

万向区块链实验室丛书

BLOCKCHAIN SOCIETY

DECODING GLOBAL BLOCKCHAIN APPLICATION
AND INVESTMENT CASES

区块链社会

解码区块链全球应用与投资案例

龚鸣（暴走恭亲王）◎ 著

独家披露258个区块链行业内投融资案例详细数据

拥抱颠覆，区块链社会的商业投资指南

区块链铅笔创始人龚鸣暴走恭亲王全新力作



中信出版集团 · CHINA CITIC PRESS

区块链社会

解码区块链全球应用与投资案例

龚 鸣（暴走恭亲王）◎ 著

BLOCKCHAIN SOCIETY

DECODING GLOBAL BLOCKCHAIN APPLICATION
AND INVESTMENT CASES

图书在版编目 (CIP) 数据

区块链社会：解码区块链全球应用与投资案例 / 龚

鸣著. —北京：中信出版社，2016. 8

ISBN 978-7-5086-6444-6

I. ①区… II. ①龚… III. ①电子货币—研究 IV.

①F830.46

中国版本图书馆 CIP 数据核字 (2016) 第 153538 号

区块链社会：解码区块链全球应用与投资案例

著 者：龚 鸣

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：北京诚信伟业印刷有限公司

开 本：787mm × 1092mm 1/16

印 张：24.75 字 数：300 千字

版 次：2016 年 8 月第 1 版

印 次：2016 年 8 月第 1 次印刷

广告经营许可证：京朝工商广字第 8087 号

书 号：ISBN 978-7-5086-6444-6

定 价：59.00 元

版权所有 · 侵权必究

凡购本社图书，如有缺页、倒页、脱页，由销售部门负责退换。

服务热线：400-600-8099

投稿邮箱：author@citicpub.com

序 一

链接金融 链接未来

李礼辉^①

最近两年，“区块链”迅速成为技术创新的热词。区块链技术应用受到越来越多的关注。国际货币基金组织（IMF）在首份数字货币报告中指出，区块链“具有改变金融的潜力”；英国政府发行的《分布式账本技术：超越区块链》提出，将优先在传统金融行业应用区块链技术；纳斯达克借助区块链建立私人股权交易平台 Linq；花旗、汇丰、富国等银行加入 R3 区块链联盟并设置自己的研究实验室，德勤借助基于区块链的 Rubix 平台提供咨询和审计。在我国，中国平安加入 R3，万向成立区块链实验室，中国互联网金融协会成立区块链研究工作组。区块链是否如同互联网一样，将会改变金融、改变生活方式、改变商业模式？这是人们正在思考和探索的课题。

^① 李礼辉，全国人大财经委员会委员，中国银行前行长，中国互联网金融协会区块链研究工作组组长，有近 40 年金融工作经验。

区块链最早作为比特币的技术应用，起源于2008年。经过不断的迭代演进，区块链形成分布式（Decentralized）、免信任（Trustless）、时间戳（Time Stamp）、非对称加密（Asymmetric Cryptography）和智能合约（Smart Contract）五大技术特征。进一步探讨，我们发现，区块链应该是一种更加切合市场经济和现代生活方式需求的应用技术。

首先，区块链的智能合约功能，可以应用于契约关系和契约原则的维护和执行。契约精神是市场经济社会的支柱，体现契约精神的契约关系和契约原则，以及上升到公法领域的公权力，对于建立良好秩序、保障市场经济健康运行具有基础性的意义。在市场经济社会中，契约原则一般是通过良俗的推行、法律的实施、合约的履行来实现的。良俗是约定俗成的文明理念和行为准则，法律是写在纸上的规则，合约既有白纸黑字的约定也有口头的承诺。这就存在一个可能被利用的“缝隙”：违背良俗、冒犯法律、背离合约的行为有时难以在实施的过程中被及时制止和纠正。

例如，票据是便捷的支付结算工具和融资工具，也是中央银行重要的货币政策工具。2015年，我国累计签发商业汇票22.4万亿元，比2001年增长17倍，金融机构累计贴现102.1万亿元，比2001年增长56倍。而现行票据业务存在的缺陷，主要在于难以有效管控和防范操作性风险和道德风险，包括贸易背景造假，票据真实性认证失效，“一票多卖”，利用票据违规融资套利等等。票据业务监管只能通过现场审核的方式来进行，缺乏全流程快速调阅和审查的手段，监管效率低、成本高。如果应用区块链技术构建数字票据，就有可能通过可编程的智能合约形式，实现商业约定的具体限制，引入监管控制节点，由交易各方确认交易，确保价值交换的唯一性。

其次，区块链的分布式、时间戳和非对称加密功能，可以应用于信息

的查询、验证和保护。现代社会产生的信息是海量的、几何级增长的。信息大致可以区分为共享信息、专有信息和私密信息。共享信息的价值在于真实，必须维护其权威性；专有信息的价值在于归属，必须维护其知识产权；私密信息的价值在于可靠，必须维护其安全。互联网的发展极大地促进了信息的生产和传播，但往往难以证明共享信息的真伪，难以确认专有信息的所有权，也难以保护私密信息的安全。

区块链的分布式功能，通过构建分布式数据库系统和参与者共识协议，有利于保护数据的完整性。区块链的时间戳功能，通过生成一定时间段的信息区块和区块之间首尾相连的数据链，能够形成可追溯溯源、可逐笔验证、不可篡改、不可伪造的数据；每个参与者在生成信息区块时加盖时间戳，能够证明原创性和所有权归属。区块链的非对称加密功能，有利于保护信息的私密性。

龚鸣所著的《区块链社会：解码区块链全球应用与投资案例》一书，向读者描述了区块链技术实际应用的场景和案例，可以让更多的人了解区块链，了解区块链将会如何改变我们的生活。

例如，Circle China、Abra 将区块链技术应用用于跨境支付汇款这个生活中经常出现的场景，节省了跨境汇款的时间成本、人力成本，使跨境汇款更加便捷。Symbiont 通过智能合约自动生成智能证券，在区块链之上自动完成证券的发行、交易和结算，让证券交易变得简单直接，能够更有效地保护合约，防止信息泄露。在奢侈品溯源、分布式交易所、物联网和供应链、医疗行业、互助保险等领域，区块链技术应用都有可能成为现实。

国务院《推进普惠金融发展规划（2016—2020 年）》提出：“金融基础设施是提高金融机构运行效率和服务质量的重要支柱和平台，有助于改善普惠金融发展环境，促进金融资源均衡分布，引导各类金融服务主体开

展普惠金融服务。”应用区块链技术，可能形成新的技术优势：成本较低，风险较小；数据完整，信息透明；智能化管理和监控。这将提升金融基础设施的服务功能，有利于推进普惠金融发展。

万向区块链实验室计划出版一系列区块链丛书，推广这一项在中国还有些陌生，但未来也许会改变世界的区块链技术。我们感谢万向区块链实验室所做的贡献。

序 二

区块链的研究与应用并重

王永利^①

一段时间以来，常常在微信圈里看到龚鸣兄（暴走恭亲王）发布的关于全球范围内区块链在多个领域应用的案例，深受启发，也特别佩服他花费那么多时间和精力收集和整理了那么多区块链应用的案例，更希望他能将这些成果进一步整理提炼，形成系统的成果并更广泛地传播。近期获知，在此基础上，他即将出版发行《区块链社会：解码区块链全球应用与投资案例》，深感欣喜，相信此书的发行，一定会为人们了解和认知区块链，特别是区块链可能的应用和投融资领域，提供很大帮助，发挥重要作用。

现在，区块链已经成为互联网领域，特别是金融科技（Fintech）领域火热的概念，吸引了越来越广泛的关注、研究乃至投资热潮。但客观讲，

^① 乐视高级副总裁，中国银行股份有限公司前执行董事、董事会风险改革委员会委员及副行长。

区块链技术于 2009 年初才随比特币首次推出并付诸应用，现在应用的时间还很短，而且比特币完全是模拟黄金，在独立的网络世界重构出一种数字货币或数字资产（财富），一开始并不是可以直接用法定货币购买到比特币的，而是必须先在比特币社区（Block）通过“挖矿”的方式产生；挖到的比特币，必须用比特币合约规定的相互认证方式加以确认（去中心化），包括所有者的身份认证与其比特币数量的认证等，而不是用现实世界惯用的主权国家公民身份证等证件，由业务或鉴证中心予以确认；比特币的转让交易，采用全网加密、分布式记账方式加以确认和记录，其中包括跨区块之间的交易，必须加入区块的加密代码以及时间代码等，形成区块之间的连接（即 Blockchain，区块链）；在形成独特的比特币世界（包括参与者的身份认证、比特币的产生与交易认证和记录、相关的管理规定等形成的体系）之后，才开始推动比特币世界与现实世界的连接，允许比特币与法定货币的兑换与交易。可见，区块链在比特币上的应用，是不受现实世界各种规制约束的，而是在人为创造的独特环境中的应用。因此，尽管区块链在比特币上得到了可以称得上非常成功的应用，但是，要将其直接应用到现实世界，却可能受到非常多和大的约束，甚至不可避免地会面临诸多挑战和阻力，是会非常艰难的。对此，必须要有清醒的认识，不能盲目追崇和胡乱投资。

但是，区块链和比特币的出现，确实给人们认识和适应新兴的网络世界带来思维方式和路径上的巨大冲击或创新：由于网络世界是在现实世界基础上随着互联网的发展而出现的，各种财富和交易，都是从线下向线上迁移和推广的。因此，线上的当事人身份认证、交易确认、资金清算和交易记录等等，也就非常自然地沿用线下的规则，或进行必要的改造以适应网络运行的需要。但随着网络世界的发展和交易的日益频繁，人们逐步发现，完全沿用线下的规则，很难适应和满足线上的需求，亟须有更大的革

新乃至革命，创造出不同于现实世界的全新的网络世界。在这方面，区块链和比特币的出现，即使还存在这样或那样的问题，其全新的思维和实践方式，却具有极其重大的启蒙意义。因此，非常有必要不断加强和加深对区块链的研究和创新，特别是寻求如何将现实世界的财富向网络世界迁移并扩大交易的可行的高效的路径与方式。

《区块链社会：解码区块链全球应用与投资案例》一书，不仅对区块链的概念和原理进行了必要的梳理，更重要的是提供了大量具有典型意义的全球应用与投资案例，突出研究和应用并重，并作为重要的研究结论，提出区块链可能成为人类首次大规模协作和相互认证的开始，分布式记账方式、去中心化自治组合和智能合约，也许会颠覆现代商业社会，重塑社会结构和运行方式。相信，这会给读者带来很多启发。

祝愿《区块链社会：解码区块链全球应用与投资案例》发行成功，也期待龚鸣兄有更多的研究成果面世！

序 三

区块链：数字另类资产的新大陆

肖 风^①

你一定知道美国著名高校耶鲁大学。如果你稍作了解，你一定也听说过耶鲁大学基金会。如果你对基金投资稍作了解，你一定看到过耶鲁大学基金会过去几十年骄人的投资业绩。作为大学捐赠基金，由于资金的长期性，它的投资目标第一是要打败通胀，第二是要战胜基准，第三是要力争绝对收益。可喜的是，这三条耶鲁大学基金会都做到了！尤其第一条和第二条目标，更是大大超越！

研究早已表明，超过 90% 的投资业绩的取得，来自于资产配置，而不是来自于个股或个券的选择。耶鲁大学基金会几十年的骄人投资业绩，就来自于他们在资产配置模式上的大胆创新。据耶鲁大学基金会 2015 年年报披露，该基金截至 2015 年 6 月的资产组合中，大宗商品占比 6.7%，私募

^① 肖风，南开大学经济学博士，中国万向控股有限公司副董事长，万向区块链实验室和分布式资本的创始人。

股权占比 32.5%，房地产占比 14%，合计超过资产组合的 50%。在全球资产管理界的经典教科书上，我们一般把股票、债券、现金归为传统资产类别，而把大宗商品、对冲基金、PEVC（PE，Private Equity，私募股权投资；VC，Venture Capital，风险投资）、房地产归于另类资产类别。人们把这种以另类资产作为组合核心资产来配置的新模式，叫作“耶鲁模式”，以区别于以股票、债券、现金等传统资产为组合核心资产来进行配置的资产配置模式。耶鲁大学基金会超越同行、超越基准目标的大部分秘密就在这里。

从耶鲁大学基金会的案例里，我们可以得到三点启示：第一，要得到比别人更高的投资回报，就不能只在传统资产类别里打转，要另辟蹊径；第二，资产类别不是一成不变的，新技术、新经济、新模式会创造出新的资产类别，要有独到眼光；第三，如何对新的资产类别进行评估分析，进行风险定价，要有新框架、新方法。谁比别人更快更好地掌握了新方法，谁就可以饮到“头啖汤”！

我们知道，15~16 世纪的地理大发现，奠定了欧洲大陆近几百年在人类社会的领先地位，为欧洲大陆创造了至今仍然可观的物质财富。而自从互联网技术于 20 世纪 90 年代初成熟以来，人类社会又开始了一次新的地理大发现运动。这次不再是物理空间的大发现，而是数字空间的大发现。20 世纪 90 年代中，MIT（麻省理工学院）媒体实验室负责人尼葛洛庞帝出版的《数字化生存》，是这场数字地理大发现的行动宣言。传统依靠土地、设备、劳动力创造财富的模式，因为资源的有限性，已经无以为继。而数字空间的无限可扩展性、比特结构的无限可复制性、虚拟世界的多维可塑性可能意味着蕴藏在这里面的待开发的财富，会数十倍于物理世界。

这些新财富的表现形式就是数字资产。

什么是数字资产？我认为数字资产有五个属性：第一，数字资产是登记在区块链账本或分布式账本上的资产，那些登记在工商局的股权，登记在房产局的房产一定不是数字资产；第二，数字资产是以比特结构存在的虚拟资产，不是像黄金那样具有原子结构的实物资产；第三，数字资产是一段计算机程序，不再是一行数字符号，可以对它进行编程，资产之间的交换是代码与代码的交换，不是数字之间的增减；第四，数字资产因为可编程性，可以在区块链上，通过编制智能合约程序，完全去中介化地自主、自治地进行点对点交易，不需要人工干预；第五，数字资产大部分情况下都是以“Coin”（数字代币）的形式存在的，数字资产跨越了资产证券化的阶段，直接达到了资产货币化的阶段。

比特币、以太币等数字货币是目前最为人们熟悉的一类数字资产。各式各样的数字货币大概有 300 多种，市值约 120 亿美元。但数字资产的范围比这要大得多。欧美主流金融机构几乎都成立了自己的区块链实验室，正在各种金融场景中，试验运用区块链技术，来创设发行智能股票、智能债券。所谓智能，其实就是利用区块链的数据不可更改性和可编程性，在区块链上登记发行股票或债券，使得这些数字化了的股票或债券，可以依靠智能合约点对点自主交易，自我结算。在另一条跑道上，还有许多推崇完全去中心化，希望在数字世界里建立一个完全自由、自主、自治的体系的技术极客们，也在尝试推出形形色色的数字资产。根据 IBM（国际商业机器公司）于 2014 年发布的物联网白皮书《设备民主》预测，到 2050 年将会有 1000 亿台设备连网在线，届时在区块链的管理下，将可以实现设备对设备的金融交易（M2M），这更是一个创设、发行、交易数字资产的更大的机会。

在这里，我可以做一个乐观的展望：十年之后，数字资产整体的市值预计可以达到一万亿美元！到那时，数字资产必将成为另类资产中的一个

举足轻重的类别。谁忽略数字资产，谁不把数字资产列入自己的资产组合，那谁的业绩回报就难以超越基准、超越同行。我们也许可以大胆预言：从资产组合回报的角度来看，未来十年，如果你的组合资产配置当中没有纳入数字资产，也许你就真的输在起跑线上了！

我想，我们一定可以在未来十年中的某一年，在耶鲁大学基金会的年报上，看到数字资产作为另类资产的新类别，加入到基金的资产组合中。

龚鸣（网民“暴走恭亲王”）先生是中国最早一批数字货币和区块链技术的研究者和实践者之一。近年来，他致力于在中国推广、传播、培训区块链的理论知识、行业资讯和创业信息，无远弗届。为中国区块链行业的发展做出了突出贡献！他自己还身体力行，创办了中国第一家专注于区块链技术的媒体——区块链铅笔，成为中国区块链行业的创业者之一，胆识可佩，勇气可嘉！

欣闻他撰写的著作《区块链社会：解码区块链全球应用与投资案例》即将由中信出版社出版，着实令人高兴！借为这本书写推荐序的机会，有幸提前拜读了书稿。这也许是全球第一本全景式介绍区块链行业情况，尤其是创业公司情况的书籍；这也许是全球第一本全景式介绍区块链行业投资情况的书籍。龚鸣先生毫无保留地把他过去几年对全球区块链行业的观察和研究心得，几乎是和盘托出。因此，这本书可以帮助我们认清数字资产的性质内容、看清数字资产的形成过程、把握数字资产的投资机会、形成数字资产的投资方法。

在此，作为一个区块链技术的中国信徒，我要感谢他的付出！

在此，郑重向大家推荐这本书！

前 言

自从 2015 年参与翻译了《区块链：新经济蓝图及导读》之后，到现在为止，“区块链”这三个字已经从极小的极客圈中走出，开始变成一个越来越火热的概念。无论是国内还是国外，都掀起了对区块链技术普及和探索的新高潮，越来越多的人开始注意到这个新技术可能产生的巨大影响。但也有更多的人，表现出了极大的困惑，因为往往在看介绍区块链相关文章的时候，觉得这个技术似乎可以彻底颠覆世界，但是如果真的在现实世界中试图探寻可落地的应用案例，却又似乎很难找到身边有价值的案例。我在许多场合中发现，很多试图了解区块链行业的人最容易产生的疑惑就是，区块链，究竟是真的会成为改变许多商业模式的神奇工具，还是仅仅是又一个包装出来的全新概念。

而本书，就试图针对这个疑惑给出一个我的答案。相对而言，国外在区块链技术上，已经完全走出了普及阶段，而早已是真金白银的大量投入。不仅仅可以看到许多大型金融机构和央行对其投入巨大的人力和物力，而且许多有趣的创业公司开始兴起。除了比特币和以太坊之外，区块

链已经在非常多的领域开始大规模尝试，在本书中你可以看到非常多的有趣的项目案例。除了经常能够看到的金融行业案例之外，还包括物联网、公证、医疗、保险、能源等非常多的领域。其中的许多尝试，恐怕会彻底颠覆一些传统商业模式的思维。无论是能够提供按分钟跨国工资发放方案来彻底杜绝拖欠工资可能性的 BitWage，建设完全去中心化的自治电子商务市场 OpenBazaar，或者是提供锚定 SDR（特别提款权）来实现稳定数字货币的 Maker 项目，以及登记全球钻石信息防止血钻交易的 Everledger 项目，都让人有耳目一新的感觉。如果有时间深入研究这其中许多案例的话，最终都可以得出同样的结果，即区块链的本质是一个大规模协作工具，绝不仅仅是改变一两个行业，而是最终会改变我们全球所有人的协作模式。

但是也有许多朋友经常问我，究竟目前有哪些领域有落地的区块链项目开始大规模应用和部署？非常遗憾，现在可能还没有任何区块链项目开始广泛应用或部署。事实上，就像互联网初期，在 1995 年、1996 年的时候，互联网似乎除了看新闻之外并没有太大的作用。特别是互联网开始发展阶段出现大量烧钱的行为，尽管不断有新的模式出现，但始终无法盈利，让很多人最终开始怀疑互联网究竟是不是就是噱头而已，并且导致了互联网第一次泡沫的破裂。而到了今天，应该没有任何人再会怀疑互联网是不是只能用来查看新闻。同样，区块链也在经历一样的过程，尽管我们的直觉告诉我们，这似乎是一个具有极大潜力的工具，但是现在除了比特币之外，我们并没有看到非常广泛的落地应用出现。事实上，区块链作为一个行业崛起，在初期还有大量的基础工作要做。就如同在 1995 年、1996 年，如果你期盼马上看到淘宝、京东未免还太早，更不用说微信这样的应用了。这都需要整个生态环境逐渐建立起来，才能够开始出现一些能够改变我们生活的应用。而又要经过相当一段的普及时间，才能够让更多人开

始意识到生活逐渐被技术所改变。不过，需要注意的是，技术始终是以加速度而不是匀速来发展的，也许不需要再等五六年就可以看到第一次高潮的来临，也许对于区块链行业而言，再有两三年的时间就可以完成第一次的技术积累。

本书在介绍区块链世界中的众多案例时，试图让大家能够注意到这个行业中始终有两条路线的斗争正在进行。第一条路线是自上而下的路线，我们所能看到的类似于 R3 CEV，HyperLedger 这样的联盟，这都是大型金融机构为了确保自己在这场未来变革中的既得利益者位置，而付出的努力。在今天的世界中，金融行业内聚集了全世界最聪明的一群人。不同于互联网初期，全球邮政机构不愿意接受电子邮件，从而最终成为互联网变革中第一个倒下的“恐龙”。而今天的金融行业，已经从区块链技术的发展中嗅到了一丝危险的味道，他们并不像传统邮政系统拒绝变化，而是愿意拥抱变化，甚至是主导变化。但他们的要求就是，在未来的世界中，依旧获得足够的主导权，并且由他们来决定技术的发展方向。

另外一条路线是一条自下而上的路线，从比特币开始，到 Ethereum（以太坊）、BitShares 都显然是其中的代表。由于区块链技术本身是来自比特币，似乎始终能从区块链技术中感受到一股桀骜不驯的力量。这条自下而上的路线中的许多项目，完全无视现有的商业规则和既定的商业模式，用一种完全不同于过去的思路在快速发展，并且颠覆了许多人对很多传统商业模式原有的思考方式。更进一步的是，这条路线甚至彻底颠覆了融资方式，不同于云计算、大数据，甚至是今天火热的 VR（虚拟现实）、AR（增强现实技术）这样的技术变革，因为他们最终会需要通过 VC、PE 的传统方式来进行融资。而作为一种极具生命力的方式，区块链自下而上的路线中的许多项目选择了 ICO（Initial Coin Offering）的方式来进行融资，从而形成了一个完整且自给自足的资金循环体系。而这也是让许多传统金