区块链革命：比特币底层技术如何改变货币、商业和世界

[加]唐塔普斯科特,[加]亚力克斯•塔普斯科特

（此为重排&校订版，仅为学习所用）

第一篇：假如需要变革 8

第一章 可信的协议 9

寻找可信的协议 12

这个世界账本是如何运作的？ 16

区块链的理性繁荣 20

在数字化时代达成信任 24

互联网的回归 28

你的个人化身及身份的黑盒子 33

走向繁荣的计划 38

新平台的前景与隐患 52

第二章 引导未来：区块链经济七大设计原则 56

七大设计原则 59

1.网络化诚信 Networked Integrity 61

2.分布式权力 Distributed Power 67

3.把价值作为激励 Value as Incentive 70

4.安全性 Security 76

5.隐私 Privacy 80

6.权利保护 Rights Preserved 86

7.包容性/普惠 Inclusion 92

设计未来 96

第二篇 转型 97

第三章 重塑金融服务形象：从赚钱机器变成致富平台 98

全球第二古老行业的新面貌 **103**

八个核心功能：金融服务领域将如何实现变革 **108**

从证券交易所到区块交易所 **113**

浮士德的区块链契约 **118**

金融公共事业 **122**

银行应用软件：零售银行业务中谁才是赢家 **125**

商业界的“谷歌翻译”：会计核算及公司管理的新框架 **130**

世界账本 **133**

三式记账法：隐私保护是为了个人而非企业 **138**

声誉：你就是你的信用分数 **141**

区块链 IPO（首次公开募股） **146**

预测市场的市场 **149**

八个核心功能之路线图 **152**

第四章 重新设计公司的架构: 核心与边缘 154

打造共识系统®公司 **154**

改变公司的边界 **163**

1.搜索成本——我们如何寻找新的人才和新的顾客？ 168

2.签约成本——我们究竟同意做什么？ 174

(1)智能合约 177

(2)多重签名：智能的复杂合约 179

3.协调成本——我们应该如何协同工作？ 183

4.建立信任所需的代价——我们为何要互相信任？ 187

决定公司边界 **191**

第五章 新商业模式:在区块链上寻找新机会 198

BAirbnb VS.Airbnb **198**

全球计算：分布式应用的兴起 **203**

Dapp 的王者：分布式商业实体 **207**

自主运作的代理人 **211**

分布式自主运作企业 **218**

七大开放式联网企业商业模式 **222**
1.大众生产 The Peer Producers 223
2.知识产权创造者 The Rights Creators 228
3.区块链合作组织 Blockchain Cooperatives 231
4.按量计费经济 The Metering Economy 233
5.平台建造者 The Platform Builders 235
6.区块链上的制造业 Blockchain Makers 238
7.企业协作 The Enterprise Collaborators 240

改变你的未来：商业模式创新 **245**

第六章 万物账本：物理世界的活化 248

为人们提供电力 **250**

物联网需要万物账本 **260**

12 个颠覆的领域：物理世界的活化 **266**

经济上的收益 **275**

未来: 从 Uber 到 Suber **279**

用智能物件的世界改变你的未来 **285**

第七章 解决繁荣悖论：区块链的经济包容性 289

一头猪不是一个存钱罐 **289**

新的繁荣悖论 **293**

通往繁荣的路线图 **302**

区块链助力人道主义援助 **317**

像家一样安全？通往资产所有权之路 **324**

实施层面的挑战和领导机遇 **328**

第八章 重建政府和民主 330

有些方面还待完善 334

高性能政府服务与运作 340

赋予公民权利，服务自己，服务他人 347

第二代民主 354

区块链投票机制 359

政治和司法的替代选择 364

让公民参与到重大问题的解决中 370

21 世纪民主手段的运用 372

第九章 在区块链上解放文化产业 377

公平的音乐交易：从音乐流媒体播放到为权利定量计价 380

为艺术爱好者服务的 Artlery:将艺术家与老顾客连接起来 400

将信息传递出去：教育所扮演的关键角色 407

文化产业在区块链和大众的支持下成长 412

第三篇 机遇与隐忧 413

第十章 克服困难：实施过程中的 10 个挑战 414

1.该技术仍未能满足大规模使用 417

2.能源消耗不可持续 424

3.政府会扼杀或扭曲它 431

4.旧范式的强大既得利益者会介入 435

5.对分布式大型协作的激励并不充足 439

6.区块链会对就业带来冲击 444

7.协议的治理就像是牧放一群猫 446

8.自主运作的代理人会形成“天网机器人” 449

9.老大哥还在监视着你 452

10.罪犯们也会使用这个网络 455

这是区块链将会失败的原因，还是实施过程的挑战？ 457

第十一章 下一代的领导者 459

谁会领导一场变革？ 464

区块链生态系统：你无法在缺乏花名册的情况下分辨出参与者 469

区块链监管的警世恒言 478

那个可能会改变世界的参议员 482

去中心化经济中的央行 484

监管与治理的对比 489

区块链治理的新框架 492

下一个数字时代的新议程 506

可信的协议和你 510

序言、注释及致谢 514

注释 515

附录 区块链专业术语表 556

赞誉 560

推荐序一 区块链革命：从《失控》说起 570

推荐序二 区块链已成为金融科技的底层技术 576

致谢 583

第一篇：假如需要变革

第一章 可信的协议

就如历史上反复出现过的场景那样，技术的小精灵似乎又一次从瓶子中被释放出来了。一个（或一群）身份和动机都无人知晓的人，在历史中的一个不确定的时刻里召唤了这只小精灵。现在，如果我们能很好地利用它,这个小精灵或许能为我们所用，带来另一场变革，并有可能革新经济格局和人类社会各种事务的旧秩序。

让我们来解释一下吧。

互联网前 40 年的发展历史给我们带来了电子邮件、万维网、网络公司、社交媒体、移动网络、大数据、云计算以及物联网的早期生态。它极大地降低了搜索、协作和交换信息的成本。它降低了以下领域的准入门槛：新媒体、娱乐业、新式的零售业、新式的工作组织架构以及前所未有的数字化商业模式。通过传感器技术，互联网将智能整合到我们的钱包、衣物、汽车、建筑、城市甚至是我们的身体上。互联网已经完全渗透了我们所处的环境，在不久的将来，我们就不需要像今天这样“登陆”到互联网上，而是会通过无处不在的（互联网）技术去运营我们的业务及管理我们的生活（持续的在线生活）。

可以这么说，互联网让很多积极的改变成为可能——对那些有着接入互联网条件的人而言更是如此。不过，对商业和经济活动来

说，互联网还是存在着很大限制的。《纽约客》在 1993 年刊登过漫画家彼得•施泰纳的一幅漫画，上面写着“在互联网上，没有人知道你是一条狗”，估计在今天，这句话还是非常贴切的。在互联网上，若没有第三方机构——如银行或政府提供的校验信息，我们依然无法在彼此之间确认对方的身份，也无法在彼此间建立经济往来活动所需的信任关系。问题就出在这里——这些中间机构恰恰利用了我们对中介的需求，为了商业目的和国家安全等理由去收集我们的数据和侵犯我们的隐私。互联网技术改善了信息交换的效率，但即使是这样，这些中间机构所产生的额外成本依然让全球范围内 25 亿的人群难以负担各种金融服务。互联网曾经给很多人带来了一个期望——建立一个由点对点协议驱动的新世界，但其带来的经济和政治效益已经被证明是不对称的，权力和财富还是流向那些已经有权力和财富的人，即使他们已经没有再积极地努力做出贡献。资本们赚取新财富的速度，比大多数人都快。

相对于技术对隐私所带来的侵害，它所创造的繁荣程度并不能让人感到满意。不过，在这个数字化的时代，无论是好的还是坏的事情，技术已经处于一切事物的中心了。技术让人类更尊重和维护彼此的权利；同样地，技术让人类能够有更多的新方式去侵害彼此的权利。在线通讯以及在线商业的爆发式增长，让黑客们有更多的机会进行网络上的犯罪活动。摩尔定律预测了运算能力每年的翻倍式增长，而这也让诈骗活动和盗窃活动的活跃程度翻倍

了，这个现象可用“摩尔的不法之徒定律”1 来描述。至于垃圾信息传播者、身份盗窃者、在网上“钓鱼”的罪犯、间谍、僵尸网络入侵者（被植入恶意软件的机器组成的网络）、黑客、网络恶霸及数据敲诈者（那些用勒索软件去控制他人数据以牟利的人），这些人给互联网带来的影响也非常大。以上提到的仅仅是冰山一角。

寻找可信的协议

早在 1981 年，一些发明家们就曾经尝试用密码学去解决互联网的隐私性、安全性和包容性的问题。由于第三方机构的存在，无论这些发明家们如何尝试重新设计互联网的基础流程，还是无法完全解决这些问题[1]。在互联网上，用信用卡进行支付是不安全的——这是因为用户需要向第三方透露很多个人数据。另外，对小额支付而言，这个过程也会产生不菲的手续费。

后来，一个名为戴维•查姆（David Chaum）的天才数学家在 1993 年提出了 eCash 系统，这是一个数字化支付系统——“在技术上这是一个完美的产品，让在互联网上安全地、匿名地进行支付成为可能……在互联网上，用它来进行一些价值极低的交易是非常合适的。”2 它是如此完美，以至于当时的微软和网景公司甚至有意将其作为一个功能整合到 Windows 95 和 Mosaic 浏览器中。3 不过，当时的在线购物客们并不关心网络上的隐私和安全问题。戴维•查姆的荷兰公司 DigiCash 最终在 1998 年走向破产。

在那段时间里，戴维•查姆的一个同事尼克•绍博（Nick Szabo）写了一篇题为“上帝协议”（The God Protocol）的简短论文，这题目是模仿诺贝尔奖得主利昂•莱德曼所创的词语“上帝粒子”，象征

[1] 讨论：隐私性、安全性、包容性/普惠，这些问题是因为第三方机构的原因造成的吗？

了希格斯玻色子(Higgs boson)在现代物理学中的重要性。尼克•绍博在这篇文章中设想了一种无所不能、可以取代所有中间机构的技术协议，即让“上帝”在一切的交易中扮演可信的第三方。其设想如下：**“所有的参与方都会将其信息和价值输入到上帝的手中，上帝会可靠地决定执行的结果，并将结果输出到参与方的手中。在这个过程中，一切涉及隐私的信息都归上帝所有，没有参与方能窥视与自己无关的信息。”**[2]4 他的想法是很大胆的——在互联网上开展业务确实是要依靠“信仰的飞跃”。由于现有的互联网基础设施并不能提供必要的安全性，中间人在各种事务中就变得尤为重要了——它就如神一般的存在。[3]

自此，十年过去了。到了 2008 年，全球金融市场出现了大规模的灾难。凑巧的是，一个（或一群）名为中本聪（**Satoshi Nakamoto**）的人在这时发布了一种点对点的现金系统及其基础协议，这就是后来被称为“比特币”的加密货币[4]。加密货币（数字货币）与传统的法币[5]有所不同，因为它们不是由国家所创建的，也不是由国家所控制的。这个协议以分布式计算技术为基础设定了一系列的规则——这让在脱离可信第三方中介的情况下，数十亿的设备能

[2] http://nakamotoinstitute.org/the-god-protocols/ Originally published in 1997

[3] 翻译不住准确，原文：Because the infrastructure lacks the much-needed security, we often have little choice but to treat the middlemen as if they were deities.

[4] a new **protocol** for a peer-to-peer electronic cash system using a cryptocurrency called bitcoin. 中本聪提出的是一个「协议」。

[5] fiat currencies 法币

够在彼此之间安全地交换信息[6]。这个看似平凡无奇的举动引发了一系列的连锁反应，它使以计算机为核心设备的世界感到兴奋、害怕，同时，也释放了这个世界的想象空间。它的影响扩展到了全球范围内的商业、政府、隐私保护提倡者、社会发展活动家、媒体理论家和记者等领域和群体——这还仅仅是冰山一角。

“他们的反应是这样的，‘天啊，就是这个了。这就是我们一直在等待的重大突破’”，首个互联网浏览器的创始人、同时也是比特币与区块链相关的风险投资活动的重磅投资者马克•安德森如是说，“‘他把一切的问题都解决了。不管这人是谁，他应该获得诺贝尔奖——他就是个天才’。这就是互联网上一直被需要却又一直没有实现的分布式可信网络[7]。”5

今天，世界各地的有识之士正在思考——尝试理解这个协议的潜在影响，它通过聪明的代码就能让普通人建立信任[8]。这在以前是从来没有发生过的——在两个或多个参与方之间直接进行可信的交易，而这些交易会通过大规模协作进行校验，并由集体的利己动机驱动，而不是像以前那样由商业化的大公司去驱动[9]。

---

[6] 重要原文：This protocol established a set of rules—in the form of distributed computations—that ensured the integrity of the data exchanged among these billions of devices without going through a trusted third party.

[7] 重要原文：This is the distributed trust network that the Internet always needed and never had.

[8] 重要原文：the implications of a protocol that enables mere mortals to manufacture trust through clever code.

[9] 重要原文：trusted transactions directly between two or more parties, authenticated

它或许不是万能的，不过作为一个能让我们进行交易的、可信赖的全球平台，我们并不能低估其影响力。现在，我们将它称为可信的协议（the Trust Protocol）。

这个协议是数量正在不断增长的全球分布式账本（被称为区块链）的基础，其中比特币是规模最大的一个[10]。虽然这项技术是很复杂的，而“区块链”这个词也不是广为人知，但其主要的构思是很简单的。区块链让我们可以直接、安全地将钱发送给你，中间无须经过银行、信用卡公司或像贝宝 PayPal 这样的支付公司[11]。

这已不仅是信息互联网了，这还是价值的互联网和金钱的互联网[12]。它也是让每个人去获取什么信息是真的平台，至少对它所存储的结构化信息来说是这样的。在底层，它是一个开源代码：任何人可以免费下载、运行和使用它，以及开发用于管理在线交易的新工具。因此，它可能释放出无数的新应用和至今仍未实现的新能力，有潜能改变很多东西。

---

by mass collaboration and powered by collective self-interests, rather than by large corporations motivated by profit.

[10] 重要原文：This protocol is the foundation of a growing number of global distributed ledgers called blockchains—of which the bitcoin blockchain is the largest.

[11] 重要原文：Blockchains enable us to send money directly and safely from me to you, without going through a bank, a credit card company, or PayPal.

[12] 重要原文：Rather than the Internet of Information, it’ s the Internet of Value or of Money.

这个世界账本是如何运作的？

World Wide Ledger

大银行和一些政府正在将区块链作为分布式账本实施，以改变信息存储和交易发生的方式。它们的目标是值得称赞的——高速度、低成本、安全性、更少的错误，以及移除中心点被攻击和出故障的可能性。这些模式并不一定内建有用于支付的加密货币。

不过，最重要的、影响力最大的区块链是建立在中本聪的比特币模式之上。下面是它们的工作方式。

比特币或其他加密货币并不是存储在某个地方的文件里的；它以交易的形式存储在一个区块链中——类似于一个全球表格(spreadsheet)或总账(ledger)中，这个区块链会利用比特币的庞大的点对点网络的资源去校验和批准每一笔交易。和比特币的区块链一样，每一个区块链有如下特点：

- 区块链是分布式的（distributed）：它运行在由全球志愿者提供的计算机上；黑客们并不能通过入侵某个中心化的数据库去破坏这个系统。

- 区块链是公开的（public）：任何人都能在任何时候查看区块链上的信息，因为它是存在在网络中，而不是存在于一个负责负责审计、保管记录的中心化机构中。

- 最后，区块链是加密的（encrypted）：它使用了高强度的

公钥、私钥加密算法（而不是像保险箱使用的两把钥匙）去维护虚拟世界的安全性。你不需要担心塔吉特百货、家得宝(美国家居连锁店)或美国联邦政府系统里的脆弱的防火墙，也不需要担心摩根士丹利职员可能发生的盗窃行为对系统的影响[13]。

在比特币网络中，每十分钟，就如比特币网络中的心跳节奏一样，在这个周期内发生的交易将会被确认、清算，并存储在一个首尾相连的区块结构上，这样就构成了一个链条。每一个区块都得对此前区块的加以引用，它才能有效。这个结构能够为价值交换活动加盖永久性的时间戳，让任何人都不能篡改这个账本[14]。如果你想盗窃一个比特币，你就必须在众目睽睽之下改写在区块链上的这个比特币的全部历史记录，而这基本上是不可能的[15]。因此，区块链就是一个分布式账本，它代表着一个网络化的共识，关于每一笔历史交易的共识。

相对于世界范围的信息互联网（World Wide Web of information）来说，区块链就是世界范围的价值账本（World Wide Ledger of

[13] 讨论：这个关于「加密」和「安全」的讨论可能有误。按我的理解，区块链并没有安全性，公钥相当于地址（或电子邮箱地址），私钥相当于门钥匙（或邮箱密码）。这种设置和安全性基本上毫无关系。

[14] 这是区块链的最基本原理。

[15] 疑问：那么比特币被盗是怎么回事？为何无法追回？

value）。它是一个分布式账本，任何人都能下载这个账本，在自己的电脑上运行[16]。

一些学者认为，复式记账法（double-entry bookkeeping）的发明让资本主义和民族国家得以走向繁华。通过编程，这个记录经济交易的新型数字账本几乎可用于记录一切对人类而言有价值和重要的事物：出生证和死亡证、婚姻证书、契约和所有权凭证、教育学位、金融账户、医学流程、保险偿付、投票、食物溯源以及其他能用代码来代表的事物。

这个新型的平台能用于大部分数字记录的实时对账（a reconciliation of digital records）。事实上，在不久的将来，现实世界的数十亿智能设备将能够进行重要信息的感知、响应、通讯和共享工作——从保护我们的环境，到管理我们的健康信息，它们几乎是无所不能的。一个用于连接一切事物的物联网（Internet of Everything），需要依赖一个能记录一切事物的账本（万物账本，Ledger of Everything）。商业、贸易和经济需要一个数字化清账技术(a Digital Reckoning)。

所以，为什么你应该关注？我们相信事实能让我们自由，分布式的信任则会给各行各业的人们带来深远的影响。作为一个音乐爱好者，或许你想用艺术品作为谋生的手段；作为一个顾客，或许

[16] 重要原文：Like the World Wide Web of information, it’s the World Wide Ledger of value—a distributed ledger that everyone can download and run on their personal computer.

你想知道眼前的汉堡肉来自何方；作为一个移民人士，或许你已经对汇款到家乡所涉及的高昂费用忍无可忍了；作为一个来自沙特阿拉伯的妇女，或许你想买一本时装杂志；作为一名救援人员，或许你需要确定某块土地的主人，这样你才能在地震后帮助他们重建家园；作为一个公民，或许你已经难以忍受意见领袖们缺乏透明度和问责度；作为一名社交媒体的用户，或许你觉得你产生的所有数据对你来说应该是有价值的，而且你的隐私权是不可忽视的。即使是在本书行文之际，创新家们也正为这些方面的需求创建基于区块链的应用程序。这仅仅是一个开始。

区块链的理性繁荣

毫无疑问地，区块链对每一个机构来说都有着深远的影响，这也是很多聪明的、有影响力的人都对此技术感到兴奋的原因之一。本•罗斯基（Ben Lawsky）还辞去了他在纽约金融服务局的负责人职位，专门创建了一个关于这个领域的顾问公司。他告诉我们：“在五到十年内，金融系统或将面临重大变革，而我想参与到这个改变当中。”6 布莱思•马斯特斯在她 20 多岁的时候就成了摩根大通的董事总经理，现在，她也成立了一个专注于区块链技术的初创企业，期望促进产业的转型。《彭博市场》的 2015 年 10 月刊将她放在封面并配上“这一切都与区块链有关”的标题。另外，《经济学人》2015 年 10 月刊的封面文章《信任的机器》(The Trust Machine)如是说——“比特币背后的技术有可能改变经济运行的方式”。7 对《经济学人》来说，区块链技术是“一个如实记录事实的大型链条”。世界各地的银行纷纷组织一流的团队去调查这其中可能存在的机会，这些团队里面还有不少的杰出技术人员。银行家们喜欢安全性、零摩擦及即时交易的概念(secure, frictionless, and instant transactions)，但他们中的一些人在开放性、去中心化及新式货币的概念面前退缩了(openness, decentralization, and new forms of currency)。金融服务产业已经重新打造并私有化了区块链技术，将其称为分布式账本技术(distributed ledger technology)，以期将比特币的优点（安全性、

速度、成本方面）与一个需要银行或金融机构授权才可使用的完全封闭系统结合起来。

对它们而言，区块链是一个比它们现有方案更可靠的数据库（database），这个数据库可以让关键利益相关者（买家、卖家、托管人及监管者）保留一个共享的、不可更改的数据库，它可以降低成本、降低结算风险及避免中心点故障。

针对区块链方面初创企业的投资额正在增加，这有点像 90 年代的互联网公司的投资热潮那样。现在，风投资本展现出来的热情让 20 世纪 90 年代的互联网公司投资者也相形见绌。在 2014 到 2015 年，就有超过 10 亿美元的风投资本涌入到区块链生态系统中，其增长速度差不多每年翻一倍。8 “我们很有信心，”马克•安德森在《华盛顿邮报》对其进行的一篇采访报道中指出，“在 20 年后，我们就会像讨论今天的互联网那样去讨论区块链技术。”9

监管者们对这个领域的关注也很快地提上了他们的议事日程，他们纷纷成立各种专项工作组，以探索这个领域是否有可行的立法方案。俄罗斯政府已经禁止使用比特币了，而阿根廷这样的民主化政府亦是如此（一些人认为，鉴于货币危机在阿根廷频繁发生，该国政府简单地禁止比特币的行为并不明智）。而在西方，一些更为谨慎的政府正投入大量的精力和资源去试图理解，这项技术能如何改变央行的角色和货币的本质，也可能改变政府的运作以

及民主本质 。加拿大央行的副行长卡罗琳•威尔金斯认为各地银行行长们应该考虑将整个国家的货币系统转移到数字货币（digital money）。英国央行的首席经济学家安德鲁•霍尔丹编写了一份建立英国的数字货币的提议。10

这是一个热闹的时期——确切地说，这里面也有不少机会主义者、投机者甚至是罪犯参与进来了。大多数人对数字货币的初始印象是来自于 Mt.Gox 比特币交易所的破产事件或罗斯•威廉•乌尔布里希的定罪——后者是在线黑市 “丝绸之路” 网站的创始人，该网站在被美国联邦调查局查封前一直在协助非法药品、儿童色情和武器的交易，其支付系统就是利用了比特币的区块链。比特币的价格一直在剧烈地波动，而比特币的集中程度也是非常高的。一份在 2013 年进行的调查报告表明过半数的比特币集中在 937 人手上，不过今天这个数据一直在变化。11

那么，这样一个曾经与色情和庞氏骗局相关联的技术，如何能给各行各业带来有用的东西呢？首先说明，除非你是一个交易员，否则你要关注的并不应该是比特币这个投机性资产。这本书介绍的是比这个资产更有意义的东西，这本书是关于底层技术平台的力量与潜力的。

这并不是说比特币或加密货币本身是不重要的，虽然有些人正极力将它们的项目与过去的这些涉及丑闻的事情保持距离。这些货币对区块链革命是非常重要的，它们是最初的、也是最重要的点

对点的价值交换，特别是金钱的交换（the peer-to-peer exchange of value, especially money）。

在数字化时代达成信任

在商业领域中，信任是对另一方遵循“诚信四原则”去处理事务的期望。这四条原则是：诚实、考虑对方利益、承担责任及透明性[17]。12

诚实 honesty

并不只是一个道德上的问题，现在，它已经是一个经济问题了。若要在雇员、合作伙伴、顾客、股东以及公众之间建立信任关系，组织就必需真实地、准确地、完整地将信息与各方交流。组织不应该通过忽略某种事实的方式撒谎，或通过增加事情的复杂程度以达到混淆细节的目的。

考虑对方利益 consideration

在商业领域，考虑对方利益通常是指交易方会诚心诚意地进行价值的交换或让渡，而信任关系的建立，需要建立在对各方利益、需求及感受的考虑上，需要在彼此间心存善意。

[17] 这个定义是在 Don Tapscott and David Ticoll 所著的《The Naked Corporation》一书中提出来的(New York: Free Press, 2003).

承担责任 accountability

意味着对利益相关方做出明确的承诺，并严格恪守该承诺。个人和机构必需展示出他们有信守承诺并承担违约责任的决心，若他们自己能提供相关的证明，或第三方机构的专家能负责对其履约能力进行验证，那就更好了。个人和机构不应该逃避或推卸自身的责任。

透明性 transparency

意味着以公开透明的方式运作。若外界有 “他们在隐藏什么事情”的想法时，这就表明该组织运作的透明度不高，最终可能会失去外界的信任。当然了，各公司的商业秘密和其他专利信息应当受到保护，但当涉及一些与顾客、股东、雇员和其他利益相关方时，还是有必要建立一个积极的、开放的沟通渠道，才能获取对方的信任。通俗点说，公司应当开诚布公，才能在未来走向成功。

在商界或其他机构中，一场前所未有的信任危机似乎已经出现了。公共关系公司埃德尔曼的《全球信任度》调查指出，在机构（特别是公司）中的信任度已经倒退到 2008 年经济危机时的低潮。

埃德尔曼的调查指出，即使是过去被视为固若金汤的技术性产业（目前还是最受信任的商业领域），在全球的多数国家中也出现了信任程度的倒退，这样的情况以前并没有出现过。在全球范围内，公司高管和政府官员们继续被评为最不值得信任的信息来源，其可信任程度远落后于学者或产业专家们。13 类似的还有盖洛普民意测试中心在 2015 年进行的一份调查报告，表明在美国人对机构的信任程度的对比中，商业机构处于 15 类被调查机构的倒数第 2 名，仅有不足 20%的受访者表明他们对商业机构有相当或足够的信任。在这个排行榜中，美国的国会是最后一名。14

在区块链出现之前，商业领域的信任关系通常要依赖于正直、诚信的个人、中介机构或其他组织才能建立起来。我们通常对自己的交易对手了解不足，更不用说考察他们是否诚实可靠（integrity）了。正因为如此，在网上交易中，我们逐渐地对第三方形成了依赖性，让他们负责给陌生人提供担保，并由他们负责维护与网上交易相关的交易记录、执行商业逻辑和交易逻辑[18]。这些强大的中介机构(intermediaries)——银行、政府、PayPal、维萨(Visa)、优步（Uber）、苹果、谷歌及其他数字化的巨头，从中获取大量的价值 。

[18] Because we often can’ t know our counterparties, let alone whether they have integrity, we’ ve come to rely on third parties not only to vouch for strangers, but also to maintain transaction records and perform the business logic and transaction logic that powers commerce online.

在正在兴起的区块链世界中，信任关系的建立是基于网络的，甚至源自网络上的某些物件的。密码学安全公司 WISeKey 的卡洛斯•莫雷拉称，新技术（即区块链）能有效地把信任委派出去，甚至可以相信物体[19]。“如果有这样的一个物体，不论它是一个传感器、通讯塔、灯泡还是心脏监测仪，如果它的工作状况或付费不被信任，它会自动被其他物体拒绝。”15 账本自身就是信任关系的根本依据。16

需要说明的是，这里的“信任”是与买卖商品和服务、信息的可信性及保护相关的信任，而非在所有商业事务中的信用[20]。不过，在本书中你会读到一个可信信息的全球账本（a global ledger of truthful information）如何能将正直性植入到我们的机构中，并创造一个更安全、更可信的世界。股东和民众将会期望所有上市公司和由纳税人养活的机构至少将它们的金库（treasuries）放到去区块链上运行。这样的话，通过增加了的透明度，投资者们将能看到某个公司的 CEO 是否应得到巨额的奖金。由区块链驱动的智能合约将会要求交易对手方遵守他们的承诺。而选民们将可以看到他们选出来的代表们是否诚实和财务清白。

[19] 英文原文： the new technologies effectively delegate trust—even to physical things.

[20] 英文原文： To be clear, “trust” refers to buying and selling goods and services and to the integrity and protection of information, not trust in all business affairs.

互联网的回归

互联网的早期就如年少时的天行者卢克（《星球大战》中的一个角色）一样，人们相信即使是来自艰苦的沙漠星球的儿童都能推翻一个邪恶的帝国，并通过建立一个互联网公司去开创新的文明体系[21]。那显然是很幼稚的，不过很多人（包括一些现在的人）希望互联网展现出像万维网那样的影响，能够逆转某些产业领域的既定格局。在这个格局中，少数人掌握多数的权力，外来的人很难往这个权力架构上攀登，更莫谈推倒它了。

与传统的中心化的旧媒体不一样的是，新式媒体是以分布式、中立的形式存在的，每个人都可以成为一个积极的参与者，而不仅仅是被动的接受者。

互联网上的低成本、大范围的点对点通信手段能弱化来自阶级的影响，有机会让发展中国家的民众融入全球经济中。

在这种模式下，某个人的价值和声誉来源于其做出的贡献，而不是他的身份或社会地位。如果你在印度努力工作，加上你本身是很聪明的话，这些长处都会给你塑造良好的声誉。世界将会变得更扁平化，更符合能者居之的理想（meritocratic），更灵活及更

[21] The first era of the Internet started with the energy and spirit of a young Luke Skywalker—with the belief that any kid from a harsh desert planet could bring down an evil empire and start a new civilization by launching a dot-com.

有流动性。更重要的是，技术将能够造福于所有人，而不只是为了少数人的财富增长服务。

以上提到的这些构想，其中的一部分已经实现了。维基百科、Linux开源操作系统或银河动物园（Galaxy Zoo）天文学星系图像分类项目都是大规模协作的例子。外包行业和联网的商业模式让发展中国家的民众能够更好地参与到全球经济中。今天，20 亿的人在进行平等的协作。我们都能获取信息，这是前所未有的。

不过，帝国们进行了反击，这似乎是一个越来越明显的迹象了。集中在商界和政界的力量根据自己的需要，改写了互联网最初的民主架构的理想。

现在，大型机构已经控制并拥有这种新型的生产和社交工具，这包括其底层基础设施；其巨量的、增长中的数据集；其正日渐用于商业和日常管理的算法；其海量的应用程序（apps）；以及日渐呈现出来的惊人能力，机器学习及自动驾驶汽车等。从美国硅谷到华尔街，到上海，再到韩国首尔，新式的贵族们正利用其既有优势，运用这种前所未有的非凡的技术、其设计目标就是让人们成为高度活跃的经济主体，从而创造出惊人的财富，并巩固其对经济和社会的力量及影响。

早期的数字化先行者们曾警示过将会发生的一些令人担忧的阴暗面，而现状与他们曾经发出的警示已经相差无几了。17 在大多

数发达国家里，尽管其国内生产总值有所增长，但就业机会的增长速度一直不如人意。这个世界的财富一直在增长，而社会不公平的程度也随之增加。强大的技术公司已经不再重视过去的那种开放、分布式、平等和带来机会的网络，而是将重心转移到了线上的封闭式系统或专有的、只读的应用程序，这与其他事情一起，就将对话的渠道切断了[22]。企业的力量已经将这些美好的点对点、民主化和开放的技术作为无节制地获取利益的手段。

这样的结果是，经济的力量变得更锐利、更集中及根深蒂固。互联网原本的构想是将数据更广泛地、更民主地分发出去，但现在大多数的数据已经被少数的实体收集、利用起来，而且这些实体还利用这些数据去控制和积累更多的权力，这对大众来说并不是一件好事。如果你积累了足够的知识及随之而来的权力，你就可以通过产出更多的专有知识去巩固你的地位。无论如何，特权（privilege）的重要性已经击败了贡献和实效（merit）——不管这些特权是怎么来的。

还有，强大的“数字巨无霸”，如亚马逊、苹果和脸书（Facebook），曾几何时它们也是互联网的初创企业，现在正在私有的数据池里收集民众和机构产生的数据，并没有将它共享到网络上。当他们为顾客创造带来很大价值的同时，也使得数据成为一种新型的资

[22] 重要原文：Powerful technology companies have shifted much activity from the open, distributed, egalitarian, and empowering Web to closed online walled gardens or proprietary, read-only applications that among other things kill the conversation.

产，甚至比以前的资产都更有价值。这种趋势也侵害了我们传统的个人隐私和自主权的价值观。

各国的政府使用互联网去改善运作和服务的效率，不过它们也在部署各种技术去监视甚至是控制民众。在很多民主国家，政府使用信息与通信技术去监视公民、改变公众意见、推动其狭隘利益、破坏权利和自由，最终目的是保留权力。

当然了，实际的情况也不完全符合某些人提出的“万维网已死”的观点。万维网对数字世界的未来是极端重要的，我们所有人应当行动起来捍卫其发展。另一方面，在如万维网联盟这样的机构里，他们的成员也在积极抗争，以让互联网变得更公开、中立及不断进化。

现在，采用区块链技术，一个新的可能性的世界正在展开，它可能逆转上述趋势。 这个真正的点对点运作的平台（a true peer-to-peer platform），让我们在本书里讨论的很多令人兴奋的事情成为可能。我们可以掌控自己的身份和个人数据。我们可以进行交易，在无须强大的中介机构充当金钱和信息的仲裁者的情况下创造和交换价值。数十亿被排除在经济体系外的人很快有望加入全球经济体系。我们可以保护自己的隐私，并使用自己的信息谋求自身利益。我们可以保证新事物的创造者能够得到来自他们知识产权的补偿。我们或许不需要通过重新分配财富的方式去解决日益恶化的社会不平等问题，而是通过在一开始就改变财富分配

和创造的方式去实现。这样，来自世界各地的人，无论他们是农民还是音乐家，都可以更全面地、更优先地享有他们所创造的财富。这似乎是有无限的想象空间。

若要打个比方的话，比起上帝来说，这更像是《星球大战》里的尤达大师的角色。这个新式的协议，让一个急需可信协作关系的世界看到了曙光，这已经是很了不起的事情了。

你的个人化身及身份的黑盒子

在历史进程中，每一种新式的媒介都让人们跨越了时间、空间甚至是躯体的局限性。这样的能力最终让我们重新审视存在主义者们对身份的观点：我们是谁？作为人类，意味着什么？我们如何能对自身进行概念化？就如马歇尔•麦克卢汉观察到的结果那样，媒介即信息（the medium becomes the message over time）。人们塑造媒介，并被媒介塑造 。我们的大脑、机构和社会都在适应这个趋势。

“今天你需要一个授权机构给你提供一个身份认证工具，如银行卡、飞行常客卡或信用卡。” 18 WISeKey 的卡洛斯•莫雷拉说。在出生时，你的父母会给你起名字，而在政府注册的产科医生或助产士会给你接生并记录你的脚印、重量和身高，双方对时间、日期和出生地进行确认并在出生证明上签字。现在，他们可以在区块链上登记这个证书，并将其与出生公告和大学基金关联起来。你的朋友和亲戚可以将比特币发送到你的账户上，以资助你的高等教育。这样，你的数据流就开始运行了。

在互联网的早期，汤姆•彼得斯写道，“你就是你自己的项目”。19 他的意思是，工作和职位已经不再是定义我们的唯一要素。现在若要找一句类似的话，那就是“你就是你自己的数据”。不过这其中的问题正如卡洛斯•莫雷拉说的那样——“现在，身份是你

的，但你的身份在世界中的活动所产生的数据却是由他人所掌管的。”20 大多数的公司和机构眼中，你就是一堆数据——这些数据来自你在互联网上的活动踪迹。它们收集你的数据并将其变为一个“虚拟的你”，并通过这个虚拟的身份给你提供很多难以想象的便利。21 不过，这样的便利是要付出代价的，那就是隐私权。我并不赞同那种“隐私权已经没希望了，别执着了”的思想。22 隐私权是自由社会的基石。

“人们将身份看得太简单了”，23 安全专家安德烈亚斯•安东诺普洛斯如是说。我们用“身份”这词去描述自我、这个自我在世界中的映射以及这个自我或其映射所带来的属性。这些信息或许会来源于自然界、国家或私营机构。我们或许会有一个或多个角色，及随之带来的一系列指标。想象一下你的上一份工作——你角色的变换是由于工作需要做出的改变，还是由于你的职位的变化？

想象一下，如果这个“虚拟的你”能真正地被你掌管，那么世界会变成怎么样？这是你的个人化身，它“生活”在你的身份所构成的黑盒子里，你可以从你的数据流中获得经济利益，当有人申请对你的数据进行访问时，你可以决定向对方公开特定的数据。[23]你的驾驶执照为什么要包含除了“你已经通过驾驶考试并且有能力开车”以外的信息呢？

[23] 重要原文：What if “the virtual you” was in fact owned by you—your personal

想象一下，如果有一个互联网的新时代，你的个人化身能够管理和保护你的黑盒子里面的内容。这个可靠的软件仆人会根据具体的情况向对方公布必需的细节或金额，同时妥善地处理在网络活动中所产生的各种遗留信息，以保护你的隐私权。

这听上去可能像《黑客帝国》或《阿凡达》这类电影里描绘的科幻故事。不过，今天的区块链技术让它有机会成为现实。以太坊生态圈区块链公司共识系统®（Consensus Systems）的首席执行官约瑟夫•卢宾将这个概念称为在区块链上的“永久数字 ID 和角色”。“在与大学的朋友互动的过程中，我展示出来的自己与我在芝加哥联邦储备银行演讲时是不一样的”，他说，“在这个在线数字经济里，我会在拥有不同身份的平台展示出我各方面的特质，并与这个世界进行互动。”约瑟夫•卢宾希望拥有一个‘典型的身份（canonical persona）’——这个版本的他会缴税、申请贷款及购买保险。“我或许会有一个业务上的身份以及一个家庭里的身份，以与我的‘典型的身份’相关的事务隔绝开来。我或许会有一个游戏玩家的身份，这我是不希望与我的业务身份联系在一起的。我甚至可能会有一个暗网上的身份，永远不会跟其他的身份联系在一起。”24

avatar—and “lived” in the black box of your identity so that you could monetize your data stream and reveal only what you needed to, when asserting a particular right.

你的黑盒子可能会包含以下的一些信息:政府颁发的身份 ID、社保号码、医疗信息、服务账号、金融账号、文凭、执业证书、出生证明、其他证书以及一些你并不希望公布但想要产生经济价值的个人信息，如性取向或身体状况等，这些都可以用于民意调查或研究性学习。你可以根据特定的目的，在某个特定的时间段将这些数据公布给特定的机构。你可以将你身份属性的一个子集发送给你的眼科医生，以及一个不同的子集发送给你希望进行投资的对冲基金里。你的化身可以替你回答“是与否”的问题，而不需要公布你的实际身份，这些问题可能包括：“你的年龄是 21 岁还是更 21 岁以上？你在过去三年内每年收入超过 10 万美元吗？你的身高重量指数在正常范围内吗？” 25

在现实世界中，你的声誉是本地化的，你的本地商店的店主、你的雇主以及在一个宴会上碰到的朋友都对你有特定的看法。在数字经济里，你的化身中不同身份的声誉是“便携”的。这样的便携性将会把世界各地的人们带入数字经济里。在非洲，拥有一个数字钱包和化身的人将可以建立自己的声誉，而这样的声誉往往是在如贷款创业这样的事情上是必需的。“看，这些人都认识我并给我作担保。在财政能力上我是可以被信任的。我是全球数字经济的一个自治的公民。”

身份只是其中的小部分。其他部分是一个身份云，这个身份云是由那些松散或紧密地与你的身份联系起来的信息组成的。如果我

们尝试将这些信息记录到区块链这个不可篡改的账本上，我们就无法理解社交互动的精妙之处，也会失去“遗忘”带来的好处。人们永远都不应该由自己状态最差的那个时候定义[24]。

[24] 重要原文：If we try to record all these into the blockchain, an immutable ledger, we lose not only the nuance of social interaction but also the gift of forgetting. People ought never be defined by their worst day.

走向繁荣的计划

- ☐ 创建一个真正的点对点共享经济
- ☐ 以高速、包容的目标重构金融体系
- ☐ 在全球范围内保护经济权利财产权
- ☐ 终结汇款的高费用
- ☐ 消除对外援助中官僚主义和腐败
- ☐ 让价值的创造者先受益
- ☐ 重构作为资本主义引擎的公司架构
- ☐ 让物体活动起来并让它们工作
- ☐ 培育区块链企业家
- ☐ 实现为人民所有并为人民服务的政府

这个可信的协议驱动了数十个项目，在这本书中你将会了解到它们的故事。繁荣首先是关于一个人的生存水准。若要实现繁荣，人们必需有手段、工具及机会去创造物质财富及在经济上兴旺发

达。不过对我们来说它包括了更多——人的安全性、安全的环境、健康、教育、环境的可持续性、改变和控制自身命运及参与到经济和社会中的机会。

为了实现繁荣，一个人至少需要能够接触到一些基本形式的金融服务以存储和移动价值，另外还要有通信及交易工具以接入到全球经济当中，最后是土地所有权及其他合法持有资产的安全性、保护及执行措施。26 这些以及更多的特性就是区块链所展示出来的潜力。

这些故事能让你感受到一种未来——为每一个人带来繁荣，而不只是给富人和强权者带来更多的金钱和权力。你甚至能感受到一个我们能拥有自己的数据并保护隐私权和个人安全的世界。那是一个开放的世界，每一个人都可以为我们的技术基础设施贡献力量，而不是由被围墙包围起来花园，由大公司给我们提供私有的应用程序.那是一个当前的数十亿被排挤在主流经济秩序之外的人群能够参与到全球经济并分享其成果的世界。下面，我们就来给你描绘一下这个世界。

创建一个真正的点对点共享经济

Creating a True Peer-to-Peer Sharing Economy

当专家们讨论“共享经济”的例子时，通常会谈到 Airbnb(空中食宿)、Uber（优步）、Lyft（打车应用“来福车”）、TaskRibbit（劳务平台 “跑腿兔”）以及其他的一些平台。这是一个很好的概念——体系中的每一个参与者创造并分享价值。

不过这些商业模式其实跟 “共享”(sharing)的关系不是太大。事实上，这些商业模式之所以走向成功，恰恰是因为它们并不进行共享(share)——它们是聚合（aggregate）的模式，这是一个聚合经济。

Airbnb 这个市值 250 亿美元的硅谷宠儿专门将空闲的房间资源聚合起来。其他的一些业务模式通过它们的中心化、私有的平台将闲置的汽车、设备以及杂务工人聚合起来，并将这些资源转卖出去。在这个过程中，它们为了商业目的进行数据的收集。这些公司在十年前并没有出现的原因是当时并没有技术上的先决条件，如无处不在的智能手机、完整的 GPS 功能以及复杂的支付系统。

现在，有了区块链技术，就又有了彻底改造这些产业的技术条件了。今天的曾经的巨型 “颠覆者” 快要被颠覆了。

想象一下如果不使用中心化的平台，而是用去分布式技术实现的 BAirbnb（区块链版本的 Airbnb），这样实质上就会是一个由其成

员共有的合作社（协作组织）。当有潜在的租客希望租一个房间时，这个 BAirbnb 软件就会在区块链上搜索所有的房源，并将符合租客要求的房源过滤后显示出来。由于这个网络会在区块链上存储交易的记录，这样一个好评就会提高房源提供者的声誉度并塑造他们的身份。这样，就不需要由一个中介机构去负责这个事情了。以太坊区块链的创始人维塔利克•布特因称：“大多数技术都是趋向于将自动化的技术应用在边缘的地方去做一些烦琐的任务，而区块链是在中心实现自动化的。区块链不会让出租车司机失业，而是会让 Uber 失业并让出租车司机直接为顾客服务。”[25]27

以高速、普惠的目标重构金融体系

Rewiring the Financial System for Speed and Inclusion

金融服务产业是全球经济发展的动力，但它现在已经存在着不少问题了。其中的一个问题是，这可能是世界上中心化程度最高的一个产业，而且技术变革在其中的进展非常缓慢。由银行等机构

[25] “Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.”

组成的旧式金融秩序像一座座城堡一样，不遗余力地维护垄断的体系并给颠覆性的创新设下障碍。这个金融体系同时也是运行在已经过时的技术上，而且是被可以追溯到 19 世纪的监管规则所治理的。它里面充满了相互矛盾的事情，发展状态也不平衡，使得其有时运行得很缓慢，经常出现安全性问题，其运作过程对很多利益相关的人来说也非常不透明的。

分布式账本技术可以将很多金融服务从旧式机构的束缚中解脱出来，促进竞争与创新，这对终端用户来说是很有好处的。虽然很多人已经能连接上互联网了，但是数十亿人还是被排除在主流的经济体系之外，这其中的原因很简单，金融机构并不将银行业务这样的服务提供给他们，是因为他们对银行来说是一类无法盈利及高风险的顾客。通过区块链技术，这些人不仅能被连接起来，更重要的是能被包容到金融活动里面，能够进行购买、借贷及出售等活动，因此也有了一个创造繁华生活的机会。

现有的机构可以将利用区块链技术进行自身的转型——如果它们能找到一个领导者去做的话。这项技术有希望为这个产业带来变革，让其发展得更好——从银行到证券交易所、保险公司到会计事务所、经纪商、小微贷款提供商、信用卡网络、房地产经纪以及金融产业的其他机构。当每一个人都共享同样的分布式账本时，交易结算可以即时完成，而不需要等待几天，每个人都可以

看到执行结果。数十亿的人将会受益于这项技术，这样的转型将会解放与赋能世界各地的企业家。

在全球范围内保护经济权利财产权

Protecting Economic Rights Globally

与我们的资本主义民主制度有着不可分割的联系——杰弗逊在《独立宣言》的初稿中将生命、自由和对财产权的追求列入了人类不可剥夺的权利中，而不是后续版本中改写成的“对幸福的追求”。28 这些有雄心壮志的原则为我们今天在发达世界里享有的现代经济和社会秩序奠定了基础，但直到今天世界上很多人还没法享受到这些权利。这个世界虽然在生命权和自由权的保护问题上有了一些进步，但世界上的大部分财产持有者的房产或土地可能会被腐败的政府官员们肆意地剥夺——这个过程只需按下中心化的政府产权数据库里的一个软件按钮即可实现。如果没有财产所有权的证明方式，土地所有者不能得到贷款、申请建筑许可证或出售该财产，而且这些财产随时可以被剥夺。这都是通往繁华的障碍。

著名的秘鲁经济学家、自由民主学院主席及世界领先的经济学者赫尔南多•德•索托表示，世界上多达 50 亿的人口并不能完全地参

与到全球化所创造的价值中，因为他们对土地的所有权得不到保证。他认为区块链能够改变这个现状。**“区块链的中心思想是商品的所有权可以被交易——不管它们是金融、实体或智力资产。其目标不仅仅是记录这个地块，还记录所涉及的所有权，这样权利的所有人就不能被侵犯了。”**29 统一的财产权有可能为全球正义、经济增长、繁荣及和平的新议程奠定基础。在这个新的范式里，权利的保护并不是通过枪械来实现的——而是通过技术。“区块链是为一个由现实（而不是虚幻）事物所支配的世界而设的。我认为那是很有意义的。”30 赫尔南多•德•索托说道。这是一项去中心化的技术，其中没有中心化的机构去控制它，每一个人都知道其中在发生的事情，它里面的记录会被永久保存起来。

终结汇款的高费用

Ending the Remittance Rip-off

每一份评估加密货币相关收益的报告、文章或书籍都讨论过在汇款业务上的应用，这是有正当理由的。在进入发展中世界的资金流中，最多的一部分并不是来自外国援助或国外直接投资，而是其身处海外的国民给他们的贫穷国家寄回去的汇款。这个过程需要时间、耐心，有时还需要每星期跑到同样的电汇办事处的勇气

（可能坐落在治安不良的地区），每次都要填写同样的文件及支付同样的 7%的费用。其实，有更好的途径能够解决这个问题。

去中心化汇兑公司 Abra（后文统称“Abra”）和其他的一些公司正在使用区块链来搭建一个支付网络。Abra 的目标是让其每个用户都成为一个出纳员，资金从离开一个国家和到达另一个国家的整个过程只需要几个小时，在以前这是需要一个星期的；在费用方面，这种方案只需要 2%而不是以前的 7%甚至更高的费用。Abra 希望它的支付网络的节点能够超过世界上所有的实体 ATM（自动提款机）数量的总和。西联汇款花了 150 年的时间才在世界范围内达到了 50 万名代理人，而 Abra 将会在第一年拥有同样数量的出纳员。

消除对外援助中官僚主义和腐败

Cutting Out Bureaucracy and Corruption in Foreign Aid

区块链能解决外国援助项目上的问题吗？2010 年的海地地震是有史以来最致命的自然灾害之一，约有 10 万~30 万的人口遇难。海地政府后来被证明是一个累赘——全球的社区给红十字会捐

献了超过 5 亿美元的资金，而一份事后的调查报告表明，这些资金有不少是被滥用的，一部分甚至直接消失了。

区块链可以在外国援助分发的过程中移除不必要的中间人的角色。其次，区块链作为一个不可篡改的资金流向管理账本，让机构具有更多的可追责性。你可以在智能手机上跟踪你给红十字会捐赠的每一笔钱（从其起点到终端受益的人）；也可以将资金放在托管账号上，在红十字会完成每一个标志性任务后释放相应数额的资金。

让价值的创造者先受益

Feeding the Creators of Value First

在第一代的互联网上，很多知识产权的所有人并没有得到适当的补偿。第一个例子是音乐家和作曲家与唱片公司签约了，而这些唱片公司并没有想象到互联网对这个产业带来的冲击。他们并没有拥抱这个数字时代，也没有重新构造其商业模式，逐渐地就将控制权让给了有创新性的在线内容分发商。

我们来看一下主流唱片公司对在 1999 年创立的点对点音乐文件分享平台 Napster 的反应。音乐产业里面的在位者们联手起诉这

个新企业、其创始人及其 18000 位用户，在 2001 年 7 月彻底瓦解了这个平台。Napster 的一份相关纪录片的导演亚历克斯• 温特对《卫报》说， “在大规模的文化转型的事情上，我并不喜欢黑白分明的想法，而在 Napster 这事上，在 ‘我可以分享我购买的一切东西’ 的立场和 ‘即使你只分享你已经购买的文件，你也是一名罪犯’ 的观点间之间存在着不少的灰色地带” 31 。

我们同意这个观点。与顾客共同创造价值通常是一个更可持续的商业模式，而不是去起诉他们。这个事件给音乐产业带来了不少的关注，揭露出其过时的营销实践、内容分发的低效率以及被一些人认为是 “反音乐家” 的政策。

从那时起，情况并没有发生太大的变化，直到现在。我们可以看到英国创作歌手伊摩琴•希普、大提琴家佐伊•基廷及区块链开发者、企业家们在引领实现区块链上的新型音乐生态系统。这项技术有可能颠覆每一个与文化相关的产业，而它所带来的希望是创作者可以根据自己创造的价值得到补偿。

重构作为资本主义引擎的公司架构

Reconfiguring the Corporation as the Engine of Capitalism

为身份、信任、声誉和交易管理（identity, trust, reputation, and transactions）而设的全球性的点对点平台的兴起，让我们终于有机会重建公司的深层架构，这个机构会为创新、共享价值的创建甚至是为大多数人享有的繁荣而服务，而不是只为少数的有钱人服务。这并不意味着我们要建造一个收入或影响力较小的小型机构。相反，我们说的是建造 21 世纪的公司，其中的一些可能是大型的创富创造者，在它们各自的市场都可能会很强大。我们确实认为企业将会更像网络（network），而不是工业时代的垂直化层级机构(the vertically integrated hierarchies of the industrial age)。这样的话，就有机会更民主地分发（而不是重新分发）财富。

我们也会带你预览一下智能合约、新型自主经济代理、及被称为分布式自主企业的神奇世界，在其中，智能化的软件会对很多方面的资源和权限进行管理和控制，甚至取代公司[26]。智能合约让基于新型商业模式或应用区块链技术改造的现存商业模式基础上的开放式网络化企业（open networked enterprises）成为可能。

让物体活动起来并让它们工作

Animating Objects and Putting Them to Work

[26] where intelligent software takes over the management and organization of many resources and capabilities, perhaps displacing corporations.

技术专家和科幻作家们长期期盼着由联网的传感器构成的无缝全球网络可以捕捉世界上的每一场事件、行动和产生的改变。区块链技术可以让事物进行协作，进行能源、时间、金钱这些价值单位的交换，并根据共享的需求和供应信息去重新配置供应链和生产流程。我们可以为智能设备添加元数据，并为它们编程，使得它们能够根据其他物件的元数据进行相互的识别，并根据预先定义好的情况展开行动或做出反应，这个过程无须担心由错误或篡改带来的风险。

随着物理世界的复苏，从在澳大利亚内陆需要电力耕作的小型农民，到世界各地能参与到一个分布式的区块链能源网络的房产所有者，每一个人都有机会走向繁荣。

培育区块链企业家

Cultivating the Blockchain Entrepreneur

企业家精神对一个蒸蒸日上的经济体系和一个繁荣的社会是至关重要的。互联网原本应该解放企业家们，为他们提供大公司才有的工具和能力，而无须担心随之而来的陈旧文化、僵化的流程

及固定的负担。不过，互联网公司及其创造出来的亿万富翁的耀目成就掩盖了一个令人不安的事实：在过去的三十年间，很多发达经济体中的企业家精神以及新企业的尝试一直在衰退 32 。

在发展中世界里，互联网并没有为那些受死气沉沉的政府官僚主义影响的准企业家们降低门槛。互联网也没有改变数十亿人无法获取金融服务的现状——而这些服务对创业者来说是必需的。当然了，并不是每一个人都可以成为企业家，不过即使是对那些想获取一份体面工资的普通人来说，这些金融服务和工具的缺失及政府的繁文缛节使得实现这一点也不容易。

这是一个复杂的问题，不过区块链可以在很多重要的方面实现更高的全球繁荣的程度。对那些生活在发展中世界的普通人来说，若他们希望有一个可靠的价值储存方式及与他们所在社区之外的人做生意的话，现在他们只需要有一个联网的设备就可以了。接入到全球经济中，意味着更容易获得新的信用、资金、供应商、合作伙伴和投资机会的来源[27]。哪怕你的才能或资源价值再小，也能通过区块链实现其经济价值[28]。

[27] Access to the global economy means greater access to new sources of credit, funding, suppliers, partners, and investment opportunities.

[28] No talent or resource is too small to monetize on the blockchain.

实现为人民所有并为人民服务的政府

Realizing Governments by the People for the People

你也要准备好政府及治理领域的大变革。区块链技术已经可能重塑政府运行的方式，并使其变得更高效，成本更低。它也为民主制度自身的改变创造出新的机会——政府如何能够更开放、摆脱说客的控制及以正直的价值观念行事。从投票、获取社会服务、解决社会的一些大难题及让选出来的代表们对其竞选诺言负责等事项，我们可以看一下区块链技术能如何改变作为公民及参与到政治体系中的意义。

新平台的前景与隐患

若这个“裸露”的城市里有 600 万的人 33 ，那么这项技术实现其潜力的道路上就有 600 万个障碍。另外，也有人对此技术持负面态度。一些人称这项技术还没到大规模使用的程度；一些人称这项技术很难使用，而杀手级的应用还在萌芽阶段。其他的一些观点还批评了达成网络共识所需的巨额能耗——当数以千计甚至数以百万计互相连接的区块链每天在处理数十亿的交易时，会是什么情况？到时候网络中会有足够的激励机制让人们参与进来并长期遵守规则吗？他们会不会尝试攫取网络的控制权？区块链技术会导致大量的失业吗？

这些问题应该由领导者和治理者，而不是由技术来回答。互联网的第一个纪元得以蓬勃发展，是因为它的核心利益相关方的视野及共同利益——政府、民间社会组织、开发者和像你我一样的普通人。在本书中，我们将会进一步讨论这个新的分布式范式的领导者们将需要如何参与进来，并释放一系列的经济及制度上的创新力量，以确保这项技术能实现其潜力。我们邀请你成为其中的领导者之一。

这本书源自加拿大多伦多大学罗特曼管理学院的一个 400 万美元的全球解决方案网络（Global Solutions Networks）项目,它的资金主要是由大型的技术公司及洛克菲勒基金会、史考尔基金会、美

国国务院及加拿大工业部（一个致力于寻求解决全球问题和治理方案的新机构）提供的。我们都参与到了这个项目当中。唐塔普斯科特创建了这个项目；亚历克斯领导了加密货币方面的项目。在 2014 年，我们发起了一个研究区块链革命及其对商业和社会影响的一年期项目，并将其成果归纳到这本书中。在这个项目里，我们深入思考了这个新平台能带来的好处及其风险。

如果商业机构、政府和民间团体创新家能够正确实现这项技术，我们就能舍弃一个主要由不断降低的搜索、协调、数据收集和决策制定的成本所驱动的互联网——根本目的是监控、中介和变现网上的信息和交易——升级到一个由不断降低的交易、监管、执行社会和商业协议的成本所驱动的互联网，其根本目的是保护所有交易及价值创造、分配过程的正直性、安全性和隐私性[29]。

这是策略上的 180 度大转弯。这样的结果可以是一个真正具有分布性的、包容性的、授权性的机构所构成的经济体系——最终就是合理的。通过对我们在网络上可以做的事情、如何去做、谁能参与——这些问题做出根本性的改变，这个新平台甚至能成为调和令人烦恼的社会和经济挑战的技术前提条件。

[29] we will move from an Internet driven primarily by the falling costs of search, coordination, data collection, and decision making—where the name of the game was monitoring, mediating, and monetizing information and transactions on the Web—to one driven by the falling costs of bargaining, policing, and enforcing social and commercial agreements, where the name of the game will be integrity, security, collaboration, the privacy of all transactions, and the creation and distribution of value.

如果我们不能正确地处理这项技术，区块链这个拥有前景的技术将会受到限制甚至被摧毁。在更差的情况下，它还可能成为强大的机构们用于巩固其财富的工具，或者被政府攻击，可能会成为某种新的监视型社会所用的平台。与此紧密相关系的技术有分布式软件、密码学、自主运作的代理人甚至是人工智能，这些技术都有可能失去控制并反过来对付人类。

这项技术被延迟、拖延或无法充分利用的可能性是有的。区块链及加密货币，特别是比特币，其影响力已经很大了，但我们并不会预测这项技术到底会不会成功，也不会预测它走向成功需要的时间有多长。34 预测总是一件有风险的事。就如技术理论家戴维•蒂科尔所说：“我们中的很多人在预测互联网所带来的影响时实在做得很差。ISIS 那样类型的不良现象也是被我们忽略的事情之一，而一些极度乐观的预测最后被证明是错误的。” 他说，“如果区块链像互联网那样巨型和普遍，我们对其优点和缺点的预测水平可能也会跟当初预测互联网的时候一样差。” 35

我们不再预测区块链的未来，而是积极拥抱区块链的未来。我们认为它应该成功，因为它可以帮助我们实现一个繁华的纪元。我们相信经济运行的最佳状态是它为每一个人运行，而这个新的平台是普惠的引擎。

它极大地降低了像汇款这样的资金传递活动的成本。它极大地降低了拥有一个银行账号、获得信用记录和投资的门槛。而且，它

提倡企业家精神及积极参与到全球贸易中。它催生了分布式资本主义而不是一个将资源和资本重新分发的资本主义。

每一个人应该停止与之抗争，并采取正确的步骤参与进来。我们应该利用区块链这项技术为大多数人谋福祉，而不只是为了少数人的眼前利益[30]。

今天，我们都对这个新一代的互联网的潜力感到兴奋无比。我们对正在出现的大量创新成果及其实现繁荣及更美好世界的潜力充满了热情。这本书是我们告诉你该如何对这个下一代的潮流产生兴趣， 理解它，并采取行动以确保其潜力能实现。

因此，坐下来并继续读下去吧。我们正处于人类历史的关键节点中。

[30] Everyone should stop fighting it and take the right steps to get on board. Let’s harness this force not for the immediate benefit of the few but for the lasting benefit of the many.

第二章 引导未来：区块链经济七大设计原则

加拿大瑞尔森大学隐私与大数据研究所执行理事安•卡沃基安认为：“自由是建立在隐私之上的。我第一次认识到这一点是在 30 年前，那时我刚开始参加在德国的各种会议。在隐私及数据保护方面，德国在全世界都处于领先地位，这绝非偶然。德国人民曾饱受希特勒第三帝国摧残，他们曾被彻底剥夺自由，而这一切都是从丧失隐私权开始的。在悲剧结束后，德国人民表示，“决不能再重蹈覆辙”。1

这么看来，第一代用于保护用户隐私的去中心化点对点计算平台之一 Enigma（英格码）的命名就显得颇具讽刺意味了（或非常贴切）。这名字与“二战”时期德国工程师亚瑟•谢尔比乌斯创建的一种用来转录加密信息的机器的名字是一样的。谢尔比乌斯创建英格码机本来是用于商业用途的：这一设备能够让全球各公司，及时、安全地传递交易机密、股票消息及其他内部信息。在几年内，德国的军队生产出了一个军用版本的英格码机，从而借助无线电将加密信息广播给军队。战时的纳粹党人曾利用英格码来传播战略计划、详细目标信息以及进攻时间。当时的英格码机就是施加痛苦与压迫的工具。

我们当代的英格码则是推动自由与繁荣的工具。全新的英格码由麻省理工学院媒体实验室的盖•斯金德和奥兹•内森创建，它不仅

体现了区块链公共账本的优点，即其透明性——它“为诚实行为提供强大的激励机制”，还融入了“同态加密”及“安全多方计算”技术。2 简单地说，“英格码会提取你的信息（任何信息），然后打散它们并为其加密，形成零散数据，之后再随机分布到网络节点上。它不在一个地方保存完整数据”，安•卡沃基安表示，“英格码利用区块链技术来嵌入数据，并追踪所有的数据片段。”3 你可以将数据与第三方共享，而第三方在无须解密的情况下也能将这些数据用于计算。4 如果这个新的英格码网络能够奏效，那么它将改变我们处理网上身份的方法。设想一下现在你自己有一个储存了你个人信息的黑盒子，只有你能控制并访问里面的数据。

不管这听起来有多酷炫，鉴于以下几个原因，我们在前沿的加密技术上还是要步步为营。首先，它需要一个建立（bootstrap）一个由参与者组成的大型网络。

其次，区块链公司 Blockstream 的奥斯汀•希尔说过，“密码学是一个你永远不希望使用最新、最先进技术的领域，因为之前每次出现一种大家都觉得安全的新算法，四五年后就会有一些聪明的科学家站出来说这算法有问题，然后整个机制都会被推翻。所以通常情况下，我们会选择保守但已经被确认过的、持久有效的算法。这种东西需要后期很长时间去验证，而比特币的设计就考虑到了这一点”。5

尽管如此，这个概念还是值得认真研究的，因为它在隐私、安全及可持续性方面，具有深刻启示。“英格码正在提供它们声称能够确保隐私的技术”，安•卡沃基安说道。“这是一个很大胆的主张，不过这样的东西在这个联网、互联的世界确实有着日渐提升的需求。”6

在我们的研究过程中，我们接触到了一些基于区块链的项目，它们的开发者对基本的人类权利的维护有着类似的愿望——不仅是保护隐私和安全的权利，还有财产权、在法律下被视为人的权利以及参与到政府、文化和经济事务中的权利。你可以想象一下，无论我们居住在哪里、出生在哪里，都有一种技术能够保留我们及家庭的选择权、在世界上表达出这种选择的权利以及控制我们自己命运的权利。如果有了这样的技术，我们将可以创造什么样的新型工具、工作机会、新型商业模式和服务？我们应该如何看待这些机会？得益于中本聪的发明，这答案就在我们面前。

七大设计原则

我们相信下一个新纪元将会由中本聪的愿景所启发，围绕一系列的隐含原则所设计，并由那些充满激情而又富有才华的社区领导者实现。

中本聪的伟大构思仅限于货币方面，而不是要创造第二代互联网这样的更高目标。他并没有提到重塑公司、改变我们的机构或者改善文明程度等事宜。不过，中本聪的这一见解，还是体现了其令人惊叹的简易思维、独创能力以及对人类的深刻洞察力。那些读过 2008 年论文的人，会越来越清楚地意识到，数字经济新时代即将来临。计算与通信技术的融合推动了第一代数字经济的出现，而计算机工程、数学、密码学及行为经济学的结合或许能推动第二代数字经济。

民谣歌手戈登•莱特富特在他的歌中浅唱道：“如果你能读懂我的心，那你一定能读懂我的爱。” 自 2011 年来中本聪就一直处于与外界隔离的状态（尽管这个名字会时不时出现在网络社区讨论板块），不过我们认为，他独创的这套信任协议，为机构及经济的重新组建提供了参考原则。

每个与我们谈论过的人，都迫切地想要分享他们关于区块链技术的见解。我们根据每一场对话、每一份白皮书以及每一个论坛帖

子展示出了一系列的主题，而我们将这些主题提炼成设计原则——在区块链上创建软件、服务、商业模式、市场、机构甚至是政府事务方面的原则。虽然中本聪并没有具体提到过这些原则，但它们一直暗含在他发布的技术平台上。我们其视为塑造数字经济及革新信任的新纪元所需遵守的原则。

如果你刚刚接触区块链领域，我们希望这些原则有助于你理解区块链革命的基本原理。即使你是一个坚定的比特币区块链的怀疑者，在你以后的企业家、投资者、工程师或艺术家的生涯中，如果你需要与志趣相同的人进行创意协作；如果你是各种资产的所有者或投资者；如果你是一个希望重新构想你在这个区块链经济的早期所扮演角色的管理者；那么，这些原则对你来说都有一定的参考价值。

1.网络化诚信 Networked Integrity

原则 :信任源自内在，而非外在。(Trust is intrinsic, not extrinsic.)

诚信被编码到流程的每一环节中，它是分布式的，而不依赖于任何一个成员。参与者之间能够直接进行价值交换，并可以期望另一方以诚信的方式行事。也就是说，诚信价值观——包括言行上的诚实、考虑对方利益、对自己的决定与行为负责及决策与行动的公开透明等——会以编码形式体现在决定权、激励制度以及运作过程中，这样个人或机构就必需以诚信的方式行事，否则就可能会耗费更多的时间、金钱、能量和声誉。

有待解决的问题： 在互联网上，人们一直无法直接进行金钱交换，这纯粹是因为金钱本质上和其他信息产品或知识产权是不一样的。你可以把同一张自拍照传给所有朋友，但是你付给另一个人的一美元不能再付给你的朋友了。钱必需从你的账户离开并转入你朋友的账户，它不可以同时存在于两个账户中，更不应该在多个账户中了。所以，就有可能出现这种风险，即在两个地方使用了同一个单位的数字货币，并让其中一笔像空头支票那样被退回来。这种就是双重支付的问题。这对那些想重复支付同一笔钱的诈骗分子来说是一件好事。但对那笔无效款项的接受者来说就是一件坏事了，而且还会对你的在线声誉度带来不良影响。在传统情况下，在进行在线支付时，我们会借助第三方中央数据库对每

一笔交易进行清算（clearing every transaction），从而解决双重支付问题，比如通过汇款服务（如西联汇款）、商业银行（如花旗银行）、政府机构（如澳洲联邦银行）、信用卡公司（如 Visa），或者在线支付平台（如 PayPal）等等。在世界上某些地区，结算(settlement)可能要花好几天甚至是好几周才能完成。

突破性进展： 中本聪利用现有分布式点对点网络及一些聪明的密码学技术创建了一套共识机制，从而以跟可信的第三方相当（或更好）的效果解决多重支付的问题。在比特币区块链上，网络会为所有者花费某个币时涉及的第一个交易盖上时间戳，然后拒绝后来重复花费这个币的交易，这样就消灭了多重签名的问题。网络上运行比特币全节点的参与者叫作矿工，他们负责采集近期交易，以数据块的形式进行结算，并且每十分钟重复执行这一过程。每一个区块必需引用前面一个区块的某些数据才能视为合法。此外，协议还提供了磁盘空间回收渠道，这样所有节点都可以高效地存储完整的区块链了。最后一点，区块链是开放式的，任何人都能见证交易的进行。没有人可以隐藏一个交易，因此追踪比特币比追踪现金还要容易。

中本聪不仅希望去除中央银行的中介角色，也希望去除有关事实记录的含糊及互相冲突的解读方式。让代码来解释一切吧，让网络通过共识算法就所发生的事实达成共识并用密码学在区块链上进行记录。达成共识的机制是至关重要的。以太坊区块链的先

驱者维塔利克•布特因在博客中提到：“共识是一个社会过程，即使在缺乏算法帮助的情况下，人类也非常擅长于处理共识问题。”他解释称，如果一个系统的规模超出了人们的计算能力，那么他们就会寻找软件代理人的帮助。在点对点网络中，共识算法分配了对网络状态进行更新的权利，即就所发生的真相进行投票的权利。算法会把这些权利分派给一群构成经济组织的平等对象，这群人在这个体系中有着利益关系。据布特因所言，这个经济组织的一个重要特点是它是以可靠的方式进行分布的：任何个体或联盟都不能控制大部分的权利，即使他们有动机和手段去这么做。7

为了达成共识，比特币网络采用了“工作量证明”机制。这听起来有点复杂，但这个想法其实很简单。鉴于我们不能依靠矿工的身份来选择创建下一区块的人，**那我们就设置一个非常难（比如它需要耗费大量工作）但是很容易被验证（比如其他所有人都可以快速查阅答案）的谜题。**参与者都同意第一个解决问题的人可以创建下一个区块。于是矿工们必需通过投入资源（如计算机硬件和电力）并找到正确哈希值（有点像一段文字或数据文件的独特指纹）的途径来解决这个难题。他们找到的每一个区块都对应着一定数量的比特币作为奖励。这个谜题是以数学的原理设计的，确保了任何人都没有快速解决的捷径。因此，当网络其他人看到答案时，每个人都会相信这个答案得来不易。此外，根据迪诺•马克•安格里蒂斯所述，这个谜题的过程已经进行到“每秒执行

500000 万亿次哈希运算”的规模。矿工们“都在寻找符合这一要求的哈希值，据统计，这个值每十分钟就会出现一次。这就是个泊松分布过程，有时候只要一分钟，有时候要一小时，不过平均是十分钟一次。”迪诺•马克•安格里蒂斯解释了其运作方式：“矿工把网络中所有待处理交易收集起来，然后通过加密摘要函数来运行数据。这个加密摘要函数又叫安全哈希算法（SHA-256），一般输出 32 字节的哈希值。如果这个哈希值低于某特定目标（这个目标由网络设定且每隔 2016 个区块调整一次），那么就说明矿工已经找到了答案，并‘破解’了该区块。但不幸的是，对矿工而言，找到正确的哈希值非常困难。如果哈希值错误，那矿工就得稍微调整输入的数据，然后再次尝试。而每次尝试都会得出一个和之前截然不同的哈希值。他们不得不反复试验，直到找到正确答案为止。截止至 2015 年 11 月，哈希值尝试的次数平均达到 3.5 亿兆次。这个工作量非常大！” 8

你可能听说过其他共识机制。第一版以太坊区块 Frontier 也采用了工作量证明算法，不过以太坊 1.1 版的开发人员想改用“权益证明机制”。权益证明机制要求矿工购入并保留某种形式的价值储存手段（比如点点币、未来币 NXT 之类的区块链原生代币）。他们不必花费能量去投票。而其他区块链，比如瑞波以及恒星币，它们则要依靠社会网络来实现共识，并且他们会建议新的参与者（比如，新节点）给出一份独一无二的节点列表，这份列表至少包含 100 个他们所信任的节点，对事务的状态进行投票。这类证

明机制会有所偏倚：新来的人需要具备社交治理和声誉才能参与其中。还有一种是“活动证明机制”，它是工作量证明与权益证明的结合体，在区块被正式承认前，一个随机数量的矿工必需利用加密密钥对一个区块进行签名。9 而“容量证明机制”就是要求矿工配置超大硬盘空间来进行挖矿。还有一个相似概念，即“存储量证明”，这种机制需要矿工在一个分布式云平台分配并共享磁盘空间。

存储空间是有一定影响的。区块链上的数据和互联网上的数据有很大不同。在互联网中，大部分信息具有延展性并快速流动，而该信息的确切发布日期和时间对过去或将来的信息而言并不重要。而在区块链上，从比特币的产出开始，其在网络中的动向就被盖上戳记。要验证一个比特币，不光要引用其自身的记录，还要参考整个区块链的历史。因此，区块链也必需以完整的方式进行保存。

挖矿过程非常重要，这包括了将交易集合到一个区块里、投入一些资源、解决问题、达成共识及保存完整账本的副本——甚至有人把比特币区块链当成类似互联网那样需要有公众支持的公共设施。安永会计师事务所的保罗•布罗迪认为我们应该把所有电器的处理能力都投入到区块链维护中，他说：“如果你的割草机或洗碗机有一个中央处理器，然后这个中央处理器的处理能力可能是实际所需的一千倍，这样的话为什么不用它来挖矿？这并不是

为了赚钱，而是用来维护你在区块链上的权益。”10 除了共识机制，区块链还能通过智能代码来保障诚信，而不是靠人类自己去选择做正确的事。

对区块链经济的影响： 我们不用再依靠大公司和机构来验证人们的身份，为他们的声誉进行担保了，取而代之的是我们可以信任网络了。我们有了一个平台，在这个平台中，无论另一方如何运作，都能保证信任，这一点是前所未有的。

对大多数社会、政治以及经济活动来说，其影响是惊人的。信任不仅关乎婚姻嫁娶、投票选举、钱财支付，对那些追求可信记录和交易保障的人来说，它也很重要。比如这个东西的所有权归谁？这是什么东西的知识产权？谁是从医学院毕业的？耐克、苹果设备还有婴幼儿配方奶粉是谁发明的？这些钻石从哪儿来？信任是数字经济的必要条件，而一个安全可靠的广泛合作平台，或许能够推动新型社会与组织的出现。

2.分布式权力 Distributed Power

原则 ：系统通过一个点对点网络来分配权力，而不再进行单点控制。任何参与者都无法关闭系统。如果某个体或团体的电源被切断了，系统也还是能够运行。如果有超过一半的网络试图覆盖整个网络，那么每个人都可以看到事情的发生。

有待解决的问题 ：在第一代互联网中，任何拥有庞大用户基础（可能是员工、市民、消费者或者其他组织）的大型机构，都没怎么考虑过社会契约的问题。中心化的力量一次又一次证明了他们对用户的忽视，他们随意存储并分析用户数据，在用户不知情的情况下把数据提交给相关部门以满足其要求，还未经过用户同意就大范围改变数据。

突破性进展 ：比特币区块链运作所花费的过高能源成本可能会超出它所带来的财务效益。中本聪采用的工作量证明机制需要用户进行大量运算（这非常耗电）来维护网络运作，从而铸造新币。密码专家亚当•巴克开发了哈西现金（Hash cash）解决方案来减少垃圾邮件以及拒绝服务攻击，而中本聪也从这一解决方案中获得了灵感。亚当•巴克的算法需要发件人发送邮件时提供工作量证明，实际上就给邮件盖上了“特殊递件”的戳记来显示这份信件对发送者重要性——“这份信件非常重要，我花了所有精力来传

送给你。”这样一来，发送垃圾邮件、恶意软件以及勒索软件的成本就会增加。

任何人都可以免费下载比特币协议，并且保留一份区块链副本。它利用了一种名为 bootstrapping（自展开）的技术，通过一些简单的指令触发程序的其他部分从而把程序上传到志愿者的电脑或移动设备上。它就如 BitTorrent 一样是完全分布在一个由志愿者组成的网络上的。它是一个建立在世界范围内成千上万台电脑之上的知识产权的共享数据库。

当然，它确实能使网络免遭干预，不过这一点有利也有弊。在区块链上，再也可不能像富兰克林•罗斯福执政时期发布 6012 号行政命令那样，随意冻结资产。当时的 6012 号行政命令要求市民要么把所有“金币、金条、黄金凭证”都转交给政府，要么就等着罚款坐牢。11 美国乔治梅森大学的乔希•费尔菲尔德直白地说：“以后想对付中间人也没办法了”12 ，区块链无处不在，志愿者会保持区块链副本更新，并将多余的计算机处理器的性能用于挖矿，从而实现区块链的维护。区块链中不会有后门交易，每一个交易动作都会在全网广播以供后续校验和验证。整个过程都不会涉及中心化的第三方，也不会在一个中心化服务器中存储任何数据。

中本聪也通过将账本中新区块的创建过程与比特币发行连接起来的方式，将铸币权分发出去，从而将铸币权放到了对等网络中

的每一个节点中。无论是哪个矿工，只要是第一个解出难题并提交工作量证明的，就可以收到一些新的比特币作为奖励。这里面没有美联储、中央银行或财政部来控制货币的供给。此外，每个比特币都能直接连接到创世块并追踪到所有后续交易。

这样就不再需要中介机构了。区块链的功能运作是一场完美的大规模协作。你能够控制你的数据、你的财产以及你的参与度。它的分布式计算能力同时让分布式的、集合的人类能力成为可能。

区块链经济所带来的影响 ：或许这种平台能够为财富创造提供一种新型分布式模式；也或许这类点对点协作能够缓解人类最棘手的社交问题。或许我们应该通过将真正的权力移交给公民的方式解决现在机构中的信任危机甚至是合法性问题，从而为他们带来真正走向繁荣和参与到社会的机会，而不是像现在那样通过公关方面的手段去解决。

3.把价值作为激励 Value as Incentive

原则 :系统把所有利益相关者的奖励都结合到一起。比特币或者其他有价代币都是这个系统的一部分，也与声誉度是相关的。中本聪编写了这一软件，用来奖励那些参与其工作的人，而它是属于那些持有并使用其代币的人，这样他们都会认真维护这个软件。这有点像终极版本的电子宠物，区块链就是一个全球分布式的储备金。13

有待解决的问题 :在第一代互联网中，企业权力集中、规模庞大、制度复杂，而且运行不透明，这使得他们从授予其权利的网络中获取了大量不成正比的价值。大型银行对金融系统的利用已经让其几乎到了崩溃的极限，因为“那些为高管和信贷服务人员而设的激励架构必然会鼓励短视及过分忽视风险的行为，”约瑟夫•施蒂格利茨说道。这也包括了“专挑美国最穷的人下手”，他把这个问题总结为：“如果你为人们提供一个不良的奖励机制，那么他们也会做不良的事，而他们是以大家应该预期到的方式行事的。”14

大型网络公司利用一些零售、搜索或社交媒体方面的免费服务，来换取用户信息。根据安永的调查，近三分之二的调查对象（经理）表示，他们收集消费者信息是用来推动业务发展的，而近 80%的经理称，这样的数据挖掘增加了他们收入。但是一旦这些公司

遭到黑客攻击，消费者也就跟着遭殃——信用卡和银行账户信息被窃取，他们不得不处理一大堆烂摊子。因此也难怪在同一调查中，近半数消费者表示，在接下来五年他们会逐渐切断这些公司对他们数据的访问渠道，还有超过半数消费者表示，比起前五年，他们现在提供的数据已经越来越少，比如他们删掉了自己在社交媒体上的信息。15

突破性进展： 中本聪希望参与者能够在符合自身利益的原则下行事。他明白博弈论，他知道，没有守护者的网络很容易遭到女巫攻击（Sybil attacks），这种情况下，节点会伪造出多重身份、稀释权利并且让声誉的价值贬值。16 如果你不知道自己到底是在和三个参与方还是和一个挂着三个身份的参与方进行交易，那么点对点网络的正直性及其节点的声誉就没有很大的价值了。因此，中本聪编写了源代码，这样一来无论人们如何自谋私利，也无论他们的身份是什么，其行为都会给整个系统带去好处，而且反之还能为他们累积声誉度。这一共识机制要求的资源投入及其比特币奖励机制，能够激励参与者做正确的事，让他们变得可靠——因为从某种程度上说，他们的行为是可以预测的。这样女巫攻击在经济上也就不可行了。

中本聪写道："按照惯例，区块上的第一笔交易是一个特殊交易，它会创建一种由区块创建者所持的新币。这样就为节点支持网络的行为增添了激励机制" 17 。比特币是一种鼓励矿工参与到区块

创建中并将新区块同前一区块相连的激励机制。那些率先完成区块创建的人能够得到一定数量的比特币。**在中本聪的协议中，他用比特币来慷慨地奖励早期采用者：刚开始的四年，矿工成功开采一个区块能收到 50 个比特币，之后每隔四年，每个区块的奖励就减半到 25 个，12.5 个，以此类推。因为现在他们也持有比特币了，所以他们就有动力去保障平台在长期的成功，购入顶尖装备来挖矿并更高效地花费能量从而维护账本。**比特币不仅是对与参与挖矿和交易的一种激励机制，也是对平台所有权的一种体现。分布式用户账户是加密网络基础架构的最基本元素，一个人在持有并使用比特币的同时也在资助区块链的发展。

中本聪选择那些有计算机运算资源的人作为其经济组织。如果矿工想参与奖励系统，就需要投入网络外部的资源——也就是电力。偶尔也会有不同矿工挖到两个容量相当并且同样有效的区块，这样其他矿工就必需选择他们希望在哪个有效区块之上构建新区块。他们一般会选择他们认为赢面较大的区块来构建，而不是在两个区块之上构建，否则他们就得分散运算力去处理几个分叉链条，而这种方法会损失价值。参与者会选最长的链条作为区块链的权威状态，因为区块链越长就代表所投入的工作量越大。相比之下，以太坊选择“代币持有人”作为经济组织，而瑞波币和恒星币则选择社交网络。

关于这些共识机制的矛盾点是，一个人通过为自身的利益行事，就能为点对点网络提供服务，这反过来会影响个人作为经济组织成员中的声誉。在区块链技术之前，人们很难利用到他们网络声誉的价值。这不仅仅是因为女巫攻击会让电脑中进驻多个角色。身份具有多面性，它是瞬态的，并且存在微妙差异。很少有人能够看到其所有面，更别说是发现微妙之处和捕捉全过程了。针对不同情况，我们不得不生成文件等相关证明，来证实我们身份的一些细节。“没有证明文件”的人，就不能进入其社交圈寻求合作。在类似 Stellar 的区块链上，这是个不错的开始，它创建一种永久的数字存在证明并建立其名誉，这种名誉的便携性超出了一个人所在的地理社区。

价值储存方面的另一项突破就是被编码到软件中的货币政策。尼克•绍博写道：“人类至今使用过的所有货币都或多或少的存在安全问题。这种不安全体现在各方面，比如伪造、盗取等，但是最恶劣的，可能就是通货膨胀了。” 18 中本聪采取逐步发行 2100 万比特币来限制供应，从而防止通胀。由于区块中能挖到的比特币每四年就会减半，而且目前的挖矿率是每小时 6 个区块，所以大概要到 2140 年这 2100 万个比特币才会全部投入流通。因此在这个系统中是不会引发恶性通货膨胀或货币贬值这类情况的。

货币不是唯一可以在区块链上交易的资产，“我们才刚开始探讨潜在的领域，” Blockstream 的奥斯汀•希尔说，“如果以可以利

用网络并向世界展示的应用程序和协议为标准，我们仍处于 1994 年的时候。 ‘这是你能做的事情，它们完全是突破性的。’ ” 19 奥斯汀•希尔希望看到不同的金融工具，包括资产证明真伪鉴定到财产证明所有权等等。他还表示，希望比特币运用到 Metaverse（一个虚拟世界）中，用比特币换 Kongbucks，然后雇佣伊罗•普托塔格尼斯特——小说的主人公，黑客、武士兼披萨饼快递员——来帮你黑到一些数据。20 或者你可以亲自进入 OASIS（一个充斥着各种虚拟乌托邦的世界），在这个世界你真的能找到复活节彩蛋，赢得哈里得的财产，将 OASIS 的虚拟定位权授权给 Google，并且购买一辆无人驾驶车导航到多伦多。21

当然，还有物联网，通过物联网我们注册设备并为其设置身份（英特尔已经在做这个事情），然后借助比特币而不是各种法定货币来协调支付。奥斯汀•希尔说：“你可以规定所有你想做的新业务，让其在网络中实现相互操作，并且可以使用网络的基础架构，而无须自己建造一个新的区块链。” 22 。

和法定货币不同，每个比特币都可分割到八位小数。在一笔交易中，随着时间的推移，用户可以合并、拆分价值，也就是说一个输入项可以在多个时间内，输出多个项，这比执行一系列交易要高效得多。用户可以设置智能合约来计量服务的使用量，并定期进行小额支付。

对区块链经济的影响 ：第一代互联网错过了这一切。现在的平台中，人们，甚至是物品，都拥有适当的资金奖励，以鼓励大家参与到有效合作中去创造一切。可以设想一下：一个线上讨论小组中的参与者，能够因此有动力去提高他的名誉，其中一部分原因是若有不良行为会让他们付出经济上的代价；太阳能板的点对点网络中，房主能够收到区块链实时补偿，因为他们生产了可持续能源；在开源软件项目中，贡献合格代码的人，开发者社区会为他们提供补偿。这些其实不难实现。12

4.安全性 Security

原则 ：网络中嵌入的安全措施是不会出现单点故障的，它们不光保证机密性，而且保证所有活动的真实性以及不可抵赖性。任何想要参与其中的人都必需使用加密技术（无法选择不使用），如果有人做出鲁莽的行为，那么其后果也只由当事人本人承担。

有待解决的问题 ：黑客攻击、身份窃取、诈骗、网络欺凌、网络钓鱼、垃圾邮件、恶意软件以及勒索软件——这些都会破坏社会个体的安全。第一代互联网既没有体现透明性也没有减少违规行为，它并没有加强对个人、机构以及经济活动的安全保护。普通互联网用户一般只能依靠薄弱的密码环节来保护邮件和网上的账户，因为服务提供商或雇主并没有给出更好的保护措施。比如最典型的金融中介机构：他们的特长是金融创新而非研究安全技术。根据身份盗窃资源中心表示，中本聪发布白皮书的那一年，纽约梅隆银行、美国国家金融服务公司（Countrywide）、通用电气金融等金融企业资料外泄事件中出现的身份盗窃报道，占同年同类报道的 50%以上。24 截至 2014 年，在金融领域中这一数据已经减至 5.5%，但是在医疗保健领域，资料外泄报道增加到全年总数的 42%。美国国际商用机器公司（IBM）总结出了资料外泄的平均代价是 380 万美元，这意味着过去两年资料外泄带来的总损失至少达到了 15 亿美元。25 每起个人医疗身份诈骗所带来的损

失平均接近 13500 美元，而这类违法事件还在增加。消费者不知道接下来被入侵的会是他们生活中的哪一个方面。26 如果接下来数字革命涉及各方之间直接进行金钱交易，那么就必需保证通信不会遭受黑客入侵。

突破性进展 ：中本聪要求参与方使用公钥基础设施（PKI）来搭建安全平台。公钥基础设施是非对称加密算法的一种高级形式——用户拥有两个功能不同的密钥：一个用来加密，另一个用来解密，因此它们是非对称的。比特币区块链是目前全世界公钥基础设施最大的平民化应用，仅次于美国国防部公共访问系统。27

非对称加密起源于 20 世纪 70 年代，28 并于 20 世纪 90 年因电子邮件免费加密软件获得了关注，例如 Pretty Good Privacy（PGP，一款加密软件）。PGP 非常安全，但是使用起来也非常麻烦，因为网络中的每个人都需要使用它，你必须时刻留心自己的两把密钥以及每个人的公钥。它没有重置密码这一功能，如果你忘记了密码，你就得全部重来。根据 Virtru 公司介绍， “加密邮件的数量正在增加，然而只有 50%的邮件是在传输过程中加密，而端对端加密的邮件仍旧很少”。29 也有人不采用加密和解密操作，而是采用数字证书（无须加密和解密技术的情况下提供保护信息的代码）去实现这个需求，不过，用户要使用个人证书就必需进行申请（还有付年费），而大多数常见的邮箱服务，比如谷歌、Outlook 还有雅虎，它们是不支持这一功能的。

安德烈亚斯•安东诺普洛斯说：“过去的方法都失败了，因为他们缺少奖励机制，而且人们从不把隐私当作维护系统安全的动力。”30 比特币区块链几乎解决了所有问题，它为公钥基础设施在所有涉及价值的交易中的广泛采用提供了奖励，这一点不仅反映在比特币的使用上，而且还体现在共享式比特币协议中。我们不需要担心脆弱的防火墙、盗窃的员工或保险金黑客。如果我们都使用比特币，并且我们能够安全地存储并交换比特币，那么同样的，我们也能在区块链中，安全地交换数字资产和高度机密的信息。

这是它的工作方式。数字货币并不是存储在一个文件里的。它是被一个密码学的哈希值所对应的交易而代表的。用户持有可以控制他们自己财产的密码学钥匙，并在相互之间直接交易。这样的安全性也让用户需要确保自己私钥的隐私性。

安全标准是很重要的。比特币区块链在 SHA-256 上运行，这是一种非常有名的算法，由美国国家标准与技术研究院发布，被认定为美国联邦信息处理标准。为了找到区块的解决方案，需要反复进行这类数学运算——这样计算设备需要消耗大量电力，来解决难题并挣取新的比特币。其他算法消耗的能源就相对较少，比如权益证明机制。

本章开头奥斯汀•希尔说过，不要采用最新、最好的算法。奥斯汀•希尔目前正同 Blockstream 的密码学专家亚当•巴克共事中，对那些没有采用工作量证明算法的加密货币，奥斯汀•希尔流露出了

担忧，他表示：“我不认为权益证明能够奏效。对我而言，那种系统就是让富人更富，而手持代币就能决定共识。工作量证明则是以物理学为基础的系统，我比较喜欢这个算法，因为这个系统和黄金采用了相似的系统。”31

最后，最长的链一般也是最安全的链。中本聪区块链的安全主要得益于其相对成熟性以及其建立的字节币用户与矿工基础。入侵这种区块链，需要投入比攻击短链更多的计算力。奥斯汀•希尔说：“不论什么时候，只要有新网络搭建起新的链，那就会有一群人把自己隐藏的计算能力、所有电脑和中央处理器都从比特币挖矿中撤出，目标直指这些新网络，从而操控它们，实质上也就是攻击这些网络。”32

对区块链经济的影响 ：在数字时代，技术安全很显然是社会个人安全的前提条件。如今字节可以在我们的防火墙和钱包间传播，而小偷可以从世界另一端盗取我们的钱包，甚至是劫走我们的车。由于我们每个人都越来越依靠数字工具与数字平台，这种威胁也在我们不知情的情况渐渐出现。比特币区块链的设计更加安全，也更透明，我们可以借此来进行价值交易，并保护我们的数据。

5.隐私 Privacy

原则 :人们应当控制他们自己的数据。他们可以自主决定哪些身份信息、在什么时候、以何种方式、透露多少给其他人。尊重别人的隐私权和与尊重别人的意思是有区别的。这两点我们都需要做到。中本聪去除了人们信任他人的需要，也就去除了沟通交流中对他人真正身份了解的需要。安•卡沃基安说：“我已经和多位工程师还有电脑科学家沟通过了，他们每一个人都告诉我——‘当然了，我们可以把隐私嵌入到数据架构和程序设计中。我们当然可以这样做了。” 33

有待解决的问题 :隐私是人类的基本权利，也是自由社会的根基。在互联网时代过去的 25 年时间里，公共和私有领域的中央数据库，已经采集到了个人和机构所有种类的机密信息——有些连他们本人都不知道。各地的人都很担心公司会通过数字世界，采集他们的信息来制造我们所说的“网络克隆”。甚至是一些政府也在建设监视国家，比如最近美国国家安全局就通过互联网进行了不正当监视，这是过分使用其监视权的表现。这种行为对隐私构成了两次冒犯，其一是在我们不知情的情况下，或未经我们同意，就擅自收集并使用我们的资料；其二是未能保护好这些具有吸引力的信息不受黑客盗取。“这不是零和博弈，不是非此即彼的选择，也无关输赢，你可以对一样东西感兴趣，也可以对另一样东

西感兴趣。但是这对我来说已经过时了，而且根本达不到预期目标，”安•卡沃基安说，“我们用一种正和模式取代了它，从本质上说，这种模式能够让你拥有隐私，并且填补空白信息。” 34

突破性进展 ：中本聪没有为网络层设置身份认证要求，这意味着在下载并使用区块链软件的时候，所有人都不需要提供姓名、电子邮箱地址或其他个人数据。区块链无须了解每个人的身份。（而且中本聪也不需要获取他们的信息来出售其他产品，他的开源软件将意见领导营销的手段发挥到了极致。）全球银行间金融电讯协会（SWIFT）的运行模式是——如果你用现金付款，SWIFT 一般不会要求身份验证——但是我们认为许多 SWIFT 办公室还是有监视的渠道，而且金融机构要加入并使用 SWIFT 的话，就必需符合反洗钱以及客户识别规定的要求。

此外，身份识别及验证层同交易层是分离的，也就是说，对于比特币从甲方地址转移到乙方地址这个过程，甲方会进行广播，而交易过程中不会提及任何人的身份。之后网络会证实甲方的确控制这一批比特币，而且甲方已经批准这笔交易，之后再把甲方的信息标为“未使用交易输出项”，并与乙方地址关联起来。只有在乙方要使用这一笔比特币时，网络才会确认现在这些比特币由乙方控制。

我们可以将其和信用卡使用做个比较，信用卡的模式是以身份为绝对中心，所以每次数据库资料外泄，就有几百万人的地址和手

机号被盗。最近一些数据外泄事件中涉及的记录数目如下：T-Mobile，1500 万条记录；摩根大通，7600 万；蓝十字与蓝盾协会，8000 万；易趣，1.45 亿；联邦人事管理局，3700 万；家得宝（美国家居连锁店），5600 万；塔吉特公司，7000 万；索尼，7700 万；还有一些小型资料泄露事件，包括航空公司、大学、天然气和电力公司，还有医院设施公司，这些都是我们最宝贵的基础设施资产。35

而在区块链上，参与者可以选择保持一定程度的匿名性，这样他们就不需要附加其他与身份相关的具体信息，或在中央数据库中录入这些细节。这一点有多重要，我们就不再强调了。区块链上不会放置对别人有吸引力的大量个人数据。通过区块链协议，我们可以选择某项交易或某个环境中，我们能接受的隐私级别。这能帮助我们更好地管理身份信息，并维护我们同世界的交流。

身份识别初创公司“个人黑盒子”（Personal Blackbox）的目标就是帮助大型企业转变其消费者数据关系。个人黑盒子首席市场官哈洛克•库林告诉我们：“像联合利华或保诚集团这样的公司正在联系我们，希望采用我们的平台。他们对建立更好的数据关系很感兴趣，并且非常想减轻现在担负的数据责任。显然他们已经意识到了，数据逐渐成为公司内部的有毒资产。”36 这个平台可以让客户访问匿名数据——就像临床试验中，药剂师只知道与患者健康相关的信息一样——而不用承担任何数据安全风险。一些消

费者可能用比特币或公司提供的其他好处而将自己的信息让别人观看。在后台，个人黑盒子平台采用的是公钥基础设施，因此只有消费者能够通过私钥访问到他们的数据。甚至连个人黑盒子自己都无法访问到客户数据[31]。

区块链的平台可以提供相对灵活的选择和匿名证明的形式。奥斯汀•希尔把它比作互联网，他说：“一个 TCP/IP（传输控制/网络通信协定）地址并不能视为一个公共 ID（身份）。网路层本身并不了解。任何人都能加入互联网，获得 IP 地址，并且自由地在全世界范围内收发数据包。在社会中，我们已经发现了这样层次的匿名性质所带来的巨大好处……比特币的运行方式就和这个差不多。网络本身不会强制要求身份认证。这对社会和正确的网络设计来说都是好事。”37

因此虽然区块链是公共的——任何人在任何时候都可以进行浏览，因为它就存在于网络上，而无须由中心机构进行交易审计、数据记录——但是用户身份是匿名的。这也就意味着，如果你想知道特定的公钥持有者是谁，你就不得不对数据进行大量三角定位。发送人可以只提供收件人需要了解的元数据。而且，任何人都可以拥有多个公钥/密钥集，就像他们可以拥有多个设备和网络接入点以及各种不同化名的电子邮箱地址一样。

[31] On the back end, PBB’ s platform deploys PKI so that only consumers have access to their data through their private keys. Not even PBB has access to consumer data.

也就是说，类似时代华纳这种负责分配 IP 地址的互联网服务提供商，确实会保留身份与账户的关联记录。同样的，如果你从比特币交易所 Coinbase 这类授权在线交易所中获得比特币钱包，那么这个交易所就必需按照客户识别和反洗钱要求进行严格评估。举个例子，这是 Coinbase 的隐私政策：“我们会收集你们电脑、手机或其他设备传来的信息。这些信息必需包括你的 IP 地址、设备信息（包含但不局限于标识符）、设备名称及型号、操作系统、位置、移动网络信息以及标准网络日志信息（比如浏览器种类、进出我们站点的渠道和访问我们网站的页面）。”38 所以，政府能够传讯互联网服务提供商，并交换这类用户信息，但是他们无法对区块链进行传讯。

还有一点很重要——只要所有利益相关者同意，我们就可以让任意交易、应用程序或者业务模式做到更加透明。我们会在各种情况中，见识到完全透明化后所展现出新性能。公司对消费者、投资者，或者生意伙伴说真话，其实就是在建立信任。39 而这就是个人隐私的体现，是组织、机构和公职官员工作透明的体现。

对区块链经济的影响 ：当然，区块链阻止了“监控社会”的蜂拥出现。现在，我们来思考一下每个人所面临的企业大数据问题。如果企业拥有你全部信息将意味着什么？我们进入全球互联网时代已经 20 多年了，现在企业能够了解到我们个人生活最隐秘的细节——而这还只是刚刚开始，很快我们的个人健康和健身数

据、日常来往、家居生活等所有你想得到的事，都将被人窥探到。很多人还没有意识到自己每天在网上签订“浮士德契约”。消费者通过简单地使用网页，就授权了这些网页的所有者将数字的零散信息汇聚成详细的路线图，从而让它们可以用于商业用途。

除非我们转变到新的范式，否则这不是科幻小说，我们无法预见未来是否会有数亿个体的数亿个替身在数据中心谈笑风生。通过区块链技术，你可以拥有你的个人身份，就像你在《第二人生》虚拟世界里一样。那个虚拟的你会保护你的个人信息，只有在社会或经济交往中得到你同意的前提下才会透露部分所需信息，并确保只要你的数据给别人带去了价值就能收到一定的补偿。这是从大数据到私人数据的转变。可以将这称为“小数据”。

6.权利保护 Rights Preserved

原则： 所有权公开透明且可执行。个人自由是可以被承认和尊重的。我们坚持这一不证自明的真理——所有人具有与生俱来不可剥夺的权利，这些权利应该也能够受到保护。

有待解决的问题 ：第一代数字经济主要致力于寻找方法来更有效地行使这些权利。互联网成了新形式的艺术、新闻和娱乐的媒介，供人们进行诗歌、歌曲、故事、照片、音频、视频等版权的创造。我们也能够把现实领域所采用的统一商法典应用到网络上，让其执行在现实世界已经有的功能，目标是消除针对某一物品的交涉及合约创建步骤，不管这个物品价格有多低（比如一支牙膏）。可是即便如此，我们也不得不依靠一个中介来管理交易，而这些中介有权否认交易，推迟交易，并且把这笔钱存在自己账户上（银行人员把这笔款项叫作“浮款”），或先执行交易但一段时间后就回撤交易。他们预料到了作弊者所占的比例，并接受了一定数量的作弊者的存在确实是无法避免的现状。

效率确实大幅提升了，可合法权益却遭到了侵害，这不仅包括隐私权和安全权，还包括名誉权以及平等参与权。人们可以匿名地对我们进行审查、污蔑与妨碍，而他们自己却只要承担很小一部分风险与损失。电影制作者主要依靠企业联合赞助、视频平台点播、后期 DVD 销售以及有线电视播放权等来赚取收入。但是他们

发现，几十年前发行的影片收入变得越来越少。因为粉丝把电影的电子档都上传到了网上，这样大家就能免费下载。

突破性进展 :铸币所需的工作量证明还要求交易附上时间戳，这样一来，就只有第一个使用代币的人能够进行清算与结算。这意味着区块链——同公钥基础设施相结合——不仅仅能防止二次使用，还能够证实流通中每一货币的所有权，而且每一笔交易都不可改变、不可撤回。换言之，在区块链中，我们不能用不是我们的东西进行交易，无论是不动产、知识产权、还是人格权利。此外，如果未经授权，我们也不能以机构代理角色，代表他人进行交易，包括律师或公司经理等。

“个人黑盒子”公司的哈洛克•库林说 :“人类社会交流几千年来，每次我们剥夺人们的参与权，他们都能回来并破坏这个系统。我们认为，即使是在数字世界，盗窃他们的自主同意权也是不可持续的。”40 区块链作为涵盖一切的账本，通过存在证明(Proof of Existence)这样的工具能够充当一个公共登记中心，这就是一个站点，用来在区块链创造并注册契约、产权、收据、许可等对象的加密摘要。“存在证明”不会保存任何源文件副本，文件的哈希值是在用户机器上进行运算，而不是在“存在证明”站点内，因此确保了内容的机密性。即使一个中心化的权力机构关闭了“存

在证明”，这些证明还在区块链上[32]。41 这样，区块链提供了证明所有权及在无须审查的情况下保留记录的方法。

在互联网上，我们不能真的执行合约权利或者对其实施进行监督。所以，针对涉及多项权利并有多方参与的复杂交易，就由智能合约——即包含特殊目的的一组代码——来执行区块链上复杂的指令。“软件与法律描述的十字路口是基础，而智能合约就是踏上这条道路的第一步，”自我感知系统（Self-Aware Systems）的智囊团主席史蒂夫•奥莫亨德罗说，“当如何将法律代码数字化的原则变得更容易理解后，那么我认为各个国家都将开始这一工作……每个辖区都能明确地实现法律代码化、数字化，而且法律间会有翻译程序……去除所有法律摩擦问题将会是一个巨大的经济效益。”42

智能合约会通过某种途径为另一方提供使用权，就像作曲家把完成了的音乐作品发给唱片公司一样。合约代码会包含期限、版税以及终止合约的相关条款。发行公司要在规定期限内将版税转到作曲家的比特币账户中。例如，如果作曲家的账户连续 30 天收到的款项都小于四分之一个比特币，那么所有权利就会自动转移回到作曲人手里，发行方则无法再获得作曲家登记在区块链上的

[32] Proof of Existence doesn’t maintain a copy of any original document; the hash of the document is calculated on the user’s machine, not on the PoE site, thus ensuring confidentiality of content. Even if a central authority shuts down Proof of Existence, the proof remains on the blockchain.

作品。这一智能合约的执行，需要作曲家和发行方（以及或许是发行公司的财务和法律团队代表）用它们手中的私钥进行签署。

此外，智能合约还能为资产所有者提供一个渠道，从而在区块链上集合资源、成立公司，其间公司条款都会被编为合约代码，清楚地记录并执行所有者的权利。相关机构的聘用合约会规定管理人的决定权，即通过编码来规定在没有所有权许可的前提下，他们能利用公司资源做什么以及不能做什么。

对于保障合约合规性这一点来说（包括社会契约），智能合约提供了一种史无前例的方法。“如果你能通过一种特殊的控制结构来进行一场大型交易，那么你在任何时期都可以预测出其结果，”安德烈亚斯•安东诺普洛斯说，“如果我有一笔交易完全通过了验证，并且这笔交易的多方签名账户中涵盖了多个签名，那么我就可以预测这笔交易是否能通过网络验证。如果通过了，那么这一交易的金额就可以被领取且不可回撤。所有中心化权力机构或第三方都不可以撤销这一交易，也没有人能绕过网络共识。这在法律和金融领域都是一个新概念。比特币系统为一个合约的执行结果提供了很高程度的确定性。”43

这个合约无法被扣押、中止或者重新转到不同的比特币地址。无论发送地址是哪里，无论采用何种媒介，你只需要把签署过的交易传输到任何比特币网络节点中就可以了。安德烈亚斯•安东诺普洛斯说：“就算人们关掉互联网，我仍旧可以通过短波无线电以

摩斯代码的形式传输交易。政府机关可能会审查我的通信记录，但我可以在 Skype 上用一系列表情符号传输交易。只要另一端的人能够解码交易，并记录到区块链上，那我就能让 ‘智能合约’生效。也就是说，我们把一些法律意义上很难担保的东西，转变成了可以进行验证并且具有数学确定性的东西。” 44

在考虑实物产权以及知识产权时，BitPay 执行总裁斯蒂芬•佩尔表示：“所有权只是政府或某一机构颁发的一种认证，即承认你确实拥有某物，而且他们会捍卫你的所有权。它就是由任意权威机构签署的一纸合约，用来保障你的权利的。机构会根据你的身份进行签署，而你拿到合约后，所有权就被记录在册，之后你有权将其转交给其他人了。这个过程简单明了。”45 根据诺贝尔经济学奖得主埃莉诺•奥斯特罗姆的金字塔形权利关系（按强弱顺序排列）来看，共享资源社区也可以考虑采用这种权利分布。在最底层，是授权用户，他们可能只能访问并提取资源；然后是申请人，他们也有这些权利，但他们还能排除他人访问这些权利；经营者除了上述两个权利，还具有管理权；而所有者享有的权利则更多，能够访问、使用、排除他人、管理和出售这些资源（如转让权）。46

下面再来考虑隐私权和宣传权，“个人黑盒子”公司的哈洛克•库林说：“我们的模型就是针对市场权利的。” 他们公司采用区块链技术来代表并执行个人权利，从而再从他们个人数据中提取价

值。“区块链给我们带来了一大群人，他们因任务和技术聚集到一起，创造各种途径，让企业利用到这些独特的数据库，而不是保护它们的数据孤岛。”47 简单地说，人们自己创造的数据，比那些公司追踪到的数据还要好，而且在感情色彩上，比起公司，消费者更容易与品牌站一起并影响他们身边的人。

对区块链经济的影响 :作为一种经济设计原则，权利的执行始于对这一权利的阐明。在经营管理学领域，全体共治(holacracy)是一个非常有趣（也具有争议性）的行动方案——组织成员会先规定需要完成的工作，再分配权利及职责，然后分头行动，各司其职。48 那么公司里谁来决定并安排这一系列活动呢？这个问题的答案会编写到智能合约中，然后存放在区块链上，这样整个目标决定、执行过程、奖励机制就能够在达成共识的同时，实现完全透明化。

当然，这不仅仅是技术问题。它远远超出实体资产、知识产权或“个人黑盒子”公司为卡戴珊家族将形象权的模块添加到其隐私保护工具的范畴。我们需要增强对权利的了解，需要形成对权利管理系统的最新认识。一些初创公司正在努力开发一套权利仪表板（一览表），从而反映人们的公民参与度，其中一个度量指标是投票，而其他的指标还有投入技能、声誉、时间以及比特币，或者提供实体产权、知识产权的免费访问权等。让我们拭目以待吧。

7.包容性/普惠 Inclusion

原则： 经济发展的最佳状态就是它能兼顾到所有人。也就是说，要降低对参与者设定的门槛，要为资本主义分布式发展创建平台，而不仅仅是重新分配式的资本主义。

有待解决的问题 :第一代互联网为人类创造了诸多奇迹。但正如我们发现的，其实世界绝大多数人仍无法使用一些技术，也无法访问金融系统及享受到经济机会。还有，那种声称要让这一新型通信媒介惠及所有人的承诺也只是空头支票。没错，它确实为发达国家公司的新兴经济体带去了数百万个就业岗位，也确实为企业家创业降低了门槛，而且还为弱势群体提供了机遇与基本信息。

但这些还远远不够。如今还有 20 亿人 49 没有开设银行账户，在发达国家，由于社会不平等现象持续出现，繁荣程度也在下降。在发展中国家，手机常常是人们唯一买得起的通信工具。大多数金融机构都有移动支付程序，这种程序将摄像头和二维码结合在一起。但是，支撑这些中介所涉及的费用使小额付款变得不切实际。最低账户余额、最低支付金额或者使用这一系统的交易手续费等，对处于金字塔底端的消费者来说依旧负担不起。其基础设施成本使得小额付款以及小额账户的设想就此幻灭。

突破性进展 ：中本聪设计的系统在互联网堆栈(TCP/IP)顶层运行，但是如果有需要的话，它也可以脱离互联网运行。中本聪设想的是，某个人会通过他所谓的 “简化的支付验证” （simplified payment verification, SPV）模式同区块链进行交互——在手机上也能运行该模式来调动区块链。现在任何人拿着翻盖手机，就可以以生产者或消费者的身份参与到经济或市场中。区块链技术的使用不需要提供银行账户、公民证明、出生证、家庭住址、稳定的当地货币之类的信息。区块链技术将大幅降低汇款等资金传输的成本，并降低银行开户、信用获取以及投资的门槛。而且，区块链还会支持人们创业并参与到全球贸易中。

这是中本聪的部分设想。他知道发展中国家人民的状况还要糟糕。某些出现问题的国家，需要资金来维系运作，于是就简单地印刷更多货币，然后从生产成本和货币面值中赚取差价——也就是硬币铸造税。货币供应量增加其价值就降低。如果当地经济真的崩溃了——就像阿根廷和乌拉圭，以及最近的塞浦路斯还有希腊——这些机构可能就会冻结那些无法提供 “贿赂” 的人的银行资产。考虑到这种可能性，有钱人会把资产存放到更值得信任的地区，或换成更加稳定的货币。

而穷人就没法这样，他们拥有的任何资产都会变得毫无价值。官员可以大肆从外国援助中攫取利益，将用繁文缛节封锁本国边界，阻止任何希望帮助它们的人民的尝试。这些人民中，有需要食物

和药品的妇女儿童，有饱受战争摧残的难民，也有忍受常年干旱或其他自然灾害的灾民。

澳大利亚小额支付服务商 mHITs（Mobile Handset Initiated Transactions 的简称，即移动终端发起的交易）发行了一项新服务 BitMoby——它可以让 100 多个国家的消费者，通过短信给 mHITs 发送一定量的比特币，从而完成手机充值。50 比特币核心开发者加文•安德烈森说：“你不会看到每一笔交易，你只会看到你所关心的交易。你也不用花钱去相信别人，你只要相信他们会通过网络传递给你想要的信息就可以了。” 51

奥斯汀•希尔认为：“在新兴世界，财产记录是与贫困相关的一个大问题，挖掘区块链在财产记录方面的潜能非常重要。现在没有一个可靠的实体来管理土地所有权。如果能让人们由衷地说出他们拥有哪片土地，并让他们用这片地做抵押，从而改善全家的生活状况，这将会是一个非常棒的用例。” 52

从技术层面考虑，加文•安德烈森参考了互联网带宽的尼尔森定律，即高端用户带宽每年会增加 50%，而普通群众带宽则会滞后两到三年。带宽落后于电脑处理能力，后者每年能增加 60%左右（根据摩尔定律）。因此根据尼尔森所言，带宽是主要控制因素。53 大多数设计——包括界面、网站、数字产品、服务、组织等等——都需要适应大众所需的技术，从而发挥网络效应。因此，包容性就意味着要技术覆盖要全面，不仅仅要惠及处于科学前沿的高

端用户，还要惠及世界边远地区穷困人民，考虑到他们科技发展较慢及偶尔还会出现断电等情况。

对区块链经济的影响 ：在本书后半部分，我们会回答与繁荣相悖的问题——第一代互联网为西方国家带去了繁荣，但是大多数人的生活却并没有提高，这说明互联网还存在很多问题。繁荣的基础是包容，而区块链能够帮助其实现。我们需要明白，包容包含了方方面面。它意味着社会霸权、经济霸权、种族霸权的终结，也意味着健康歧视、性别歧视、性别鉴定的终结。一个人居住的地方、他是否在监狱中过了一晚及一个人如何投票，这些事情都可能给一个人带来访问某些资源的障碍，它也意味着要消除这些障碍，并移除那些无形的障碍及无数的变量。

设计未来

和安•卡沃基安的对话激励了我们，我们要继续完成德国“绝不重蹈覆辙”的抱负。还记得德国联邦总统约阿希姆•高克在希特勒政权的受难者纪念日当天的发言，他说：“我们的道德义务不能单单靠纪念来完成。我们要永远记住纪念日给我们下达的任务。这个任务要求我们保护人类，维护人权。”54 他的话是在暗指德国人民在宣誓“绝不重蹈覆辙”后，叙利亚、伊朗、达尔富尔、斯雷布雷尼察、卢旺达和柬埔寨地区发生的种族屠杀？

我们相信区块链技术是保护人类，维护每一个人的权利的重要手段，也是沟通真理、传播繁荣的重要手段。它也是拒绝社会中那些可能会以无法想象的方式生长的阴暗面的手段（就像这个网络拒绝虚假的交易一样）。

这的确是非常大胆的言辞，不过至于是非对错，还得读者自行审视。

从更狭隘且更实际的角度来看，这七大原则能够成为设计下一代的高效能及有创新精神的公司、组织及机构的指南。如果我们的设计能够融入诚信、力量、价值、隐私、安全、权利保护以及包容性等元素，那么我们的经济和社会机构就能重建信任。下面，我们就来看看这些问题该如何深入，对你而言又该做些什么。

第二篇 转型