O'REILLY®

万向区块链实验室丛书

区块链

新经济蓝图及导读

Blockchain

新星出版社 NEW STAR PRESS

[美] 梅兰妮·斯万 著

万向区块链实验室丛书

区块链：新经济蓝图及导读

[美] 梅兰妮·斯万 著

新星出版社 NEW STAR PRESS

图书在版编目（CIP）数据

区块链：新经济蓝图及导读／（美）斯万著；韩锋主编．—北京：新星出版社，2016.1

ISBN 978-7-5133-1972-0

Ⅰ.①区… Ⅱ.①斯… ②韩… Ⅲ.①电子商务－支付方式－研究 Ⅳ.①F713.36

中国版本图书馆CIP数据核字（2015）第281748号

区块链：新经济蓝图及导读

[美] 梅兰妮·斯万 著

责任编辑：汪　欣
责任印制：李珊珊
封面设计：Ellie Volckhausen　张健

出版发行：新星出版社
出 版 人：谢　刚
社　　址：北京市西城区车公庄大街丙3号楼　100044
网　　址：www.newstarpress.com
电　　话：010-88310888
传　　真：010-65270449
法律顾问：北京市大成律师事务所

读者服务：010-88310811　service@newstarpress.com
邮购地址：北京市西城区车公庄大街丙3号楼　100044

印　　刷：北京盛源印刷有限公司
开　　本：787mm×1092mm　1/16
印　　张：17
字　　数：140千字
版　　次：2016年1月第一版　2016年1月第一次印刷
书　　号：ISBN 978-7-5133-1972-0
定　　价：50.00元

翻译及导读： 龚　鸣　初夏虎　陶荣祺　达鸿飞
曾林钏　张凯悦

特约导读： 沙　钱　罗　佳　吴志峰

审　　校： 孙　铭　李　戈　陈　峤

主　　编： 韩　锋

特约编辑： 刘　刚

出版说明

感谢清华大学的顾学雍教授向我推荐了Melanie Swan的这本《区块链：新经济蓝图及导读》。我和龚鸣（暴走恭亲王）、陶荣祺、达鸿飞、顾颖（初夏虎）、孙铭（高素质蓝领）、曾林钏、张凯悦一拍即合，认为这本书提供了现在全球区块链产业从理念到创业比较全面的叙述，决定一起翻译并导读这本书。其中暴走兄贡献最大，翻译了其中第二、三、四、七章并导读第三、四、七章，初夏虎翻译了第一、六章，曾林钏和张凯悦翻译了前言和附录，陶荣祺翻译了第五章并导读，达鸿飞导读第二章，初夏虎、高素质蓝领、陶荣祺、张凯悦和李戈做了出色的审校工作，后来沙钱、罗佳总和吴志峰博士也参与了导读工作，中国万向控股副董事长肖风写了序，阿里巴巴副总裁高红冰和我对话形成了前言总导读，我后来又在译后注上补充了《区块链的人工智能》，孙铭、蒋海分别写了跋一、跋二，李戈制作了《中国区块链创业项目一览表》。

感谢以上各位参与者和一直关注支持本书出版的每一位朋友，希望本书可以给广大中国区块链爱好和创业者以思想的启迪和创业的帮助。

感谢万向区块链实验室把本书列为“万向区块链从书”第一本，并大力支持本书的出版工作。

主编　韩锋

目录

序

区块链——互联网金融的终局

肖风

近期的《福布斯》杂志中文网上有一篇文章说道：没听过区块链？你可能对互联网金融知之有限！

这可绝对不是标题党的作为。在互联网金融几乎家喻户晓的中国，关于世上是否真有互联网金融的争论，居然还能像沉渣一样时不时地泛起，也难怪有人要作此提醒了。其实，我们在中国看到的任何互联网金融的技术或商业模式雏形，都发源于欧美，无一例外！只是他们不叫互联网金融，叫FinTech——金融科技！ 如果美国驻华大使给你一张中文姓名的名片，你可千万不要按中文拼音去美国查人！在FinTech中，目前最热闹的就是区块链技术了。据报道，全球主要的金融机构甚至纳斯达克交易所，已经或马上要建立区块链实验室，以试验区块链技术在各种金融场景中的应用。花旗银行甚至在内部发行了自己的数字货币“花旗币”。瑞士联合银行（UBS）在区块链上试验了二十多项金融应用，包括金融交易、支付结算和发行智能债券，等等。

有人预言十年之后互联网金融会消失，因为届时互联网金融如同互联网一样已经融入世界，万物互联，化为无形。我一直在想象，那个时候的互联网金融会是怎样呢？《区块链：新经济蓝图及导读》这本书也许可以

帮助我们更好地找到答案。

我们都知道，信任是世界上任何价值物转移、交易、存储和支付的基础，缺失信任，人类将无法完成任何价值交换。最初人们靠血缘和宗族来建立信任，接着人们靠宗教和道德来建立信任，后来人们靠法律和组织来建立信任，否则人类社会无法完成越来越多的各种各样的价值转移和交换。随着人类社会越来越数字化，随着互联网由传递信息、消除信息不对称的信息互联网向传递价值、降低价值交换成本的价值互联网进化，人们开始尝试通过数学算法来建立交易双方的信任关系，使得弱关系可以依靠算法建立强连接，从而去促成人类有史以来如不依靠互联网技术，几乎不可能完成的价值交换活动，包括甚至更主要的是金融交换活动。

区块链本质上就是交易各方信任机制建设的一个完美的数学解决方案，而比特币就是区块链技术的第一个伟大的应用。区块链技术原理来源于一个数学问题：拜占庭将军问题。该问题的背景是，在东罗马帝国时期，几个只能靠信使来传递信息的围攻城堡的联盟将军，如何防止不会被其中的叛徒欺骗、迷惑从而做出错误的决策。数学家设计了一套算法，让将军们在接到上一位将军的信息之后，加上自己的签名再转给除发给自己信息之外的其他将军，在这样的信息连环周转中，让将军们得以在不找出叛徒（找叛徒将是成本最高、效率最低的解决办法）的情况下达成共识，从而能保证得到的信息和做出的决策是正确的。

区块链的基本结构也是这样的。人们把一段时间内的信息，包括数据或代码打包成一个区块，盖上时间戳，与上一个区块衔接在一起，每下一个区块的页首都包含了上一个区块的索引（哈希值），然后再在页中写入新的信息，从而形成新的区块，首尾相连，最终形成了区块链。到2015年8月29日，比特币区块链上共有372016个区块，总数据容量40GB，算力400PFLOPS（也就是每秒400千万亿次浮点计算），目前我国的天河二号超级计算机的算力也只有33PFLOPS。区块链技术一是用纯数学方法来建立各方的信任关系，二是交易各方信任关系的建立完全不需要借助第三

方，三是建立信任关系的成本几乎降到了零。这也正是我所预言的区块链将帮助达成互联网金融的终极模式的核心所在。

以区块链为基础，再加以一系列建立在区块链上的辅助方法，人们正在互联网上建立一整套互联网治理机制。包括：（1）工作量证明机制（要篡改区块链上的数据，需要拥有超过全网51%的算力，这使得作伪的成本会高于预期获得的利益）；（2）互联网共识机制（以共识来确保正确，而无须甄别好坏）；（3）智能合约机制（以程序代替合同，约定的条件一旦达成，网络自动执行合约。金融活动由交换数据变为交换代码）；（4）互联网透明机制（账号全网公开而户名匿藏，交易不可逆转且交易由第三方“矿工”记账）；（5）社交网络的互动评分机制（这使得专车司机的笑脸能换来利益而出租车司机的笑脸却不能）；（6）密码学特别是公钥密码等这些互联网治理机制正在给经典的经济学、金融学、管理学甚至社会学带来巨大的冲击。理论结构、公司结构、金融结构甚至社会结构都面临解构与重构的命题。

区块链是互联网金融的底层技术架构。只有区块链技术的成熟，才能带来互联网金融的成熟。这是因为：

它是数字世界里一切价值物的公共总账本。任何数字资产的认证、记录、登记、注册、存储、交易、支付、流通，一个账本统统解决。

它是去中心化的大数据系统。记录、传递、存储、分析、应用，一应俱有。

它是分布式的云计算网络，没有中心服务器。仅比特币区块链已经拥有400PFLOPS的计算能力，而这个计算能力是由全球接入比特币系统的无数台计算机免费提供的。

它是未来去中心化组织结构的基础架构。

它是互联网治理机制的底层协议。前述的互联网治理机制，大部分建立在区块链上。

站在区块链之上，遥想互联网金融的未来，我认为它会有如下几个

特点。

它是智能化的。金融交换载体由数据变为了代码，传统金融成为可编程的智能金融。

它是去中心化的组织结构。点对点、端到端、P2P。

它是算法驱动的金融，摩擦系数接近于零。

它是一体化的系统，身份识别、资产登记、交易交换、支付结算都在区块链一个系统上一账打通。

它是实时化、场景化、7X24小时、现实世界与虚拟世界、物理世界与数字世界无缝衔接的金融体系。

韩锋博士和数字货币界（尤其是对数字货币2.0有研究）的几个同仁，计划翻译出版《区块链：新经济蓝图及导读》一书。为让更多的人能够了解区块链的意义，他们结合中国经验为每一章节都写了导读，拳拳之心可鉴！正值我在上海紧锣密鼓地筹备创立区块链实验室，以在中国推广区块链技术。目前中国的区块链圈子并不大，很快我们就见上面了。双方相谈甚欢，相见恨晚。当场达成以这本书为起点，以区块链实验室为支撑，未来几年出版一套区块链实验室丛书的计划。一方面借以推广这项在中国还比较陌生但未来也许会扮演终结者角色的区块链技术；另一方面也想在这可能改变历史的关键时刻，能够留下一系列的文字记录，以见证这伟大的变迁。

让我们翘首以待在区块链上浴火重生的更普惠、更智能、更实时、更跨界的未来金融！

肖风，博士，万向区块链实验室发起人，中国万向控股有限公司副董事长兼执行董事、民生人寿保险股份有限公司副董事长、万向信托有限公司董事长、民生通惠资产管理有限公司董事长，通联数据股份公司董事长、通联支付网络服务有限公司董事长。肖风博士拥有超过20年的证券从业经历和资产管理经验，其创建的博时基金公司，是目前中国资产管理规模最大的基金公司之一。

关于区块链认知的对话

高红冰　韩锋

以下对话中：

“高”代指阿里巴巴集团副总裁、研究院院长 高红冰

“韩”代指清华大学博士生、I-Center导师 韩锋

地点：阿里巴巴研究院

高：关于“区块链”的认知，我们在微信群里已经有很多交流，但是不系统。

关于“区块链”，我需要向你学习，需要同你讨论并进一步求证几个问题。第一，当我们谈论到“区块链”（blockchain）时,这个概念应当如何翻译？我也把这个话题发在了群里，有许多人进行了回应。第二，“区块”这个词的意思，你拆开来理解“区”和“块”，很简单。如果是对“区块链”已经有所认知的人，反过来看这个词语时，会觉得“区块”的确较好地保留了“blockchain”这个单词的意思。但是，对于不熟悉“区块链”的人，会认为这个词很生僻。第三，朋友圈中回应的人提到，刚刚把 “移动互联网”搞清楚，突然又冒出了“区块链”，认为技术与时代变革很快。但是，严格来讲，这说明人们对于“区块链”这个概念的认识

还很模糊，“区块链”的界定需要进一步探讨，“区块链”的应用场景还需要开发和梳理。

韩：其实互联网当时也是从好几个词组合过来的。

高：对，互联网（internet）这个词当年存在多种解读。比如，当时翻译成“因特网”，在政府文件中广泛使用这个概念。即使到了今天，争论仍然在进行之中，主要是由于互联网技术在不断升级演进，人们对于互联网的本质，存在各种讨论和争论，甚至延伸到“互联网思维”的讨论。当年，甚至有人认为，internet＝inter+net。台湾翻译成“网际网”。但是，今天来看，互联网真正革命性的起点，始于1973年发明的TCP/IP协议。

韩：我一直坚信互联网是全人类的基础协议。TCP/IP协议其实极其简单，妙就妙在这里。它用简单的代码协议解决全人类都不能解决的问题。我们俩传递信息怎么能保证是信道可靠？如果没有这些基础协议，我们会变得很困扰。在过去，传递信息首先会受到“中心控制”的制度限制，其次还有地域、物理上的限制以及成本的限制，而这些限制现在被打破了。

“区块链”正是这个基础协议的升级。我们依靠第一代互联网保证信息传输没有问题了，但是你给我的信息是否是真实的？这一点我没法证明。所以互联网一度让人认为上面的信息都是假的，作假太容易。即使现在也是这样。这样一来，想解决这个问题，计算机就需要克服“拜占庭将军”问题。假设一群将军互不信任，其中一定有坏人，但只要保证坏人不大于将军的三分之一，计算机就存在一个算法，能保证将军们达成的共识是真实的。

“比特币”和“区块链”尝试解决的是重复支付的问题。按理说如果每个电子货币都不依靠中心，让人感觉防止重复支付是无解的。谁都会想作假，去蒙骗别人来占便宜。而“比特币”就是依靠一种机制，即全网记账。我研究量子信息，从这个角度看比特币机制是压缩虚假信息，依靠挖矿的能量付出，来压缩和筛选出可能的重复支付交易信息。我在清华一次课上讲到这个问题（请参看本书译后注：“区块链的人工智能”），其实

这就是一种类似量子计算的分布式人工智能。

中本聪写的“比特币”的基础协议很简单，协议就是盖时间戳，全体矿工一起记账，一起公证，而不是相信一个人，每十分钟确认一次，这就形成记录了全网这十分钟所有正确（没有重复支付）的一个账本数据库“block”，我们称之为“区块”。如果大家都一致，达成共识，叫作共识机制，那么大家就承认这个区块上的信息是真的，原则上不可篡改（修改按协议需要控制全球挖矿记账51%以上的算力），然后每个合法的区块连成一个个链条，就是区块链，形成一个分布式共识数据库，未来会成为全人类真实信息的共同来源。这个机制的熵压缩非常大，把你可能做的假账和欺诈的混乱都筛除掉了。

最近，我和德勤的一位亚太合伙人在写一篇文章。德勤正在准备大量使用“区块链”。“区块链”对于德勤这样做审计的事务所来说太有用了。原来最头疼的就是被审计的公司做假账怎么办？如果被查出来，负责审计的单位是要承担责任的。所以，为了严防假账，他们需要耗费大量的人力物力。一般来说，使用“区块链”，这个问题就可以很好地获得解决。全球数万用户、德勤和监管机构共识记账，可以追溯，不可更改，记账都是盖了时间戳的。这样审计成本一下子就下降了。现在才刚开始使用“区块链”，据说成本就下降了好几亿美元，所以未来德勤绝对会花很大力气做这件事，毕竟他们每年审计收益是三百多亿美金。德勤如果参与到区块链技术中来，情况就绝对不一样了。

高：这就叫作数据化会计？

韩：对，信用成本下降，而且是全球化的，解决了原来最头疼的问题。“区块链”远不止用于金融、财务、审计，还可以用于其他更多的领域。比如，最近在讨论智能化城市。泸州市科委来探讨的就是当地特产的可回溯性。任何品牌特产，都是因为造假的人而导致市场被破坏。怎么做到可回溯？如果区块链和物联网结合，从产地就开始全网公证，那作假成本就非常高了。就好像比特币系统，做假币需要几个亿的成本，让作假跟

你盗取的利益相比不成比例！

高：明白。我在想，对于“区块链”的认知，在还没有大量应用场景的初级阶段，如果没有充分的好奇心，一般人是听不下去的。在“区块链”面前，当人们一旦把自己归类到从事某一个行业或者学科领域研究，对“区块链”的认知就会止步。

这些问题，似乎回到了“元问题”的讨论，就是所谓的不可测量，进而带来了不可测的定义。如果我们只是在概念上进行定义，本身是没有多大意义的。如果没有实际的测量作支撑，那么定义就会有争论。这就成了一个“是非问题”，而不是一个“真相问题”。是非的问题就是你认为你有自己的体系，他则坚持自己的体系，两个体系放在一起，是不可验证的，所以测量共识本身是很重要的。

那么为什么会有不可测量？我举个例子。人的神经系统是不可测量的。或者说，人死了，那口气没了，这里的“气”是不可测量的。它没有重量，甚至没有电波。这个不可测量的背后，却是人体的不同生物系统连接在一起时，共同产生了神经功能系统。不可测量，那么你只能说相信，或者靠着感知、经验去抓住某个东西，但这不是大众能够抓得到的。那些气功大师、做针灸的、号脉的人，我相信是有这种功夫的，但这不是大家抓得住的。

这就是我们今天说的区块链以及你说的智能这个概念，尤其是智能，其背后存在着一种“计算+数据+算法+存储”的逻辑。那么，不可测量也就是刚才我们讲的量子论的结果。

韩：我也思考了很多，不可测量含义是什么？我是这么看的。你如果站在牛顿的世界观，那是不可测量的。因为牛顿，包括爱因斯坦认为，世间万物都是定域决定性的，存在都是准确的时间和地点。这是牛顿建立他的整个世界体系的出发点。但是到了量子力学，不是这样了。万物不存在固定的时间和地点，它本质是非定域性的，事物它看得见的粒子部分和看不见波的部分是同时出现和互相转化的（量子力学中的Englert–Greenberg

关系）。所以我们突然发现世界至少有一部分是不可（定域）测量的。

但是这一点是否真的不可以接受呢？事实上从整个人类文明的历史看，我们的先哲很早就发现了万物非定域的本质。老子最早就谈“有”和“无”，而且老子的“无”是在“有”之前，他说：“有生于无”[①]。这样高的智慧，人类后来反而丢了。整个现代科学体系是建立在希腊的原子论体系之上。原子论最早认为，一切物体是定域原子构成的，剩余的就只有“虚空”了，两者机械的结合构成我们整个宇宙[②]。但是老子在两千多年前就以他的智慧提出，他的世界观是“有生于无”。就是说我们的世界很大部分是你看不见的，但是不代表说什么都没有，现在量子力学称之为“波函数”或者叫“场”。

在知道无法精确“定域”测量后我们怎么办？其实现在互联网已经回答了，就是“大数据”。没有大数据的话绝对没法描述非定域整体关联。因为在那一部分你还看不见的世界中没有定域因果性，你只有几个数说明不了问题，就只能说它是随机的，找不到规律。但有了大数据以后就不一样了。关联、纠缠等现象全部都发现了。所以现在一切都在走向数据化，没有数据，那就只能说无测量了。

高：我觉得有几个认知，我们回过头来再确认一下。一个是我们对世界的认知和理解，放在牛顿力学或者普通化学层面去理解，先不要升级到量子层面，到了量子论这个层面就很哲学了。测量时，有测量者、被测量者、观察者等多个角色。其实，人一直是我们这个世界既有的观察者，但是，我们常常会忘记这个前提。你刚才说的老子说了很多，是以他当时既有的经验和知识进行的测量、感知或想象。人，是一个观察者。作为一个观察者的人，今天只能“看到”这么多东西，看不到更多未来能够“看到”的东西。比如，未来，“大数据+算法”产生的人类群体智能，可能

① 老子：《道德经》。

②阎康年：《自然科学史研究》1983 年第 2 卷第 2 期，第 183–192 页。

会帮助人“看到”更多的东西。

现在有很多的工具，但借助这些工具去观察的时候，观察本身就发生变化了。你看到结果的发生。比如说我们测量ph值，我们把ph试液倒在被测试的杯子里，变成红色或紫色，我们借此来判断ph值的多少。这是肉眼可观察的。就是说你只要把酸加进去，你就能看到结果。这就验证了。这个验证一定是带有你作为人的肉眼的尺度这个量级去看。如果我们换成一个人类肉眼看不到的微观层级，那颜色这个维度就不存在了。

韩：你在进行这种观测的时候，其实已经划定了一种范围。

高：对，划定的范围就是人本身。认识，被人类自身的观察能力所决定。所以有些观察者，或者说佛道比较高的人，能够看到人的灵魂。当然他对灵魂的定义可能和普通人的定义不一样。他能看到的跟我们看到的也不一样。有些人就是有“特异功能”，这一点是没有办法的。他就是在某些方面比一般人强。有些人腿脚厉害，就是比别人跑得快，而有的人可能天生缺少某个器官，诸如此类。总之，存在观察者角度的问题，而这一点，往往被我们忽略。这个本身是有问题的，人类要认知到这一点。现在，我们再看“区块链”、人工智能，也是一样的。过去，以日常生活的观察尺度去看，我们都不会怀疑。但跨出这个尺度以后，我们就产生各种怀疑。

再回过头来看，我们对今天经济运行的计量、统计、观察或者宏观调控，实际上是基于现在人们对于经济的认识。

韩：我印象很深的，马云说过一句话：“现在公开的数据有真实的么”？

高：如果继续这么问下去的话，就成了不可知论了。我们就必须划一条线。在我们讨论问题的时候，当你把视线朝着粒子更小的世界去看，或者朝向地球之外更大的尺度去看，已经远远超出了现在人类的观察能力。我们如果想观察粒子、量子，就必须用一个质子去轰击它，否则就“看不到”。这是测量工具的问题，肉眼看不到也是因为肉眼是靠光。