VBR 蛋壳研究院 VCBeat Research
未来医健趋势研究 KOALA CAN 考拉看看

走向未来医疗系列丛书

区块链+医疗

新技术赋能医疗的应用与未来

动脉网蛋壳研究院◎编著

BLOCKCHAIN + HEALTHCARE

The application and future of new technology in medical field

机械工业出版社
CHINA MACHINE PRESS

蛋壳研究院 VCBeat Research
未来医健趋势研究 KOALA CAN 考拉看看
走向未来医疗系列丛书

区块链+医疗

新技术赋能医疗的应用与未来

动脉网蛋壳研究院◎编著

BLOCKCHAIN + HEALTHCARE

The application and future of
new technology in medical field

机械工业出版社
CHINA MACHINE PRESS

本书是区块链与医疗行业结合的权威读本，内容全面，结构清晰，包括区块链的起源、发展、应用及趋势预测，为万亿医疗健康产业构建了未来的蓝图。书中案例丰富、实战性强、语言通俗易懂，让读者轻松理解区块链与医疗结合的深度价值。

本书适合人群：相关领域企业领导、高管，医疗行业从业人员，区块链研究及开发者，金融科技企业工作人员以及对区块链、数字货币感兴趣的读者。

图书在版编目（CIP）数据

区块链＋医疗：新技术赋能医疗的应用与未来 / 动脉网蛋壳研究院编著 . —北京：机械工业出版社，2019.4
（走向未来医疗系列丛书）
ISBN 978-7-111-62380-9

Ⅰ . ①区… Ⅱ . ①动… Ⅲ . ①电子商务－支付方式－应用－医疗保健事业 Ⅳ . ① R199.2

中国版本图书馆 CIP 数据核字（2019）第 058180 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：刘怡丹 责任编辑：侯春鹏
责任校对：李 伟 责任印制：张 博
三河市国英印务有限公司
2019 年 4 月第 1 版第 1 次印刷
170mm × 242mm · 11.25 印张 · 1 插页 · 142 千字
标准书号：ISBN 978-7-111-62380-9
定价：69.00 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
服务咨询热线：010-88361066
读者购书热线：010-68326294

网络服务
机 工 官 网：www.cmpbook.com
机 工 官 博：weibo.com/cmp1952
金 书 网：www.golden-book.com
教育服务网：www.cmpedu.com

封面无防伪标均为盗版

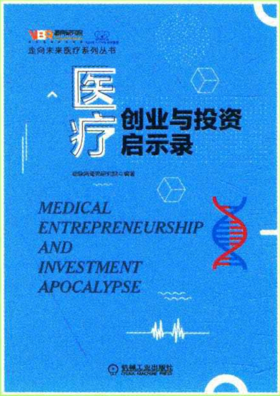
动脉网，一家关注全球医疗健康产业与创新科技的媒体机构，医疗行业最大的原创内容生产渠道和权威研究机构之一。动脉网旗下的蛋壳研究院通过洞察隐藏在医疗健康产业背后的商业逻辑，集合产业专家、资深观察者的智慧，为医疗行业的创业者、投资人及战略规划者提供有前瞻性的趋势判断和分析报告。

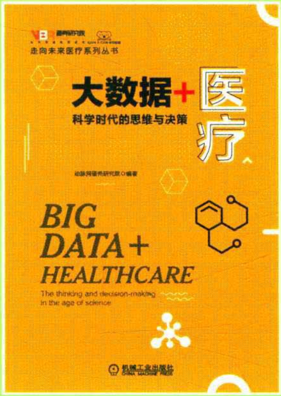
刘宗宇，动脉网蛋壳研究院执行院长，曾任《微型计算机》杂志社IT硬件评测室主任、主编。在加入动脉网之前，拥有13年的IT媒体经验。2012年开始关注比特币并进行挖矿，成为国内第一批科普比特币、区块链知识的媒体人。

特约策划：考拉看看·马　玥
特约编辑：考拉看看·侯佳欣

蛋壳研究院
VCBeat Research
未来医健趋势研究

走向未来医疗系列丛书





为中华崛起传播智慧

封面无防伪标均为盗版

策划编辑：刘怡丹

咨询电话：010-88379703

丛书序

近年以来，互联网已经颠覆了太多产业，但并未彻底改变健康医疗产业，无论是服务的形态还是质量，我们相信这个产业一定会被互联网及其他新的技术改变。

医疗的公共服务属性及上百年来形成的固有利益格局、思维体系不可能在短时间内被改变，需要几十年乃至更长时间才能达到产业的新恒态，这就是媒体及研究机构的巨大价值所在。

2014 年 4 月，动脉网诞生了，这是中国第一个聚焦健康医疗产业变革的第三方机构，并一直在“产业传播”与“产业研究”两个维度构筑自己的核心能力。自创办以来，动脉网始终关注“新技术”和“新医改”双轮驱动下的、以“新医改”为核心的大健康产业变革，尤其是这种变革带来的新商业机遇、新产业生态、新技术创新企业，以及在变革时代中产业人的重新定位。

每一个伟大企业成长的背后，都会有苦难的一面，乔布斯曾被自己的董事会赶出公司，马云曾在北京一再碰壁，马化腾也多次想卖掉自己的公司。企业的成长，本身就是一部辛酸史。因此，我们更愿意用发展的眼光和期待未来的心态去关注一个企业的发展沉浮，并提供力所能及的帮助。

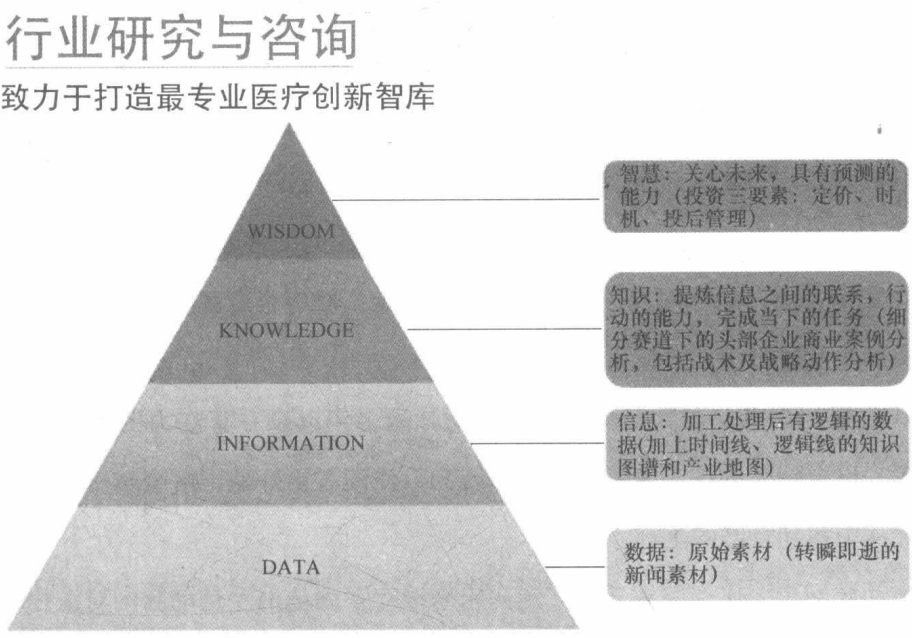
动脉网诞生的时间正好是在健康医疗产业变革的起点上，与中国乃至世界的

健康医疗产业变革同步。在将近五年的时间里，动脉网的小伙伴们用手中的笔，写下了8 000多篇文章、2 000万字的材料、100多篇报告，报道了近4 000家公司，覆盖了医疗创新的81个细分领域，初步构建起了全球医疗创新脉络图谱，已经成为20万医疗创新专业人群的信息家园。这些文字记录了我们在创新医疗健康领域五年时间的所见、所思和所得，以信息和数据为基础，呈现出逻辑清晰的医疗创新行业地图。

1. 我们的方法与逻辑

医疗的创新是全世界最重大的命题之一，关系着人、社会和国家的根本，要深入去理解、解释医疗创新发生的逻辑、原因，需要有耐心、有方法，最关键是下定决心深入到行业中，成为其中的一份子。

动脉网从医疗领域的宏观向中观、微观进行探索，在成立之初就引入了源自哈佛商学院的DIKW金字塔模型，从深层次探讨医疗领域的产业变迁，如下图所示。D，即DATA，涵盖了动脉网五年来积累的医疗创投领域的海量数据；I，即INFORMATION，是动脉网通过对医疗行业的专家、企业家的采访所整理出的资料和信息；K，即KNOWLEDGE，是从数据和信息中整理出来的知识体系；W，即WISDOM，是基于数据和信息得出的对于未来趋势的判断。从一个新闻事件中，我们去发掘企业做这件事情的商业逻辑和判断；从大数据中，我们分析细分领域的全貌；在对历史的掌握以及对当下的理解的基础上，我们形成了对未来趋势的判断能力。信息大爆炸时代，真伪边界越发模糊，动脉网要起到信息的筛查和过滤器的作用。



以此模型为底层的研究方法论，动脉网开始了对复杂医疗创新世界的描述和重构。

2. 医疗创新世界脉络图是如何塑造的

在数据方面，动脉网知识库目前已经积累了 13 000 多家全球医疗创新公司的数据、5 000 多家机构数据、56 000 多条政策数据、9 700 多条全球投融资数据。这个数据还在持续增长之中。

与全球知名医疗健康平台 STARTUP HEALTH、ROCK HEALTH 发布的数据对比，动脉网投融资数据覆盖的范围更广，统计的数据更全面。前二者的统计范围仅限于数字医疗公司，且对中国公司的统计不够全面，而动脉网将统计范围扩大至全球医疗健康行业。

在信息方面，动脉网四年来完成了近 4 000 家的企业报道，其中国内 2 400 多家，国外 1 400 多家，覆盖了全球医疗创新企业，70% 的投融资信息都在动脉网首发。

目前，动脉网的医疗专业内容团队已经超过 20 人，融资完成后将继续扩大内容团队，实现全球医疗创新信息的全覆盖。

在报告方面，动脉网是最早在行业内成立研究院的新媒体，2014 年就成立了“互联网医疗研究院”（动脉网蛋壳研究院的前身）。四年以来，动脉网蛋壳研究院完成了 100 多份原创行业报告，拥有超过 20 万人次的报告下载量。

在案例方面，动脉网蛋壳研究院从早期开始，就对全球医疗创新领域的核心企业、头部企业进行深入解读。

从数据到信息，再到案例、报告，动脉网多年以来一直在力图实现产业链的全覆盖，以全球化的视野解读企业创新行为，使读者更好地了解全球医疗创新的趋势，并从中找到自己的坐标。

由动脉网蛋壳研究院编著的“走向未来医疗系列丛书”是动脉网对医疗领域新变革、新技术和新方向的总结，记录了行业如何通过技术创新和模式创新改变医疗流程、降低医疗成本和提高医疗服务效率。《医疗创业与投资实践》记录了医疗领域在政策、产业和资本层面的发展，总结了近五年来医疗投资市场的变化；《大数据 + 医疗：科学时代的思维与决策》从医疗大数据的行业发展现状、应用场景、企业布局、政策监管等方面进行探讨，对医疗大数据的行业发展做了全面的分析和展示；《区块链 + 医疗：新技术赋能医疗的应用与未来》描绘了区块链技术在医疗健康领域的落地场景和未来发展前景。

这是一个充满了无限可能的时代，新技术的到来将引起医疗领域的重构，我们正处于一个新旧时代交替的入口。底层结构的创新、社会关系模式的再造，无不预示了一个充满想象的未来。医疗，将会是这个时代最富有想象空间的行业之一，而动脉网作为记录者，也会在这段波澜壮阔的进程中留下自己的印记。

动脉网 CEO

刘辉光

前 言

自从比特币问世以来，一种新的技术和商业模式诞生了。区块链已经从单纯的数字化货币技术发展到被认为是未来颠覆整个互联网商业模式的核心技术。随着技术的发展，人们意识到区块链可以在各行各业中发挥巨大的价值，其去中心化、不可更改、分布式存储的特点将颠覆行业应用中的底层数据存储方式。

2017 年，区块链技术成为全球关注的焦点，资本趋之若鹜。除了发行数字货币之外，人们也在考虑区块链如何与我们现实的行业应用相结合，各领域都在探讨用区块链技术进行变革的路径。

区块链从比特币的基础技术开始发展，随着技术的迭代，它和实际应用场景的结合也越来越紧密。区块链满足了数字金融领域对账本安全性、完整性的要求。医疗领域需要记录的数据是病人的病历信息、医疗服务的事件记录信息、设备交换信息、药品流通信息、保险合同信息等，这些都是不能公开且需要很高安全保障的重要信息，并且不能被篡改。其次，数据存储方需要严格验证数据的使用者、上传者的身份认证信息，通过电子签名、人脸、指纹、虹膜等身份识别方式确认身份，同时防止信息泄露。而这些要求，都是用区块链技术可以解决的。

医疗健康领域的数据安全与流通问题存在已久，而且长久未得到有效解决。区块链的重要特征是不可更改、分布式存储和先进的身份验证管理，这可以解决医疗

数据管理中的部分问题。首先，区块链上的数据不能被篡改。任何链上的篡改都会留下痕迹而迅速被发现。其次，分布式存储方式让每个节点都有数据备份，因此单个节点的故障不会对数据完整性造成影响，单点的篡改也会被所有节点发现。另外，区块链可以通过不同的私钥，对医生、护士、患者或保险公司进行身份的验证和权限管理。

医疗机构面临着无法跨平台安全共享数据的问题，区块链技术的出现让数据共享所担心的安全性问题得以解决。随着区块链技术对金融领域的改造逐步成为现实，医疗健康领域也开始探索使用区块链技术对其数据管理进行改造，并希望实现金融级的安全性和效率。

从 2016 年开始，医疗区块链企业将这项新的技术逐步应用在医疗保健用途上。除金融、医疗之外，区块链技术在大多数行业中的应用都还处在理论研究阶段。

医疗健康领域的数据有很强的安全性要求，区块链技术虽然有很多优点，但并非完美。区块链在医疗领域的试验和应用进程不会特别顺利，还有很多问题需要解决。同时，在鼓励技术创新的同时，也要防范区块链所带来的风险。

这本书比较详细地从底层技术到商业应用层面描绘了区块链如何在医疗健康领域落地。阅读之后可以使读者对区块链技术的本质有较为深刻的理解，同时明白区块链技术和医疗健康领域之间的关系？未来，随着技术的革新，每个人都可能是区块链技术的参与者。

目 录

第一章
区块链浪潮：1976—2018 年

区块链发展的历史，是多种技术共同进步的历史。从1976年到2018年，伴随着密码学、计算机技术和互联网的发展，区块链逐渐拥有了今天的技术范式。

1.1 区块链技术的孕育阶段

创新是进步的源泉，一项伟大技术的发展背后是无数紧密连接的创新成果的涌现。大众现在所见到的区块链技术，并不是完完全全新创的技术，它其实包含了不同历史时期多个领域的研究成果。对这些技术背景的回顾将有助于我们了解区块链技术的过去，把握区块链技术的现在，预测区块链技术的未来。

区块链技术的进步依托于密码学（Cryptography）的发展。密码学的发展使得人们匿名操作的安全性得以保证。那么，究竟什么是密码学？密码学包括密码编码学和密码分析学两大范畴，前者的主要研究内容是密码体制设计，后者的主要内容则是密码体制的破译。密码编码技术和密码分析技术是相互支持、密不可分的两个方面。

1976 年，惠特菲尔德·迪菲（Whitfield Diffie）、马丁·赫尔曼（Martin

Hellman）发表了一篇具有划时代意义的文章——《密码学新方向》;1977 年，美国的数据加密标准（DES）公布。这两件事情的发生让密码学得到了空前的关注度。在此以前，人们都认为密码是政府、军事、外交、安全等部门专用的。而在 1977 年后，密码学由公用研究转为民用研究，正是这种转变，让密码学得到了飞速发展。

1977 年，罗纳德·李维斯特（Ronald Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）三位教授提出了 RSA 公开密钥密码系统，这是迄今为止所有公钥密码体系中最著名、使用最广泛的一种密码体系。RSA 的名称来自于这三位发明者姓氏的第一个字母，他们也因此在 2002 年获得了计算机领域的最高荣誉——图灵奖。

1980 年，《密码学新方向》的两位作者之一赫尔曼的博士生默克尔（Ralph Merkle），提出了默克尔树这种数据结构和相应的算法，其主要用途之一是对分布式网络中数据同步正确性的校验。值得指出的是，在 1980 年时，哈希算法、分布式的网络都还没有出现，我们熟知的安全哈希算法（Secure Hash Algorithm，简称：SHA-1）、消息摘要算法第五版（Message Digest Algorithm MD5，简称：MD5）都是在 20 世纪 90 年代诞生的。在那个年代，默克尔就发布了这样一个数据结构，并且对密码学和分布式计算领域的发展起到了重要作用，这多少有些令人惊讶。

1982 年，莱斯利·兰伯特（Leslie Lamport）在一篇描述分布式系统一致性问题（Distributed Consensus）的论文中抽象出了一个著名的例子，即拜占庭将军问题（Byzantine Failures）。拜占庭帝国想要进攻一个强大的敌国，他们的军队分散在敌国的四周，依靠骑马的通信兵相互通信来协商进攻意向及进攻时间。任一支军队单独进攻都毫无胜算，至少六支军队（一半以上）同时袭击才能攻下敌国。困扰将军们的问题是，他们不确定他们中是否有叛徒，叛徒可能擅自变更进攻意向或者进攻时间。假设不用考虑通信兵是否会被虏获或无法传达信息等问题，即消息传递的信道绝无问题，

在已知有叛徒存在的情况下，其余忠诚的将军如何在不受叛徒的影响下达成一致的协议，拜占庭将军问题就此形成。这一问题的提出，标志着分布式计算的可靠性理论和实践进入了实质性阶段。

同年，大卫·乔姆（David Chaum）提出了不可追踪的密码学网络支付系统。我们可以看出，随着密码学的发展，眼光敏锐的人已经开始尝试将其运用到货币、支付相关的领域了。

1985 年，科布利茨（N.Koblitz）和米列尔（V.Miller）各自独立提出了著名的椭圆曲线加密（ECC）算法。此前发明的 RSA 算法由于计算量过大，并不实用，ECC 算法的提出使得非对称加密体系产生了应用于实际的可能。因此，可以说到了 1985 年，也就是《密码学新方向》发表 10 年左右的时候，现代密码学的理论和技术基础得以完全确立。

有意思的是，1985—1997 年这段时期，密码学、分布式网络以及支付 / 货币等领域，没有什么特别显著的进展。这种现象很容易理解：在新的思想、理念、技术产生之初，大家总要经过相当长时间的学习、探索、实践，才有可能获得突破性的成果。其前十年，往往是理论发展的时间，后十年才会进入到实践探索阶段，1985—1997 这十年左右的时间，应该是相关领域在理论方面迅速发展的阶段。在经过了 20 年左右的时间后，密码学、分布式计算领域终于进入了爆发期。

1998 年，比尔·盖茨的微软如日中天，Windows 98 操作系统风行全球；亚马逊公司刚刚成立三年；第一次互联网大泡沫正在酝酿，并将在 2000 年破裂。而电子商务的发展迫切需要支付方式的变革。互联网电子商务的开展，使得网络支付成为一种潜在需求，数字货币是解决这一问题的方式之一。

一群先驱对数字货币进行了应用实践。戴伟发表文章阐述了一种匿名的、分布式的电子现金系统，他将其命名为“B-Money”；同一时期，尼克·萨博（Nick Szabo）发明了“Bit Gold”，“Bit Gold”设置了一种机制，用户通过竞争性地解决“工作量证明问题”，将解答的结果用加密算法串