

BLOCKCHAIN  
QUANTUM WEALTH

# 区块链

量子财富观

韩 锋 张晓玫 主编  
龚鸣 蒋昊然 张夏 等 参编



机械工业出版社  
CHINA MACHINE PRESS

BLOCKCHAIN  
QUANTUM WEALTH

# 区块链

---

量子财富观

---

韩 锋 张晓玫◎主编  
龚鸣 蒋昊然 张夏 等◎参编



机械工业出版社  
CHINA MACHINE PRESS

本书从区块链的技术将降低整个人类的“信用”产生成本出发，论述了互联网新经济从生产大爆炸到交易大爆炸的本质意义：信用可以通过共识协议和密码学算法产生，大数据可以确权，信用资源可以来自市场底层，消费者可以转化成投资者，经济活动中的大部分可以在数理空间智能合约下运行，经济摩擦系数将大幅度下降。在这种前景下，原来无法成为个人财富的大数据、创新思想、人脉关联等将成为人们的主要财富来源。本书最后从量子力学的非定域本体论出发，从信息学麦克斯韦妖的角度，论述了新的财富观的物理基础。本书预言了一个新的数字财富时代即将来临。

### 图书在版编目（CIP）数据

区块链：量子财富观 / 韩锋，张晓玫主编；龚鸣  
等参编. —北京：机械工业出版社，2017.6（2017.9重印）  
ISBN 978-7-111-57261-9

I. ①区… II. ①韩… ②张… ③龚… 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 133041 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：坚喜斌 杨 冰

责任编辑：马碧娟 刘林澍

责任校对：黄兴伟

版式设计：张文贵

责任印制：李 昂

三河市宏达印刷有限公司印刷

2017 年 9 月第 1 版·第 4 次印刷

170mm×240mm·12.25 印张·141 千字

标准书号：ISBN 978-7-111-57261-9

定价：49.00 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

网络服务

服务咨询热线：（010）88361066

机工官网：www.cmpbook.com

读者购书热线：（010）68326294

机工官博：weibo.com/cmp1952

（010）88379203

教育服务网：www.cmpedu.com

封面防伪标均为盗版

金书网：www.golden-book.com

本书指明了一条非常鲜明的数码网络时代财富产生的新途径，值得读者仔细品味。

阿里研究院专家委员会研究员 周子衡

我期待量子的概念在新的领域中开花结果。

清华大学物理系教授、前系主任 张礼

## 序一

为序之始，当交代一下序者与区块链的缘起及与作者的渊源，请容我从介绍几位师友开始吧。

2009年起，我将研究重心放诸货币史上。2011年秋，友人向我推介朱嘉明老师的货币史研究，遂心向往之；2012年1月，正值赴香港参会，期间，购得朱老师出版的新著《从自由到垄断——中国货币经济两千年（上）》，手不释卷，反复读之；2012年秋，与朱老师在北京初见，诚如沐春风，畅谈复长谈，获赠该书下册，读来受益匪浅。2013年1月，朱老师邀我赴台湾，且留住他在台湾大学的专家公寓，于其课时之外，常受教益。期间，特安排台湾年轻学子在紫藤庐茶楼讲解比特币，这是我第一次了解比特币的概要，以我的货币史学术立场来看，即接受与认可比特币的货币属性及其货币发展之代表性。自此，与朱老师的货币史研讨中便不知不觉地从货币的历史成长延伸到货币发展的未来走向或趋势。于此，十分感念朱嘉明老师，他是我研究数字货币的引路人。

2013年秋，王俊秀兄邀请我参加中国信息经济学会主办的“杨小凯经济思想研讨会”。诚惶诚恐之际，我亦言明对杨氏经济思想既无研究，更无权发言，俊秀兄称无妨，仅主谈金融危机问题即可，是或为我所熟悉。会开下来，与会的阿里研究院梁春晓院长、阿里巴巴集团副总裁高红冰对我的讲解很感兴趣，自此亦有许多话题，我也获邀多次参加阿里研究院的务虚研讨会议，红冰兄更邀我赴杭州参加“小微班”与诸同学分享。时值，余额宝牛刀初试斩获颇丰之际，其热潮拉抬了互联网金融的热潮。由此，我便开始关注并研究网络数字货币。

2013年9月，在北京的一次阿里互联网金融研讨会上，我对于“互联网金融”的概念颇为保留，认为除非货币层面上发生变革，否则难以更新金融名词。当时，还以网络文学做比拟，称没有网络文字的网络文学，终究不是什么新文学。然而，有鉴于“现代货币是账户货币”，虽然货币层面的变革尚未充分展开，但是，账户层面的的确确发生了网络革命，“互联网金融”姑且不失为一种权宜的表达。接下来，我担任了阿里研究院的顾问，有机会广泛地接触网络新经济，参与更多层次的调研，就像是周身透析换血一般，对于数字网络经济有了深刻的体认。这使我更关注数字货币，特别是比特币。

正是对比特币的持续关注与热情，使我有缘结识了韩锋博士。然而，我们两人的来路大不同，我是从货币史、经济史的思路来审视与研讨货币发展及未来走向，并依从网络经济的逻辑推演来分析看待数字货币的，他是从量子物理、数学及区块链技术来解读数字货币的。彼此各说各话了好一阵子，有似庄周梦蝶，抑或是量子纠缠吧。韩兄确是比我睿智，他先听懂了我，而我只是大体上了解到一些他的思路，看来我所理解的经济或金融尚是“粗浅”的，但所幸也是“易通”的。

韩锋兄嘱托我为其主编的新书《区块链——量子财富观》做序，而参与本书写作的张晓玫博士、肖风博士等，也都是我的好师友，实诚惶诚恐。诸位盖以量子信息、麦克斯韦妖、区块链、前沿经济金融研究等高深理论立说与写作，我心虽向往之，然实则只或晓得点儿皮毛，甚或皮毛不见，直是懵懂无知，确不知如何攀续，怎生做得了序？然既受抬爱，亦不揣冒昧，甘为驱驰。原因很简单，我和韩兄一见如故。故此，于此为序，权作为文字上的一次畅聊吧。

### 1. 社会经济财富正向数理环境大规模搬迁

历史地看，社会经济财富大体可以被分成三类：实体性资产、权益性资产和数字资产。实体性资产的英文称作 Tangible Assets，从词义上，不难发

现，这类资产主要发生在物理原子环境下，其发生途径根本而言取决于生产。权益性资产的英文称作 Intangible Assets，词义上直接来看，就是触摸不到的，或者说不是物理环境下的资产，这类资产是权益性的资产，比如证券、版权，以及合同项下所设立的资产等，可以说，权益性资产是法律或制度环境下的资产。数字资产的英文称作 Digital Assets，从词义上看，它是数字化了的资产，就是说，数字本身并不直接成为资产，数据也并不直接等同于资产，而是说，只有在数理环境下那些特定确权化了的数字或数据才是数字资产。而特定确权化，便是数字资产产生的途径或依据。

在农业经济条件下，资本几乎不创造什么社会财富，或者说社会财富不是或不主要是由资本创造的。在工业经济条件下，资本则积极地创造社会财富，或者说社会经济财富主要是由资本所创造的。资本则是制度设定的，它要体现为数量化的货币，并记入到账目中去，从而使财富创造成为一种可在账目上发生的活动，虽然这并不是财富的所有来源，但是，账目上的社会经济财富或者说法律支持下的权益性资产总量上已经超出了实体性资产。这个时期也被称为资本主义阶段，社会经济财富相当程度上等同于资产，而这些资产是可以或已经账目化了的，整个社会经济体系可以是在账目上运行的。社会经济财富大量地资产化、账目化，虽非全部，但几乎全部可以转化为账目资产。当权益性资产成为社会经济体系中的主导部分后，人们依然认为实体性财富得到了前所未有的扩张或增长，而往往忽视了权益性资产事实上获得了更大的增长、更为迅猛的扩张。工业化国家或发达国家的社会经济财富主导部分是权益性资产，只有穷困落后的欠发达国家或农业经济体，其实体性资产才大大超过其有限的权益性资产。这种状况，也常常被表述为金融抑制，亦即资本自由度很低，或者资本本身匮乏。

数字资产既非实体性资产，更非权益性资产，从现实来看，它主要有三种：音乐、图像、数字货币。未来，数字资产无疑从种类来讲更加丰富、总



量也将大大超过权益性资产。举例来说，2000 年悉尼奥运会上第一次采用数码技术来获取体育赛事的影像，而 2016 年的里约奥运会就出现了机器人发稿。这就表明，体育市场的图片或图像已经完全数码化了，数码已经从体育拓展到了新闻传播，而这种拓展几乎是覆盖性的。起初，部分数字资产是从非数字资产转化过来的，之后，数字资产自始便是数码形态的。权益性资产向数字资产的转化，在技术上更加依靠区块链技术，随之出现的是智能合约，等等。

正是从这个意义上说，本书阐释了一条非常鲜明的数码网络新时代的财富发生的途径，值得读者对其仔细品味。

不难发现，实体性资产主要发生在物理原子环境中，而权益性资产则依托于具体的法律制度环境，数字资产则发生在数理环境中。现实的物理环境，是数码网络环境，具体来说，就是相应的账户体系。

既有的账户体系是依托于柜台模式建立起来的，数码网络时代，账户体系的确立可以直接发生在线上，即所谓依托平台而建立。具体来说，实体性资产可以通过铸币或现钞等支付来进行交易；权益性资产只能直接或间接地通过银行账户体系来完成交易；数字资产的交易可以并应当通过网络账户体系来实现交易。这个网络账户体系是接近于数理环境的，是线下所难以或根本无法复制的。

正是从这个意义上说，本书所描绘的网络时代新财富是一个几乎数理环境下财富的再组织、再实现。

## 2. 数理环境下，财富革命依托于账户革命

实体性资产时代，社会经济财富立足于生产活动；权益性资产时代，社会经济财富依托于严密有效的制度保障；数字资产时代，社会经济财富则依托于有效与稳定的经济关系。举例来说，Airbnb（空中食宿）并不依赖生产活动，其商业模式是充分地利用存量铺位，它不依靠房地产的开发量，不依



靠家具、床的生产量，也不依靠严谨、精当、有效的法律合同，以适用于全球的用户，满足全球各地的法律规范要求。它依靠的是有效与稳定的经济关系，这种关系是账户关系，亦即 Airbnb 系统平台上的账户关系。

这种账户关系不仅适用于消费关系，同样适用于投资关系或生产性关系，其所反映出的本质特征是，账户之间的交易关系，或者说相互之间彼此相融的指令关系。至于消费、投资、生产，是账户体系之外的旧经济的解读，从新经济的立场来看，系统内的账户关系是系统所设定的关系模式。这种系统设定的关系模式，是所谓程序决定的，是所谓算法驱动的。

将经济活动映射到一个相对纯粹的数理环境，依托的是数字网络体系。这种将经济关系抽象为可以操控的数理的关系，其实现途径，是将经济关系简化为账户关系，进而将账户关系设定为账户系统的自运行。通信网络技术将账户终端与所有人之间实现了充分的、高效的、全时的联系，这就使得账户使用者越过了“柜台”，通过网络账户“平台”来实现交易。如此，交易便在数字网络环境中发生了“大爆炸”。交易大爆炸意味着账户体系的膨胀，账户关系发生了根本性的变革。这些便是账户革命最为直观的外在表现。

账户革命不仅体现在账户数量、规模、范围、活跃程度等方面，更为主要地体现在账户关系的变革方面。可以说，既有的账户关系的基础是报表关系，报表的基础是科目、账期等。账户关系更为直接地反映了交易关系，体现为合同关系。交易大爆炸，更是交易合同数量、规模与范围的大爆炸。这就是说，账户关系并非单纯的支付关系，更不是什么指令关系，也不需要到相应的报表变动中去找依据，而是更为直接地体现为账户主体间的合同关系。

线下购物狂潮的醒目例证是美国的星期五“血拼”，线上购物的突出例证是“双十一”，两者的共同点是，大量地消耗体能，占据消费者的时间。虽然

线上的“双十一”已经大大超出了线下的星期五“血拼”，但是，网络消费无疑占据了消费者更多的时间，这种状况很快就逼近了消费者的生理承受边界。特别是手机终端大规模、大面积且碎片化地占据人们的时间后，必须努力地将个人从大量的网络交易等活动中解放出来。最为明确的变化在于，账户交易的自动化和智能化。

这就意味着实现账户关系的自动化或智能化，亦即账户体系自身必须得到变革与提升，并非简简单单地将线下转移到线上而已。未来将日益显现出线下账户体系与线上账户体系的区别，其中最为醒目的便是，大量的线上账户体系的自动化和智能化是“标配”。自动化和智能化的交易将极大地提高交易的品质和水平，从而整体提升网络账户体系的交易质量，这就意味着交易合约将更为直接地体现为社会经济财富。

社会经济财富最为活跃的部分是财务意义上的资产，这些资产往往标注在财务报表的科目中。资产证券化使得这些财务资产更为“轻便”，使得资产的财务流转不受具体资产形态的约束。然而，即便充分地实现了资产证券化，报表上的资产依然等同于合同性质的资产。社会经济财富和财务意义上的资产，其价值往往体现在交易流转之中，换言之，体现在合同层面。大量的社会经济财富转变为财务报表上的资产，这已经表明了社会经济的巨大进步，但是，这还远远不够，这些报表上的财务资产不仅需要大规模的证券化，更需要更为彻底的合同化。正是从这个意义上说，金融资产是天然的报表化的财务资产，更是可以充分证券化的，它们甚或“天生”就是合同资产，因此金融资产是最容易交易的。但是，并非所有的资产都适合金融化、证券化。网络数字经济在这个方向取得了长足的进展，简言之，即将大量的资产账户化，且实现了账户交易的自动化和智能化。

账户交易的自动化和智能化，其基础是账户体系交易功能的整体性提升，不仅仅是所谓的交易达成或支付等基础功能，更为根本的是，账户关系是体

系化的、规范化的，是程序约束下的，其基础技术是区块链技术，这是确保账户交易真实、完整、有效与不可更改的保障。账户体系的技术基础得以确保，智能合约才会得到普遍的应用，而恰恰是智能合约等将成为账户项下资产的主要形态。

正是从这个意义上说，区块链是社会新经济财富的密码。我想，几位作者的精彩论述更能使读者走进财富新世界，揭开谜团。

### 3. 关于金融中介

序者浅见，旧金融依托中介，新金融摆脱中介。这个部分尚需与作者多商榷。

金融中介的逻辑基础是，信息、技术等方面存在差距，所以，需要更具信息或技术能力的经纪人来完成中介活动。众所周知，区块链技术是以“去中心化”为指向的，那么，在交易双方中嵌入的中介就是“中心”，而区块链技术去中心化的本质是“去中介化”。在金融领域，最大的中介经纪人就是商业银行体系，银行账户体系几乎是一切金融交易活动的账户基础。银行的运营是中心化的，商业银行体系自身也是中心化的，中央银行往往就是商业银行体系的中心所在。既然区块链去中心化与去中介化是一而二，二而一的事情，那么，我们就难以用中介化的旧金融逻辑来解释去中介化的新金融。

在其他领域，学者们往往用“多中心化”来“去中心化”，但是，在金融或经济领域，这样的提法就有问题。事实上，回归到“中介”，更有助于说明与解释问题，而不是制造出更多的问题。

区块链技术所支持的账户体系，将更为有力地操控资产或社会经济财富，然而，这里究竟是否为中介者提供了空间？这是一个根本性的问题，换言之，旧金融体系下的中介者是否能够在新金融体系中依然占据“中心化”的位置，并事实上操控一系列的账户资产呢？对此，序者持否定之立场与态度。在旧金融或旧经济环境中，集中交易或中介交易是有效的，甚

或是必需的，但是在新金融或新经济环境下，这几乎是无效的，甚或是有害的。区块链技术正是从根本上排斥之，换言之，新财富的“密码”与中心或中介之类不兼容。

区块链技术是数字网络技术不断快速发展所达到的一个新阶段，它自身不仅在应用中会面临各种机遇与挑战，而且这一技术亦将不断地提升与拓展。正是从这个意义上，几位作者通过本书所展现给读者的是一幅变化中的关乎未来财富的美妙图景，帮助我们打开视界。

周子衡

## 序二

量子力学自从创建以来，关于其基本诠释的争论一直存在。持续时间最长和影响最广泛的当属阿尔伯特·爱因斯坦（Albert Einstein）关于“量子力学是不完备的”的评价。他反对量子力学中态的非定域性，即主张相距类空距离的两个态不能有纠缠，并主张物理的可观测量必须是“真实”的，即具有确定的值，不应该是一个分布。尼尔斯·玻尔（Niels Bohr）在具体的事例上给予了反驳。爱因斯坦的挑战实际上是一个建立“定域并真实”（local and realistic）的理论的号召。长期以来，许多物理学工作者响应号召进行了这方面的努力，但没有成功。直到1961年约翰·贝尔（John Bell）提出了定理，证明要用“定域并真实”的理论获得关于物理现象的预言与量子力学的结果完全一致是不可能的。这个定理通过一系列不等式表达。“定域并真实”的理论对于一个特定的物理过程都会给出一些不等式，而量子力学会突破这些不等式。一系列的实验结果以越来越精确的结果表明，“定域并真实”的理论不能重现量子力学的结果，而这些结果在物理学的很多领域都经过实践的检验。反对者从多方面对这些验证不等式的实验提出存在漏洞。直到最近才出现了“不存在漏洞”的实验，为争论“关上了大门”。对于量子力学诠释的争论，理查德·费曼（Richard Feynman）说过：“在理解量子力学所代表的世界观方面，我们曾经有过很大的困难。每出现一个新的概念，都要经过一两代人才会让大家都认为它是没有问题的。”

在争论的同时，量子力学在物理学各方面的应用高歌猛进，不仅在基础科学方面有很多创造，而且在核能、电子学、计算机、激光等多方面改变了人类的生活。在量子力学发展的早期，它对分子结构、化学反应、高

分子结构等方面的理解对于化学做出了贡献，“量子化学”早已形成了学科。近年来由费曼提出的量子模拟在量子通信和量子计算方面开辟了一片新天地，它的基础在于量子力学的非定域性和量子纠缠。这个新方向的发展同时也促进了量子力学基础的进展。量子力学对生物学的重要性也日益受到关注。

最初量子力学被认为适用于微观体系。20 世纪中期发展起来的超导和超流已经属于宏观体系了。对于生命科学的应用已经很显然了。但在 21 世纪居然把它用到了金融学中。对此，我没有学习，不敢妄加评论。读了《区块链——量子财富观》一书的前言，我认为这个方向是应该热情欢迎的，当然应该用严格的科学态度去对待它。我期待量子的概念在新的领域中开花结果，对人民生活的提高做出贡献。

张礼

## 前 言

本书是和我在清华大学的导师张礼先生、西南财经大学的张晓玫教授和中国社会科学院金融研究所副研究员、阿里研究院学术委员会成员周子衡先生多次讨论后成篇的。

信用生产的历史，几乎可以覆盖金融发展的历史。而每一次金融技术的革命，都会导致信用生产成本的大幅下降。在本书的上篇“区块链的价值：金融中介发展的视角”，张晓玫教授等用大量翔实的史据，充分地论证了以上观点，进而自然而然地得到了结论：区块链，是互联网时代，通过大数据产生更低成本信用的一种终局性技术解决方案。

为什么互联网新经济就一定需要产生低成本的信用呢？在和周子衡副研究员数次的讨论中这个问题渐渐清晰了起来。按照周子衡的新经济理论，交易速度正在超越生产速度，经过我们的反复讨论，终于厘清了超越生产的那一部分交易的真实经济意义：它会自发地转化成一种投资行为。就像现在的共享经济，以 Uber（优步）为例，本来买辆车是一种典型的消费行为，但是由于交易成本太低、太便捷，进而使这辆车的部分空余时间都可以拿到市场上销售，这多出来的交易行为，实际上可以把原来的消费行为，部分地转化成一种投资行为。

当然，这显然现在还是凤毛麟角的个案。在目前互联网已经呈现交易大爆炸的局面下，为什么这种把交易转化成投资的做法没有成为普遍的现象？这就是本书中篇要讨论的问题。

本书中篇第 5.6 节论述了：用区块链把“剁手党”的手接起来。其中的逻辑就是要通过区块链技术，让网络大数据确权，让传统的柜台账户，不仅



进化为中心化的网络账户，更要升级到去中心化的区块链账户，才能产生大量低成本的信用资源，才能更普遍地让互联网上的交易行为转化成投资行为。

根据秘鲁总统的经济顾问赫尔南多·德·萨托（Hernando De Sato）的那本著名的《资本的秘密》（The Mystery of Capital）中的观点：第三世界国家为什么穷？不是传说中的发达国家总是在剥削掠夺他们，更根本的原因是第三世界国家缺乏发达国家那一套对私人资产的确权和保障的法律和制度体系，从而无法形成健全的资本市场，整个社会缺乏创造财富的功能。

本书中篇用麦克斯韦妖的理论证明了，一个去中心化分布式的麦克斯韦妖系统，才能最有效地保持系统的低熵，从而达到不断创造价值和财富的基本条件。而对私人资产的确权和保障，才能让消费者和投资人，成为一个正常的麦克斯韦妖，才能按照市场基础协议有充分选择的自由，才能充分保障市场不断繁荣和创造财富。

耶鲁大学的陈志武教授多次撰写文章说明：美国人民的财富，主要来自健全和发达的资本市场。尼尔·弗格森（Niall Ferguson）在他那本著名的《货币崛起》（The Ascent of Money）中更是有具体的说明：如果在1964年投入一笔钱到美国股市，则其造富功能保证到2007年该资产能升值70倍。但是如果只是投资国债，那该笔资产只能升值12倍，刚刚跑过通货膨胀。

对于我们中国人，印象最深刻的例子是30年前我们几乎没有房地产的确权，当时基本都是单位分房。现在我们只做到了对房地产的部分确权，即所谓70年使用权，但是房地产市场给我们带来的财富，已经让很多中国家庭的经济状况有了天翻地覆的变化。

所以金融史上，任何一次资产的确权，都很有可能形成一次新的造富运动。

那么如何对我们每个人在互联网上的大数据进行确权呢？

本书中篇中肖风博士对这一前景有精彩的描述：“传统的依靠土地、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，会数十倍于物理原子世界。”

我的朋友龚鸣（网名：暴走恭亲王）在本书的中篇中具体地分析了 ICO（数字资产发行），让开源软件运动有了新的造富功能。我们具体地给出了以太坊的发展过程。

在这一场全球新财富运动中，我们更加关注中国社区发挥的至关重要的作用，对一些关键性事件进行了综述。

大量的事实说明：思想的变现是创新最大的动力。而区块链能够为互联网上的大数据确权，同时也为思想的确权、创意的确权、关系的确权，创设完美的技术前提。

作为本书主编之一，我跟随清华大学的导师张礼先生，学习了将近 20 年量子力学，特别是反复研读张礼先生的名著《量子力学的前沿问题》<sup>①</sup>，让人终生受益的是终于建立起一套自洽的量子世界观。

本书下篇通过量子本体论，说明了量子科学的发展已经严格地证明：我们看见的原子世界只是宇宙的一部分，其中存在大量“看不见”的非定域关联和纠缠，也是物质存在的另一部分。这让两千年前的东方“有无相生”的太极智慧，有了科学的依据和数理描述的方法。

这对于我们数字资产财富观的启示，《经济日报》的记者黄芳芳，有一段精彩的论述：“从量子力学的角度看，我们眼见的实物只是世界的一部分，背后隐藏着错综复杂又符合逻辑的纠缠关系，这其实也是资产的一部分，需要数理环境加以描述。”

其实，创意关系、信息、人情、声誉，这些都是经济活动中极为重要的

---

① 张礼，葛墨林．量子力学的前沿问题 [M]．北京：清华大学出版社，2000．