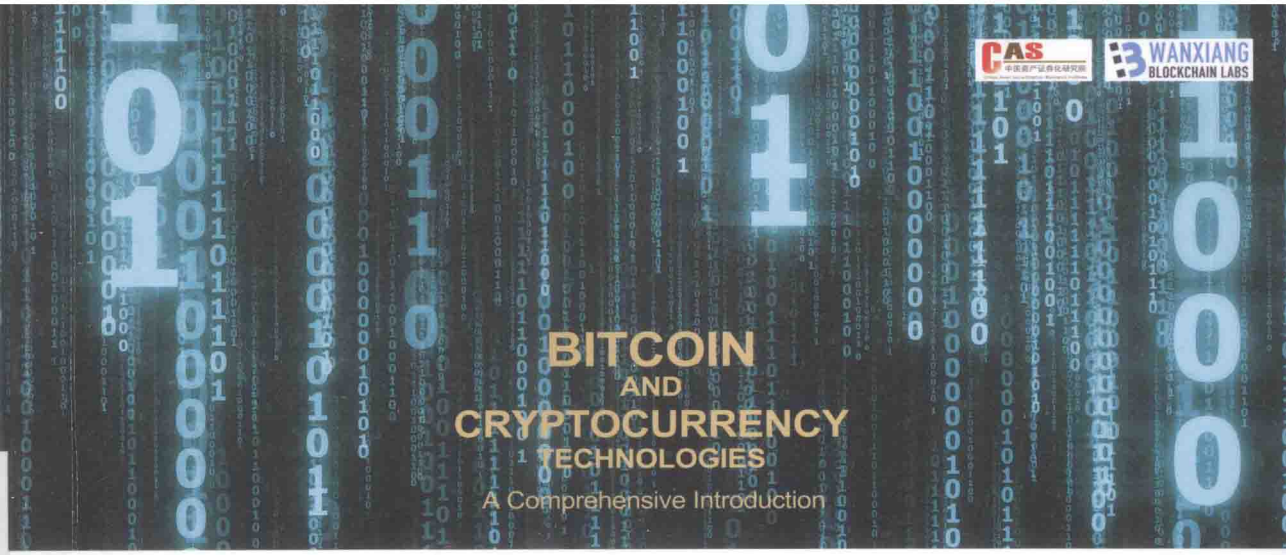

区块链
技术驱动金融

数字货币与智能合约技术

[美] 阿尔文德·纳拉亚南 (Arvind Narayanan)　约什·贝努 (Joseph Bonneau)
爱德华·费尔顿 (Edward Felten)　安德鲁·米勒 (Andrew Miller)
史蒂文·戈德费德 (Steven Goldfeder) ◎著
林　华　王　勇
帅　初　蔡凯龙　许余洁　李耀光　高晓婧　洪　浩 ◎译

解密区块链，用技术重构金融世界

谢平 中国投资公司前副总经理　肖风 中国万向控股有限公司副董事长　倾情作序

邢早忠 金融时报社社长　霍学文 北京市金融工作局局长　刘信义 浦发银行行长　黄世忠 厦门国家会计学院院长　唐　斌 深圳前海金融资产交易所总经理　联袂推荐

中信出版集团 CHINACITICPRESS

BITCOIN
AND
CRYPTOCURRENCY
TECHNOLOGIES
A Comprehensive Introduction

区块链
技术驱动金融
数字货币与智能合约技术

[美] 阿尔文德·纳拉亚南(Arvind Narayanan) 约什·贝努(Joseph Bonneau)
爱德华·费尔顿(Edward Felten) 安德鲁·米勒(Andrew Miller)
史蒂文·戈德费德(Steven Goldfeder)◎著
林 华 王 勇
帅 初 蔡凯龙 许余洁 李耀光 高晓婧 洪 浩◎译

中信出版集团 · CHINACITICPRESS · 北京

图书在版编目（CIP）数据

区块链：技术驱动金融 /（美）纳拉亚南等著；林华等译 . — 北京：中信出版社，2016.8（2016.10 重印）
书名原文：Bitcoin and Cryptocurrency Technologies: a Comprehensive Introduction
ISBN 978-7-5086-6584-9

I. ① 区… II. ①纳… ②林… Ⅲ . ①电子货币－基本知识 Ⅳ . ① F830.46 ② TP3

中国版本图书馆 CIP 数据核字（2016）第 182827 号

区块链：技术驱动金融

著　　者：〔美〕阿尔文德 · 纳拉亚南　约什 · 贝努　爱德华 · 费尔顿　安德鲁 · 米勒　史蒂文 · 戈德费德
译　　者：林　华　王　勇　帅　初　蔡凯龙　许余洁　李耀光　高晓婧　洪　浩
策划推广：中信出版社（China CITIC Press）
出版发行：中信出版集团股份有限公司
（北京市朝阳区惠新东街甲 4 号富盛大厦 2 座　邮编　100029）
（CITIC Publishing Group）
承 印 者：北京楠萍印刷有限公司

开　　本：787mm × 1092mm　1/16　　印　　张：27　　字　　数：400 千字
版　　次：2016 年 8 月第 1 版　　印　　次：2016 年 10 月第 2 次印刷
京权图字：01-2016-5558　　广告经营许可证：京朝工商广字第 8087 号
书　　号：ISBN 978–7–5086–6584–9
定　　价：79.00 元

资产证券化可能成为区块链最好的一个应用

/谢平

区块链，这个原本“高冷”的技术词汇，自2015年以来，引起了当前一波又一波最为火热的争议。到底什么是区块链呢？一般人都是因为知道比特币而知道了区块链，也都知道区块链是比特币的一项关键底层技术，通俗些说，它就像是一个数据库账本，安全记录所有的比特币交易信息。按照专家们更为专业的解释来说，该技术的实质是，不同的节点共同参与的分布式数据库，是一个开放式的公共账簿。从数据包形成区块，中间有一个加密的哈希值计算（密码学技术），把不同时间段的交易信息链接起来，就形成了区块链。

信用是金融活动的根基。具体到金融行业，人们正是希望能够通过区块链技术，低成本地解决金融活动中的信任问题。传统金融体系安排中，所有金融活动的监管及中介机构，包括产品登记、证券发行与交易、信息披露、资金托管等方面，都是解决信任问题或者说金融中最为核心的信息不对称问题。由于信任问题是一直难以解决的社会问题，所以，我们这个社会有很多的公信力机构。从反面来说，本次让市场投资者失去信心的长达10年的全球金融危机，全球货币与资产价值的不稳定，就是数字货币和区块链技术被国内外众多金融机构和个人追捧的一个重要背景，区块链技术给我们创造了一

个用“共信力”来解决公信力问题的途径。

互联网科技与传统金融机构有待进一步的融合。比如银行业，就需要更加重视业务经营管理的数字化、智能化建设，更加深入地推广应用移动互联、大数据、云计算、人工智能等先进技术，以科技改造业务、以科技推动创新。正是在这样的思想和认识下，我认为区块链技术也可能为包括银行、保险在内的机构提供当前许多问题的解决方案，不然当前很多以该技术为核心的金融科技公司并没有存在的必要。另一方面，银行家们也明白，区块链不会是银行终结的信号，区块链可以帮助银行和金融机构寻找新的机会，更好地服务客户。

由于对数字货币与区块链有一定的兴趣，希望增加认识和了解，我与本书译者林华教授畅谈了上面的认识与体会。这本著作是根据普林斯顿大学公开课改编的一部教材，主要讨论了比特币的一系列重要问题。比如，书中着重介绍了比特币的运作方式、比特币与众不同的技术知识、比特币安全性如何保障、比特币的匿名性特征、区块链如何帮助比特币实现没有身份的共识、人们在比特币这一平台上可以创建哪些应用程序、比特币的存储和使用、比特币挖矿、比特币监管，以及作者们对比特币的未来发展展望。我认为，在阅读完如此专业的教材之后，对当前热议的比特币和区块链的各种争议观点，我们就可以具备去伪存真的能力，或许还能掌握基础概念，并能够开发出安全的、能与比特币网络互动的软件，甚至能够把比特币相关理论应用于自己的项目中。

林教授曾经告诉我，资产证券化与区块链有一个很好的结合点，这是我非常感兴趣的一件事。众所周知，区块链被人们认识主要起源于比特币。比特币的本质是数字货币，区块链的本质在于它是一个分布式账本，而货币系统本身就是一个账本，这是它们能够天然结合在一起的很好解释。只不过，原来的货币系统账本是由央行控制和维护的，现在区块链则是分布式的（也有说成所谓的去中心化），是大家一起共同维护的一个账本。

资产证券化和区块链如何结合呢？一直专长于资产证券化的林教授告诉我说，数字货币的一个延伸在于代币（Token Coin），什么是代币呢？就是把资产

变成货币，代币作为资产使用权的证明，或者资产内在价值的所有权证明。资产变成货币，就是一种证券化。如果我们能够建立一个账本，将资产证券化池子中的资产，全部挪到这个账本上，基础资产的各种特征都做好标记，不断循环，按交易时间更新区块，不可篡改，定期跟踪，就能够实现资产证券化与区块链的一个有效结合。资产挪到账本，还需要从三个层面来说，第一个层面是资产，第三个层面是账本，中间需要一个开关或者说场景，形成一个映射关系，即将资产映射到对应账本上，实现所谓的货币化。中间层需要一个场景，最可能的场景就是交易所，可以实现资产和货币的交易。

当然，我和林华教授都一致认为，这背后还有一个担心，从金融角度来看，区块链在技术上仍然不够成熟，尤其是在交易环节。国内外许多专家都明确估计过，区块链技术可能还需要 3 ~ 5 年时间才能真正成熟。在这样的背景下，如果区块链技术被滥用，就会酝酿很大的风险，就好比前两年的比特币投机潮一样。我认为，如果区块链在交易活动中的跟踪、项目资金使用的全程监控以及智能资产合约所需要的风险控制措施等效用发挥不出来，只是利用分布式的分散管理效果，希望在没有一个第三方公信力机构的情形下保证信用，其结果会很容易搞得像 P2P 中的债权分拆分包一样，现实中的风险并没有缩小，只是被转移分散到广大投资人中去，最后出现我们看到的 P2P 机构跑路现象，更要防范的是，现有的 P2P 都将自己做的债权分拆，包装成所谓的区块链金融。正如北京金融工作局霍学文局长近期所说的，“如果现在不规范区块链技术，它又会成为非法金融活动的来源”。因此，我个人也强烈呼吁，我们要发展的其实是符合金融监管和行业规则的技术创新，如果在区块链技术基础上从事不规范的金融行为的话，也会造成新的非法集资或者金融不稳定的来源。

不过，我依然看好区块链技术在金融领域的运用，它不仅仅是货币创造，而且是价值传输与公共账户。现在国内外很多金融机构在价值传输，比如在支付结算、资产登记以及资产转让等方面也都有积极的探索。同时，由于区块链是一个公开、透明、可追溯、不可篡改的分布式总账系统，区块链技术可以有效降低支付、清算、结算步骤的出错率，同时监控每一步资金的流入流出情况，

是推动诚信社会建立的有效手段，区块链有利于金融监管的一面。随着监管与市场主体对区块链技术的认识不断加深，以及该技术不断走向成熟来保证资产的真实性，和林教授一样，我相信资产证券化极有可能成为区块链最好的一个应用。

基于以上的理解和认识，我欣然为林华教授这部翻译作品作序。

谢平

2016 年 7 月

区块链到底是什么？

/肖风

有关于区块链是什么的话题，在时下的中国，可能已经被包括我自己在内的人说成了陈词滥调了。但是每每我们都会看到这样一种情形：一些我们认为已经是常识的概念，却往往别有洞天！借着《区块链：技术驱动金融》中文版出版之际，我愿意把我最近对区块链概念的反刍心得写下来，作为这本书的推荐序。

区块链首先是一种社会思潮。它预示着人类社会转型、换代的新时代的到来。区块链的社会学基础是凯文·凯利《失控》一书里观察及论述到的基于生物逻辑的自然、社会、技术的进化规律：分布式、去中心；从边缘到中心再到边缘，从失控到控制再到失控。微信之父张小龙奉《失控》为自己行动指南的行为，最好地说明了互联网时代的组织及经济发展规律已经变了。区块链的技术基础是分布式网络架构，正是因为分布式网络技术的成熟，去中心、弱中心、分中心及共享、共识、共担的组织架构、商业架构和社会架构才有可能有效建立起来。本书就是从工程技术的角度来介绍基于分布式网络架构的区块链技术的，分布式网络架构对人类社会的影响和冲击，也许我们都还无法估计，不可测量！

当然，任何事物都是精华与糟粕相生相伴、优点与缺点共存共荣的，区块

链技术也一样。在社会实践中我们已经看到，传统金融机构在接受区块链技术的精华的同时，已经扬弃了区块链技术当中的纯粹去中心化的无政府主义色彩和对人人都可以发行货币的去管制、去监管的追求。

区块链其次是一串技术组合。第一，它是分布式账本：全部机构一本总账、各种事务一本总账；第二，它是新型数据库：没有中心机房，没有运维人员，第三方按共识算法录入数据，非对称加密算法保证数据安全，数据客观可信，不可篡改；第三，它是智能合约：是一段能够自动执行约定条件的计算机程序，依靠智能合约技术，理想中的世界就好像一台精密运行的计算机，一切都可以事先约定，编成代码，依程序行事；第四，它是 TCP/IP 模型（互联网模型）里的点对点价值传输协议，它的发明标志着过去 20 几年，互联网技术在帮助人们更好地进行信息传输之后，开始帮助人们可以不借助任何第三方的信任背书，点对点、端到端、P2P 地来传递、交易、支付、汇兑价值物。互联网从此进入新时代：价值互联网时代到来了！

区块链还是 FinTech（金融科技）的核心。继互联网金融之后，金融科技最近大热大火。我们注意到，前几年互联网金融在中国活跃的时候，欧美国家几乎不为所动。而最近一年，欧美国家反过来把金融科技的火把传输到了中国，在互联网金融一地鸡毛的时候，点燃了中国金融创新的新热点。一开始我也认为，互联网金融和金融科技应该就是一回事。但细细想想，它们之间虽然没有本质不同，却还是重心各有侧偏。互联网金融侧重于场景革命，而金融科技侧重于技术革命；进一步，互联网企业拥有场景优势，所以在互联网金融阶段挟场景的优势，略胜传统金融机构一筹。其实就连互联网公司本身，也有场景能力的高低之分，电商和社交网络公司创建场景的能力最强，所以互联网金融的能力也就最大。其他类型的互联网公司，基本难以望其项背。

而就金融科技而言，侧重的是云计算、大数据、机器学习、人工智能等创新技术。技术是中立的，这意味着：一是技术公司固然有技术先发优势，但金融机构在应用先进技术方面也没有不可逾越的障碍；二是技术逻辑必须与业务逻辑结合才能创造价值，而金融机构在业务逻辑方面相比技术公司有优势，业务逻辑的经验积累也是需要时间和过程的。无怪乎最近我们看到太多的互联网

公司到金融机构挖人的消息，因为在金融科技阶段，互联网公司急需懂得业务逻辑的金融人才。

面对互联网公司的业务竞争，过去几年金融机构的应对举措大概分三类：一是无力回天，沦为通道；二是热情拥抱，全面对接；三是自建场景，创新模式。我们其实在多年以前就已经看到过飞信与微信演绎的故事了，它已经充分说明了切勿以己之短搏人之长的道理。

金融科技有可能是金融机构在与互联网公司业务竞争中的一次最好的机会，因为技术面前人人平等。

所以我们看到，这一次华尔街表现出来的热情超越硅谷。华尔街的金融机构都纷纷表白自己是一家科技公司或马上将成为一家科技公司。

区块链可以算得上是金融科技里的核心技术。因为区块链技术是金融业的底层技术革命。大家知道，现代银行业起源于意大利。之所以起源于意大利，一是意大利是欧洲最早开始海洋贸易的地区，复杂的、高风险的海洋贸易必然需要相配套的金融服务；二是意大利人发明了复式记账法，使得复杂的经济活动在会计上可计量。复式记账法几百年来一直没有重大的改进，区块链技术将是自复式记账法被发明以来，人类社会记账方法的第一次革命性改进。作为分布式账本技术，区块链必将给任何需要记账的行业带来降低成本、提高效率、创新业务、创新服务的机会。金融业因为其早已经数字化的特点，首当其冲，也必先蒙其利！

最后，希望本书的出版，能够从工程技术层面，推动区块链技术在中国的发展，推动相关应用的落地。祝《区块链：技术驱动金融》一纸风行！

肖风

2016 年 8 月

这是一本关于比特币和区块链技术的专业著作，起源于业内所熟知的比特币和加密货币技术的普林斯顿网络公开课。以普林斯顿大学计算机科学助理教授阿尔文德·纳拉亚南（Arvind Narayanan）为首的专家，与我们分享了他们关于数字货币与区块链的权威研究成果和重要理论观点。

目前，国内对于比特币和区块链技术的热捧和争议，或者将其过度神秘化，或者将其贬斥得一无是处，还有很多别有用心的人不适当地鼓吹，正是反映出人们并没有真正搞清楚到底什么是比特币，它在技术层面到底是如何运作的。“他山之石，可以攻玉。”本书讨论的是比特币的一系列重要问题。比特币是如何运作的？它因何而与众不同？你的比特币安全吗？比特币用户如何匿名？我们可以在比特币这一平台上创建什么应用程序？加密数字货币可以被监管吗？创建一种新的数字货币将会带来什么样的变化？未来将会如何发展？本书中，作者承认比特币及区块链技术为各种领域带来了颠覆性的创新，但他们并不认可那种以去中心化为目的的观点。

我和王勇教授积极联系与申请，与中信出版社合作，通过激烈的竞争拿到了本书的翻译版权，书中内容的专业性非常强，从翻译初稿到终稿，经过接近一年的辛勤和努力，终于完成了本书的翻译。

在此，我首先要感谢中国投资公司前副总经理谢平先生和中国万向控股有限公司副董事长肖风先生不辞辛苦，亲自提笔为本书作推荐序。感谢金融时报社社长邢早忠先生、北京市金融工作局局长霍学文先生、浦发银行行长刘信义先生、厦门国家会计学院院长黄世忠先生以及深圳前海金融资产交易所总经理

唐斌先生为本书撰写推荐词，感谢您们的鼓励和支持。

我要感谢参与本书翻译的每一位译者。感谢帅初提供了 1 ~ 9 章的翻译初稿，蔡凯龙提供了其余两章和原版前言的翻译初稿。由于本书涉及多个专业领域，翻译初稿在专业性和体例统一等方面有待完善，我组织了所有译者进行重译和修订。其中，高晓婧负责前言与第 7 章，王勇负责第 1 章和第 2 章，洪浩负责第 3 章和第 4 章，蔡凯龙负责第 5 章，许余洁负责第 6 章和第 10 章，李耀光负责第 8 章、第 9 章和第 11 章。我、王勇和许余洁确定了全书的术语表，并一同再三审校全书。许余洁在整体校稿的基础上，还多次与出版社老师们对接书稿的最后内容的完善。每一位译者都在工作之余花了很多时间精推细敲、反复斟酌原文和译文，几经修订才使本书得以呈现在读者面前，感谢每一位译者的辛苦付出，也因此我们采用联合署名的译著方式。

另外，我要感谢杨昌丽、黄红华、韩世光、董方朋、王克祥等对本书在翻译过程中所提供的帮助。

最后，我还要感谢中信出版社编辑的精心编校，没有大家精益求精的团队努力与合作，这本书的中文版本不可能如此顺利与读者见面。

区块链技术在中国的健康发展，还是要基于我国监管的框架和逻辑下，与适当的行业进行有效结合。我们衷心地祝愿本书的引进，能够有助于大家正确理解比特币金融技术的创新与发展。

林华

2016 年 7 月于北京

比特币和加密数字货币是当前的热门话题。乐观主义者认为比特币将从根本上改变人们的支付方式、全球经济甚至政治格局；悲观者则认为它生来就不完美，其失败是注定且彻底的。

究其根本，这些分歧之所以存在，是因为人们没弄清楚到底什么是比特币以及它是如何运作的。本书的目的就是帮助人们跳过噱头切入重点，看清比特币的特殊性。要真正了解比特币的特殊性，我们需要了解它在技术层面的运作模式。比特币是一项新兴技术。把它与现有技术进行简单类比，很难帮助我们做到这一点。

阅读本书需要具备计算机科学的基础知识，了解计算机的工作原理、数据结构和算法，拥有一定的编程经验。如果你是一名计算机专业本科生或研究生、软件工程师、创业者或技术爱好者，那么这本书很适合你。

本书将讨论比特币的一系列重要问题：比特币是如何运作的？它因何而与众不同？你的比特币安全吗？比特币用户如何匿名？我们可以在比特币这一平台上创建什么应用程序？加密数字货币可以被监管吗？创建一种新的数字货币将会带来什么样的变化？未来将会如何发展？

完成本书的学习之后，对比特币和加密数字货币的观点，你应该具备了去伪存真的能力；同时也掌握了基础概念，能够开发出安全的、能与比特币网络互动的软件；还可以把比特币相关理论应用于自己的项目中。

> 本书网上补充阅读材料中，还包含系列配套练习题，可以帮助你更深入理解每一章节。此外，你还需要运用到一些要求运用比特币的简化模型，来完

成一系列编程任务。本书的大部分内容都有视频，如有需要，可以在免费公开在线课程[①]上获得（补充材料获取网址为：http://press. princeton. edu/titles/10908. html）。同时，建议读者补充比特币相关知识，你可以阅读比特币维基、论坛、研究报告，并与比特币从业者及兴趣相同的人进行讨论。

① Coursera，是免费大型公开在线课程项目，由美国斯坦福大学两名计算机科学教授创办。旨在同世界顶尖大学合作，在线提供免费的网络公开课程。——译者注

通往比特币的漫长道路

/杰里米·克拉克（Jeremy Clarek）

在通往比特币的道路上，布满了无数失败的尝试。我收集了一份由约100个加密支付系统组成的名单。它们的技术基于电子现金（e-cash）和信用卡，在某些方面获得显著成就，见表0.1。其中一些是被广泛引用的学术研究成果，还有一些是已开发和测试过的实实在在的系统。在这份名单上，被大家所知的大概只有一个——贝宝（PayPal）。而贝宝之所以幸存，得益于它及时纠正了最初想在移动设备上进行加密支付这一想法。

这段历史会让我们吸取很多教训。比特币的想法从何而来？为什么一些技术成功了而另一些则一败涂地？如何成功地商业化那些复杂的技术创新？即便不去思考这些，它至少让我们明白，一个真实可行的基于互联网的支付体系是多么来之不易。

传统金融体系

设想在政府和货币出现之前，人们以物物交换的方式进行着交易。比如，爱丽丝（Alice）需要工具，鲍勃（Bob）需要药品。如果他们正好都有对方所需物品，就可以进行交换，满足各自所需。

但是，如果爱丽丝有食物，愿意拿食物换工具，鲍勃有工具但不需要食物，

表 0.1　一些优秀的电子支付系统和构想

ACC	CyberCents	IKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
Checkfree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

他想要药品。在这种情况下，爱丽丝和鲍勃就没法直接与对方交易。但是，如果有另一个人卡罗尔（Carol），他有药品，而且愿意拿药品换取食物。那么，这三个人就可以进行交易，各自获得所需物品。

当然，难点在于协调，即组织一群供需匹配的人在同一时间、同一地点进行交易。为解决这一难点，出现了两个体系：信用和现金。二者哪个更早出现，历史学家、人类学家和经济学家们就此争论不休，但这对本书的讨论无关紧要。

在上面的例子中，在信用体系里，爱丽丝和鲍勃可以与对方交易。鲍勃给爱丽丝她所需的工具，得到一个人情。换言之，爱丽丝欠下一笔债务，未来终将偿还给鲍勃。爱丽丝的物质需求即刻得到了满足，但她希望尽快还清债务，因此，她又有了新的需求。然后，爱丽丝又遇到了卡罗尔，她可以用自己的食物交换卡罗尔的药品，然后把药品给鲍勃。这样，她就偿还了债务。

对比而言，在现金体系里，爱丽丝可以购买鲍勃的工具，然后把食物卖给卡罗尔，卡罗尔再把药品卖给鲍勃，完成整个闭环交易。只要每场交易的买方有充足的现金，这些交易就可以按任意顺序发生。当然，最终的结果是，看上去现金似乎从未易过手。

很难说这两个体系哪个更优越。现金体系首先需要现金分配来触发，否则交易无法发生。信用体系不需要这样，但债权人需要承担债务人不偿还债务的风险。

现金还可以让我们知道物品的准确价值。物物交换时，我们很难说工具和药品到底哪个更值钱。现金交易把物品的价值标上数字，这就是为什么我们现在将这两种体系混合使用，即便使用信用，我们依然用现金来衡量所需偿还的债务金额。

这些观点被应用于许多场合，特别是用户在进行虚拟物品的线上交易时。例如，在进行点对点（peer-to-peer）的文件分享时，我们就可能遇到吃白食的人，他们只下载，不分享。进行文件交易可能是一个可行的解决方案，但是如何找到两个相互需要对方文件的人是个协调上的难题。在一些项目如莫佐（Mojo Nation）和学术构想如卡玛（Karma）中，用户自动获得一定数额的虚拟货币。接收文件时，用户可以用虚拟货币支付费用；向其他用户发送文件时，赚取虚拟货币。无论是接收还是发送文件，一个或者多个服务器跟踪记录用户的账户余额，而且可以把虚拟货币兑换成真实货币。虽然莫佐项目在推出货币兑换功能之前就消失了，但它算得上是我们现在使用的比特流（BitTorrent，一种内容分发协议）和塔荷（Tahoe-LAFS，一种分布式数据存储方式）的鼻祖。

网络信用卡的弊端

许多电子支付方式都可以根据信用和现金这两个基本概念进行分类。比特币显然属于现金类，但我们先来谈谈信用类。

信用卡交易是目前主要的线上支付方式。如果你在亚马逊这样的网站购过物，那么你应该很清楚流程。首先，输入你的信用卡信息，点击发送，亚马逊收到这些信息后反馈给“系统”，这一系统包括信息处理器、银行、信用卡公司及其他中介。