BLOCKCHAIN

区块链+

商业模式革新与全行业应用实例

张 浪◎著

金融业、制造业、农业、贸易、教育、医疗、传媒、物联网，
从前沿到传统，各行业均已被卷入这场技术革命和认知革命。

中国银行、中国邮政储蓄银行、IBM、蚂蚁金服、
微众银行、Airbnb、众安科技、亿书，
从商业巨头到小微企业，都已成为参与者和见证者。

中国经济出版社
CHINA ECONOMIC PUBLISHING HOUSE

区块链+

商业模式革新与全行业应用实例

BLOCKCHAIN

张 浪◎著

中国经济出版社
CHINA ECONOMIC PUBLISHING HOUSE
·北 京·

图书在版编目（CIP）数据

区块链＋：商业模式革新与全行业应用实例/张浪著.
—北京：中国经济出版社，2019.1
ISBN 978-7-5136-5464-7
Ⅰ.①区… Ⅱ.①张… 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（2018）第 268117 号

责任编辑　焦晓云
责任印制　马小宾
封面设计　任燕飞装帧设计工作室

出版发行　中国经济出版社
印 刷 者　北京富泰印刷有限责任公司
经 销 者　各地新华书店
开　　本　710mm×1000mm　1/16
印　　张　17.75
字　　数　238 千字
版　　次　2019 年 1 月第 1 版
印　　次　2019 年 1 月第 1 次
定　　价　58.00 元
广告经营许可证　京西工商广字第 8179 号

中国经济出版社 **网址** www.economyph.com **社址** 北京市西城区百万庄北街 3 号 **邮编** 100037
本版图书如存在印装质量问题，请与本社发行中心联系调换（联系电话：010-68330607）

区块链 +： 未来已来

你有比特币吗？这可是目前区块链中价值最稳定的加密货币。

如果这句话让你摸不着头脑，很可能是因为“比特币”“区块链”“加密货币”这些词还没有进入你的大脑。

可事实上，这些词代表着未来的趋势。

什么是趋势？

1980—1990 年，摆地摊的个体户是趋势；

1990—1997 年，下海自己做老板是趋势；

1998—2007 年，炒股票，进军房地产业是趋势；

2005—2012 年，加入直销，成为直销大军中的一员是趋势；

2012—2015 年，“互联网 +”是趋势；

2016 年以后，“区块链 +”是趋势。

区块链是未来，虽然眼下大多数人并不知道它到底是什么、它是如何运作的，但在可以预期的未来，区块链将成为社会运作的核心。如果你不相信这一现实，那么，你已经落伍了。

这就如同 20 世纪 90 年代初期出现的互联网一样，在当时，对大部分人来说，它都是一种不必要的技术，但也有人意识到了，这是一种能够颠覆未来的技术力量。而区块链因为本身就是基于互联网技术发展而

来的，因此，它所产生的力量要远比互联网大。

在诞生与发展的过程中，区块链借鉴了来自数字货币、密码学、分布式系统、控制论等多个领域的技术成果，可谓博采众家之长，而其核心就是一个由不同节点共同参与的分布式数据库，是开放式的账本系统。比特币大火，带动了区块链技术的大热，但以比特币为代表的虚拟货币只是区块链技术中的一项应用而已——在区块链的世界里，拥有着数百种甚至是上千种能够重新定义现有商业逻辑的技术。

美国著名商业媒体 Fast Company（快公司）在一篇文章中指出："区块链重建了信任模式，它可以模仿多个领域内巨头们的诸多功能，比如优步、亚马逊、Dropbox、Airbnb 和 Kickstarter……但是没有低效的官僚作风和分享利益的中间商。"

当然，你可能认为这是快公司的一面之词，不过，听听各路巨头对这一新技术持什么样的态度，你可能会对它更重视：

阿里巴巴集团董事局主席马云认为，区块链技术有着超乎想象的未来。

摩根大通 CEO 杰米·戴蒙曾在不了解的情况下称"如果你蠢到投资比特币，早晚有一天你会付出代价的"。不过很快他就改口了，说："区块链技术是实实在在的。"

美图公司董事长蔡文胜认为："区块链经济的核心不在技术，而在于商业逻辑的重构。因此，这不仅仅是一场技术革命，更是一场认知革命。"

新东方教育 CEO 俞敏洪直言，现代连接是"互联网 + 人工智能"的连接，区块链的出现，使人与人之间的连接没有了中心载体，成为完全去中心化的概念。

……

如今，在各路大佬的认可之下，巨头们探索的区块链应用边界才开始显现。蚂蚁金服、腾讯、中国银行等一流企业，早已开始将区块链技

术应用到公益捐款、食品溯源、供应链金融等多个领域。

当这种既可以被视为一种行业，又可以被视为一种技术的新互联网科技变得越来越普遍时，先行者们早已明白：它可能是社会升级成乌托邦式世界的关键——听起来虚无缥缈，但这恰恰是区块链的目标所在。

对普通人来说，未来，区块链会越来越多地进入、出现在我们生活的方方面面。这是一个不可避免、必将到来的新时代，而我们在时代的汹涌大潮前必须要做的，就是了解它、参与它，进而利用它。

目录

1

从零开始认识链接一切的区块链

从区块链的价值被发现，到区块链应用实际落地，这期间超过100种区块链技术解决文案被探索。这意味着，过往概念性的区块链已经真正地融入了我们的生活。对于这种正在呈现井喷式发展的新事物，我们有必要从其发源之处开始，了解它是如何诞生的，又是如何发展起来的。

1.1 谈区块链，先要认识中本聪

谈区块链，就必然会谈起“中本聪”。对区块链爱好者来说，如果该领域也有“十大求解之谜”的话，那么，“中本聪到底是谁”肯定列在其中。

严格来说，“中本聪”只是由“Satoshi NaKamoto”而来的音译化名，因其日本化发音，被多数人假设为日本人。

中本聪是网络世界坚定不移的匿名捍卫者，这一点，从他加入的“密码朋克”小组就可以看出。

“比特币之父”的首个身份：密码朋克

数字领域中的先行者们，其实一直想要创建一个匿名、独立、能够保护买卖双方隐私的数字货币，对于这一梦想，最著名的实践小组就是由美国物理学家蒂莫西·梅所创建的“密码朋克”小组。该小组使用自己创造的加密法，而不是外界免费提供的加密工具，这让他们的交流与身份都变得神秘起来。中本聪正是“密码朋克”中的骨干人员。

如图1-1中所展示的那样，在这个以邮件交流的小组中，每个人都是数字与加密界的先行者。

显然，这些行业精英完全尊重中本聪的匿名选择，因此，他们也从

图 1-1 “密码朋克”小组成员

未发表过对他的评价，但一些细节可以帮助我们了解中本聪在该小组中的领导地位：哈尔·芬尼是中本聪的早期助手。密码小组中交流的种种迹象表明，中本聪的地位高于密码学货币的先行者大卫·乔姆。2011年，维基解密宣布支持比特币捐赠时，中本聪对该网站此举持否定态度，并对阿桑奇提出了建议。后来，维基解密淡化处理了此事。而这也是中本聪最后一次公开发表意见。显然，他对阿桑奇有着不小的影响力。

中本聪发明比特币时，他已经在密码朋克中拥有了较高的影响力

那是2008年，在一个隐秘的密码学讨论组上，中本聪发表了一篇名为《比特币：一种点对点的电子现金系统》的研究报告，报告中阐

述了他对电子货币的新构想，由此，“比特币”概念正式面市。

2009 年 1 月 3 日，中本聪开发出一个人人都能发现电子货币的加密金融体系，并将比特币的最小单位定为“聪”（Satoshi），1 聪 = 0.000 000 01 个比特币——比特币软件客户端正式开始运营，中本聪本人则挖出了创世区块中的 50 个比特币。

挖币的同时，他还在该区块中写入了 2009 年 1 月 3 日当天《泰晤士报》的头版新闻标题——“英国的财政大臣达林被迫考虑第二次出手缓解银行危机”。如其他被多方解读的名言一样，这句话被后来的“中本聪信徒”解读为“对传统银行一类中心化金融机构的嘲讽”。

随后两年间，越来越多的新技术爱好者参与到比特币网站的数字货币挖掘活动中，并与中本聪展开了交流。他们不断升级、扩展这套网络，使比特币社区不断发展成为互联网世界不能被忽视的力量。

在与他人的交流中，中本聪展示了自己对比币特的信心，并认为，第三方化、中心化的电子金融体系与传统金融体系一样，都是不值得信任的：“政府擅长击溃 Napster 那样拥有中央控制的网络，但是 Gnutella 和 Tor 这样完全 P2P 的网络看起来依旧安枕无忧。”

这种交流在 2010 年 12 月戛然而止。12 月 5 日，维基解密泄露了美国外交电报。随后，在比特币社区中，有成员提议，用比特币帮助维基解密打破国际权威集团的全球金融封锁。对此，中本聪坚决反对，在他看来，比特币技术并不成熟，根本经不起折腾。随后，他与阿桑奇进行了沟通，并使对方对此事进行了淡化处理。

或许是由此嗅到了身份被曝光的危机，12 月 12 日 6 点 22 分，中本聪在论坛上预言，美联储将很快再次实施货币量化宽松政策。随后，他告别网友，从此再也没有出现过。而他所挖到的百万量级比特币，依然在其比特币地址上。

1.2 从“拜占庭将军问题”看互联网通信的复杂性

中本聪在盛名之下选择匿名，再一次成就了他“密码朋克”的身份。隐匿的是身份，留下的却是成就：中本聪发明的比特币，并不仅仅是一种能够对国家正式的中心化货币体系造成冲击的虚拟货币，而是一种能够改变整个世界的新技术。它解决了IT领域一直以来的“拜占庭将军问题”，预示了区块链时代的正式开启。

难以互信的“拜占庭将军问题”

你或许听说过中本聪，了解一些有关比特币的知识，也大概知道区块链成了全球范围内最火的新技术；但是，你未必知道“拜占庭将军问题”。

“拜占庭将军问题”不仅是区块链的发源，也是一个困扰了计算机科学家数十年的问题。该问题是由“图灵奖”获得者莱斯利·兰伯特（Leslie Lamport）在1982年提出的，在分布式系统中认知一致性问题的描述中，它是最著名的例子。

莱斯利·兰伯特是微软研究院的首席研究员，他在2013年所获得的“图灵奖”被誉为“计算机界的诺贝尔奖”。在研究分布式系统容错性时，为了让故事能够受到普通人的关注，他用历史故事讲述了一个专业化的问题。

在莱斯利·兰伯特的口中，拜占庭将军的故事大概是这样的：

拜占庭帝国即中世纪的土耳其拥有令人垂涎的财富，周围10个小城邦窥觊已久。可拜占庭兵力强大，单独行动势必会失败，还有可能被其他9个邻邦入侵。要攻破拜占庭强大的兵防，至少要有5个以上的邻邦同时发起进攻。

现在，10个小城邦的军队都由各自的将军管理，将军们最需要考虑的问题是：如何达到既能联合攻击，又能预防邻国背叛、保障自身安

全的目的?

“拜占庭将军问题”中的现实与困境

想解答这一问题，将军们需要直面以下现实：①10 个小城邦之间的状态是互不信任、相互对抗的；②10 个将军不能聚在一起开会商议，以妨被敌国奸细一网打尽；③10 个将军中有可能出现叛徒，叛徒会违反承诺或者擅自变更作战计划，导致其他军队攻击失败，并被其他小城邦侵略。

现在，将军们只能通过信使来协商“是否进攻”，以及“具体进攻时间”，而信使传递的核心信息也围绕这两个问题展开：“我是 A 将军，我提议在 10 月 5 日早上 9 点整对拜占庭发起总攻，你是否同意?”

在这一机制下，会引发一系列问题：①信使可能会将信息弄丢，或者被敌国杀害；②信息可能会被敌国截获；③无法确定消息发出者的身份真的是将军；④叛军将军可能会向另外 9 个将军发出 9 个不一样的消息；⑤10 个将军对具体进攻时间的商议过程可能会浪费很多时间。

因为上述问题的存在，将军们想就进攻拜占庭的计划达成一致，看上去就如同一个不可能完成的任务。

达成协议最难的一点在于：在任意时间系统内可能存在着多种提案，这样，便很难让 5 个以上的人在同一个时刻对结果进行一致性确认。可见，这一信息链传输系统极其复杂。

“拜占庭将军问题”其实是莱斯利·兰伯特在工作期间遇到的问题：1982 年，他正在斯坦福担任美国国家航空航天局的顾问，而提出这个问题，也并不是考虑互联网和比特币的应用场景，而仅仅是为了解决航天飞机的安全控制系统。

“拜占庭将军问题”的四大根本难题

在中本聪发明比特币以前，世界上并没有一个非常完美的方法来解