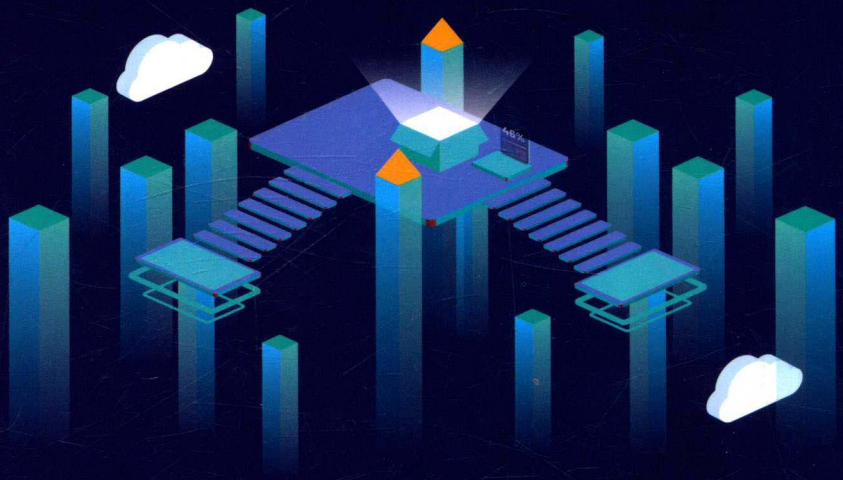
赋能第四次工业革命

BLOCKCHAIN ECONOMICS

区块链经济学

激励、监管与分布式赋能

熙代 著



区块链技术的理性繁荣，从信息互联到价值互联的飞跃

深入探讨以通证经济 / 智能合约 / 智能社群 / 机器信任 / 金融科技为形态的

区块链技术的融合与创新

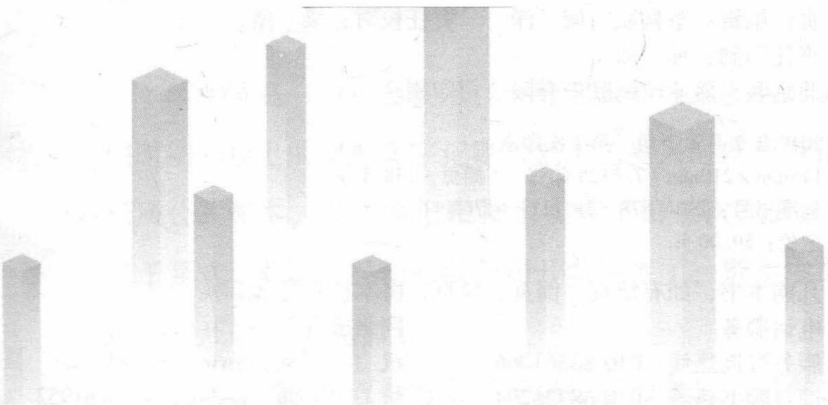
机械工业出版社
CHINA MACHINE PRESS

BLOCKCHAIN ECONOMICS

区块链经济学

激励、监管与分布式赋能

熙代 著



机械工业出版社
CHINA MACHINE PRESS

本书从经济学的角度，阐述了区块链演化的历史脉络，揭示了区块链的本质是一种分布式“加密账术”；进而从加密经济学的角度，解释了区块链经济系统运行的激励机制；并从制度经济学的角度预测：随着区块链技术的普及，区块链将会从“智能货币”“智能合约”“智能社群”三个层次重塑社会经济形态。

本书从技术融合的角度，分析了区块链将会对金融行业、传统互联网行业、文化创意行业、医药卫生业、能源行业和制造业等行业造成的影响。本书认为，对区块链进行合理的监管是非常必要的，并前瞻性地阐述了如何才能利用好这项技术，趋利避害。

图书在版编目（CIP）数据

区块链经济学：激励、监管与分布式赋能 / 熙代著.
—北京：机械工业出版社，2018.12
ISBN 978-7-111-61768-6

Ⅰ.①区… Ⅱ.①熙… 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（2019）第 006317 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：坚喜斌 何 洋 责任校对：梁 倩
责任印制：孙 炜
北京联兴盛业印刷股份有限公司印刷

2019 年 2 月第 1 版 · 第 1 次印刷
145mm × 210mm · 7.8125 印张 · 3 插页 · 138 千字
标准书号：ISBN 978-7-111-61768-6
定价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
服务咨询热线：010-88361066
读者购书热线：010-68326294
010-88379203

网络服务
机 工 官 网：www.cmpbook.com
机 工 官 博：weibo.com/cmp1952
金 书 网：www.golden-book.com
教育服务网：www.cmpedu.com

前　言

“区块链不过是一些陈旧技术的组合。”（比尔·盖茨）区块链至今仍未有“杀手级应用”出现。以太坊（Ethereun）的创始人维塔利克·布特林（Vitalik Buterin）曾经把以太坊比喻为一台“建立在世界网络之上的超级智能手机”，但他又不得不承认其运行速度比 2G 时代的手机还要慢。同时，由于技术不成熟，经常会有区块链项目被黑客攻破的新闻。

然而，这一切都不能掩盖这项技术的光彩。就像莱特兄弟发明的第一代飞机，尽管简陋笨重，但其未来前景仍然令人心驰神往。

区块链是一种新技术，解决的却是和人类文明一样古老的问题：信任问题。

区块链是一种社会技术、一种记账的技术。从苏美尔文明时期泥板上的楔形文字记账，到文艺复兴时期佛罗伦萨的纸质公共账本，人类的记账技术实现了第一次飞跃。从此，基于复式记账法的股份有限公司开始诞生了，资本主义的生产关系开始在全球蔓延。

然而，当世人逐渐将复式记账法奉为真理的时候，记账者却辜负了世人的信任。肇始于华尔街的金融危机，本质上

是一种账本危机。于是，人们开始探索一种不再受人为操纵的公共账本，区块链技术应运而生了。

这种分布式加密记账技术的应用前景极为广阔：资产登记、清单编写、价值交换，涉及金融、经济、货币的各个领域。硬资产，如有形财产、住宅、汽车等；以及无形资产，如选票、创意、信誉、意向、健康数据、信息等。

区块链技术的应用前景如今尚不明了，现在说它是一场革命仍言之过早。但它显然蕴含着巨大的机遇，不论其最终会带来什么样的变革，我们都不应错过这次可以“换道超车”的历史机遇。

历史不会重复，但历史往往有着相似的韵脚。区块链有可能成为下一轮重大的、全球性的计算范式的第五次颠覆式创新。前四次是大型机、个人计算机、互联网、移动智能手机，有潜力像 Web 网站一样彻底重塑人类社会活动形态。

近年来，笔者受一些机构委托，做了一些区块链方面的研究工作。怀着野人献曝的心情，将工作中的心得加以总结，撰写成书，与读者诸君探讨。惴惴之余，更期待方家不吝指教。

目 录

第1章 货币本源

——货币的本质是一种记账技术

演化，是以一种极度去中心化、平行发生的方式进行的。

——尼克·萨博（Nick Szabo）

记账货币（Money of Account）是表示债务、物价与一般购买力的货币。这种货币是货币理论中的原始概念。

——约翰·凯恩斯（John Keynes）

什么是货币，货币的本质是什么？

这是一个开放式的议题，因为从来就没有一个标准答案。

经济学家对货币的定义通常有三种：交易媒介、价值尺度以及价值储藏手段。

众所周知，区块链是比特币的底层技术。因此，弄清楚比特币与货币的异同，是理解区块链经济学的一把钥匙。

当然，比特币仅仅是区块链的首个应用案例，而且未必是最重要的应用。

货币，智人独有的社会技术

1776 年，亚当·斯密（Adam Smith）的《国富论》出版，标志着古典经济学的创立。

斯密在《国富论》的扉页上写下："献给女王陛下的一本书。"

斯密认为，人天生具有交换的倾向。这是人与其他动物相互区分的一个重要标志。

斯密写道，我从来没有见过两条狗会公平审慎地交换骨头，也从未见过一个动物以肢体或语言示意：这是我的，那是你的，我想与你做个交易。

斯密的判断是对的。对于其他动物来说，交换尚且困难，更不用说拿劳动去换钱，或建立复杂的金融体系了。

事实上，地球上曾经存在过很多种人类，我们只是其中的一个亚种，学名叫智人（Homo Sapiens）。

尤瓦尔·赫拉利（Yuval Noah Harari）在《人类简史》一书中指出，我们这个物种有几万年跨群体交易史，是其他人种所未有的；人类很可能在 3 万年前就发明了货币。

考古学家在欧洲中心地带挖掘有 3 万年历史的智人遗址，偶尔会发现来自地中海和大西洋沿岸的贝壳。这些贝壳极可能是通过不同智人群体之间的长距离交易，从而抵达大陆内部的。

尼安德特人遗址缺乏这种交易的证据。每个尼安德特人群体，都采用本地材料制造自己的工具。这也是尼安德特人与智人在长期竞争中消亡的一个重要原因。

互惠，是很多灵长目动物都具有的本能——你帮我挠挠背，我就帮你抓抓痒。尼安德特人之间也极有可能存在互惠的行为——今天你送我一把石斧，明天我送你一张鹿皮。这

种礼物交换更接近于货币出现之前真实的交换场景。

使用语言、文字、工具都不是智人独有的能力，只有使用货币，才是智人独有的技能。所以，亚当·斯密的说法可以进一步精确为：人之为人，在于货币。将我们智人与其他动物区分开来的，乃是货币。

货币是一种记账的“方便法门”

亚里士多德是最早描述货币起源的哲学家之一。他推测，人类最初是以物易物，为了应对越来越复杂的交易而发明了货币。

亚里士多德在《政治学》一书中写道：“可想而知，从简单当中诞生了更加复杂的交换形式……由于各种生活必需品无法随身携带，因此，人们约定在相互交易当中使用某种具有内在用途并且容易满足生活需求的东西，比如铁、银等。最初仅仅以尺寸和重量衡量其价值，但是后来人们在上面盖上印记，以此标定价值，免得每次都要称重。”

亚里士多德的这个猜测，成了后世各种版本货币简史的标准开头。

新古典主义经济学家威廉·杰文斯（William Jevons）在其著作《货币与交换机制》中写道：“交换的最早形式是用不想要的东西直接换取想要的东西。我们称这种最简单的交换为物物交换或以物易物。”

杰文斯认为，物物交换是建立在需求的双重巧合（Double-Coincidence）基础之上的——你拥有的香蕉正是我想要的，我拥有的鱼恰好也是你想要的。

也就是说，“你必须找到这么一个人，既有你想要的东西，同时他也想要你有的东西”，如果没有双重巧合，交换就不会发生。建立这样的匹配，也就是觅客，要么靠运气碰，要么费时间苦苦寻找——也许找到时鱼已经腐败变质了。

仅仅是建立这种匹配，交易成本就已经非常高了。此外，就算实现了“双重巧合”，后面复杂的换算技术，也会让人困惑不已。要知道，公元前500年左右的希腊，还认为10000是一个超出人类理解范围、“大得无法计算”的数字。

诸如“3条鱼能换5根香蕉，20根香蕉能换1头山羊，7头山羊能换1头麋鹿，那么，多少条鱼能换1头麋鹿”之类的问题足以让算术并不高明的古人崩溃。

假设世上真的曾经存在过一个以物易物的经济体，不管你是打鱼的渔夫还是种水果的农民，每天都得搞清楚几十种商品的相对价格。假如市场上有100种不同的商品，把汇率列出来就足足有洋洋洒洒的4950条。这种计算的难度对于古人来说，还不如发明一种交换筹码——货币来得简单。

偏爱捷径，是人类行为的一个基本特征。

货币的发明，是为了简化物物交换的难题。

也就是说，货币不仅是一种交易的媒介，也是一种记账

的“方便法门”、一种快捷的记账技术。假如人类真的存在过以物易物的时代，那么以货币记账绝对堪称“某个懒惰天才划时代的发明”。

货币通过降低巧合问题，大大降低了交易成本，比如搜索、觅客、价值换算等。通过增加交易机会，让涉及更多种类的商品和服务的交易成为可能。通过货币这一被广泛接受并可以重复使用的介质，让信任成本最小化，陌生族群之间也可以合作，增加了社会可扩展性，大大拓展了人类合作的范围。

货币的起源是一种自发秩序

货币的出现，可以说是人类行为自然演化的结果。

奥地利经济学派创始人卡尔·门格尔（Carl Menger）在《论货币的起源》一文中，试图阐明这一观点。

奥地利经济学派的杰出代表哈耶克（Hayek）将其提炼为“自发秩序”（Spontaneous Order）这个概念。

自发秩序是奥地利学派的核心思想之一。它的意思是，我们今天在社会上看到的秩序，不是由哪一个人或者哪一个权威机构主动设计出来的，而是由无数人的行动汇合而成的。哈耶克认为，“道德、宗教和法律、语言和书写、货币和市场”都是自发秩序。自发秩序这一理念深受自由主义经济学家所推崇，布坎南（James M. Buchanan）甚至把它视为经济

学的“唯一原则”。

比如，我们日常使用的语言就是一种典型的“自发秩序”。因为它绝非任何单一理性设计的结果，同时又具有自律性和高度复杂的结构，而且还规范着人们的社会活动。今天你买几本最新的权威词典就会发现，一些当年在学校时拼命规范的读音，现在又“从俗”改回去了。例如，“说服”的汉语拼音最新注音是“shuō fú”，而不是过去语文老师努力强调的“shuì fú”。

另一个相反的例子是世界语，它是波兰籍犹太人柴门霍夫（Zamenhof）博士于 1887 年创立的一种具有“科学性、逻辑性”的语言。一直有人在非常认真地推广世界语，但迄今为止它几乎没有任何影响力。

门格尔认为，货币的起源、货币的形态，与语言的发展非常相像。货币也是一种自发秩序。正如一句话、一个词能否流行开来，不仅仅在于说的人，还在于听的人，在于别人是否接受。货币从物物交换演变而来，是一个自然而然的、自发的过程。

门格尔表示：“只有学会将我们所研究的这个社会程序的建立看作是一个自发的结果，看作是社会各成员具体的个人努力偶然产生的结果，我们才能够充分理解货币的起源。”

经济学家约翰·史密森（John Smithin）在论文集《什么