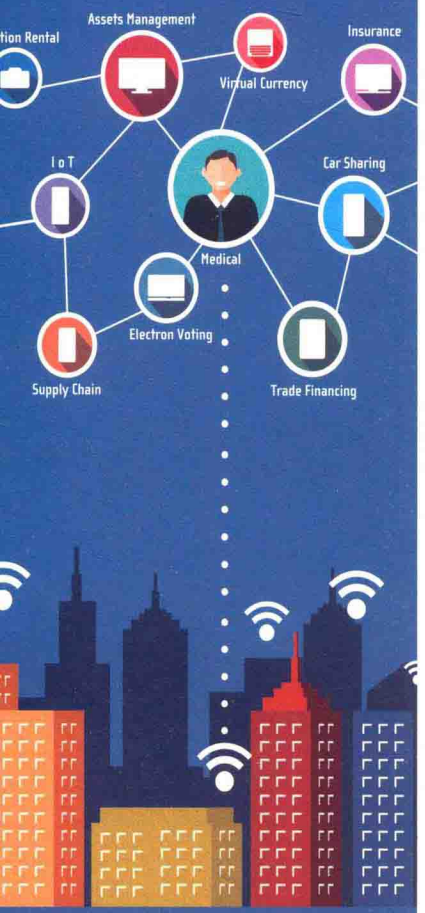
加密货币与区块链所预见的世界

科技将为我们实现怎样的梦想

暗号通貨とブロックチェーンの先に見る世界

监修　JBCIA（日本区块链产业协会）
著　［日］栗山贤秋　辻川智也　铃木起史
译　田宇韬



上海财经大学出版社

加密货币与区块链所预见的世界

科技将为我们实现怎样的梦想

暗号通貨とブロックチェーンの先に見る世界

监修　JBCIA（日本区块链产业协会）
著　［日］栗山贤秋　辻川智也　铃木起史
译　田宇韬

上海财经大学出版社

图书在版编目(CIP)数据

加密货币与区块链所预见的世界:科技将为我们实现怎样的梦想/(日)栗山贤秋,(日)辻川智也,(日)铃木起史著;田宇韬译. —上海:上海财经大学出版社,2019.8

ISBN 978-7-5642-3324-2/F·3324

Ⅰ.①加… Ⅱ.①栗… ②辻… ③铃… ④田… Ⅲ.①电子商务-电子支付-支付方式 Ⅳ.①F713.361.3

中国版本图书馆 CIP 数据核字(2019)第 144855 号

加密货币与区块链所预见的世界

——科技将为我们实现怎样的梦想

作　　者:[日] 栗山贤秋　辻川智也　铃木起史　著

田宇韬　译

策划编辑:李志浩

责任编辑:李志浩

版式设计:朱静怡

封面设计:张克瑶

出版发行:上海财经大学出版社有限公司

地　　址:上海市中山北一路 369 号　(邮编 200083)

网　　址:http://www.sufep.com

电子邮箱:webmaster@sufep.com

经　　销:全国新华书店

印刷装订:上海华业装璜印刷厂

开　　本:890mm×1240mm　1/32

印　　张:5.75(插页:3)

字　　数:99 千字

版　　次:2019 年 8 月第 1 版

印　　次:2019 年 8 月第 1 次印刷

定　　价:50.00 元

图字:09-2019-705 号

暗号通貨とブロックチェーンの先に見る世界

——テクノロジーはどんな夢を見せてくれるのか

by 栗山賢秋,辻川智也,鈴木起史

前言

随着人们对加密货币认知度的提升，“区块链”的概念被人们所关注，媒体也开始频繁地提及关于加密货币的问题。现在，不仅是业内人士，各行各业的人都开始研究如何更有效地利用区块链，或许将加密货币引入生活之后，在将来能探索出新的生活方式。

如果能有效利用区块链技术，可以预见，各类企业自然不用说，行政、医疗、社会福利、健康、教育等各方面存在的可能性都将被拓宽。“相信在不久的将来，我们生活中的很大一部分都将逐渐变得和区块链技术息息相关”，这样的预测，应该是大势所趋。

然而，遗憾的是，即使是当下，区块链这个概念也没有被人们所充分认知，因误解产生的矛盾并没有完全消除。和区块链有关的信息正处于一个玉石混淆、混乱发展的状态。甚至在一大批出版的书籍中存在着一些让人感到十分疑惑的内容。另

外，通过现状可以发现，区块链从根本上改变了现有的社会关联方式，甚至可以轻易超越国家的构筑框架，逐渐构建出一个全新的，由人、事、物组成的网络工作环境。但是，为了正确地迎接这种潮流，大众需要拥有一定程度的该领域的能力。

不过，现在的日本真的达到了一个能迎接区块链潮流的足够的等级了吗？对此我们感受到了极大的疑惑。例如，对于加密货币和区块链之间有着何种关联持有疑问的人，即使是提出了“区块链是什么？”这样的问题，能够准确地回答这个问题的人，也只有少部分。另外，讽刺的是，2018 年 1 月发生的以 Coincheck 的 NEM 被盗事件为代表的恶性事件，竟然成为一个促使人们对于区块链的认知度上升的契机，但同时，错误的信息和负面的认知也随之扩散开来。

再这样下去，日本将会成为区块链技术后进国，这可能会极大地左右今后社会应有的状态。如果无法有效利用区块链技术，这对于日本在融入国际社会方面可以说是致命的也不为过。虽然前面有提到区块链是能够“超越国家的构筑框架”，但是如果在技术和知识尚未达标的情况下发展区块链技术的话，这绝不会成为一个理想的状态。

以打破这样的局面为目的而创设的组织，正是日本区块链产业协会（Japan Block Chain Industry Association，JBCIA）。

关于日本区块链产业协会(以下简称 JBCIA)

JBCIA 是为了推进、发展日本区块链社会的教育,从而达到“培养全球领先”以及“实现最好的实践效果”的目的而设立的。

另外,JBCIA 的使命是推进区块链的全球化采用,同时对可持续发展经济产生实际影响。此外,通过拟定一个关于区块链的基准点,努力使日本成为区块链领域的一个主要国家。为了达成这些目标,需要采取各类行动。概要为如下几点:

- 教育:培养、支援下一代负责区块链技术的工作人员。
- 研究与开发:推进区块链技术的研究和开发,建立产业发展的基础。
- 知识的传播与普及:使区块链知识以更加易懂的方式进行传播,以启发更多人为目标而努力。
- 合作与发展:促进开发者之间的合作,创造出全新的区块链技术。
- 建立国际联盟:开拓区块链关联市场,与国际合作伙伴建立联盟。
- 集体活动:共享情报、会员业务,建立能让活动迅速发挥作用的体系。

关于区块链的详细内容会在本书中再一次提及,它的一个特征是“P2P”,也就是非中央集权的网络构筑。在这个系统中,

互相支持、互相监督的同时，兼具着能够排除不正当和虚假信息的功能，这不仅仅是为了利益，也是为了提供一个整体和谐的环境。这与 JBCIA 的创设理念相吻合。

通过采取各类行动，正确地拓宽区块链的知识和技术，创造一个能让用户享受到正当利益的环境，减轻风险，排除恶性事件。更进一步地说，在下一代区块链的变化到来时迅速地察觉到，规划出道路并按指示执行。作为面向这些行动纲领中的一步，共享区块链及其关联的信息，是本书的主旨。

希望通过本书的一系列的阐释，传播对区块链的正确的理解，共享面向将来的可能性和愿景。希望在全球，除日本之外还有源源不断的国家能有效利用区块链技术，为其发展做出贡献。

日本区块链产业协会(JBCIA)　铃木起史

2018 年 10 月

目 录

1 前 言

第一章 关于区块链

3 区块链是什么?

13 区块链的开发者兼创始者、谜一样的人物“中本聪”

16 区块链的结构和特征

30 区块链的用途

40 区块链技术是否有风险

46 区块链成立的原则

54 栏目 1 关于“拜占庭将军问题”?

第二章 加密货币

63 加密货币的历史

72 加密货币的现状

80 加密货币的种类

89 加密货币的功能

97 栏目 2 任何人都能胜任挖矿工作吗?

第三章 ICO

105 ICO 的定义

113 ICO 和 IPO

120 ICO 的风险

127 栏目 3 作为一种亚文化工具时,区块链所拥有的可能性

第四章 区块链与加密货币所预见的世界

135 数字技术的进步

139 区块链为我们展现的未来

147 加密货币为我们展现的未来

159 栏目 4 为什么加密货币能够拥有价值

165 **结语**

第一章

关于区块链

区块链是什么？

在唐·塔普斯科特、亚历克斯·塔普斯科特的著作《区块链革命》的开头，他们将区块链比作“科技界的精灵（妖怪）”。这确实可以说是体现出了区块链的本质，是一种十分恰当的比喻。

《阿拉丁神灯》中登场的神灯精灵，拥有可以满足人们任何愿望的魔法，如果被阿拉丁这样的善人所拥有，那么就可以帮助任何需要帮助的人，如果被像加尔法这样充满权欲的人获得，那么就会成为邪恶的工具甚至是混乱的元凶。区块链也可能隐藏着这种遇优则优、遇恶则恶的性质。

区块链是科技的产物，是管理、运用信息的一种手段。在那里没有意识形态的存在，因此，没有偏见、没有差别，谁都可以平等地参加，公平地享受利益。在区块链的功能正常发挥的范围内，进行不正当行为的概率几乎为零，同时，区块链能正常地持续运作的可能性，和过去的种种科技技术相比要更高。这可以说是十分创新化的设计，是比互联网的诞生更具冲击性的现象级事件。

然而，创新化的发明和突出的技术常常会被巨大的组织独占，被扭曲着朝着与初衷不同的方向暴走。这个事实，历史早有例证且数不胜数。诺贝尔、爱因斯坦、冯·布朗都没有预想到自

己的发明和发现会让许多人遭受不幸。

无论多么出色的工具到了愚者的手中都会成为混乱的源头。最近，由于ICO泛滥导致的一部分近似诈骗的行为（有时是欺诈行为本身）可以说是完全符合这个说法。区块链依旧处于一个正在发展成熟的阶段，在这个过程中，会产生像人类的生长痛一样的问题。但是，这些问题大体上并不是由于区块链本身所持有的不完整性导致的，而是因为误解、误用、恶意使用所导致的问题。以这样的背景为前提，以区块链“不只是盈利工具”，“更不是使有权者和巨大组织变得壮大的工具”这两点为中心作为本书的基础，继续我们的话题。

前文的铺垫稍微有些长。现在进入正题吧。关于区块链的概要，有以下几点说明。

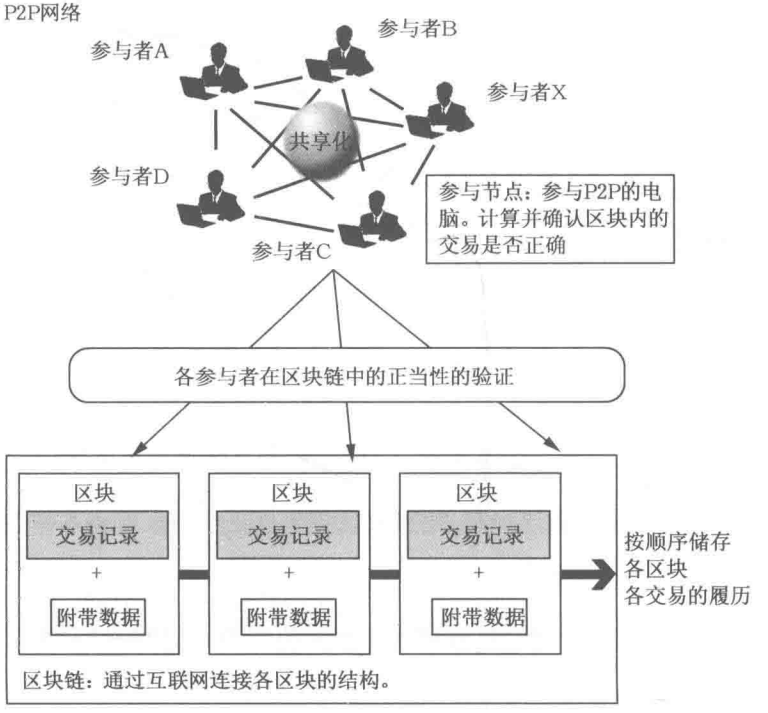
看见这个“区块链是什么？”的标题，也许有人会认为“我已经完全熟知区块链了”。然而，区块链尚未拥有一个明确的定义，个人与个人之间对于区块链的认知会有细微的差别。在本篇文章中，为了使“区块链的定义”变得明确，我将再一次对区块链的概要进行描述。

区块链，简单来说，就是“将巨大的账本分布化，通过网络将其联结在一起的东西”（虽然生成的顺序是相反的，但是为了更好地理解便进行了如上叙述）。日语中的“分布式账本”，也有

“分布式网络”的含义。区块链也就意味着构成了分布式账本的技术，也指代分布式账本本身，一方面也包含了分布式账本中的一切，在本书中，将以“区块链＝分布式账本”作为定义。

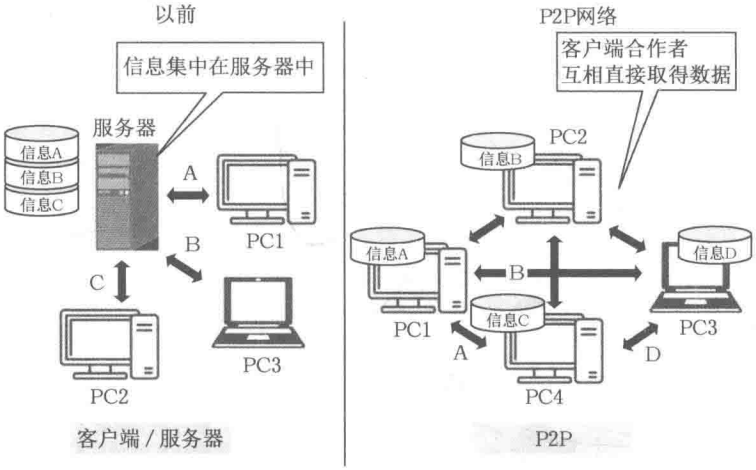
区块链，顾名思义，由“区块”和“链”两个要素构成。通过“P2P”的方式连接起来。

区块—— 一定时间内保存交易记录以及其产生的附带数据的部分。



链——将“区块”通过互联网连接起来的结构。

P2P(peer to peer)——不通过服务器就能将电脑上的合作伙伴连接到一起的方法。



例如比特币交易，大约十分钟的交易数据会被保存在一个区块中。这个数据被构成区块链的电脑终端——节点所拥有。节点通过网络进行连接，以此共享数据。通过拥有众多的节点间的联系共有了庞大的数据，使其对数据的管理变为可能。另外，数据管理的高度加密，使篡改信息等不正当手段变得基本上毫无可能。

关于更具体的内容和特征会在其他项目中进行说明，为了使这个结构成立并发挥作用，并没有必要使用以前的“客户端/

服务器型”为代表的“中央集权型”信息管理结构。

如果只听到这些，可能会被认为是“不就是设计一种新的数据库吗”。如果只看到了区块链的这一个部分，这样解释可能并没有错。但是，这个“创新”对于区块链来说并非是“进化”，而可以说是一种达到了“革命”级别的创新，为了从以前的数据库那样的思考方式中取得飞跃性的提升，包含着区块链的项目产生了与以往截然不同、独一无二的信息流。

以前常识性的“中央集权型”的信息管理体系变为“全部对等”的信息管理体系是非常具有划时代意义的。中央集权型的信息管理，是将所有信息汇集并管理在一个巨大的服务器中，在那里进行客户端信息的交接的许可，并获取、阅览信息。由于信息属于服务器所有者，可能会产生所有者根据自身意愿篡改、删减、限制阅览信息等情况。当然，也有为了所有者的利益而利用信息，发放给他人的可能性，而客户端并不能对此进行控制。实际上这样的中央集权型的管理体系引起的问题，之后都没有完全被解决。大型企业的数据外泄、政治方面的在世界政界中为了某人的利益篡改信息、服务器宕机影响了我们生活中的权益……谁都体验过，但是只能眼睁睁地看着一切发生。

作为区块链的特征之一，使用“P2P”管理信息，就不会存在有权者篡改信息的情况。影响力被分散化，信息不会因为特定