔树的结构，再让梅克尔树的根哈希值构成线性哈希链。这样既增加了查找效率，又避免了梅克尔树多向延伸的弊端。

（3）隶属证明与非隶属证明[①]

当一个人宣称自己拥有的区块已被记录在区块链上时，他首先要向验证者公布区块通往所在梅克尔树根节点路径上的所有区块。由于哈希函数的性质是实际上不可能找到两个不同的输入对应同一个输出，所以伪造一份文件的哈希值必定不能与另一个哈希值共同输入得到父节点的哈希值。这样仅通过展示梅克尔树的有限部分（假设梅克尔树包含 n 个区块，则只需要公布 $\log_2 n$ 个区块，这个比例相对于全部区块总数是极其微不足道的）就可以验证到根节点。再通过线性哈希链查找有无这个根节点出现，就可以判断数据是否已经被区块链所记录过。同样，如果验证者了解到位于待查数据时间戳前后的区块在树上是连续的，那么待查数据必定不存在于区块链上。

2. 比特币的交易机制

（1）交易的实质

我们介绍比特币数据结构的核心意义在于理解比特币的交易机制。现在我们知道，记录在比特币区块链上的记录都是可以便捷地验证和溯源的。让我们思考一下交易的实质是什么：交易是双方各取所需的过程。对于以物易物的方式，交易使双方直接获得了生产生活资料。对于用商品或服务换取金融资产（如货币、证券等）的方式，付出商品或服务的一方希望获得的其实是一个凭证，证明自己曾付出的劳动。他们只是暂时性地没有将这笔劳动转换为直接的生产生活资料，而是储存了起来。当他们下次向其他人出示这张凭证时，他们希望其他人可以认可自己之前的劳动。因为这种凭证需要他人相信才具有价值，所以我们称这种交易模式为基于信用的交易。

作为信用交易的媒介，我们需要凭证具有保值和流通的性质。黄金，因储量固定、难以开采而具备稀缺性，具有保值作用；比特币，因总量固定、难以创造而具备稀缺性，因此是一种“数字黄金”。黄金，化学性质稳定，

① 阿尔文德·纳拉亚南等：《区块链：技术驱动金融》，2016。

易于分割和交换，无法双重支付，所以具有流通价值；那么比特币该如何实现可流通性呢？

（2）比特币的生命周期

数字货币没有物理形态，因此复制相对容易。虽然比特币创造起来困难，但是如果创造出来可以支付任意次数，显然也是不能作为流通货币的。在之前关于 RPOW 代币的介绍中，我们已经思考过这个问题。哈尔·芬尼对这个问题的想法是每完成一次支付就销毁一次货币，接受者再转换一个等价值的新货币。中本聪延续了这一构想。一定数目的比特币自从被获得之后要么静静地躺在一个地址中，要么被完全地花费出去。如果比特币的价值高于支付金额，就创造两个新的货币，一个支付给交易对象，一个支付给自己的账户。这样算来，这部分特定数额的比特币的生命周期其实只有一次支付过程。例如一个地址从上一次交易中获得了 8 个比特币，但只希望购买价值为 5 个比特币的商品，那么它仍然要将全部 8 个比特币支付出去。交易对象与自己的账户各获得 5 个比特币和 3 个比特币。这 3 个比特币的获得相对于上次 8 个比特币是完全独立的。我们还可以拿现实生活中的纸币作类比。例如我们交给银行一张破损的 100 元纸币，银行将其销毁后还给我们一张 50 元的纸币，并将剩下的 50 元留在银行作为手续费。这个过程货币总价值没有任何改变，只是面值变得更小了。

（3）交易结构

表 1-1 所示为在比特币官方文档 https：//en.bitcoin.it/wiki/Transaction 中对于比特币交易结构的划分。

表1-1　比特币官方文档中对于比特币交易结构的划分

项　　目	附　　注	大　　小
版本号	现在是1	4字节
输入计数	非负整数	1～9字节
输入列表	区块中第一个交易的第一个输入被称作“币基”	不限
输出计数	非负整数	1～9字节
输出列表	区块中第一个交易是给矿工的奖励	不限
锁定时间	如果非0且块序号小于0×FFFFFFFF，那么就指区块高度；如果是区块最后一笔交易，则指的是时间戳	4字节

可以看到一笔比特币的交易输入与输出是不受限制的，因此既可以是多个地址共同支付，又可以是一个地址多向支出。

既然发生支付，就必然涉及两个核心问题：支付者有没有那么多比特币，支付行为是否是支付者的真实意愿。这里我们将要澄清一个非常重要的概念：去中心化账本。在中心化的账本中（如银行），中心化机构可以查验每名用户的账户余额，通过要求提供身份证件、输入密码等方式完成身份核对。去中心化账本则有基于账户和基于交易两种。基于账户指的是网络中所有节点拥有全部节点的实时余额，每一笔交易发生之后都要迅速在账户上进行改动。在存在异步性的网络中，这种要求是灾难性的。因为节点之间的交易不能及时被所有节点记录会导致节点间的账本出现差异，而且彼此之间统一成本太高。投票决定的方式同样不可行，既然交易信息都无法实时传播，又如何在同一时间点进行投票呢？很多人的印象中比特币与区块链仿佛就是一种基于账户的去中心化账本，这其实是不正确的。

比特币采用的是基于交易的分布式账本，这正是比特币吸收 RPOW 代币精髓而产生的创新。由于每个比特币的创造过程是不同的，所以比特币可以实现与上一交易相关联而非与所在账户相关联。上文提到比特币的存在周期只有一个交易周期，因此每个比特币指向之前交易信息就意味着每个比特币携带有其从被创造伊始到当前交易的全部来龙去脉。支付者有没有比特币的检验就变成了找到生成此比特币的上一笔交易是否被记录在链上。每一枚比特币都带有独一无二的历史，听起来很有趣不是吗？

采用基于交易的分布式账本还有几个好处：一个是支持了交易的并行验证，因为每笔交易都是独立验证的而且并不严格排序；另一个是避免了通过注册垃圾账户导致账户信息暴增而引起的网络瘫痪，这种攻击也可被称为女巫攻击，我们在下文中会继续提到它。

关于确定支付者是否拥有比特币所有权的问题，我们不如先来看一笔简单的比特币交易输入[①]：

① https：//blog.csdn.net/pure_lady/article/details/78654570

Previous tx 指所关联上一区块的哈希值，index 指该区块中的第几笔交易。以上两样信息就是待支付比特币的“上辈子”身世。ScriptSig 被称作签名脚本，由公钥和对应私钥持有者的签名链接而成，作用是确认支付者的支付权利。这就是对支付者是否愿意进行这笔交易的认证。

除了在去中心化账本上进行创新，比特币还创造性地加入了“矿工”这一角色。以上我们所说的两种验证，都是由专职的“矿工”完成的。他们负责比特币的创造、脚本运行和交易校验，相当于维护比特币系统的安全员。对他们的工作，比特币系统设计了两种奖励：挖矿奖励与交易费。挖矿指的是把众多交易记录按照梅克尔树的结构组织起来，计算出哈希值并链接到当前最长链的末尾。

这里展示有比特币的区块结构，如表 1-2 所示。①

表1-2 比特币区块结构表

项　　目	附　　注	大　　小
魔法数	常数，值为0×D9B4BEF9	4字节
区块高度	区块之后部分的大小	4字节
区块头	由6部分组成	80字节
交易计数	非负整数	1～9字节
交易列表		差异较大

每个交易列表包含至少一个交易，就是位于交易列表首位的“币基交易”。它与其他交易唯一的不同之处就在于这笔交易的输入没有关联区块。为了直观地了解它，在这里把最原汁原味的币基交易数据呈现给大家。

01000000010000000000000000000000000000000000000000000000000000000000000000ffffffff4d04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73ffffffff0100f2052a01000000434104678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5fac00000000

如果不是对比特币有着狂热爱好的人，看到这个由 430 个杂乱无章的

① https：//en.bitcoin.it/wiki/Block

数字构成的字符串，第一反应一定是把它跳过去。的确，在没有切分之前，这只是一个普普通通的十六进制数。不过，当你知道它就是中本聪创造最开始的 50 个比特币的币基交易时，有没有产生一点点想了解它的兴趣呢？

我们用表格的方式对它进行拆解，如表 1-3 所示。

表1-3　币基交易数据表

01000000	版本号
01	输入计数
0000000000000000000000000000000000000000000000000000000000000000000000000000	前项交易ID
ffffffff	输出序号
4d	签名长度
04ffff001d0104455468652054696d65732030332f4a616e2f3230303920436861e63656c6c6f72206f6e20627269e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73	签名脚本
ffffffff	序列号
01	输出计数
00f2052a01000000	输出的比特币价值
43	公钥脚本长度
4104678afdb0fe5548271967f1a67130b7105cd6a828e03909a67961e0ea1f61deb649f6bc3f4cef38c438c435504e51ec112de5c384df7ba0b8d578a4c7026bf11d5fac	公钥脚本
00000000	锁定时间

由于这笔交易是币基交易，所以并不存在与这笔交易关联的前项 ID。因为这些数字遵循的都是十六进制编码，所以十进制下的签名长度是 77 位，对应下面的签名共 154 位。这一签名是支付者的签名加公钥，不过对于币基交易而言，不存在支付者，所以这段空间就成为矿工们自由发挥的场所。中本聪在比特币第一个币基交易的签名脚本中留下了这段著名的黑色幽默：“当时正是英国财政大臣第二次出手疏解银行危机之时。”

币基交易的输出也由三部分构成：生成的比特币数目、公钥签名长度和公钥签名。如果我们调换 00f2052a01000000 的字节存储次序，再转化成十进制数字，就可以得到 5000000000。这正是第一个区块创造出的按聪计价的比特币数目。之后的公钥脚本包含着中本聪使用的地址（公钥的哈希值）。

除了币基交易，其余的交易都会存在输入的比特币金额和输出金额。

如果输入小于输出，这将是一笔无效交易而被矿工舍弃。如果输入大于输出，中间的差额部分将作为交易费成为矿工的另一部分激励。

（4）比特币的脚本

每笔交易不止包含输入输出的地址和交易金额，它同时还指定了一个脚本。由于比特币的地址只是公钥的哈希值，所以地址既未告诉我们公钥所在，也未提供一种检验签名的方法。因此我们需要比特币脚本，将交易输出转化为这样的描述："凭借哈希值为 X 的公钥，以及这个公钥所有者的签名，才可以获得这笔资金。[①]"

比特币脚本要求交易的输入脚本与上笔交易的输入脚本串联起来，以确保本次比特币的使用是从已经确认的上笔交易中正当获得的。由于比特币的脚本太过技术性，我们在这里更多的关注这些脚本能为比特币的交易机制带来什么作用。实际上，它赋予了比特币更多的交易模式。

目前比特币的脚本存在两种类型——Pay-to-Pubkey Hash 与 Pay-to-Script-Hash（P2SH）。[②]Pay-to-Pubkey Hash 就是把我们上述的公钥脚本与签名脚本联系起来，完成最简单的支出和收取。由于这种交易模式需要提前知道整个公钥，这就意味着更长的支付地址与 ECDSA 签名中断时更少的保护，因此在现在版本的比特币中已经不再经常使用。

P2SH 主要解决两方面问题：支付工作的简单化和矿工追踪输出脚本的复杂度，这使得"多重签名"成为可能。多重签名是比特币脚本体系中的一个指令，作用是使得交易必须经过多人共同签署才能生效。多重签名的应用非常广泛，如第三方支付。这个想法其实早在戴维的 B-money 中就有雏形。在 B-money 的体系里合约可以数字化，利用特殊账户与仲裁方作为公信力的背书。在第三方支付中，仲裁方与特殊账户合为一体，因此在交易中拥有更强的影响力。在整个交易体系中，合约双方与第三方中任意两方签署交易都可以使交易生效，从而划走比特币。当交易正常进行时，双方可以在商品或服务给付完成后共同签署；当交易双方发生龃龉，就交易的完成情况存在分歧时，双方就可以交由第三方决定。第三方与其支持的一方可以共同决定比特币的流向。这样的方式也可以用于投票。因为比特币的交

① 阿尔文德·纳拉亚南等：《区块链：技术驱动金融》，2016。

② https：//en.bitcoin.it/wiki/Script

易中没有对输入的数目划定上限，所以可以设计当 50% 以上的投票者签署时就自动完成比特币的支付。

即使只有两方，多重签名仍能发挥重要作用。对于一个施工单位来说，其不希望委托方把资金支付一次性地放到最后，否则它们要承担委托方的破产及拖欠的风险。对于委托方而言，阶段性支付施工单位对自己也有诸多风险。如果工程质量最后验收不合格或施工单位中途退出，委托方将遭受重大损失，支付的工程款也未必能得到追偿。因此可以设计这样一种交易方式：委托方将全部工程款转入一个多重签名账户，同时要求这笔交易需要双方同时签署才能有效。然后每一阶段委托方进行一次签署，从多重签名账户向施工单位进行一次支付。同样需要委托方完成全部的签署和施工单位才能生效。这就意味着一旦施工单位违约，委托方将拒绝签署第二笔交易，施工单位也就无法从多重支付账户中获得比特币。而委托方违约将导致施工单位签署最开始转入多重签名账户的全部工程款，从而避免委托方转移资金。只有当双方共同签署两份交易，交易才能完全地被记入区块链，资金才能顺利地从委托方账户通过多重签名账户转移到施工单位账户中。另外，还记得交易最后的锁定时间吗？它的作用是让矿工们在一定时间之后才把这笔交易放到区块链上。利用锁定时间可以实现交易的延后性，可以保证在施工单位恶意拒绝签署的情况下让委托方从多重签名账户拿回比特币。

类似的应用还有很多，主要集中在小额支付、共同财产处置、低信任管理等领域。

具备了可交易、可验证、可自由分割组合和保值功能的比特币现在拥有了良好的可流通性。如果排除去中心化要求的话，它现在已经是一个完整的货币体系了。

1.3.2.3 去中心化

这是比特币最后一个要解决的难题，也是比特币最颠覆性的创造。接下来，我们将为大家讲述比特币是如何维护稳定的共识机制、保障区块链的安全性并保持比特币的价值的。这三者神奇的相互作用实现了比特币的完全去中心化。

1. 共识机制

共识机制是去中心化要解决的关键问题。中本聪和比特币最初使用者

的初衷都是希望创立一个不依赖于传统中心化信用机构背书的货币体系，所以要求货币使用者之间就货币使用、流通、贮藏等问题达成一致。如前所述，比特币的使用依赖于分布式的记账协议。当各节点对一笔比特币的币基交易进行认可，这笔交易创造出的比特币才会在矿工支付时被接受。一笔交易使用的比特币也要依赖于与该比特币关联的上一笔交易，又涉及对上一笔交易是否有效的判定。如何进行认可和判定，就是我们所关注的共识机制。

为什么我们认为将共识机制简单地理解为基于账户的分布式账本极为有害，因为在数字货币的世界中没有中心化的机构与各节点直接相连。节点间的拓扑结构错综复杂，部分节点可能存在恶意或宕机，网络通信可能存在延迟，更为重要的是缺少统一的时间标准。在中心化的世界中通过全覆盖广播、依据社会身份赋予不同权利、按照时间顺序进行规定等方式在比特币世界失去了效果。那么比特币体系中的节点之间如何建立沟通、达成共识呢？

2. 一致性

达成共识机制相当于达到计算机科学中分布式系统的一致性。由于分布式系统能增强系统的可用性，防止单点故障引起的系统宕机，同时提高系统的整体性能，在负载均衡技术的帮助下让不同地方存储的数据副本都能为用户提供服务，如何解决分布式系统的数据复制在计算机领域具有重要意义。[①] 一致性的强度十分多样，可以粗略地分为强一致性和弱一致性。强一致性非常直观，就是系统写入用户输入后，在用户调取时可以立即给予输出。这对系统性能要求太高，至少要存在一个全局时钟，在每一个时钟周期结束前将每一次写入都存储在所有处理器的高速缓存中。[②] 弱一致性则是在用户写入后并不保证能立刻读到写入的值，也并不承诺多长时间后全局能就数据达成一致。其中存在一类比较特殊的最终一致性，指的是系统保证在一定时间内能够达到数据一致的状态。最终一致性是业界在大型分布式系统设计中比较推崇的一致性模型，也为比特币所采用。

最终一致性对数据同步的要求是在数据被下一次读取之前应当满足以下三个要求。

① https：//blog.csdn.net/en_joker/article/details/78604625

② https：//en.wikipedia.org/wiki/Consistency_model#Slow_Consistency

（1）读取修正：当读取过程发现存在不一致时，应当能对读取及时更改，尽管这会延缓读取过程。

（2）写入修正：当写入过程发现存在不一致时，应当能对写入及时更改，尽管这会延缓写入过程。

（3）异步修正：修复过程本身不是读取或写入的一部分。

接下来让我们观察一下比特币达成共识的过程，其完美地符合了以上三个要求。

3. 比特币的共识机制

当一笔交易产生的时候，比特币全网是这样达成共识的：

（1）比特币的支付者向与之建立联系的矿工广播这笔交易（建立联系的过程在成为比特币节点时就已完成）。

（2）随时都在监听周围交易的矿工验证交易签名是否有效，以及交易输出是否是一笔双重支付。

（3）矿工监听最新的区块，并确保这个区块是有效的，即其中每笔交易有效，区块的哈希值也满足最新的难度要求（作为一名希望获得比特币的矿工，他可不希望自己没发现这一点而其他矿工意识到了，因为这意味着自己在这条区块后面进行延伸的区块不会得到其他矿工的承认，通过币基交易创造的比特币也无法支付出去）。

（4）矿工开始在自己认定的最新区块后面组建自己的区块。这一过程包括确认即将放入的每笔交易有效并按照梅克尔树的结构组织监听到的交易。（还记得区块结构中的交易列表吗？）

（5）矿工开始进行哈希计算，使得打包好的区块哈希值符合全网要求的难度水平。这是一步耗时耗力的过程，在现阶段需要依赖专门进行哈希计算的设备才能完成，这也是比特币达成共识的过程中需要花费巨额成本的原因所在。

（6）最先找到打出有效区块的矿工会迅速向全网广播。接收到此信息的矿工会停下当前区块的打包，排除自己正在打包区块中与最新有效区块的交易重叠部分，加入新监听到的交易并重新开始计算哈希值（因为其链接的上一区块哈希值已发生改变），然后开始新一轮的（2）～（5）过程。

（7）发现交易被记入最新区块的比特币接受者会继续等待，他要确保

这笔交易所在区块后有足够多的区块延伸，以保证交易确实是在比特币记录的最长链上（通常等待时间是 6 个区块，因为 6 个区块之后该笔交易所在区块仍不在最长链上的概率已经微乎其微，等待更长的时间没有实际好处）。

（8）比特币接受者向支付者支付商品或服务，而这笔比特币的转账成为比特币交易记录的一部分。所有及时同步区块信息的节点都能看到这笔交易，这时节点之间对这笔交易的记录达成了一致。

什么时候会出现不一致呢？就是当矿工对某一区块生成的合法性存在质疑或对区块内的某笔交易存在质疑时。比特币设计的机制并不是全网进行表决（在异步性的网络里这肯定行不通），而是“用脚投票”。如果矿工认为某一区块不合法，他就可以在其之前的区块上进行延伸，或者说分叉。如果其他矿工也这么认为，他们就会在分叉的这个区块后面进行延伸，之前的那个区块由于无人延伸而成为“孤块”，从而被排除在比特币的最长链之外也就不属于比特币共识的一部分。如果一笔交易不合法（如属于双重支付），就不会有矿工愿意将其打入自己的区块而增加无人延伸自己区块的风险。尽管整个流程没有任何投票式通信，但矿工通过自己的行为完成了对区块和交易认可的表决。

把这种机制与最终一致性达成的条件进行对比。数据下一次被调取是在上一次输出的比特币即将被支付给另一地址的时候。写入修正指的是在有问题的交易希望被写入区块链时，矿工及时甄别并舍弃此交易从而修正不一致。读取修正是在这笔支付被打包进矿工的区块时矿工对其进行的检验。如果矿工发现交易有误，他会拒绝在包含此交易的区块后延伸区块，并随着更多的矿工发现这个问题，包含这一交易的区块逐渐被排除在最长链之外而修正总体账本。

4. 打破不可能

Edsger W. Dijkstra 分布式计算奖 2001 年颁给了一篇只有 6 页的论文，因为它包含了一个分布式领域最为重要的结论——Fischer-Lynch-Paterson 不可能性，或简称 FLP 结论。它说的是在多个进程组成的异步系统中，哪怕只有一个进程突发性地不可靠，都无法达成一个完全正确的异步一致性协议。这个结论是如此的骇人听闻，因为它的假设十分简单：没有对进程

的处理速率和信息传输延时的假设，没有对信息系统是否可靠的假设，只是假定网络的异步性和一个进程无法判断另一个进程是否不可靠，因为另一个进程可能只是在慢速运行。这个不可靠的进程可以是崩溃、丢失或损坏信息，甚至发送恶意信息。如果我们不再进一步对计算环境进行进一步的假设和容忍错误类型的限制，三位分布式系统领域的专家下了定论：就是无解的。

尽管论文的最后给出了一种弱化方案：如果运行过程中没有进程死掉，同时有半数以上的进程是正常的，那么就存在一个部分正确的一致性协议，可以保证所有正常的进程可以达成协议。但这对于需要所有人就每一笔比特币交易都达成一致的比特币系统来说（试想一下现实生活中存在有一些货币不被部分人接受的混乱吧），这仍然是远远不够的。FLP 不可能性导致部分人改为着力去研究同步系统，因为同步系统下的拜占庭将军问题在部分进程出错的条件下仍然存在解（关于同步系统下的拜占庭将军问题我们将在第 3 节具体解释）。这个结论的权威性显然是不容置疑的，在中本聪给出的比特币方案中也并没有对 FLP 不可能性进行挑战，不过他却换了个角度巧妙地解决了这一点，就是引入一个在之前设计分布式系统时完全没有被考虑过的因素：激励。

激励对于分布式系统设计的改造正如同把蒸汽机安在轮子上一样：喔，原来还可以这样。虽然比特币的共识按理论是不可能达成一致的，但到 2019 年为止它运行了 10 年，情况却比很多分布式领域专家预测的要好得多。因为激励机制的出现，并没有改变进程仍会存在崩溃或作恶的事实，但是却大大提高了他们这样做的成本。在理性的状态下，进程最有利的就是按部就班处理数据。整个体系处于一个纳什均衡的状态。在其他节点不改变行为的条件下，节点没有理由改变现在的行为。究竟比特币的设计存不存在纳什均衡，存在多少纳什均衡解的问题仍在讨论，但从现实来看，应该是有的。

比特币引入激励机制让体系内的比特币持有者都倾向于维护体系稳定和安全，这样他们自己手中的比特币才有价值，才能被花费出去。比特币并不要求人们更道德，只是遵循了人们逐利的本性，问题就圆满地解决了！当然，有激励就有惩罚，不过比特币体系的惩罚方式不过是不给奖励。由

于构造区块计算哈希值的过程需要消耗巨大的算力，现有技术不再能成倍地提高比特币的挖矿速度，导致这实际上变成了一场比拼电力的竞赛。高昂的电力成本使得不获得比特币奖励就是对恶意者的惩罚。

除此之外，比特币还引入了我们上文所提到的最终一致性。它并不要求共识能迅速地对每笔交易进行确认，只是告诉大家多等等。随着时间的流逝，每个节点对一笔交易的认识会与其他节点趋于一致，当这个概率足够高的时候，就可以认为所有人达成了一致。

5. 稳定三角形

共识机制的确立保证了比特币账本的安全性，比特币的安全性赋予了比特币价值，比特币的价值又激励着共识机制的确立。这三者形成生物学意义上的正反馈循环，促使比特币体系不断向安全与稳定的方向发展。这给了其他数字货币开发者一点启示：在体系建立的初期要尽可能创造这三种条件，使体系进入正反馈循环，如召集更多的算力加入以增强安全性，或利用其他方式保证体系初期只存在诚实节点，或者提升数字货币的价值。事实上绝大多数现在数字货币的实践都是同时促成这三种条件。关于这部分的进一步讨论我们放在了第 3 篇关于“通证经济学”的讨论中。

6. 安全性

比特币的安全性是一个很值得研究的大问题。就目前看来，比特币的安全性良好，经过 10 年的运行这个体系变得更稳定，而不是像哈尔·芬尼接受中本聪的第一笔比特币支付时那样对交易是否会被接受一无所知。关于各类可能的攻击形式，我们仅在此介绍它们的目的、方式和比特币的应对策略。对于技术实施的细节，我们推荐大家参考一些更为专业的书籍。

（1）双重支付

双重支付攻击在前面已经有所提及。总而言之，在攻击者没有掌握绝对算力时，其他矿工会因为激励机制废弃双重支付交易和其所在区块，导致攻击者遭受损失。掌握绝对算力之后，由于比特币打包区块过程并不是一个“赢者通吃”的过程，而只是概率占比更大。当然一直保持概率更大从概率计算的角度确实能使得双重交易成功（即使比特币接受者等待了 6 个区块才支付商品或服务），但这种维持算力的成本过于高昂。而且当其他节点意识到攻击发生时，它们会因为安全性的崩塌而放弃比特币体系，这会打击比

特币的价值并降低双重支付的收益。逐利的矿工并不会这样做。

（2）女巫攻击

女巫攻击指的是黑客恶意制造大量节点导致混乱，因为在比特币中女巫攻击只是自然身份的创造，而比特币给予每个自然身份的权利都是相同的：贡献算力来获取比特币和自由使用它们。制造更多的节点既不会增加算力，也不会给予节点更大的使用特权，所以女巫攻击只是徒劳的。另外，基于交易的分布式账本也避免了女巫攻击造成存储崩溃的局面。

（3）盗用比特币

盗用的发生只可能在私钥发生泄露的时候，不过这已经是比特币体系之外的事了。毕竟比特币以自然身份为节点，不能保证在用户受到威胁或诱骗而吐露私钥时，对其真实的社会身份进行验证。如果用户的私钥没有丢失，哈希函数的性质告诉我们：盗用就是不可能的。当然，拥有 SHA-256 也并不就能就让我们高枕无忧了。它也有被日益提升的算力攻破的可能，但至少还需要一段时间。

（4）黑名单攻击

这是一个理论上存在的攻击方式。例如一名占有全网 0.01% 算力的矿工宣称自己不会将来自 A 地址的交易打进区块里，并且不接受任何打有含 A 地址交易的区块。虽然拥有这一点点算力的矿工貌似并不会改变其他节点的行为，但请让我们从概率的角度思考。如果一名其他的矿工打了含 A 地址交易的区块，它的区块下一次被延伸的可能性只有 99.99%；而如果它不打含 A 地址的交易，假如自己挖到区块，被承认的概率将是 100%。如果矿工打进 A 交易获得的交易费小于他打整个区块的收益乘以 0.01%，他理性的选择就是不把这笔交易放入区块，于是最后 A 的交易就真的没有矿工愿意打入区块。A 相当于上了比特币的黑名单，它再也无法使用比特币了。不过这种攻击也有前提，就是 A 需要把这种想法让绝大多数矿工知晓，而这是很困难的。另外如果出现这种攻击，同样会损害比特币的安全性，进而影响比特币的价值。对于以挖矿收益作为支撑其电费的矿工来说这也是难以接受的。

（5）分叉攻击

拥有一定算力的人可以这样做，连续打两个区块但不公布，然后在第

一个区块已经公布而第二个区块尚未公布的情况下直接公布两个区块，使得两个区块所在的链成为最长链而被延伸。第一个公布的区块成为“孤块”而遭废弃。不过这样的收益并不大，而且概率很低。即使矿工拥有全网 10% 的算力，这样做成功的机会也只有 1%。在剩余 99% 的概率中，矿工都要担负挖掘这两个块的成本，显然是得不偿失的。

（6）匿名性与透明性

我们常说比特币既具有匿名性，又具有透明性，这仿佛是一对矛盾。实际上，这是对比特币两个不同维度的刻画。匿名性是说自然身份与社会身份的割裂关系，透明性则是说自然身份在比特币体系中每笔交易的来龙去脉都向全部节点公开。这是在去中心化体系中做的一次取舍。节点需要公开一部分隐私，让其他节点相信并愿意帮它记录交易。这包括了交易的对象、金额、时间和频率。从这些信息我们也许能推测自然身份后面隐藏的真实身份，因此之后还专门有混币交易、零币、零钞等增强匿名性的改进方案。现实生活中我们可能把社会身份与交易细节向特定的中心化机构公开，因此在它们面前我们是完全可视的；比特币的世界中自然身份是可视的，社会身份则不是。匿名性与透明性都是比特币去中心化产生的特征。

（7）关于双重支付的安全性证明

其实我们不愿过多的涉及数学计算，但我们认为这段关于双重支付的安全性证明委实重要。它说明了尽管双重支付是事实上可能发生的，但概率上是不可能发生的。如果读者朋友们对数字实在不感兴趣，跳过这一部分即可。

如果我们只考虑最简单的情况，算力攻击可以抽象成如下问题：区块链体系中诚实者增加一个诚实区块我们称之为“成功事件”，需要给结果加 1；而如果攻击者增加一个虚假区块我们称之为“失败事件”，需要给结果加 -1。由于攻击者需要重新伪造一个区块，所以可以假设他们先天就少一个块，而目标是赶上诚实节点增加区块的速度，从而使自己成为最长链。这与赌徒破产理论颇为类似。假设一个赌徒最开始先欠一定的钱，但是可以无限投掷，那么如果可以不限尝试次数的话，赌徒最终能够收支平衡的可能性是可以计算的。类比赌徒破产理论，在这里攻击者创造的链长（块数）超过诚实节点创造的链长（块数）的可能性也是可以计算的：

$$q_z=\begin{cases}1 & \text{if } p\leqslant q\\ (q/p)^z & \text{if } p>q\end{cases}$$

式中，p 为诚实节点成功打包下一个块的可能性；q 为攻击者成功打包下一个块的可能性；q_z 为攻击者经历 z 个区块后最终赶上诚实节点的概率。

假定 $p>q$（否则的话一个区块链中的诚实算力就小于攻击算力了，而这在正常的体系内不会发生），那么随着 z 增加，概率就会呈指数级下降。由于概率对攻击者不利，如果攻击者不能在早期靠运气赶上诚实节点的话，越往后机会越渺茫。

那么，现在我们进一步思考一下。对于收款人来说，一个交易打包进新块后需要等多久才能确认付款人无法改变交易了呢？假定付款人就是那个攻击者，他希望收款人相信他已经完成支付了，然而他等会儿会把这笔钱再转给自己。一般来说，如果出现这种支付作废的情况时，系统会给收款人提个醒，所以付款人希望的是这个提醒最好是等来不及了的时候再发，如等到收款人已经兑现了服务之后再说。

攻击的过程通常是这样的：收款人会为这个交易生成一对新秘钥，然后在付款人准备签名支付前才会把公钥发过去。这样就可以防止付款人预先准备好一系列合法的区块，并提前进行工作量证明从而能够瞬间执行交易。一旦这个要撤回的交易发送出去后，付款人同时悄悄建立一个（篡改了之前那笔交易的）并行链条分支。

收款人待交易加入一个区块之后还要再等 z 个块。他并不知道攻击者已经创建了多个块，但假定诚实区块建立时间为平均建块时间，攻击者可能的进程就会符合带有期望值的泊松分布。

$$\lambda=z\cdot\frac{q}{p}$$

为了计算出攻击者从现在起仍然能够赶上正常链的概率，我们将他可能做的每一步的泊松密度与他在那一步之后可能赶上正常节点的可能性相乘：

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{cases}(q/p)^{(z-k)} & \text{if } k\leqslant z\\ 1 & \text{if } k>z\end{cases}$$

为避免将分布中的无限小项求和，可将公式化简为

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left[1-(q/p)^{(z-k)}\right]$$

转换成 C 语言代码：

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

运行代码后，我们可以看出随着 z 增加，概率会随着 z 增加而呈指数级下降：

q=0.1

z=0 sum=1.000 000 0

z=1 sum=0.204 587 3

z=2 sum=0.050 977 9

z=3 sum=0.013 172 2

z=4 sum=0.003 455 2

z=5 sum=0.000 913 7

z=6 sum=0.000 242 8

z=7 sum=0.000 064 7

z=8 sum=0.000 017 3

z=9 sum=0.000 004 6

z=10 sum=0.000 001 2

q=0.3

z=0 sum=1.000 000 0

z=1 sum=0.177 352 3

z=2 sum=0.041 660 5

z=3 sum=0.010 100 8

z=4 sum=0.002 480 4

z=5 sum=0.000 613 2

z=6 sum=0.000 152 2

z=7 sum=0.000 037 9

z=8 sum=0.000 009 5

z=9 sum=0.000 002 4

z=10 sum=0.000 000 6

如果限定攻击者攻击成功概率 <0.1%，可以计算不同攻击者算力占比条件下的对应等待时间 z：

$p < 0.001$

q=0.10　z=5

q=0.15　z=8

q=0.20　z=11

q=0.25　z=15

q=0.30　z=24

q=0.35　z=41

q=0.40　z=89

q=0.45　z=340

由此可以看出，当攻击者算力占比非常低时，等待 6 个块以上即可以达到非常安全的保障。而即使攻击者算力占比增大到一定程度，也可以依赖增加交易确认后延伸的区块数目使双重支付的风险被限定在很小的比例内。

到现在为止，我们介绍了比特币作为数字货币的全部特点。它现在已经是高度成熟和完备的数字货币了。2009 年 1 月，比特币正式开始运行。接下来，就让我们看看比特币之后发生的故事。

1.3.2.4　后中本聪时代

1. 挖矿

（1）挖矿进化史

挖矿是维护比特币体系重要的一步，是节点通过贡献算力获得奖励，

达成共识的过程。但现在挖矿的发展已经大大超越了中本聪时代的想象。中本聪挖掘一个区块用的还是通用中央处理器（CPU）。2010 年之后，随着可以进行非图像处理类工作的通用语言 OpenCL 的出现，显卡或者图形处理器（GPU）由于其高吞吐量和高并行处理的特点被应用于挖矿。不过技术手段提升算力的速度并不能跟上投入比特币体系算力的增长速度，所以挖矿对于个体来说是一件越来越困难的事。

图 1-6 所示为 2017—2018 年的挖矿难度。

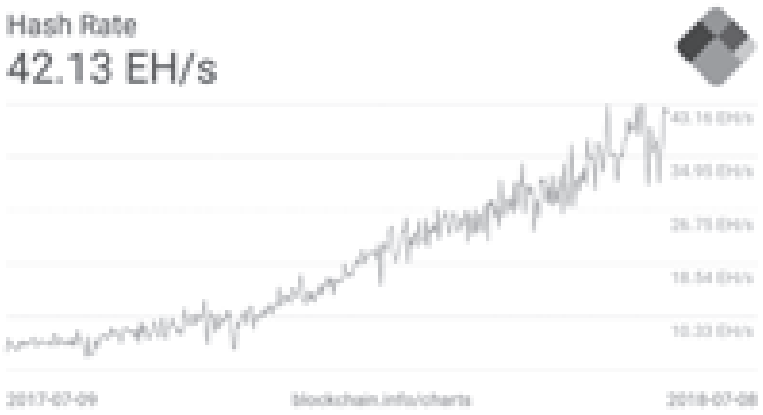

图 1-6　2017—2018 年的挖矿难度

1 EH/s 相当于 10 000 亿 MH/s，或者说按 2017 年初的算力计算，哪怕使用组合 100 个顶级显卡进行挖矿，也只占有全网千万分之一的算力。在比特币挖矿的随机机制下，也就意味着矿工每次只有千万分之一的概率挖到区块。如果我们假设矿工接入网络足够长的时间，如一个月，在这期间共会经历 30×24×60=43 200 分钟。按照最近一年的平均出块速度，约为 12 分钟产生一个新区块。因此矿工在一个月内共能经历 3 600 次出块。因为出块的方法毫无规律可循，所以每次出块都可视为彼此独立的事件。每一次矿工得到的结果无非打包成功和打包失败两种（无论他是被别人占得先机还是错误地组织了交易）。这种只有两种结果的事件在概率论中被称为伯努利实验。多次的伯努利实验结果概率满足泊松分布，而泊松分布在事件非常多的时候又可近似为二项分布。二项分布的结果非常简单，它在一个月内发现的平均区块数是 3.6×10^{-4} 个。即使在比特币价格最高的时候，这也只相当于 50 美

元的收益。很明显，这笔钱连电费都不一定够，哪里能支撑矿工持续挖矿呢？不过显卡挖矿仍然适用于一些衍生的数字货币。在全网算力不是很充足、价值波动较大的其他货币中，仍有矿工试图利用这一方式获取利润。

现场可编程门阵列挖矿（FPGA）是 2011 年出现的新的挖矿方法。在冷却和数位操作上 FGPA 都强于 GPU，因此更适合构建大型阵列。但 FGPA 的运行报错率高，而且搭建起来的专业性太强，远不如 GPU 对于一般人的亲和度。

当今最主要的挖矿方式已经换成了专用集成电路技术（ASIC）。进化到这一步的挖矿已经彻底地与中本聪希望每个节点都能参与挖矿不同的初衷不同了，因为 ASIC 矿机需要大量能源，用于供电和冷却。ASIC 矿机被高度专业化用于挖矿，意味着这是一笔赌徒性质的投资。如果不能从挖矿上赚到足够的钱，设备将毫无用处。另外，比特币的价格波动巨大，个人在巨额投资的面前承担着巨大风险。因此个人挖矿逐渐退出了历史舞台，取而代之的是许多个体组成的矿池。

当事件的成本很高、波动性很大的时候，结群是人类的优良传统。例如远古时期的狩猎采集社会，每一个个体单独打到猎物的概率都很低。但是如果一个人一天都不吃东西的话就会变得十分虚弱，失去了第二天继续打猎的可能。这会导致每个个体都无法生存下去，所以人们需要部落平摊风险。在自己没有打到猎物的时候，让别人分自己一口吃的。当然任何人也都不能独吞猎物，因为这样的话当自己没有打到猎物的时候，就没有人再愿意帮助自己。以上的内容在 1.3 节已有探讨，在此不过多赘述。想想看，这个过程与矿池的结合何其相似。实际上，对于私藏和叛变行为的担心，也正是现在的矿池所面对的。

矿池的规模差异很大，图 1-7 所示为 2017 年 7 月比特币算力的分布图，可以看到个人挖矿已经消失。矿池的算力分布从表面上看也已足够去中心化，但是由于不同矿池背后可能由相同的人控制，对于一个矿池内部，也难以设计一个公平的挖矿机制保证利益分配，矿工可以随时切换矿池，所以对于算力中心化的程度难下定论。

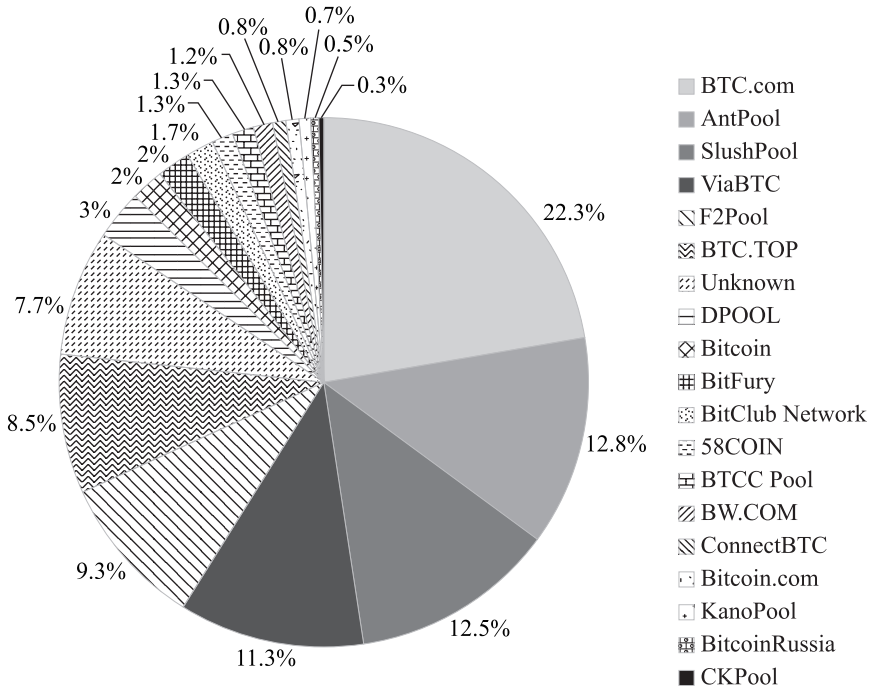

图 1-7　2017 年 7 月比特币算力的分布图

不过为什么比特币算力的中心化让比特币的持有者如此谈虎色变呢？据计算，现在对比特币数据的篡改成本约为 100 亿美元。这对于任何有意攻击它的人来说代价都太高了。因为问题的棘手之处在于体系对于激励的引入，这曾经是比特币解决问题的关键，所以在考虑潜在的风险时，我们也必须考虑激励机制崩溃的影响，而这大大降低了对比特币进行攻击的门槛。

（2）潜在的致命一击——自私挖矿

攻击比特币的方式并不需要从事实上改变什么，而只需要改变共识机制的形成。还记得稳定三角形吗？共识机制的确立、比特币的安全性和比特币的价值是一个相互保证的关系。破坏共识机制就足以构成对比特币安全性的严重威胁。康奈尔大学计算机科学系的两名研究人员 Ittay Eyal 和 Emin Gün Sirer 在 2013 年发表了一篇对比特币社区颇有震动的论文——《无须大多数——脆弱的比特币挖矿》①。它的逻辑是矿工可以进行自私挖矿，导致比特币的分配并不严格与其贡献的算力成正比。但获取超额收入的前提是

① Ittay Eyal and Emin Gün Sirer，“Majority is not Enough：Bitcoin Mining is Vulnerable”，2013

他们必须具有一定程度集中的算力。具体说来就是矿池可以隐瞒一些区块的发布，而不是一生成就立刻向全网广播。他们会在某些时候一次性公布多个区块，以迫使其他矿工放弃区块而损失收入。这种方式会导致进行自私挖矿的矿工损失一定挖出来的比特币，不过其他矿工损失的更多。[①] 如此伤敌一千、自损八百的过程逐渐会将小矿工们清除出去，越来越多的矿工则加入自私挖矿的矿池中来，进一步提升自私挖矿的可能性，最终超过全网 50% 的算力而导致区块链面临随时可能被分叉、交易可能永远得不到记录的高度不确定性状态。比特币的使用者会放弃它作为货币，持有者会在二级市场上疯狂抛售比特币导致体系的公然崩塌。

比特币的矿工理性是由激励进行保证的。人类的历史告诉我们：“人是靠不住的，靠得住的是制度。”依赖于矿工对于比特币的信仰是一件太过于理想化的幻想，他们保持诚实的唯一理由就是：这样做对他们更有好处。如果现在出现了一种不诚实（恶意打包区块）却带来更高收益的方法，我们相信矿工们是很愿意这么做的。更为可怖的是，Eyal 和 Sirer 指出这种能导致自私挖矿的算力聚集临界值近乎为零，也就是说除非比特币 100% 的节点都是诚实的，否则比特币系统理论上就是不安全的。但是这种算力聚集要求彼此之间通信良好且被统一控制，因此距离现实可能仍过于遥远。然而在之后的论证中，Eyal 和 Sirer 又发现了自私挖矿的安全上限——当算力集中在 33% 以上的自私挖矿者手中时，体系必定会遭到自私挖矿攻击。而在 25% 时，矿池可以通过很小的挖矿方式改变就能变成自私挖矿者。

对于自私挖矿的监督，两位作者十分悲观。且不说分散比特币地址和 IP 这种方式可以轻松地伪装身份，尤其是在创造比特币地址并没有什么成本的基础上，就是制定出详尽的保护机制，自私挖矿者也不会光明正大地公布自己的行为，他只要小心翼翼地避免达到红线就可以了。

唯一破解的方法似乎是依赖卧底潜入其中，然后暴露被藏起来的区块来揭露这种隐秘的自利行为。但矿池的管理者只要不定期地公布一些区块，通过二分法确定泄露机密的节点是一件十分迅速的事情。

在经济学中有一个重要的结论，叫作“the expectation matters”，即人

① https：//bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/

们的预期很重要。例如通货膨胀，当所有人预计将要发生通货膨胀时（哪怕实际上并没有货币超发或产量下降），商店就会抬高价格，工人也会要求更高的工资。为了迎合这种趋势而不造成经济的波动，央行就会增加货币总量，于是价格就真的提高了，人们预期的事变成了现实。在比特币中也是如此，当人们发现有的矿池接近安全上限时，人们会担心攻击的发生。为此矿池对策更可能是停止使用比特币而避免攻击的威胁，而非增加算力以抗衡（毕竟这样做的成本太高了）。当他退出之后，全网的算力就进一步减少，矿池的算力占比也进一步增加，又引发更多的人放弃比特币。抽象一点说，当一些人不相信这个体系时，他们选择了离开，进一步加剧了共识的崩塌。因此，攻击可能不会从算力集中度达到 25% 的时候开始。当有人向这个警戒线靠近的时候，别人就已经提高了警惕性。他胆敢越雷池一步，就会毁坏整个体系，也包括他自己。

因此现在的矿池已经远远不如之前那样中心化了。在比特币挖矿最为火热的时候，曾经有的矿池联合起来一度逼近 51% 的算力。而现在，为了所有人的利益，他们宁愿放弃那么高的占比。这不得不说也是一种博弈达到新的公平的结果。

2. 比特币的分叉

分叉其实很好理解，就是矿工对区块链的延伸方向产生了分歧。尽管从主链分叉会有很高的可能性被全网抛弃，但毕竟比特币是讲求共识的。只要有足够多的矿工愿意在这条分叉上延伸，它也可以成为一个新的比特币。

（1）硬分叉

分叉大概是最令数字货币设计者和相信它的人们烦恼的一件事了。从数据记录上，分叉意味着区块链延伸方向出现分歧；从共识机制上，分叉意味着人们对原来的共识机制不再认可而分道扬镳。在数字货币体系中出现的分叉有两种，其中硬分叉危害更大一些。它指的是部分节点为了实现某一目的而达成了新的协议，而其他节点可能由于失联或者单纯地不赞成而拒绝这一协议。硬分叉会造成两种节点对对方协议下产生的区块互不承认，因此社区完全分裂成两部分。硬分叉的目的可能看上去十分有益，或者确实十分有益，如提升比特币延伸区块的速度、提高区块容量或者排除特定交易，抑或是对比特币进行更大的改动，像是增加功能和弥补漏洞。有些改动的

确是迫在眉睫的事情，如区块的延伸速度和容量。最新的数据显示[①]，一个区块内平均容纳的交易约为 1 000 笔，区块的延伸速度约为每 12 分钟一个，这样每秒可记录的交易只有可怜的 1.39 笔。这样的速率显然无法用来进行大规模的商业应用，因此有很多人希望能降低区块产生的时间间隔或将区块的容量扩充几倍。

类似的改动需要社区同意才能进行。由于比特币的代码在 Github[②] 上是完全开源的，任何人都有权利向社区提交比特币改进协议（bitcoin improvement proposal，BIP）。Amir Takki 于 2011 年提交了第一份 BIP，其中规定了 BIP 的工作流程。到目前为止，Github 上共记录有 199 项 BIP，但其中只有第 2 项与第 123 项两项 BIP 受到了认可，可想而知比特币改进的艰难。

比特币现在已发生的硬分叉难以统计，但可以举出几个著名的例子，如近期出现的一些比特币改进币，如表 1-4 所示。

表1-4　比特币的改进币的历史和发展

改进币名称	分叉起点区块序号	分叉时间	分叉目的
Bitcoin Cash（BCH）	478558	2017.8	提高区块高度
Bitcon Gold（BTG）	491407	2017.10	改变挖矿方式
Bitcoin Private（BTCP）	511346	2018.2	提高隐私性

尽管类似的尝试还有很多，但目前观察到的现象是绝大多数改进币在短暂热度过后被矿工们迅速抛弃。绝大多数设想最终都没能实现，比特币很大程度上还是保持着它最开始的样子。

硬分叉是现在绝大多数数字货币都极力避免的事，但它也不是没有积极意义。它赋予了付出算力的劳动者很大的自由选择空间。如果矿工不同意，他可以单独创建新的共识进行尝试，而非放弃自己之前的劳动成果，然后默默地离开。

（2）软分叉

听起来，软分叉要好得多，也的确是这样，不过实现难度更大。软分叉意味着部分节点产生的新协议可以被其他节点继续执行，但是新协议将

① www.blockchain.info

② Github 提供开源软件代码的托管服务，是最大的源代码存储主机。

不再承认旧协议产生的部分区块，除非它满足新协议的要求。例如，硬分叉给公路加了个岔路，司机可以自由选择驶向完全不同的方向；软分叉好比在国道旁边又修了条高速公路，尽管有些司机仍然偏爱国道，但因为高速公路明显的优势，将会有越来越多的人使用高速公路。之前提到的 P2SH 就是成功进行软分叉的经典案例，它为比特币增添了许多功能。但在不对比特币结构作出更大调整的束缚下，进行有意义的软分叉已经是越来越困难的一件事。

3. 更多的匿名性

数字货币的匿名性是一个颇大的话题，现在已经出现了混币、合币、零币、零钞等手段，以期实现匿名性的进一步提高。毕竟通过 IP 地址追踪和交易行为分析等愈加发达的追踪手段，将一个自然身份与其背后的社会身份对应起来貌似也不是一件特别困难的事。不过这些技术并不完全成熟，介绍起来也太过复杂，本书并不过多涉及，有兴趣的朋友可以参阅《区块链——技术驱动金融》一书。在这里我们就介绍一种最朴实无华的方法：一个地址只使用一次，并且用不同的 IP 地址生成这些比特币地址。一个地址接收到比特币之后，它只会把比特币全部花出去，并不再使用，这会大大提高追踪的复杂度。

离中本聪创造比特币已经过去了 10 个年头，但是比特币的主要框架仍然保持着原貌。尽管其受到了很多当初未曾设想到的威胁和挑战，我们仍不得不感叹这套体系的精巧。

1.3.2.5 关于比特币的一点联想——希腊民主与比特币

公元前 5 世纪，夕阳下的爱琴海宁静而温柔，绯红的云飘荡在古老的雅典城天空。宽阔的广场上，人们激烈地辩驳着城邦的事务。不时进行的举手、投票，彰显着这片土地上的公民时时刻刻追求的自由与平等。没有人拥有绝对的权威，每个公民充分地享受着民主制度赋予他们的政治权利。

公民大会作为古希腊城邦的最高权力机关，负责讨论并解决国家的重大问题，如战争与媾和、选举高级官员和进行法律裁决。在伯利克里时代，参与者甚至还能获得少量津贴。雅典城中，所有 20 岁以上男性公民均可以公平参与公民大会。为落实公民大会作出的决议，克里斯提尼于公元前 6 世纪提议创设了五百人会议。五百人会议是雅典城邦民主政治的核心机构，

其中人员的选举严格遵守轮换制和随机制。通过频繁的更换和概率的绝对均等，保证每名公民都有相同机会参与政治事务决策。

归结起来，古希腊城邦是一个平民政体，公民的利益大体一致，公民之间保持和谐。他们社会生活中的重要部分都被赋予完全的公开性。

同时，这又是一个权力相互制约的政权。任何人都有权管理他人，不过是通过轮换的方式。

在这里，法律之上。没有人能凭借自己的意愿改变公民的集体意志，所有的行为都要服从于业已存在的规则。

人民对于政治权利的意识空前觉醒。他们践行规则的同时积极投入新的规则创造中。

这是比特币追寻的乌托邦，一片高度自由、自治、自决的净土。在比特币世界里自然身份平等，每个矿工都有挖矿的权利。挖矿保证体系稳定，同时代表着对体系满意度的投票，没有人凌驾于他人之上。善良的人会从他人的认可中得到回报，恶意的人则会受到来自社区的惩罚。体系从建立之初就很完美，人们希望把它打造成一条“千年之链”。对于无政府主义的信徒，这真的是一个梦幻般的理想国吗？

我想我们可以继续看看城邦们的历史。

公元前 399 年，发生了一起著名的“多数人暴政”——哲学家苏格拉底被全体公民投票判处死刑，因为他的思想不合时宜。这颇令人唏嘘，但请让我们想想那些对于比特币颇为有益的提案最终石沉大海的情形。

再之后，公元前 4 世纪后半期，日渐衰微的希腊被北部崛起的马其顿王国所灭。盛极一时的希腊城邦民主制被蛮族的铁蹄踏在脚下。这一步也许到现在还没有发生到比特币身上，不过盛极而衰一直是历史颠扑不破的道理。

古希腊城邦民主是小国寡民的产物。过于泛滥的直接民主反而导致了政治腐败，部分缺乏教育的公民疏于行使自己的权利又容易被煽动感情。社会动乱阻塞了社会和经济的进一步发展。最后，他们不得不屈服于一个比他们更具有统一意志的国度。这很奇怪，为什么一种理想化的民主会最终落败。但可以肯定的是，决策效率的低下与发展速度的巨大差异是重要的原因。

了解历史的原因不是让我们凭吊古人的光辉，更多的还是在于指导我们现在的生活。比特币时至今日已经面临众多的竞争者。效率，这个对于

交易体系十分重要的概念，已经严重掣肘了比特币共识的进一步扩张。当越来越多的人加入这个体系的时候，体系的效率受到挑战，却也越来越难达成对体系的修改。这是去中心化最脆弱的软肋。在完全竞争的市场里，它同时意味着淘汰。也许比特币的体系缺失很好，但如果我们不希望马其顿王国来征服它的话，我想是时候思考一下对策了。

以上就是比特币作为数字货币的全部。现在比特币已经平稳运行了 10 年，被挖掘出来的比特币多达 1 700 多万，主链上共延伸有 53 万多个区块，每个区块平均大小约为 0.55 MB，平均每天记录 15 万笔交易。比特币与其他主权国家货币的兑换比例也以令人难以置信的速度跃升了无数倍。

如果在最后用一句话概括比特币的话，我们会说：作为创世纪的货币，它已经做到了最好。

1.3.3 区块链行业发展

比特币，为区块链行业打开了大门。区块链的广阔前景和独特魅力吸引着研究者、探索者、创新者不断地拥入这个新型的行业，为区块链行业带来了勃勃生机。在 1.3 节，我们已经向大家介绍了区块链基本的去中心化进程。而本节中，我们将为大家展现比特币出现后的区块链行业发展状况和去中心化持续推进的过程。

1.3.3.1 公链

1. 公链简介

行业内通常按照共识机制的开放程度将基础设施和平台建设分为公共区块链（公链）、共同体区块链（联盟链）和私有区块链（私链）三种。

公共区块链，或简称公链，是最重要的一种。它是指节点彼此完全陌生，仅凭共识机制建立信任，允许节点自由加入或退出，任意节点拥有读取全部交易权限并负有贡献算力、维护共识机制稳定之职责的去中心化区块链项目。

共同体区块链是指共识形成过程受到共识机制以外制约的区块链项目。节点由共同体成员产生，彼此认识，所以对交易安全性的要求远不如公链。共同体区块链允许每个节点都能读取，也可以设限于部分节点，或

走混合路线，开放区块的根哈希（创世区块中的哈希值）给外部用作有限次数的查询。

私有区块链，或简称私链，是指写入权限仅掌握在一个组织下的区块链项目。读取权限或对外开放，或被任意程度地进行了限制。由于不存在恶意节点或恶意交易的风险，其对安全性的要求比较低。尽管数据库可能会作为公共审计的窗口，很多情况下，公共的可读性并非是必需的。

由此可见公链的重要性在于节点的自由进出和数据的写入读取权限。良好的公链体系必须满足在节点真实身份完全不可知的情况下，节点有激励主动维护共识并排斥破坏共识达成者。这就要求公链要合理设计加密奖励，使得维护共识获得奖励，破坏共识受到惩罚。此外，公链要求所有数据必须对全体节点可见，而且拥有公平的写入权利。这样才能最大程度上避免权力集中，保留去中心化本质。这两点对公链安全性和机制设计提出了充分的挑战。虽然它最难实现，但价值也是最大的。以此为基础可以创建独立的经济体系，也能真正实现“去中心化自治”这一初衷。

行业内倾向于把公链划分为三代，依据的是共识机制和实现的功能。以比特币为首的应用于加密货币领域的区块链项目为第一代公链，它们的典型特点是依赖于原始的工作量证明机制。各种加密数字货币要么在比特币基础上增强了匿名性，要么只是更改了比特币的参数，典型项目包括比特币、莱特币、门罗币、达世币等。这一代公链只能完成交易信息的链上记录，最大的应用就是加密货币，而且往往受到效率低、耗费能源的指责。

以以太坊为首的加入了智能合约功能的区块链项目称为第二代公链，典型项目有以太坊、EOS、NEO、波场等。它们的共同之处在于都将智能合约开发作为重要的公链功能进行开发，而且往往采取新的共识机制，如之前提到的 POS 权益证明机制、DPOS 授权股权证明机制等。这一代公链发展时间较短，主网还没有得到普遍认可，智能合约理论也尚处于发展阶段，实际效果有待进一步观察。

第三代公链的概念并不明确，也没有明确的代表项目。通常它是指采用 Casper、DAG、混合共识等更新一代共识机制的区块链项目，如 IOTA、Zilliqa、TrueChain 等。从理论诞生距离此类项目诞生往往只有数月，所以理论尚未得到检验。部分项目主网也未上线，正处于开发状态，所以第三

代公链更偏向于一种概念上的称呼，具体情况需要等待主网上线之后再做判断。

不过在我们看来，这种划分有些过于牵强。本质上看，即使是第三代公链，很多设计也是仿照比特币进行的，不少项目的共识机制仍然需要工作量证明机制作为支撑。现在尚看不到类似于比特币一样划时代的突破性项目，可以明确地将之与其他项目区分。而且智能合约等理论在比特币出现前业已有之，比特币也可以作为智能合约实现的基础。所以如果不做过于精细的区分的话，现在的公链只是10年前比特币发展的延续。如果一定要做区分的话，可以以以太坊的出现作为公链的划分点。因为在它之前，共识机制一直是单一的工作量证明机制，而在它之后人们认识到了其他共识机制的可能。尽管如此，以太坊现在还是处于工作量证明机制的阶段，其权益证明机制的实施尚未确定正式的引入时间。

接下来，我们将为大家介绍几个典型的公链案例作为参考。

2. 以太坊[①]

（1）以太坊简介

以太坊是一个所有人都可以参与搭建和使用去中心化应用的开放式区块链平台。像比特币一样，没有人控制或拥有以太坊——它是一个开源的世界性项目。不同于比特币的地方是，它更具可变性和适应性。以太坊开发者自称在以太坊上创建新的应用程序十分容易。而且在“家园”版本发布后，以太坊的安全性得到进一步保证。

（2）以太坊创始人 Vitalik Buterin

以太坊的创始人是俄罗斯人 Vitalik Buterin，被以太坊的追随者们称作V神。他在17岁时便开始在父亲的影响下了解比特币，并在比特币论坛中发表博文。获得一定的名气后，Buterin作为联合创始人创办了《比特币杂志》，并担任首席撰稿人。19岁时，他进入加拿大滑铁卢大学学习，并在那里发表了初版以太坊白皮书。2014年，Buterin在自己任编辑的《比特币杂志》上发表了极具野心的论文《以太坊：一个下一代加密货币和去中心化应用平台》。他首次公开提出了以太坊专属概念，试图从区块链基础协议上改进比特币的技术，如通用型合约、加密货币协议等。相比于其他项目在比

① http：//www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

特币上修修补补，以太坊直接向比特币的地位发起了挑战，意图建立一个任何人都能创建应用平台的公链。2015 年 7 月，以太坊开启了为期 42 天的募资，筹集到了价值 1 800 多万美元的比特币，用于偿还初期开发时欠下的债务和技术人员酬劳。2016 年，以太坊的价值开始得到市场认可，其通证价格在交易所开始暴涨，吸引了大量开发者以外人群关注以太坊。①

（3）以太坊账户

以太坊的运作融合了比特币的许多功能和技术，但同时也具有许多颠覆性的创新。以太坊一个大胆的改动是将比特币体系中以交易清单为基础的做法转变为以账户为基础。以太坊区块链选择跟踪每个账户，每一笔交易都是账户间信息和价值的交流。

这里存在两种账户：由私钥控制的外部拥有账户（EOA）和只能由 EOA 激活、由合同代码控制的合同账户。对于大多数用户而言，他们的区别在于用户通过掌握私钥控制 EOA，而内部代码控制合同账户。合同账户被用户掌握的情况只能是它们被编程服从于特定地址 EOA 的控制。“智能合约”，这个时尚的名词，指的就是为合同账户编程。当一笔交易发送给合同账户后，“智能合约”就得以自动执行。任何用户都能在以太坊上创设新的合约。

合同账户仅在 EOA 指示时执行操作。因此，合同账户不可能执行本级操作（如随机数生成或 API 调用），它们只会在 EOA 提示时进行调用。这是因为以太坊要求节点能够就计算结果达成一致，而这需要保证执行具有严格的确定性。

以太坊在进行交易时改变的是全局所有账户构成的状态集，而且每个账户拥有一个特殊的检查字段——我们称之为交易次数。每当账户进行一笔交易时，交易次数会增加 1。这两种设计一定程度上是为避免双重支付和恶意广播交易的行为。对于双重支付攻击，节点存储的状态集可以对交易者账户余额进行查验，不过仍然存在分叉进行双重支付的可能。对于恶意广播交易的行为，假设攻击者将一笔他人的正常交易又广播了一次，节点会发现交易者写入交易中的交易次数与自己状态集中的交易者的交易次数不一致而拒绝该笔交易。

① http：//mini.eastday.com/mobile/180313191716270.html

（4）以太坊挖矿

初期的以太坊同样利用了工作量证明机制。矿工就是以太坊网络中接收、验证、确认并执行交易的节点。他们将交易打包进区块，其中包括许多对账户状态的更新；然后彼此之间展开竞争，争夺延长下一个区块的权利。每一个成功打包区块的矿工都将得到一定数目的以太坊奖励，这激励着人们将算力源源不断地投入以太坊网络中。

这一切都与比特币十分相似。不过在区块的加密流程上，以太坊做了一些改进。我们知道区块的打包需要解决一道计算复杂的数学问题，所耗的巨额算力阻止了一般人打包的可能，这不利于去中心化的维护。以太坊的解决方案是把加密流程改成解决一道占用内存的问题。如果一道问题的解决依赖于内存和 CPU，那么最理想的挖矿硬件就是一般的电脑。这使得以太坊具有了抗 ASIC 挖矿的特性，相当于实现了一种更加去中心化、增加安全性的方式。

除此之外，针对挖矿过程产生的短暂分叉，以太坊允许分叉的两个区块在通过检验后合并。如果分叉包含的交易没有出现双重支付等情况，分叉也可以获得一部分挖矿奖励。这样可以在一定程度上减少算力浪费的情况并加快交易记录进程。

（5）以太坊技术路线[①②]

按照以太坊官网描述，以太坊的技术路线分为五个阶段。准备阶段，就是 2015 年 5 月发布的奥林匹克测试网络。现在以太坊已经经历了 2015 年 7 月发布的第一阶段“前沿”，和 2016 年 3 月发布的第二阶段“家园”，进入第三阶段“大都会”。在前两个阶段，以太坊并未作出明显的技术变革，主要是解决了用户体验和使用难度的问题。在“大都会”阶段，以太坊希望进行四项改变——引入 zk-Snarks（基于“零知识证明”），开始早期实施 POS（权益证明机制），使智能合约更稳定和灵活以及建立抽象账户。以太坊将“大都会”阶段又切分成“拜占庭”和“君士坦丁堡”两个阶段，相当于两个硬分叉。2017 年 10 月 16 日，以太坊按照原定计划于第 437 万个区块进行了第三阶段升级，产生“拜占庭”硬分叉，引入了零知识证明

① https：//blog.csdn.net/xilibi2003/article/details/78671384

② http：//www.360doc.com/content/17/1217/20/30724179_714021406.shtml

和抽象账户。分别将于届时引入 Casper 共识机制，一种 POW 与 POS 相结合的新型共识。以太坊开发者暂未公布进入第四阶段“宁静”的时间。

（6）以太坊改进方案

以太坊改进方案（EIP）类似于比特币改进方案，都是由社区成员提出，经过初期过滤，公布给社区。如果在社区中取得了绝大多数人的响应，它就能成为一条切实的改进方案加入以太坊体系中。比较重要的改进方案包括 EIP-2，EIP-7 和 EIP-8。它们的主要作用是修复了创建合同的过度激励和交易延展性，并保证节点的客户端软件可以应对未来的网络协议升级。

（7）The DAO 攻击事件 ①

The DAO 攻击事件是区块链历史上最大的一次抢劫案。

The DAO 的想法来自一位理论物理学家 Christoph Jentzsch。联想到互联网众筹，他想到每个新的创业公司都需要自己寻觅独立的融资途径，搜索成本太高，为什么不能通过去中心化的方式建立一个资金池来为他们提供资金呢？

Jentzsch 在 2015 年向全世界介绍了自己的想法，并于 2016 年 5 月将它变成了现实。他希望筹集足够多的资金用于资助以太坊上应用程序的开发。投资者可以用以太币购买 DAO 代币，然后投票支持他们喜欢的项目。一个 DAO 代币对应一票。如果他们支持的项目有盈利，那么代币持有人可以分享这部分利润。短短 29 天之内，The DAO 就获得了价值 1.5 亿美元的以太币融资，远远超出了最开始 500 万美元的预期。人们为什么这么钟爱这种投资方式？一个原因可能是 The DAO 作出投资决策是完全去中心化和透明的。The DAO 相当于一个省略了董事和基金经理，由投资者直接管理资金的基金。每一个投资决策都要征求所有 DAO 代币持有者的意见，这让饱受委托风险的投资者很是满意。

然而接下来发生的攻击事件震惊了所有看好这个区块链界有史以来最大的众筹项目的人。2016 年 6 月 17 日，The DAO 遭受了攻击。这次攻击组合了两个漏洞 ②：第一个漏洞是递归调用 splitDAO 函数。方法是 splitDAO 函数被第一次合法调用后再次非法地调用自己，然后不断重复非

① http：//news.ifeng.com/a/20170627/51324936_0.shtml

② https：//blog.csdn.net/sportshark/article/details/51820008

法调用过程。这一过程可以使得攻击者的 DAO 代币被清零之前，数十次地从 The DAO 的资产池中重复分离出理应被清零的攻击者 DAO 代币。第二个漏洞是 DAO 资产分离后避免从 the DAO 资产池中销毁。正常情况下，攻击者的 DAO 代币被分离后，the DAO 资产池会销毁这部分 DAO 代币。但攻击者在递归调用结束前把自己的 DAO 代币转移到其他账户，这样就可以避免这部分 DAO 代币被销毁，然后再利用第一个漏洞进行攻击，把安全转移走的 DAO 代币再转回原账户。这样攻击者实现了只利用两个账户和有限的 DAO 代币进行两百多次攻击，获得了价值 360 万以太币的 DAO 代币控制权。由于 the DAO 完全是由自动执行的代码组成，在社区成员达成一致的修改意见之前，没有任何人能够阻止攻击。

但是 the DAO 的设计方案是任何人都需要至少 27 天才能脱离 the DAO，因此这段时间成为了宝贵的寻找解决对策的“救援期”。Vitalik Buterin 在得知攻击后立刻通知了以太坊社区，并提出了一种解决方案：软分叉。他希望矿工们升级客户端来支持软分叉，使得从第 176 万个区块之后所有与 the DAO 相关的交易均认作无效，以此来阻止攻击者提现。[①] 这样可以避免交易出现回滚，尽可能减少攻击造成的负面影响。

软分叉的方案需要征求矿工们的意见才能实施。方案发布后，攻击者停止了攻击，并宣布对不支持软分叉的矿工给予 100 万以太币奖励。然而最后软分叉方案还是顺利通过了，以太坊开发者退出了针对 the DAO 进行软分叉的版本 Gethv1.4.8，但是这个版本再次出现了致命漏洞。

这次的漏洞更为低级。简单而言，每笔以太坊上的交易都需要矿工检查 the DAO 智能合约是否与其子 DAO 地址相关。如果是，则拒绝该笔交易，从而锁定 the DAO 内的所有资金。逻辑本身没有问题，问题出在没有收取执行交易的手续费上。矿工可能已经对交易进行了打包，却由于其关联了子 DAO 地址而被迫放弃，而且获得不了任何补偿。以太坊随后遭到了 DDos 攻击，就如同不间断地接受骚扰电话一样，攻击者以及低成本发起海量交易，导致以太坊网络瘫痪，正常交易记录被阻断。节点们被迫回滚了软件版本，软分叉方案宣告失败。

这时距离攻击者脱离 the DAO 系统还有两周，Stephan Tual 在此时提出

① https：//juejin.im/post/5b28ffdef265da59bc2ca147

了更为激进的想法——硬分叉，回滚这段时间内的所有交易，以太坊相当于回到了 the DAO 存在之前的状态。没有以太坊交换 DAO 代币，没有 DAO 攻击，没有 DAO。

最终大约价值 450 万的以太币持有者参与了投票，90% 支持这一想法。2017 年 7 月 20 日，以太坊在第 192 万个区块处进行了硬分叉。The DAO 合约中的全部资金被转移至新的智能合约中。该合约只有一个功能——退回 the DAO 众筹参与者的以太币。众筹参与者通过调用 Withdraw 函数可以从 DAO 代币换回以太币。

尽管攻击者最终貌似未能得逞，但此次攻击在以太坊社区乃至区块链界引起了轩然大波。人们质疑不可篡改、不可回滚的区块链为什么突然被人为重塑了。很多社区成员并不认可此次更改，选择在原有的区块链上继续延伸。原来的以太坊分裂为两个项目——以太坊与以太经典。尽管以太经典的坚持者认为他们才是恪守区块链本质的人，不过从后续的发展上看，以太经典发展得远远不如经历了硬分叉的以太坊。

但对于 the DAO 来说，这次攻击无疑意味着项目的终结。虽然只有短短两个月寿命，但它引起的震动并不小。美国证券交易委员会 2017 年 7 月发布报告时称，the DAO 发行 DAO 代币是一种提供和出售证券的行为，因此受联邦证券法的约束。DAO 违反了联邦证券法，所有的投资者也违法了。

更重要的是，这引发了区块链行业对区块链本质的思考。其本质究竟是一条共同维护、不可修改的数据存储链，还是一个社区自治的去中心化组织。通过 the DAO 攻击，我们看到了大多数人更倾向于后者。一个区块链体系难免会存在诸多的安全隐患或隐藏问题，但重要的是社区共同应对解决。说白了，重要的还是人，不是数据。这也是为什么我们把共识机制看作公链开发最关键的要素。体系健全、安全提高都是可以循序渐进完成的事，只有节点共识是从一开始就要想清楚的东西。

3. 初链（TrueChain）

（1）初链简介

初链是一个典型的混合共识公链项目，结合 PBFT 与 fPOW 两种共识机制，意图解决阻碍公链实际应用的三大障碍——交易速度、存储和安全，最终打造能承载商业化应用的可靠公链。在共识设计、工程实现、分片记录、

产品支持等方面，初链都是行业内的先行者。

（2）初链共识机制

初链的共识机制可以归为混合共识。我们可以将共识机制笼统地归为两种——异步性共识与同步性共识。同步性共识必须在同步性网络内才能实现，如 PBFT（实用性拜占庭容错机制）。异步性共识可以在异步性网络内生效，如 POW。初链使用的是 PBFT 与 fPOW 两种不同的共识，利用同步性共识与异步性共识效率之间的差异，搭建 PBFT 在上层，fPOW 在下层的共识结构。具体而言，PBFT 为快速链，由选举出来的委员会构成；fPOW 为慢速链，由矿工构成。初链希望这种共识机制能打破去中心化、安全性和效率不能兼得的“不可能三角”。

fPOW 是初链的核心创新。作为 POW 的改进版，fPOW 主要对 POW 算力过于集中导致普通节点无法挖矿获得通证分配进行了改进。在矿工挖矿的过程中，可以挖得 fruit（水果）。具体说来，在 fPOW 体系中，挖矿方式与比特币基本相同，只不过末位拥有一定长度的零的哈希值为区块。而在随机尝试 nouce 值过程中，会产生开头满足一定长度的零个数的哈希值，这就是 fruit。挖到 fruit 的矿工需要进行广播，但必须等待下一个区块诞生才能全部被记入 fPOW 的区块链中。

在混合共识的框架下，一笔交易的记录需要如下过程：首先 TRUE（初链的通证）的持有者声明发起一笔交易，该笔交易会进入等待被记录的交易池中。PBFT 作为记账委员会，从交易池中抓取交易，检验交易的真实性和合法性。如果这笔交易尚未被记入 PBFT 的区块链（快速链）上且通过检验，则将其记入自己的区块中并把交易达成一个包，我们称之为 Message。Message 的摘要会被放到 fPOW 的慢速链上，由矿工再次进行打包。

（3）分叉风险

对于潜在的分叉风险，初链将其区分为故意分叉和无意分叉。故意分叉往往存在重大原因，参考比特币分出比特币现金，以太坊分出以太经典，每一次都是对项目的重大改进和净化过程。这对于项目的长足发展是有益的，因此初链更多地担心无意分叉情况。比如当两名矿工同时完成了 fPOW 链上的区块打包时，初链的解决办法是比较谁打出的 fruit 较多。当 fruit 数目相同时（虽然这种情况出现的几率很低），继续等待各自延伸后的区块

打入的 fruit 数量。通过 fruit 的参与，初链实现了迅速确定主链，防止双重支付的目的。

（4）交易的检验

交易的检验，一旦交易被打包的快速链上，并通过 PBFT 委员会验证签名，该交易即被最终确认，慢速链将以水果的方式将快速链数据块的摘要打包进慢速链，使得快速链避免被长程攻击以增加安全性。

（5）坚持去中心化

去中心化是初链设计公链考虑的核心问题之一。它采用了两种方式来保留去中心化本质：

其一是利用 fPOW 挖 fruit 的方式，为矿工提供更加平滑的激励，使得每个人都能参与到挖矿中。在比特币现行的状态下，ASIC 矿机挖矿已成必然。其高于 CPU 数百倍的计算能力让普通用户挖矿完全无收益。在初链的体系中，针对这一问题进行了精巧的设计。首先 fruit 彼此作用完全相同，针对每一个 Message 都可以挖掘 fruit，但其记录具有顺序。这一顺序由 Message 的顺序决定，而 Message 的顺序又由 PBFT 委员会决定。所以只能进行计算的 ASIC 矿机快速挖掘 fruit 将无法被记入区块。其次，初链会不定期更换算法，而算法的种类又与近期交易的哈希值相关，所以完全不可预测。ASIC 矿机的弱点是不能编程，而且开发到投入使用的周期长。通过更换不确定的算法可以使得 ASIC 矿机失去作用。更加分散化的挖矿使得通证被更广泛地分散到不同节点手中，间接性帮助了去中心化。

其二是将 PBFT 委员会的名额向所有节点开放。初链的想法是去中心化如果与效率相结合，那么做的应该是权力去中心化。对于具体的一项事物，仍然可以交由一个相对集中的组织完成，不过该组织的加入完全是对每个人公平的。初链中的 PBFT 委员会将从候选委员会中按照简单随机的原则选出。候选委员会的规则是成为一名节点并在规定时间内挖掘出一定数量的 fruit。这样为成为候选委员会成员划定了门槛，以防止女巫攻击或不具有记账、存储能力的节点成为记账人，同时保持了相当程度的开放。据初链开发者估计，一个租用阿里云服务的节点即可满足算力要求。

值得一提的是，由于快速交易记录的权利被收归 PBFT 委员会，PBFT 委员会又受着 fPOW 上矿工的监督。自私挖矿行为在初链中并不成立，这

也保证了体系的相对公平性。

（6）初链技术路线

初链将在 2018 年 9 月底完成 beta 测试版主网的搭建，用于测试可能存在的安全隐患和网络承载量。2019 年 3 月 30 日，初链上线了第一个版本的主网，各种应用目前都可以开始在其主网上开发。初链未来的 PBFT 记账会借鉴流行的分片机制，将 PBFT 委员会划分成主片区和普通片区。主片区负责记录任务的分配，以及回收记录时的排序；普通片区负责交易记录打包。这样将赋予初链很好的扩容能力，根据交易费用和交易量的多少，初链可以通过调整普通片区数目实现网络承载力裂变。不过在第一个版本的主网中，将仅存在一个分片。这个分片的领导者（leader）会起到主片区的作用，分片内的其他成员通过签名的方式对交易予以确认。

初链的主网目前已经上线，之后将逐步发展成为类似于比特币一样公开运营的项目。初链的主网成为应用的承载者，担负起基础设施的作用，初链后续的维护和升级将交由全体初链社区成员，也就是通证持有者们，这时初链就逐步成为一个真正的去中心化运营项目。

（7）智能合约

正如同以太坊赋予了智能合约可能，初链也将搭载智能合约作为了重要的开发内容。初链希望其上搭载的智能合约能对以太坊合约实现向下兼容。初链将使用 Solidity 作为智能合约开发语言，而虚拟机则是快速链节点的必备。同时，需要做好应用程序编程接口（API），用于不同开发语言（如 Go，Python，Java）间的兼容。

（8）初链的挑战

作为意图超越以太坊和比特币的第三代公链，初链面对的挑战非常大，另外包括来自竞争公链的压力和行业的波动周期。技术方面，初链需要解决交易速度和存储两大难题。如果初链希望承载足够多的商业应用，其至少需要几万的 TPS，而初链目前的设想只有 10 000 左右，性能方面，可以考虑使用大规模并行计算技术提升批量交易的处理速度，提升单链的执行效率和性能。存储方面，由于快速链的区块生成时间被压缩为一秒一到两个，交易的数据量将会海量增加。现在比特币的全部交易数据大小为 160 ～ 170G，也就是一个硬盘可以轻松地存储下这么多。但对于初链来说，尽管存在空

块，其交易数据的增长速度也绝非硬盘可以容纳下的。设置时间节点抛弃已被确认的交易记录已被证实是极大有损于安全性的。一个可能的解决办法是存储到中心化的服务器中，同时开放下载接口。通过鼓励下载、鼓励共享、鼓励查询的方式使更多的节点愿意主动备份数据。更理想的方式可能是 IPFS，一种去中心化的存储方案，用户可以通过提供存储和带宽挖矿。尽管有许多研究存储方案的公司，但尚未出现行业认可的存储方案，在公链领域更是少见。

1.3.3.2 联盟链[①②]

1. 联盟链简介

联盟链，顾名思义，是由若干个机构共同参与交易记录的区块链。区分于公链网络中基于交易或账户的分布式账本，联盟链采用的是多中心化网络。联盟链上的数据只能由系统内的成员节点进行读写，交易也只能由成员发起，不存在公链中节点自由进出并拥有一切权限的情况。有一个类比非常好，可以作为公链与联盟链区别的解释：联盟链是面向企业的，消费者只是应用的用户。对于消费者而言，他们只能从应用层面感知区块链架构。企业才是达成共识机制的主体。

与公链相比，联盟链在数据安全、网络性能等方面更具优势，因此可作为分布式商业机构的基础组件，满足分布式商业中多方对等合作的发展要求。由于节点数字身份与社会身份存在良好的对应关系，联盟链较之公链更容易在现实场景中落地，运行效率更高，也方便监管。不过匿名性与去中心化在联盟链中割舍较大，导致其与公链完全是两条发展路径，所以更适合作为一个独立的子领域对待。

此外，联盟链的节点可验证身份，这一点导向了协议或商业规则的高度治理。如果出现异常情况，联盟链中很可能诞生中心化的组织，进行跟踪和治理以减小损失。

联盟链的共识机制与公链有本质性的不同。联盟链的节点存在区块链以外的身份确认方式和奖惩机制，所以在联盟链中毁坏共识的做法会导致其他节点通过联盟链以外的其他方式对节点背后的控制者施加惩罚。进入退出

① https：//github.com/toxotguo/thinking/

② 《2018 中国区块链产业白皮书》工信部信息中心、起风财经

的壁垒也导致联盟链达成共识的成本比公链小了许多。对于比特币这样全球性的异步性公共网络，必须采取工作量证明机制这样严格确定奖励和惩罚，矿工自由竞争的方式才能保证体系稳定，联盟链则大不相同。它的网络几乎可以认为是同步性的，节点之间可以两两建立联系，通信效率大大提高。而且节点的身份确认可以使得没有奖励存在，体系依旧能保持运转。类似于 PBFT、DBFT 的共识机制因此可以发挥作用。

联盟链现在存在的问题有两个：一个是技术难关；一个是关注度。在技术上，未来的联盟链需要与跨链协议结合才能发挥更大的作用，而跨链协议尚处于理论初期，没有成熟的模式指引项目发展。在关注度上，人们更多地把目光集中在公链开发上，技术、人才和资金投入都相去甚远。不过这和联盟链本身地位有关。就区块链出发的本意而言，联盟链并不是最终的目的地。

2. 超级账本 Hyperledger 与 Hyperledger Fabric

超级账本 Hyperledger 是 Linux 基金会主办的开源合作项目，旨在推动跨行业区块链技术发展。Linux 基金会本身在开放式治理下培育开源项目的历史十分悠久且非常成功。作为一个全球性的合作项目，超级账本的项目成员来自金融、银行、物联网、供应链、制造和信息技术等领域。①

超级账本最重要的子项目是 Hyperledger Fabric，其被业内简称为 Fabric。前面提到了联盟链的本意是面向企业，这也是 Fabric 项目从一开始就确定的目标。对于企业用途，必须考虑以下五点。

- 社会身份可识别性。
- 网络连接需要许可。
- 高事物吞吐量性能。
- 交易确认的低延迟。
- 与商事交易相关的数据隐私保护。

为此，Fabric 分别从以下几个方向对其进行了解决。

（1）模块化

Fabric 成功做到了模块化架构。无论是可插拔的共识、可插拔的身份管理协议（如 LDAP 或 OpenID Connect）、密钥管理协议还是加密库，该平

① https：//blog.csdn.net/MyIgnorance/article/details/78904270

台的核心都经过精心设计，以满足企业需求的多样性。

（2）可插拔的共识

由于共识是模块化的，因此可以根据特定部署或解决方案以满足要求的信任假设。这种模块化的结构使得平台可以依赖完善的工具包进行 CFT（崩溃容错）或 BFT（拜占庭容错）排序。

（3）智能合约

智能合约在 Fabric 中被称为“链码”（chaincode）。Fabric 是第一个支持在通用编程语言中创建智能合约的分布式账本平台，而不是受限制的应用于域的语言（如 DSL）。这意味着大多数企业都掌握了开发智能合约的能力，而不需要额外学习新的语言。在 Fabric 的 1.1.0 版本中，智能合约支持 Go 或者 Node.js 语言，而之后的版本中会继续加入新的流行编程语言，如 Java。Fabric 认为在区块链中运行的与订单共同执行的智能合约必须是确定性的，否则可能永远达不成共识。为了解决非确定性问题，许多平台要求智能合约以非标准或特定于域的语言编写，以便消除非确定性操作。这极大地阻碍了智能合约的广泛应用，因为开发人员在学习新语言编写智能合约时会经常地发生编程错误。Fabric 支持多种语言的做法很大程度上缓解了类似问题。

（4）隐私与保密

Fabric 是一个需要许可才能加入的平台，通过“通道”结构实现保密。简单地说，Fabric 网络可以在应该被授权可见的参与者子集与特定交易集合间建立“通道”。只有那些加入“通道”中的节点才有权查看智能合约和交易数据，同时保护了匿名性和隐私性。Fabric 还在开发零知识证明。尽管零知识证明需要耗费相当的时间和计算资源，但会对隐私保护起到进一步的加强作用。

以上内容主要来源于 Fabric 一篇经过同行评审的论文——《超级账本 Fabric：一个需授权区块链的分布式运行系统》。从中我们可以很清晰地看到 Fabric 的解决路径。其主要是从模块化和构建“通路”两个方向入手分别提高事物处理和交易确认速度以及交易隐私性。智能合约的部署在 Fabric 中尤为容易，因为它良好的兼容性。Fabric 作为备受联盟链业界关注的项目，

的确让人们看到了出现服务于企业的区块链的希望。

1.3.3.3 硬件制造

区块链的安全性以算力为支撑，提供算力的硬件也就成为了区块链行业的关键产品。目前，硬件制造厂商主要生产的都是专门用于挖矿的 ASIC 矿机，其核心是挖矿用的芯片，整机价格在几千元到上万元不等。很多矿工采用托管模式，购买矿机的所有权，直接将矿机发往算力集中的矿池。国内市场在这方面占据主导地位，比特大陆、嘉楠耘智、亿邦国际作为市占率最高的三家公司，都在 2017 年获得了较高的利润率，嘉楠耘智已经在 2019 年登陆美股，亿邦国际和比特大陆也已经在登陆美股的路途中。

硬件制造商的出现是行业的必然，因为挖矿的激励会催生更高的挖矿效率。很多人担心硬件制造商导致算力集中化，但在我们看来这是不必要的。

首先是算力集中远远没有达到想象中的程度。由于托管模式的存在，名义上归属于硬件制造商的矿机并不全部由硬件制造商掌控。虽然存在硬件制造商在矿机上留下远程控制的后门，但此举一旦被发现无异于自毁长城，所以从经济激励上他们并没有这么做的动机。而且一旦硬件制造商表现出异常举动，矿机所有者可以迅速将其算力脱离硬件制造商的控制，转向新的矿池。51% 算力攻击也并不如一般人想象的那样可怖，具体可参见我们在比特币一章的讨论。所以，算力集中并不是这个行业最需要担心的事。

其次是共识算法的改良。在 POW 中，区块头哈希值的计算占据了区块打包流程的主要环节，在这一过程中需要具有大算力的矿机参与。如果采用普通电脑（CPU）即可参与挖矿的共识机制，可能存在的问题是用户电脑被劫持为肉鸡，黑客操控肉鸡进行挖矿，反而造成了算力中心化。由于矿机很难被远程劫持，所以相对来说购买矿机并消耗电力是 POW 共识机制下挖矿唯一可能的选择，这保证了获得奖励的人付出对应多的成本。以太坊和其他公链有意采用包括 POS 在内的其他共识机制，以限制用 ASIC 矿机挖矿的可能。这会对硬件制造商产生一定的影响，但他们也会相应地生产对应新算法的矿机。ASIC 挖矿比较担心的是共识算法的不定期变化，而这会极大影响矿工对购买矿机的需求，进而缩减硬件制造商的利润。

硬件制造商面临的主要困境是收入来源单一。由于其主要利润都来自销售矿机，导致通证的价值波动对其影响较大。由于 ASIC 矿机挖矿具有特

定性，不同项目之间往往需要使用不同的矿机。这导致特定项目的风险会传导到硬件制造商身上。而且算力的增速已经放慢了脚步，未来能否继续扩大矿机销量尚未可知。

一些硬件制造商希望转向人工智能芯片方向，但人工智能芯片与挖矿芯片虽有相通之处，却不尽相同。不少拥有数十年芯片生产经验的老牌芯片生产商已经在向挖矿芯片渗透，而硬件制造商想守住自己地盘的同时从经验丰富的老手那里抢一杯羹，我们认为颇有难度。不过人工智能芯片也是未来的发展方向之一，所以市场会存在一定的增量空间。

1.3.3.4 安全防护

在很多人的印象中，区块链是绝对安全的，不可能存在数据篡改，因此无从谈起安全防护。其实不然。对于一个区块链项目而言，可能区块链上的数据由于结构相对简单，有足够算力支持，也有成熟模式可供借鉴，所以安全性能得到保障。但除此之外的智能合约、通证钱包等基础应用都有漏洞存在的可能性。

在区块链行业爆发式增长的 2017 年和 2018 年来，区块链领域已经发生多起重大的安全隐患，主要包括钱包被盗、智能合约部署漏洞等，还有一些交易所账户被盗事件，但这已经不属于区块链核心技术的范畴。这些安全隐患中尤为重要的是智能合约部署漏洞，因为其为许多区块链衍生技术和应用的基础。它的安全性关乎行业未来发展的路途。智能合约部署漏洞主要包括以下几方面。

（1）整数溢出。智能合约中危险的数值操作，可能导致合约失效、通证总量失控等风险。

（2）越权访问。智能合约中对访问控制处理不当，可能导致越权更改通证总量的风险。

（3）信息泄露。泄露的主要信息包括硬编码地址等。

（4）逻辑错误。代理转账函数缺乏必要的教研，可能导致基于重入漏洞的恶意转账等风险。

（5）拒绝服务。循环语句、递归函数、外部合约调用等处理不当，可能导致无限循环、递归栈耗尽等拒绝服务风险。

（6）函数误用。伪随机函数调用和接口函数实现问题，可能导致可预

测随机数、接口函数返回异常等风险。

这些风险的发现可能需要反复地校验和测试，而这很可能超出了项目方现有的能力。安全防护企业正是为发现、弥补这些漏洞，提出完整解决方案，帮助区块链项目安全成长而出现的。

这个领域的领头企业有链安科技和慢雾科技等公司。其中链安科技主要通过形式化验证方法，查找智能合约与区块链底层平台中存在的漏洞并自动给予相应解决办法。形式化验证在中国最早用于军工行业，方法是先将智能合约或其他程序的功能进行抽象，然后对代码进行抽象，最后通过数学手段证明代码能有效实现功能并且不存在错误。形式化验证的方法最显著的好处是自动化，节省了传统开发过程中不断测试、验证、评估的时间，因此很受区块链项目的青睐。目前，链安科技实现了以太坊与 EOS 两个主网已经上线的公链项目上智能合约的漏洞自动查找、常见性检查、功能满足性检查、功能正确性检查与底层架构核心代码检查等功能。

慢雾科技是一家对区块链各个领域均有所涉猎的安全审计企业。其针对加密货币交易所和加密货币钱包提供超越传统网络攻防的私钥架构安全、业务逻辑安全等方面的灰盒安全审计，其中重点是对认证与授权过程、身份鉴别管理以及节点安全的审计。对于区块链底层架构，慢雾科技从节点配置、节点通信、节点共识、合约虚拟机和官方钱包安全五个角度进行安全审计。智能合约更是慢雾科技的重点审计项目，在智能合约的安全设计、权限控制、Gas 优化等方面，慢雾科技都加强了审计力度。通过安全审计，区块链项目就相当于拥有了安全性的进一步保障，因此类似于慢雾科技这样的安全审计企业是区块链行业进一步发展过程中不可或缺的。

1.3.3.5 行业服务

区块链行业的行业服务主要包括媒体、投资机构、行业组织与行业研究机构。现阶段，以区块链为内容的财经媒体已经多达上百家，但存活良好、贴近行业、输出优质内容的媒体并不多。竞争激烈、内容重复、质量欠佳是目前区块链媒体行业的主要特点。很多媒体通过翻译国外报道、重述项目简介就可以形成内容，反映了其缺少深度挖掘能力的问题。即使是知名媒体平台，更多的也是作为资讯平台而存在，没有深度报道和翔实数据。近几个月来，有关区块链媒体的融资日趋减少，预示着行业寒冬已经到来，

唯有真正贴近项目、输出有价值内容的媒体才能渡过难关。我们认为区块链行业媒体的核心价值应该是引导舆论趋向正确的方向，关注行业技术动态，分析项目价值，建立大众与区块链从业者间良好的信息通路，传达可靠且具有深度的信息。诞生于风口与投机浪潮的区块链媒体行业还没有形成良性的行业规则，内部信息、误导信息层出不穷，恶意中伤、虚假夸耀、张冠李戴等现象屡见不鲜，项目分析浮于表面或主观臆断严重。也许区块链媒体行业还需要一段时间才能清澈下来，推动区块链行业的信息对称化和行业规则建立。

区块链行业组织作为行业内部交流和学术研讨平台，对区块链从业者了解行业进展、加快信息流通速度、建立合作等方面具有重要作用。目前比较知名的区块链行业组织有中国计算机学会区块链专委会、中关村区块链产业联盟、可信区块链联盟等。

区块链行业研究机构尚未形成规模，主要依附于行业组织或投资机构的研究部门。有关投资机构的介绍我们放在了后面，在此不再赘述。

1.3.3.6 全球市值前五十区块链项目梳理

我们从 CoinMarketCap 上整理了已发行通证并在交易所流通的部分区块链项目，摘取前 50 个作为全球区块链行业基本面貌的反映。现把项目名称和共识机制梳理如表 1-5 所示。

表1-5 全球市值前五十区块链项目梳理

基础设施层			
加密货币		公链与智能合约实现	
项目名称	共识机制	项目名称	共识机制
比特币（BTC）	POW	以太坊（ETH）	POW/POS（Casper）
比特币现金（BCH）	POW	以太经典（ETC）	POW/POS
BitCoin Private（BTCP）	POW	EOS	DPOS
BitCoin Gold（BTG）	POW	卡尔达诺（ADA）	POS（Ouroboros）
BitCoin Diamond（BCD）	POW	波场（TRX）	DPOS
瑞波币（XRP）	RPCA	小蚁（NEO）	DBFT
莱特币（LTC）	POW	量子链（QTUM）	POS
Stellar（XLM）	POS（SCP）	OmiseGo（OMG）	POS
门罗币（XMR）	POW	ICON（ICX）	无共识
达世币（DASH）	POW	Lisk（LSK）	DPOS

续表

Tether（USDT）	POR	本体币（ONT）	VBFT（VRF+BFT）
基础设施层			
加密货币		公链与智能合约实现	
项目名称	共识机制	项目名称	共识机制
ByteCoin（BCN）	POW	Zilliqa（ZIL）	POW+PBFT
Zcash（ZEC）	POW	Aeternity（AE）	POW+POS
Decred（DCR）	POW+POS	Rchain（RHOC）	POS
Verge（XVG）	POW	Stratis（STRAT）	POS
NANO/RaiBlocks	余额权重	IOST	POB
Maker（MKR）	基于以太坊	Digibyte	POW
狗狗币（DOGE）	POW		
通用应用及技术扩展层			
分布式账本		开放协议	
项目名称	共识机制	项目名称	共识机制
IOTA（MIOTA）	Tangle（数据结构）	0x（ZRX）	基于以太坊
智能资产		移动浏览器	
项目名称	共识机制	项目名称	共识机制
NEM（XEM）	POI	Status（SNT）	基于以太坊
比原链（BTM）	POW		
万维链（WAN）	POS		
商业应用层			
管理平台		社交平台	
项目名称	共识机制	项目名称	共识机制
唯链（VEN）	POA	STEEM	POB（类似于DBFT）
交易系统		云存储平台	
项目名称	共识机制	项目名称	共识机制
比特股（BTS）	DPOS	SjaCoin（SC）	POW
Waves（WAVES）	POS		
算力分享平台		票据金融服务	
项目名称	共识机制	项目名称	共识机制
Golem（GNT）	POS	Poplous（PPT）	POS
预测平台			
项目名称	共识机制	项目名称	共识机制
Augur（REP）	POS	Augur（REP）	POS
数字货币交易所			
项目名称		共识机制	
币安（BNB）		无	

表 1-5 仅选取了发行了通证的项目，所以一些出色的硬件制造、安全防护项目并未囊括其中。还有如 Hyperledger 的联盟链项目、国家主导开发的主权加密货币、未登录交易所的行业区块链项目和处于早期阶段的区块链创新企业也未纳入其中。不过表 1-5 中的企业包含了绝大多数主流的区块链方向，可以反映行业整体发展状况。需要说明的是，由于通证价值波动性大的问题尚未被解决，所以榜单随时都在发生变动。表 1-5 只是作为一个时间截面的见证。

区块链行业存在项目进度不公开、发展方向变化快、技术方向重复等特点，所以子行业划分十分困难。由于排除了硬件设施提供商、安全服务公司、媒体与行业研究机构等分支，我们在此利用项目希望实现的功能进行划分，可分为基础设施层、通用应用及技术扩展层、商业应用层和数字货币交易所四个方向。全球市值前五十区块链项目子行业分类如图 1-8 所示。

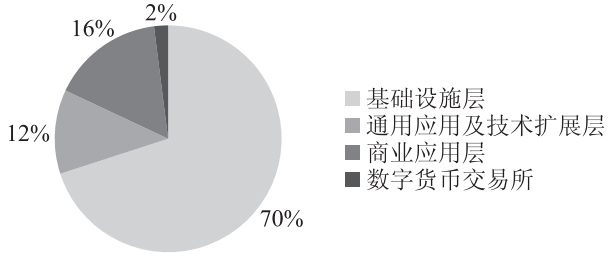

图 1-8　全球市值前五十区块链项目子行业分类

可以看到基础设施层占据了绝对的比例，达到 70%。产生这种情况的部分原因是我们将比特币之后的一系列衍生加密货币都归为基础设施层中，更重要的原因是基础设施是发展时间最长、技术投入最高、资本最密集的子行业。相当一部分早期项目在资本充足、行业认知不充分的时候吸纳资金，取得了现在的规模。

在 35 个基础设施项目中，共有 18 个加密数字货币项目，占比一半以上。其中比特币的分叉项目就达到 4 个之多。形成这种格局的一个原因是加密货币是人们认识区块链行业的窗口，也是到目前为止区块链在落地方面最成功的应用。除了比特币外，几乎所有的加密数字货币都是以比特币为基础进行改进，或扩容，或增强匿名性，抑或就是完全复制一个相同的项目。这种手段在区块链行业的早期阶段能迅速借助比特币的声望吸引投资者的

目光，但在区块链行业进入深度发展、项目比拼技术开发进度和创新能力的中期阶段，显得后劲不足。

在比特币的分叉币中，目前仍保持活力并有足够算力支持的只有比特币现金（BCH）和比特币黄金（BCG），其余的项目或者由于缺乏关注度而慢慢淡出视野，或者没有足够的改进而难以得到社区承认。在其他的衍生货币中，类似于狗狗币这样的创始团队早已脱离项目，仅靠投机者炒作生存的项目也不在少数。达世币、门罗币、Zcash 主要从匿名性上发力，但混币交易、零币零钞等技术的发展使得应用比特币达到的匿名程度也在提升。抗 ASIC 的算法现在也出现了很多种，而且有的从业者已经开始呼吁不要一味地抵制 ASIC，因为它们提供的大量算力是区块链加密安全性的保障。仅从这两个角度使一个加密货币项目独树一帜的空间已经越来越小。

在能搭载智能合约的公链开发者中，绝大多数都抛弃了单独的 POW 共识，或采用 POS，或采用新的单独共识，或采用混合共识。他们的主要目的都是开发出具有足够网络容量，能承载一定数量商业应用，实现智能合约常态化、开放性部署的区块链基础设施。但他们之间仍有方向性的不同。以太坊专攻 Casper 共识，可能还需要两年才能成型；Zilliqa 专攻分片机制；EOS 在 DPOS 共识上发力。其实最终的竞争就是看这些公链开发者谁能率先上线主网，经过检测和考验，笼住一批稳定的用户，形成完整的生态闭环。在这个过程中共识机制完善、通证经济稳定、代码漏洞少、社区良好自治都会成为决胜的关键因素。如同互联网经济一样，这很可能又是一个“老大吃肉，老二喝汤，其余人嚼骨头渣滓”的残酷竞争环境，所以现在每个公链开发者背后都已形成比较完整的开发团队和资本支持。我们认为智能合约及公链开发会成为区块链未来两年最火热，也是最值得关注的领域。

通用应用及技术扩展指的是能应用于多个项目的辅助设施。商业应用的落地则需要公链的承载。这两个领域现在并没有进入白热化的竞争阶段，因为公链体系尚不完善。可以预计，当第一个可以落地的公链项目开始上线，辅助设施和商业应用项目将呈井喷态势出现。它们其实才是区块链直接作用于消费者的端口，然而在现在，这个领域还处于迷茫的摸索状态。一些项目选择押宝以太坊，所以一切的设计都是根据以太坊设定的。这是一种收益和风险都相当程度上提高的做法，因为以太坊市值排名第二，被认为是

最有可能取代比特币地位的区块链项目。但在公链竞争如此激烈的状态下，把全部开发都集中在一个项目上确实有些太冒险了。

其实很多虚假项目、不同行业的人们对于区块链改造行业的畅想也都集中在这两个领域。由于没有公链的基础，也就没有它们落地的可能。不过公链落地之后，空气项目会很快地被淘汰出局，之前厚积薄发的项目会抢先占领市场。在之后的小节中，我们将给出一些我们观察到的具有区块链结合潜力的领域，以及正在积蓄力量的应用项目。

数字货币交易所作为非常特殊的一个区块链领域，应该算作行业服务这个子行业中。一直以来，关于数字货币交易所透明性和账户安全的问题就层出不穷，时常还可以听到掌握内部信息的人员与场外交易者勾结的新闻。我们认为这主要还是源于监管机构对其的监管态度。尽管通证是跨越主权和自由流通的，但数字货币交易所并不是，实际上也并不应该是。因为交易所并不存在于区块链的网络上，只是作为一个做市商或者交易撮合平台而存在。对交易所进行更强有力的监管有助于净化现在混乱的数字货币交易市场。这种监管可以是去中心化的，也可以是中心化的。如果是去中心化的，就要设置交易的撮合者和清算者的激励机制，对他们的行为予以奖励或惩罚。而全部的交易所信息应该对所有节点可见，以保证透明。这会伤害一些投机者的利益，但对区块链项目的长期发展是有利的。如果采用中心化的监管，需要注意避免破坏匿名性和安全性。可以考虑借鉴一些主权国家制定的法律到交易所的规则中。

其实还可以构建跨主权的交易所，交易的撮合完全由代码控制。不过这样存在的风险很大，如果代码中存在什么漏洞，发生的可能就是市场完全混乱、钱包被大规模盗用的恶性事件，对本就脆弱的区块链行业予以致命一击。而且在这种情况下，修复漏洞会变得异常困难，因为没有人拥有直接修改它的权限。

榜单特意列出各个项目的共识机制还有一个意义在于考察它们对共识机制的认可情况。现在基本各个项目比较认同的就是 POW 和 POS，其余的共识机制只在个别项目内才会被采用。

1.3.3.7 区块链项目投融资考察

据初创企业和投资机构的查询网站[①]数据，现在中国整个区块链行业内的初创项目已达 1 700 余个，基础设施方向包括共识算法、支付结算、BaaS 服务、匿名技术等，区块链应用方向包括金融、医疗、文娱、社交、能源、物流、交通、公益、房地产等诸多领域，行业服务方向包括媒体、社区、行业研究等。

区块链项目的融资手段十分多样，有发行通证、基金会提供资金、投资机构注资、成立企业等多种方式。区块链发行通证融资的方式饱受诟病，因为没有相应的监督机制保证项目方将融到的资金用于项目开发。目前比较好的解决方案有锁仓机制，类似于股票市场中新上市公司的股东存在解禁期，以防止上市前期利润冲高，上市之后套现离场的方式，利用信息不对称损害中小投资者利益。更可行的方式为尽可能分散通证的分配，确保没有人有绝对的控制权转移项目资金，形成恶意联盟的可能性也较低。

1. 传统投资机构注资

在投资机构注资的项目中，2016 年到 2019 年上半年共发生了区块链行业接近 70% 的融资事件，其中 2017 年就超过了 1/3。可见这个行业受到资本关注也只是最近两三年的事。2017 年是区块链被公众广为熟知的一年，各种项目如雨后春笋般涌现，因此也造就了一波投资的浪潮。2018 年，狂热的涌入已经逐渐转为理性的甄别，因此投资热度有所衰退。中国区块链初创企业融资年份统计图如图 1-9 所示。

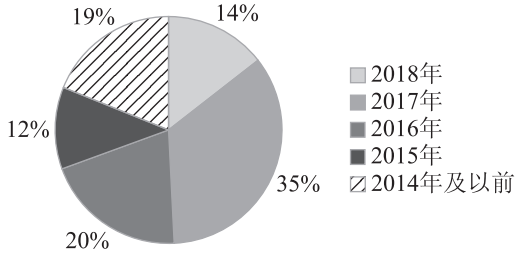

图 1-9 中国区块链初创企业融资年份统计图

在融资轮次方面，绝大多数融资都集中在天使轮和 A 轮，分别占比 31% 和 14%。可以看出行业发展非常早期。另外有 48% 的初创企业没有获

① IT 桔子

得融资，这部分中有的通过发行通证融资，但更多的还是没有受到市场认可的“空气”项目。绝大多数融资都没有披露金额，已披露的金额也从几百万到上亿元不到，呈现巨大的差异化，这反映了行业发展参差不齐的局面。预计到 2019 年绝大多数“空气”项目都会失去生命力，行业发展会出现以公链为核心的项目集群，有价值的项目开始获得市场的追捧，行业向良好态势发展。中国区块链初创企业融资轮次统计图如图 1-10 所示。

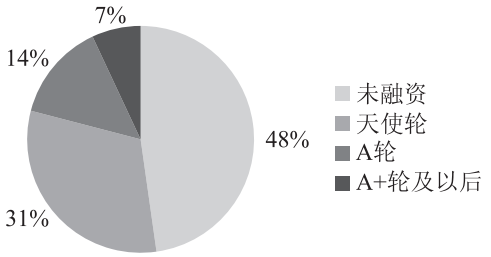

图 1-10　中国区块链初创企业融资轮次统计图

在地域分布上，区块链作为技术密集型和资本密集型产业，更加偏好北京、上海、广东这样的经济领头省份，浙江、江苏、福建等发达地区也出现了一定数量的项目，其中位于北京的区块链初创企业占比甚至达到 14%。同时中西部地区也涌现出一些优质项目，说明新的技术正在逐渐向西部渗透，为更多的人所熟知。

从投资角度来看，专注于区块链投资的投资机构已达 47 家，绝大多数都成立于 2017 年。它们的背后往往都是对区块链技术抱有极大信心的支持者和技术人员。但区块链项目现在还处于生长期，每个项目的投资回报并不可见，也难以预测估值。因此真正的投资业绩可能还要等到两年之后。

现在的区块链投资机构盈利情况难以考据，因为投资多获得的是项目通证。通证的市值不能直接对应项目的价值，也无法代表投资获利。区块链项目不同于生产型企业和服务提供商，它并没有稳定的现金流。投资获利的渠道只能是通证升值后在市场上交易卖出，存在较大的风险。而且拥有通证并不意味着拥有对项目的控制权。目前投资机构还没有形成普遍的良性投资模式，有一些更像是投机行为，甚至与区块链项目联手欺骗其他投资者。这是我们极不愿意看到的，但我们相信这种乱象会随着真正有价值的项目落地而迅速杜绝，而且会有一批更大规模、更专业化的投资机构加入其中，奠定行业良性发展的格局。

2. 去中心化投资机构

去中心化的投资机构刚出现时令人为之一振。把互联网时代人们发明的众筹模式通过智能合约的方式应用到传统投资机构中，实现去中心化决策和收益分配。如果智能合约能稳定保障通证持有者公平投票和投资收益分配，这将是一次颠覆传统投资模式的机会。然而 the DAO 的失败让我们看到了这种方式的不足，首先是应对紧急情况的反应速度。如果没有 the DAO 的延缓退出机制和以太坊社区出人意料的分叉做法，攻击者将取得一场彻底的胜利。没有设计者能保证万无一失，因此这种集资手段被暂缓地搁置了。其次，让我们考虑这种模式作出投资决策的方式。如果所有人都对某一项目进行表决，有两个好处：一是更多的人参与决策可能使得其受某一特定偏好影响较小，而且更多的人意味着更多的信息，更有可能获得项目的真实情况；二是省去了基金经理的代理成本，而这部分成本在传统的投资机构中是非常高的。但是所有人都参与投资决策也有坏处：更多的决策者意味着决策效率会变低。想想成百上千的决策者要达成统一的意见，即使采用简单多数原则，等待他们表决一次会是多么长的时间。而且这加剧了信息的分散程度。尽管更多的人意味着更多的信息，但他们缺少将这些信息有效汇总、整合并分析的能力。人数众多的网络即时通信到现在仍是一个难题。信息的不对称可能并不会提高“集智”带来的决策正确概率。不过去中心化的投资机构的出现还是给人们以无限遐想。也许某一天，更完善的代码框架和通信网络呈现在人们面前时，投资者们会选择另外一种投资方式。