ブロックチェーン革命
分散自律型社会の出現

区块链革命

分布式自律型社会出现

〔日〕野口悠纪雄　著　韩鸽　译

区块链是未来社会的主角、未来商机的宝库

人民东方出版传媒
People's Oriental Publishing & Media
東方出版社
The Oriental Press

区块链革命

分布式自律型社会出现

〔日〕野口悠纪雄 著 韩鸽 译

人民东方出版传媒
People's Oriental Publishing & Media
東方出版社
The Oriental Press

图书在版编目（CIP）数据

区块链革命：分布式自律型社会出现 /（日）野口悠纪雄 著；韩鸽 译. — 北京：东方出版社，2018.1
ISBN 978-7-5060-9968-4

Ⅰ.①区… Ⅱ.①野… ②韩… 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（2017）第293683号

区块链革命：分布式自律型社会出现
（QUKUAILIAN GEMING FENBUSHI ZILÜXING SHEHUI CHUXIAN）

作　　者：［日］野口悠纪雄
译　　者：韩　鸽
责任编辑：陈丽娜　刘　峥
出　　版：东方出版社
发　　行：人民东方出版传媒有限公司
地　　址：北京市东城区东四十条113号
邮　　编：100007
印　　刷：三河市金泰源印务有限公司
版　　次：2018年1月第1版
印　　次：2018年1月第1次印刷
开　　本：710毫米×1000毫米　1/16
印　　张：14.75
字　　数：115千字
书　　号：ISBN 978-7-5060-9968-4
定　　价：58.00元
发行电话：（010）85924663　85924644　85924641

Not within a thousand years would man ever fly.
Wilbur Wright

即使再过一千年，人类也不可能飞起来！
威尔伯·莱特

前言

人们不管面对怎样的新技术，其认知都要经历以下三个阶段。

第一阶段：这种东西肯定是骗人的。如果真有这么厉害的东西，那世界就要颠倒过来了。所以，这肯定是骗人的手段，甚至有可能是恶性诈骗。大概有谁想趁机大捞一笔吧。一旦上当，肯定会倒大霉。老天保佑、老天保佑，聪明人是绝不会插手这种东西的。

第二阶段：说不定发生了什么不得了的事情。如果不能很好应对，将落后于人。思想超前的家伙已经出手了，我也不能坐以待毙。但这么一个来路不明的东西到底是什么呢？

第三阶段：正如我最初所料，这项伟大的技术改变了世界。

1903 年，在美国北卡罗来纳州的基蒂霍克，威尔伯·莱特和奥维尔·莱特两兄弟初次试飞动力飞机获得成功。本书开篇引言，正是距此两年前的 1901 年，在基蒂霍克开往代顿的火车上，威尔伯对弟弟奥维尔所说的话。这就是本文开篇的“第一阶段”，即便是发明者本人都在说着泄气话[1]。

这也无可厚非。由于飞机是划时代的产物，即便是在飞行试验成功后，这一消息的真实性仍不被人们认可。以大学教授为首的科学家们发表评论和论文称“机械飞行在科学上是不可能的”。

就互联网而言，20 世纪 90 年代初是其第一阶段。当时人们普遍认为，如果能实现向地球任何地点几近免费地发送信息，那世界肯定要颠倒过来，

所以这种事情不可能发生。克利福德·斯托尔在《互联网是空洞窟》（草思社，1996年。原书于1995年刊行）中，列举了几个证据来说明互联网不可能走向实际应用。

从20世纪90年代末到21世纪最初10年，互联网进入第二阶段（1995年“互联网”一词获得日本流行语大奖）。目前处于第三阶段。社会确实颠倒过来了。

就区块链和比特币来说，迄今尚处于第一阶段。在这一阶段，存在各种科学性解说论述比特币为何是骗人的说法，如同当年论证飞机为什么不能飞一样。

最容易理解的就是，“若不存在中央银行此类管理机构，货币就不能发挥作用”，“但是，比特币不存在管理主体，所以不能发挥作用”这一逻辑理论。

学过互联网科学的人，可能会作如下解释：“互不信任的人们之间所形成的互联网网络不能有效运转，众所周知这是个‘拜占庭将军问题’。这一问题无解。所以，比特币运行机制不能成立。”

在区块链第一阶段的2014年2月20日，我开始在*DIAMOND online*上做连载，名叫“比特币是社会革命”。不管对其如何评价，首先必须正确理解比特币。

不久之后的2月23日，比特币交易所Mt.Gox破产。众多有影响力的报纸用整个头版版面报道“比特币破产了”。数日后，某人得意扬扬地站出来，嘲笑说“比特币果然是假货”。尽管我坚持认为比特币没有消亡，却得不到大家支持。

经过一番思考我认识到，写报道的人及坚信这些报道的人，大家都认为“Mt.Gox经营者的行动不正常”。之所以这样认为，是因为正常的小偷不会盗取没有价值的东西。更准确地说，人们不偷“一旦被盗将变得一文不

值的东西”。这被我称为“小偷的基本法则”。Mt.Gox 经营者盗取比特币正是因为明白“这样做并不会导致比特币破产，对其价值也没有任何影响”。换句话讲，Mt.Gox 事件展示的不是比特币脆弱的一面，而是其强韧的一面。

总之，该事件后，不断有朋友提醒我：“批判安倍经济学倒没什么，一旦跟比特币这种不靠谱的东西扯上关系，会降低人们对你的信任。千万别碰比特币了。”

实际上，貌似我已经被大家用奇怪的眼神看待了。其证据就是，某周刊杂志的记者曾试探性地问我：“比特币已经破产，你却说它没破产，是因为你投资了比特币的相关企业吧？”（之前持有过，但是不想被人怀疑成利益相关者，我目前已不再持有比特币。）那本周刊的目录标题是我“（就比特币破产）进行辩解”。

前不久我接受了某家主流报社的采访。本以为他们终于认识到了区块链的重要性，我欣喜万分，滔滔不绝地解释说明了一番，报道里刊登的却是我“板着脸一本正经地谈论了”区块链的未来前景。

即便国外也是一片否定之声。JPMorgan Chase 的 CEO 杰米·戴蒙嘲笑比特币宛如 17 世纪荷兰爆发的郁金香球茎泡沫。投资银行高盛在 2014 年 3 月的报告书中称：“比特币不是货币。其信奉者应该先冷静下来重新规划。”[2]

尽管如此，这两年间，世界发生了巨大变化。

我在撰稿《虚拟货币革命》[3]时，曾介绍“现阶段，虚拟货币还只是梦想”，但现在却已经开始实际运作了（这被称作“比特币 2.0 时代”或“区块链 2.0 时代”，本书将在第 9 章、第 10 章进行说明）。形势正在急剧变化，超乎人们想象。

由于国外频繁传来新闻，报道称区块链技术的应用正在不断扩大，因此，近一年左右的时间内，日本的区块链现状也发生了巨大变化。特别是在金融行业，该技术的导入正在呈井喷式增长。日本貌似也进入了第二阶段。

“黑船”这一表述虽太过陈旧，但人们无疑已经开始认识到“黑船已露

出水平线，将要唤醒这太平的沉睡”（我认为与其说是黑船，不如将区块链比作来自宇宙某个角落的外星人更恰当）。

然而，社会整体的认识水平依然很低。这也是必然的，因为这项技术过于超前，尚未被大众理解。总之，还没有达到第三阶段。

另外，存在第二阶段特有的混淆现象。

当前在金融领域，一项被称为 Fintech（金融科技）的技术革新引发大家普遍关注。正如本书第 5 章所述，Fintech 是一项可用于移动支付、网络在线融资等方面的新服务。在日本，大家对 Fintech 的关注度非常高，“Fintech”甚至成了流行语。

金融领域正在发生翻天覆地的变化，这是事实。但是，因为各种事物在同时演进，到底哪个重要哪个不重要，人们并不明了。具体而言，传统技术型 Fintech 与应用区块链技术的 Fintech 是全然异次元的东西，二者没有被正确理解。发起革命的不是前者，而是后者（关于两者区别，第 1 章第 4 节将展开论述）。

我并不是否定区块链以外的 Fintech，它们让生活更加便利。然而，它们却不是能带来颠覆性变革的技术革新。

其次，区块链包含两项不同性质的东西（即第 3 章第 2 节论述的公共区块链和私有区块链）。而传统 Fintech 几乎没有意识到二者间的巨大差异。

我在《虚拟货币革命》的“前言”部分引用了“这不是叛乱。这是革命”（这是法国革命爆发当天，罗哲福考德公爵对路易十六说的话）。

正如飞机的发明是场革命、互联网的普及是场革命一样，区块链也是一场革命。它会带来颠覆性变革。换句话讲，它将颠覆整个世界。

然而，恰如法国革命，在革命初始阶段，谁都不知道革命将引导社会走向好的方向，还是坏的方向。飞机能够短时间内到达地球任何角落，另一方面，距初次飞行仅过了短短 10 年，飞机已经作为强大的武器被投入到

第一次世界大战中使用。

互联网改变了社会，成为引领经济腾飞的主角。但是，正如当初所料，社会没有实现扁平化发展，而是少数大企业逐渐支配了世界。

为什么会变成这样呢？本书将在最后一章论述这个问题。我认为最本质的原因是，在互联网世界很难验证哪些数据是正确的，因此小组织和个人不容易建立信任关系。大型组织就成了人们信任的基础。

但是，区块链不依赖组织，并且可以验证数据信息的正确性。正因为这些条件得以实现，社会才会有巨大变化。

这样一来，就能构建一个不依赖组织，个人能力得到充分发挥的社会。不仅可以提高经济活动的效率，还可以改变组织模式，改变人们的工作方式，从而形成个人直接联系、直接进行交易往来的社会。

然而，也存在完全相反的可能性。银行等大型机构，可能会利用私有区块链提高办公效率。这种情况下，信任就不是由区块链确立的，仍是由组织保证的。所以，社会仍然会由大组织支配。

就货币而言，按照这个方向发展下去，中央银行将通过发行虚拟货币控制经济。这就是乔治·奥威尔在其小说《1984》中所描绘的老大哥的世界。关于这个问题将在第 6 章第 4 节论述。

总之，区块链可能带来以上两种截然不同的社会变化。究竟会实现哪一种，取决于今后。我们当下正站在巨大的岔道口上。要影响变化的方向，需要正确理解区块链。

撰写本书正是基于上述问题意识。为此，本书不仅在技术层面对区块链技术进行阐述，还将介绍其具体应用前景，详细描述区块链技术在金融领域之外的应用。因此，必须强调区块链对社会结构的重要影响。

本书部分内容依据 *DIAMOND online* 和周刊 *DIAMOND* 上刊载的报道

完成。在此向许可我使用的 DIAMOND 社的各位表示衷心感谢。

自本书策划阶段起，一直承蒙日本经济新闻出版社编辑田口恒雄先生多方照顾，田口先生对本书书稿给予了诸多有益建议。在此深表感谢。

2017 年 1 月

野口悠纪雄

目 录

图表目录

序章　区块链引发地壳变动

由于区块链技术引发的社会变动太过根源性，人们很难把握其整体面貌。本章意在明确这一面貌。

较之此前的信息技术，区块链哪里不同？它能做什么？变化的本质是什么？它将如何改变社会？就上述问题，我为大家简单绘一张素描。

即便不信任人和组织也能安心交易 trustless system（去信任系统）

区块链，一种记录电子信息的新机制[1]。

区块链包含以下两个要点。第一，不仰仗管理者，依靠计算机集群自主运营可信赖的业务。第二，保护数据不被随意篡改。

在区块链的相关文献中，trustless system 屡次出现。其意思不是“不能信任的系统”，而是“不仰仗个人和组织的信任也能安心交易的系统”（也有使用 trustless trust system 一词的，这个才是正确的）。

这样的系统只有依托区块链平台才能运行。这是巨大的变化。

以往，经济交易必须基于双方信任才能成立。因此，无论任何行业，必然存在管理者。管理者对交易的全部事项负责。如果管理者值得信赖，人们就会信任此项事业，决定进行交易。单是几个人的松散组织，没有管理者的话，出现问题时，就会不知道该找谁交涉。人们是不会和这样的组织进行交易的。

但是，在使用区块链的事业中，事业的运行方式已通过合约进行了设定（“合约”指计算机应遵从的程序规则集合）。计算机按其处理信息。因此，尽管不存在管理者，也可以信赖。这完全打破了以往的常识。许多人之所以感觉“比特币是奇怪的东西”，正是因为这些发明太过超前。

电子数据能够简易地被改写，因此很难验证某个数据正确有效。例如，所提交文件如果是电子形态的话，就很难判断其是原件还是被改写过的。

如果纸质文件上有印章（或签名）就能确认其有效。但是，通过电子邮件发送的电子版资料，一般得不到人们信任。因此，仅仅通过电子手段很难完成交易。

然而，区块链里写入的数据是（事实上）不能被改写的。因此，里面写入的数据肯定是真实的。

区块链出现之前，相互不信任的人聚在一起开展一项要求必须具备信任的事业是绝对不可能的。这在计算机科学领域，作为“拜占庭将军问题”被大家熟知（将在本书第 1 章第 1 节进行说明）。

“拜占庭将军问题”通过区块链得以解决。这是计算机科学领域划时代的突破。这是极其完美的机制。本书将在第 1 章的第 1 节和第 2 节说明这项机制。而且，第 3 章第 2 节的“私有区块链”与以上论述内容不同。只要管理者存在，进行交易时，就需要信赖管理者。

用互联网传递经济价值成为现实

以下两点是传统互联网不能实现的事情。第一是传递货币等有经济价值之物。第二是建立信任机制。这些问题被区块链一一攻克，极大地颠覆了经济活动和社会结构。具体来说，参考如下。

第一，借助区块链，货币等经济价值通过互联网即可传递。

这样一来，马上就会有人反驳说“即便现在这么做也是可能的”。的确

是这样，比如你在亚马逊网站购书，只要在互联网上输入信用卡号就能完成支付。

但是，这里面却存在以下问题。

首先，必须和收款方确立信任关系。

因为对方是亚马逊所以我们可以毫不担心地输入信用卡号，但是如果对方是名不见经传的网站，我们应该就不会输入号码了吧。因为信用卡号有可能会被滥用。

其次，你自认为是在和亚马逊互通信息，但对方却可能是冒牌的亚马逊。为应对以上问题，现阶段导入了“SSI 认证”机制。这样，就能够保证得到认证的（浏览器地址栏的小锁头不是 http：//，而是 https：//）网站不被冒用。而且，通信受密码保护，防止中途被盗用和篡改[①]。但是，要取得 SSI 认证，需要花费高成本。

第三，使用信用卡转账成本高。

因为不是转账方支付成本，所以一般消费者不会意识到这点。但是，对于店铺来说却是负担。亚马逊这样的大型经营者一般也没什么问题。但对于小型网站来说却是沉重的负担。所有利益所得都将按一定转账结算手续费进行收取。只有小型经营者懂得这到底是一笔多重的负担。

但是，借助区块链平台，就可以通过互联网实现经济价值的低成本转移。

互联网从本质上来说，是一种“便宜没好货”的通信系统。因此，当然不能使用它来传递经济价值。只能被迫花费高额费用去传递。

区块链颠覆了这种互联网传统。以往，交易虽已达成，但转账、结算却不能实时解决。而区块链恰好能弥补这一缺陷。世界范围内的分工体制

① 颁发认证的认证局，有着金字塔式的组织结构。处于最高位的是“路径认证局”，其他认证局，由上一级的认证局颁发证明书来证明自身的可信性。只要登录最高路径认证局浏览器，看到比其地位低的认证局的证明书就说明这家网站是可信的。在除此之外的网站打开浏览器时就会弹出警告框。详细内容请参考《虚拟货币革命》补论。