区块链书系

维京资本 VIKING CAPITAL

甲子光年 JAZZYEAR

BLOCKCHAIN

区块链行业词典

维京资本 甲子光年 编

机械工业出版社 CHINA MACHINE PRESS

区块链书系

维京资本 VIKING CAPITAL

甲子光年 JAZZYEAR

BLOCKCHAIN

区块链行业词典

维京资本 甲子光年 编

机械工业出版社 CHINA MACHINE PRESS

本书是一本专门介绍区块链行业相关概念的词典。维京资本与甲子光年系统地梳理了区块链领域的多个概念，涵盖基本定义、区块链基础技术、数字货币和法律监管等多个方面。所有区块链行业的参与者和关注者都亟需这样一份详实、客观的工具。因为长远来看，在跌宕起伏的加密数字货币行情背后，区块链技术本身才是浪潮里的坚实陆地，是未来可以承载巨大变革的基础。但许多行业参与者和关注者仍对区块链技术的基本概念认知不足，在讨论热火朝天之际，参与者对某些基本词语的定义仍未达成共识，导致交流效率低下，信息混乱。更深远的问题是，当下区块链技术获得了超出技术本身的关注，并被赋予了对立的情绪，有人极力赞美，有人大加抨击。区块链技术已到了被污名化的边缘，它需要被正名，才能更健康、长足地发展。

所有希望了解区块链以及区块链行业的相关人士都是本书的目标读者。

图书在版编目（CIP）数据

区块链行业词典 / 维京资本，甲子光年编 . —北京：机械工业出版社，2018.7
（区块链书系）
ISBN 978-7-111-60636-9

Ⅰ .①区… Ⅱ .①维… ②甲… Ⅲ .①电子商务 – 支付方式 – 基本知识 Ⅳ .① F713.361.3

中国版本图书馆 CIP 数据核字 (2018) 第 181252 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：顾 谦 责任编辑：顾 谦 任 鑫 翟天睿
责任校对：黄兴伟 封面设计：马精明 责任印制：张 博
北京华创印务有限公司印刷
2018 年 9 月第 1 版第 1 次印刷
145mm × 210mm · 6 印张 · 2 插页 · 148 千字
标准书号：ISBN 978-7-111-60636-9
定价：45.00 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	金 书 网 ： www.golden-book.com
封面无防伪标均为盗版	教育服务网 ： www.cmpedu.com

编 委 会

主 编

金健将 张一甲

参 编

曾元佐 何思谊 程曼琪 涂靖靖 邓璐

顾问委员会

清华大学学生区块链协会、NEO GLOBAL CAPITAL、万向区块链实验室、云象区块链、思否区块链、鲸准研究院、哈希世界、博聚科技、分布科技、边界智能、非小号、Roark Fund、远望资本、八维资本、王逵、曹恒、张宇文、田甲、李岩、俞之贝、神鱼、成也、闫莺、田鸿飞、钟文斌、高阳、杨文涛、Sampson Chen、JC Xu、Alan Yan

推 荐 序

《区块链行业词典》经过精心准备和反复雕琢，现在正式与大家见面了。作为区块链领域的专业人士，我为这部词典的发布感到由衷的高兴和振奋。

大抵一个专业领域需要词典的时候，正是这个专业领域的秩序由粗放自由转向精细规范的时候，更是这个领域的基础概念体系从发散走向收敛、从争鸣走向共识的时候。我国古人常说“名正言顺”“师出有名”，意在强调基础概念体系的推广和正确使用不仅具有重要的学术意义，更具有重要的社会意义。在学术技术的前沿，大家尽可以继续争鸣下去，但基础概念体系趋于共识是好事，地基稳了才好建高楼大厦。从《区块链行业词典》初稿在业界的反响来看，区块链无疑是进入了这样一个具有良性发展特征的通道。这对区块链行业从业者来说是令人鼓舞的。

区块链是一项年轻的技术。它首先是数据的一种组织方式，把代表历史、当下和未来的数据用时间不可逆的方式无缝地、可公开验证地勾稽在一起，任何一个局部数据的改变都会导致全局数据的不相容，因此可用来进行存证。区块链进一步又引入了集体见证的共识机制来达成数据的一致性和不可透支、不可双花等重要特性，保证了价值的守恒性，因此可以用来在数字化的世界里进行点对点的价值传输。区块链进一步把可编程性赋予价值，使得价值可以随着外部事件的发生和内在业务逻辑的展开而实现再分配，从而使区块链承载的信任服务与社会经济活动实现广泛的对接。

区块链技术还在发展中，性能、隐私、跨链等各方面都有待新的突破。区块链应用也在拓展中，不仅金融领域出现了落地场景，非金融领域特别是实体经济中也出现了越来越多的落地场景。基于规则的中介服务、信任服务的自动化、无人化，是区块链的精神实质。面对这样一种具有改变业态潜质的新兴技术，更多的人需要关注，更多的人需要学习，更多的人需要默默做好就业乃至创业的准备。《区块链行业词典》这样的工具书，恰好可以满足人们快速精准了解区块链技术和区块链应用的需求。

区块链又有许多不同于其他领域的特点。它诞生自民间极客之手，其源头可以追溯到密码学、分布式系统、对等网络和博弈论，是处在信息技术、数学算法和金融应用交叉地带的“混搭”产物。

也就是说，一方面，区块链从自己的邻近学科、源头学科那里汲取了很多营养，借鉴了很多概念和术语，具有了区块链技术语汇高度跨界的特点。对于读者，可以各取所需，按需查阅，管窥自己尚不熟悉的邻近学科领域中一些既有趣又有用的概念。但对于编纂者来说，编写这样一部高度跨界的词典，对自身的知识结构和对区块链概念体系的全局驾驭能力是一个不小的挑战。《区块链行业词典》的编纂者迎难而上，敢为天下先，其勇气和定力值得称赞，也值得后来者学习。

另一方面，区块链技术的飞速发展，使得在这一技术领域内工作的人们对邻近学科、源头学科的概念术语采取了一种拿来主义的实用态度，而较少顾及区块链领域，这些概念术语很可能在内涵和外延上都已经与原来有所不同。这也导致了从邻近学科、源头学科来看，区块链专业人士的某些用语或许显得不那么严谨。例如，叫币的不一定是真的币、叫合同的不一定是真的合同等。对一些在邻近学科、源头学科中有定论的命题，在区块链领域可能还有重新讨论的必要；对一些在区块链领域里得出的结论到底是古已有之，还是新的发明、新的提法有可能莫衷一是。在这样一个

交叉领域，发生这种情况是再正常不过的了。但是，实践在前行，应用在推展。为了实践和应用，不能等到学者们把头发争论白了再编写词典，而必须抓紧当下，服务当下。《区块链行业词典》立项的果断和推出的及时，都很好地印证了这一点。邻近学科、源头学科与新兴交叉学科的边界未来是什么样，其中的一些概念和术语未来会如何相互影响又保持一定的独立性，不妨在把实践和应用推向未来的同时，也把领域边界的划定工作一同推向未来。

《区块链行业词典》在词条的收录方面比较好地做到了技术和业务的均衡、文科和理工科的均衡、行业应用和社区应用的平衡、中国特色和国际视野的平衡。做到这些是很不容易的，背后是不同凡响的顶层设计，是大量的心血和辛苦，是对行业脚踏实地的了解和把握，也是工匠精神的具体体现。

我衷心地期待这部词典能够在业内充分地用起来，向更多的人传播正确的区块链基础概念，为更多的人解除对区块链的神秘感和恐惧心理，在引导区块链技术及其应用的健康发展方面起到相应的作用。我也期待这部词典的编纂者能虚心听取业界意见，特别是使用中的反馈，密切关注区块链领域的最新进展和最新论述，让这部词典不断与时俱进。

白硕

2018 年 4 月 23 日于上海

前　言

维京资本与甲子光年系统地梳理了区块链领域的多个概念，涵盖基本定义、区块链基础技术、加密数字货币和法律监管等多个方面。本书由维京研究院和甲子光年旗下研究院甲子智库合作完成。

2018年，所有区块链行业的参与者和关注者都亟需这样一份详实、客观的工具。

因为长远来看，在跌宕起伏的加密数字货币行情背后，区块链技术本身才是浪潮里的坚实陆地，是未来可以承载巨大变革的基础。

但许多行业参与者和关注者仍对区块链技术的基本概念认知不足，在讨论热火朝天之际，参与者对某些基本词语的定义仍未达成共识，导致交流效率低下，信息混乱。

更深远的问题是，当下区块链技术获得了超出技术本身的关注，并被赋予了对立的情绪，有人极力赞美，有人大加抨击。

区块链技术已到了被污名化的边缘，它需要被正名，才能更健康、长足地发展。

期望本书能帮助读者建立对区块链技术的有效认知，并更好地理解区块链项目，评估加密数字货币，做出理性决策；也使区块链技术得到更多人理解，从而更好地回归技术本质，完成技术使命。

夯实认知是一切行动的第一步。

我们会不断更新这部词典，推出2.0、3.0、……版本，也欢迎读者不断提出反馈建议。

编者

作者简介

维京资本　由全球知名能源集团和芯片制造商参与发起，投资全球新技术和新商业趋势，获得国内资深 VC（风险投资）投资人支持，是一家极其注重研究能力的创新投资基金公司。维京研究院是维京资本在我国的唯一研究机构，目前以区块链研究为主。

甲子光年　科技赋能时代领先的一站式企业决策服务平台，包含媒体、智库、社群、企业服务版块，立足于我国科技创新前沿阵地，动态跟踪头部科技企业发展，致力于推动人工智能、大数据、物联网、云计算、信息安全、金融科技、大健康等科技创新在产业中的应用与落地。甲子光年旗下已建立甲子区块链团队，持续关注区块链领域的最新进展。

目 录

引言　区块链的下一个十年

自从2008年中本聪发表了比特币白皮书，至今区块链已经发展了十年的时间。2017年，它更是获得了社会广泛的关注。以下内容或许能够帮助大家，从零开始快速熟悉十年来区块链技术的一些基本概念，以便探讨未来十年区块链领域的发展机会。

区块链技术的基本概念和基本判断

相信大家对区块链技术的基本概念已经有所理解，从这些概念出发，有四个基本判断：

1）区块链的颠覆之处，在于它解决了“信任”这个人性问题，仅仅从技术角度出发，无法理解它的强大。一些原本彼此并不信任的人或者团体，各自出一台服务器，在大家彼此监督、大多数人遵守共识协议的情况下，能维护一份公认的记录——这就足以打开无穷的想象空间。

2）抛开能够实现价值流动的“币”，仅仅考虑区块链对生产力的改造，其创新程度远远比不上人工智能。

区块链其实就是一个分布式的数据库，每个区块中保存的内容，相当

于数据库中的表格，它和传统分布式数据库的区别在于：①参与者可以任意地加入，不需要许可；②任意地离开，不影响系统运行；③数据库的内容对所有参与者公开；④以往的所有交易数据，即数据库的日志，永不删除；⑤高度冗余，高度可靠；⑥低效，需要多个确认，才能认为交易真的完成了。

加密数字货币只是区块链技术的应用之一。从数据库技术角度看来，加密数字货币的记账方式和支付宝、微信支付记账的方式并无本质的不同，比特币交易的速度还很慢，大额交易一般要等六个确认，耗时一个小时左右。

加密数字货币的优势在于它们实现了虚拟世界中价值的低摩擦力流动。法币在比特世界中流动起来有非常大的摩擦力，发送方和接收方都要和公民的身份相绑定，有各种各样的限额，而且跨境流动非常困难。与之相比，多等几个确认的时间真是细枝末节的小事了。如梁斌博士所言："财富的自由流动、不受限地自由流动是很多富人的终极需求，我想这是包括比特币在内的加密数字货币最核心的价值"。

但在加密数字货币的应用之外，作为纯粹可信数据库的区块链技术，目前看来，最先落地的应用很可能是"溯源"。

例如天猫国际的全球溯源计划，主要是通过区块链、药监码等技术，运用大数据跟踪进口商品全链路，实现集生产、通关、运输等各方面信息于一身的目的，以期为各个跨境商品添加"身份证"。

这类应用，传统的、中心化的、高可靠的数据库一样可以搞定，因此从生产角度来看，区块链只提供增量式的进步，想象空间不大。

3）区块链真正的想象力在于生产关系角度的"去中心化"。

4）和任何技术一样，不能对区块链本身进行价值判断，它有可能被用来作恶，也有可能促进经济、社会发展。

从互联网发展历史上讲，非法经济还有游戏，经常是首先应用新技术的领域。以区块链为基础的加密数字货币，就曾被非法组织作为交易货币之一。

另一个历史规律是，遏制新技术的发展从来不是解决负面应用真正有效的方法。在区块链技术已经兴起，大量资本和人才涌入的情况下，只有花更多力气发展有益应用，才能避免有害应用的流行。

从整个人类历史的高度来看，如同郑渊洁所说："某些高科技首先是为了军事目的而研制的，尔后才转为民用。"如果区块链技术真的如大家想象得那么伟大，那它在未来会带来多少美好，眼下就可能带来多少混乱。或者说，它眼下带来多少混乱，说明它未来就有潜力带来多少美好。

加密数字货币八问

首先来看区块链技术目前最杀手级的应用——加密数字货币。这是目前建立在区块链技术上最风靡的应用，甚至要撼动全球金融体系。

以至于有一种说法是"离开加密数字货币谈区块链都是耍流氓"。

加密数字货币的本质是"信"，有信货币就能成立。只要有一个群体，他们把某种可交换的物品当作统一价值表现材料，那么该物品对于这个群体而言，毫无疑问就是货币。

"群体""当作"这两个词可不简单，背后有一个大大的"信"字。黄金的价值也来自于信任、信赖、信念。信任它是有限的、稀缺的，信赖整个社会的其他人都认可它的价值从而愿意拥有它，同时，还必须抱有信

念：它在未来仍然是稀缺的、人们愿意持有的。

黄金和白银用数千年时间赢得了信任、信赖、信念。法币则依靠权力机关和宣传机关，快速建立了自己的信用——再强调一下，国家背书只是获得信用的手段之一，这个手段也未必好使，法币信用崩溃的例子，出现过和正在出现的，不胜枚举。

《人类简史》的作者赫拉利曾说："任何大规模人类合作的根基，都在于某种只存在于集体想象中的虚构故事。讨论虚构事物正是智人语言最独特的功能。人类可以一起想象，共同编制出故事：传说、神话、神和宗教应运而生。智人的合作不仅灵活，还可以和无数陌生人合作，正因如此，智人才统治了世界"。

既然数亿的人口可以共同相信某个传说，在规模不算小的群体内部，大家都笃信比特币，这又有什么稀奇？

理解了"信"字，很多关于比特币和加密数字货币的问题就很容易解答了。

问：加密数字货币的价值到底体现在哪里？它对人类有什么贡献？

答：货币对人类的贡献在于它可以让原本无法发生的交易发生。要做出这样的贡献，它就必须是有价值的。它的价值在于它的信用，即对它持有信任、信赖、信念的人的数量，以及"信"的深刻程度、专一程度。但这些标准又太虚无缥缈了，如何量化？量化标准就是人类对这个货币进行了多少交易。

问：加密数字货币可以仅仅作为类似黄金的储值手段，而不进行日常交易吗？

答：只要有人“信”就可以。但是，不进行日常交易，相当于瘸了一条腿，用上面的量化标准衡量，就大打折扣了。

问：加密数字货币如何建立自己的信用？

答：加密数字货币本身的代码和理念要好。可是复制比特币的代码无法实现另外一个比特币，在建立信用的过程中，技术只是很小的因素。

只有一件事情是肯定的：要在极大规模的人群中建立信用，主要靠人性，而不是依靠科学、理性、说服、教育——人性使然，没有办法。

问：加密数字货币或者区块链可以实现去中心化吗？

答：注意前面描述去中心化时，加了“服务器”这三个字。只有计算机科技这个领域，可以谈论去中心化。只要有人群的地方，都不存在彻底的去中心化，必然存在领袖和群众、先锋和跟随、先进和后进。换言之，只有去中心化的技术，没有去中心化的人群——人性使然，没有办法。

但是，技术上去中心化，多多少少还是降低了人群的中心化程度。例如，互联网的出现，让个人更加容易地公开发表自己的看法，以前，只能通过报纸和杂志这些传统媒体，现在只需要发微博、写知乎。

问：加密数字货币的分叉是怎么回事？

答：分叉有两种：一种是由于网络通信造成的偶发分叉和孤块；另一种是由于使用某种加密数字货币的社区内部发生共识分裂，造成永久的、非偶发的分叉。

永久分叉之后，社区中一部分人的服务器在一个分叉上追加块，用他们认为合适的代码；另一部分人用另外的代码在另一个分叉上追加块——