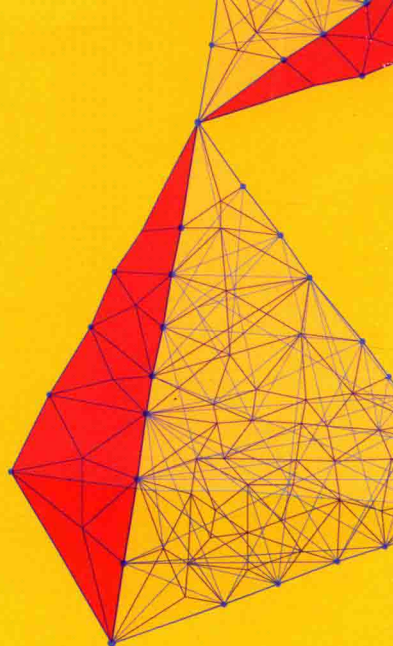




区块链是互联网的未來和未來的互联网

以实践为基础，从技术角度研究了区块链的设计与实现，

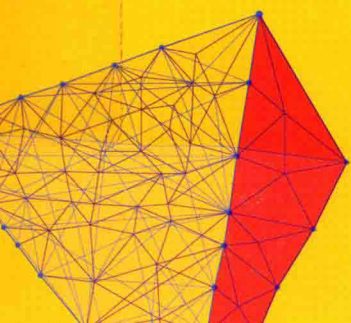
从代码层面详细剖析了使用Node.js开发区块链的技巧与最佳实践。

围绕区块链、Node.js前后端开发、智能合约、共识算法等进行全面深入的讲解，

帮助读者快速上手区块链开发！

Node.js 区块链开发

朱志文 / 编著



机械工业出版社
China Machine Press

Node.js 区块链开发

朱志文 / 编著



机械工业出版社
China Machine Press

图书在版编目 (CIP) 数据

Node.js 区块链开发 / 朱志文编著. —北京: 机械工业出版社, 2017.4 (2017.8 重印)

ISBN 978-7-111-56695-3

I. N… II. 朱… III. JAVA 语言—程序设计 IV. TP312.8

中国版本图书馆 CIP 数据核字 (2017) 第 090058 号

Node.js 区块链开发

出版发行: 机械工业出版社 (北京市西城区百万庄大街 22 号 邮政编码: 100037)

责任编辑: 吴晋瑜

责任校对: 殷虹

印 刷: 三河市宏图印务有限公司

版 次: 2017 年 8 月第 1 版第 2 次印刷

开 本: 186mm×240mm 1/16

印 张: 19

书 号: ISBN 978-7-111-56695-3

定 价: 59.00 元

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

客服热线: (010) 88379426 88361066

投稿热线: (010) 88379604

购书热线: (010) 68326294 88379649 68995259

读者信箱: hzit@hzbook.com

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问: 北京大成律师事务所 韩光 / 邹晓东

Foreword 推荐序一

技术革命创造着无数的奇迹。互联网、物联网、移动计算、大数据、云计算等技术的出现正在改变着人类生活的方方面面。

区块链技术以其去中心、完整、真实、公开、安全等特点，已经成为新一轮全球技术创新与变革的核心。英国《经济学人》杂志曾预测“区块链将重新定义世界”。麦肯锡将区块链技术称为“继蒸汽机、电力、信息和互联网科技之后，目前最有潜力触发第五轮颠覆性革命浪潮的核心技术”。

区块链是万物账本，几乎可以记录任何有价值的东西，包括账务账目、投票、版权及产权任何可以用代码来表示的东西。在万物互联的时代，每个人都可以在这个“账本”上留下不可修改的痕迹。这些痕迹可以回溯一个人过往的所有经历，这对今后的法律、政治、经济等各个方面所产生的影响将是巨大的。

传统互联网构建的是信息传递网络，区块链构建的则是价值传递网络。价值传递网络的出现，可以使万物互信、万物共享成为可能，使各行各业可以跨界互联，催生新业务、新行业和新模式，创造新机遇。作为未来互联网的基础协议之一，区块链将支撑新型信任体系的构建，由此引发“信誉革命”，其最终影响的范围和深度也会远远超出大多数人的想象。

以内容产业为例，多年来，编辑出版行业各个机构都在数字出版领域艰难地研究与探索。但是苦于没有合适的技术，导致在当下的互联网生态中，版权侵权现象严重，纠纷频发，加之举证困难、维权成本过高，严重侵害了作者的原创积极性，这已经成为内容产业的痛点。如今，区块链技术的出现使数字化知识内容的确权、确真和确价成为可能。区块链可以完整地记录一个作品从灵感到最终作品的所有变化过程，可以保证数字内容的价值转移过程的可信、可审计和透明，为版权保护提供了最完美的解决方案。区块链技术的引入将极大提升内容产业的运行效率，从确权、用权、维权三个环节解决产业链冗长繁杂的问题。

正是在这种产业背景下，国内一批区块链技术先锋积极投身到基于区块链技术的出版平

台开发中。其中，朱志文先生带领的“亿书”团队就是这批技术先锋的杰出代表，他们利用区块链技术打造的“亿书”去中心化的出版平台，实现了版权签名与认证、协同创作、一键发布等功能，这将极大激发作者的原创动力与热情。“亿书”平台的出现，是我国内容产业发展探索中的一个重要节点，更为知识的价值传播做出了重要的基础性探索。

《Node.js 区块链开发》是朱志文先生带领的“亿书”团队多年艰辛实践的结晶，相信这本书能够为广大区块链技术人员和爱好者提供有益的参考和借鉴。同时，也希望更多的开发者加入区块链的大潮中，积极推动区块链技术在内容产业中的应用实践，让区块链成为知识服务的重要工具。

我们坚信，内容产业的革命即将到来。此时此刻，我们已经站在了变革的临界点。

过去已去，未来已来。

科学技术文献出版社副社长 李 沛

2017 年 4 月 5 日

Foreword 推荐序二

微博上曾有人感慨：“小说家死了，他的小说还会有人读；程序员死了，他就被人忘了。99%的软件，其生命周期不超过5年，这意味着你现在写的代码，5年后将毫无用处。如何做一些能留得下来的事情，是每个程序员应该认真思考的问题。”这条微博一经发出，立即引得众多程序员感慨万千。

但这里有一个真实的案例显示，代码的命运并不都是这样。2008年，中本聪发布了比特币白皮书。2009年1月，他开发了比特币的第一个版本，也就是人们所熟知的satoshi客户端。8年来，无数开发者为比特币提交了代码，中本聪的代码被保留下来的微乎其微，目前仅占代码总量的2%，但他的思想被原原本本地继承了下来，那就是“去中心化”理念：区块链就如同一台信用的机器，让政府、公司、机构与个体作为平等的节点呈现在分布式网络上，各自管理自己的身份与信用，共享一部不可修改的交易总账。最近，另一个区块链项目“以太坊”不顾社区的反对，强行发起一次硬分叉，回滚了区块链数据，引来不小争议。

区块链与普通软件项目的不同之处在于，它是去中心化的。这就意味着它可能遵循不同的开发组织理念，比如官方对于区块链项目可能并不那么重要，甚至连官方这个词都是值得商榷的，因为软件是开源的，任何人都可以开发它的新版本，或者分叉出一条新链。即使存在官方，也并不意味着区块链就是其产品，官方并不拥有区块链数据修改的主导权。区块链更像是把数据（信用）写在无限纸带上的单向图灵机，能够根据指令读写当前纸带格子上的数据，每执行一条指令就往后移动一格，但不能修改过去所写入的数据。

与所有开源社区一样，比特币等区块链项目的开发方式具有这样一些特征：

- 1) 人们按照自己的兴趣和意愿选择加入，开发者并非项目发起人或官方的雇员。
- 2) 任何人都可以无偿获取开源项目的源码及相应的编程工具，并为项目贡献自己的代码。
- 3) 软件开发和发布的主体并非公司，而是一些基金组织或个人，他们不以盈利为目的。

4) 参与人员分布于全球各地，彼此间通过互联网进行协作。

然而，就是这种看似松散、不稳定的工作组织方式，却爆发了惊人的生产力。对于比特币这样的区块链项目，对规则的任何重大改变都需要获得社区的广泛共识，对软件的任何更新都必须由大多数“矿工”安装使用后才能让修改生效。正如本书的作者所言：“区块链产品都是去中心化的，去中心化的基础就是 P2P 节点众多。那么如何吸引用户加入网络成为节点，有哪些激励机制？同时，开发的重点是让多个节点维护一个数据库，那么如何决定哪个节点写入？何时写入？一旦写入，又怎么保证不被其他的节点更改（不可逆）？解决这些问题的答案就是共识机制。”

起初，本书作者以 imfly 这个 ID 在巴比特社区发帖，分享自己“用 Node.js 开发加密货币”的经验与心得，正如许多开源项目的艰难起步一样，一开始并没有得到多少支持。但令人欣慰的是，imfly 坚持了下来，并有了更多志同道合的朋友加入，从而有了巴比特社区的开发者群体，有了这本书。在此过程中，imfly 发起了“亿书”这个开源项目，旨在打造人人可用的去中心化软件，以区块链为底层驱动，促进人类知识分享。本书分享的就是亿书的源码，无论研究 Crypti、Lisk 还是 Ebookcoin，或者学习 Node.js 前后端开发技术，本书都将提高你的学习与开发效率。

区块链项目一般是基于开源的工作方式，所以只要接入互联网，任何人都可以随时随地获得开源的代码、文档并在之上做出贡献，也就是说，全社会的力量都可以贡献于同一份代码和文档系统。而传统项目往往受制于安全管理，这种情况不只是出现在不同的公司之间，即使在一个公司的内部，一个产品的代码往往也会被分割为几块，分别由不同的人访问和维护。同时由于代码涉及商业利益，即使发现错误，开发者也不一定有权限去做相应的修改，这些都会使得代码的质量不断下滑。如果你有一颗梦想的种子，与其让它在阴暗的角落独自生长，不如像亿书这样公布于社区，让众人参与其中，让它像蒲公英一样四处传播。本书将帮助你了解亿书的架构设计，帮助你快速融入亿书开源社区这个大家庭里。

长 铗

巴比特创始人兼 CEO，著名科幻作家

2017 年 1 月 14 日

Foreword 推荐序三

正如互联网的前身 ARPANET 一样，区块链的前身比特币最初也是小众圈子里的产物。从 20 世纪 90 年代开始，“密码朋克”小组的极客们就为了网络交易的实现而不断创新、实验及经受失败，直到一位自称“中本聪”（意译名）的开发者出现。这位神秘的开发者在 2008 年低调地将一篇简约而不简单的论文发表到网络上，并发布了基于论文的核心代码。此后，在人们怀疑、争议和尝试的过程中，这位神秘的开发者又悄悄地隐退，他“悄悄的走了，正如他悄悄的来”，但与《再别康桥》中不同的是，他留下了比特币及其基础架构区块链技术，更重要的是，他留下了被称为“新一代价值传递网络”的思想和原理。

转眼间 8 年过去，比特币从极客圈子中的“小玩意儿”变成了市值超过 130 亿美元的数字货币，而源于比特币的整个区块链行业的市值超过了 300 亿美元。有不少研究者认为，区块链技术很有可能会成为下一代价值互联网乃至人工智能、网络智能的基础设施级协议。

值得庆幸的是，我们离这一次的“区块链革命”，并没有像上一次互联网革命那么远。2011 年左右，比特币这一新生事物传入我国，不少敢于吃螃蟹的人从不懂、迷茫开始，逐渐了解比特币的原理，随后逐步进入这样一个新兴行业。到了 2016 年，我国诞生了十多家比特币交易所，我国交易所的总交易量占了全球交易量的 70% 以上；我国“矿工”为整个比特币网络提供了超过 60% 的算力，保障着整个比特币交易网络的安全运行。对于任何一个区块链从业者来说，不论开发、合作还是推广，中国市场都是需要着重考虑的重要因素。

然而，一个不那么乐观的事实是，中国在区块链行业开发领域鲜有建树。造成这个事实的原因主要有三个：首先，国内的开发技术整体还相对落后，在区块链技术领域缺乏积累，创新能力更加不足；其次，我国经济金融制度比较僵化，于是导致我国在这方面的研究创新比较少，在货币制度和经济发展方面有专长的人才就更加屈指可数；最后，金融和网络技术原本是非常跨界的两个领域，在互联网金融时代到来之前，在这两个领域都有研究的人少之又少。

以上所述情况导致我国虽然在区块链行业有着很重要的地位，但是核心开发的贡献率非常低，在整个行业的话语权并不高。在国内的区块链市场上，数字货币兑换交易占了非常大的比例，但在最具价值的技术开发和应用上长期空白。更令人担忧的是，不少非法分子开始利用“数字货币”的概念进行传销及非法融资等活动，给国内的区块链行业抹上了不光彩的颜色。

古人云，授人以鱼不如授人以渔。在这样的背景下，能够有朱志文这样的技术专家站出来，采用手把手的教学方式讲解数字货币的技术开发原理，分享自己“Node.js 区块链开发”的经验与心得，这是非常令人欣慰的。沟通之精要，在于深入浅出。要想做到通俗易懂，背后所要花费的时间与精力是非常之多的。朱志文陆陆续续发表了不少文章，我们从中可以看出他是经过了认真、充分的准备的。这一次修订成书，他更是对整个技术开发进行了系统地编排和审订。相信这样的技术分享能够帮助国内的区块链开发者夯实基础，逐步掌握数字货币的原理，助力他们进行进一步开拓创新。

我国的区块链行业需要更多像朱志文这样的技术大咖，也同样需要更多的资本投入，以帮助整个产业的健康发展。作为中国数字货币行业的领军企业之一，火币愿意以一个布道者的身份，传播区块链技术的理念，推广数字货币的价值，带领资本加大对区块链行业的投入，推动我国的区块链产业健康良好地发展，同时也为全球的区块链行业做出自己的贡献。

正如本书所述，不论采用什么样的技术来实现，区块链技术背后的基本原则是不会变的。诚信正直、分散运作、价值激励、权利保护、隐私保障、开放包容，这些理念不仅是区块链运行的基础，也是未来人类社会发展的基石。

区块链是一个新生事物，在拿起放大镜进行审视和用惯性思维去批判之前，让我们一起变成一块虚心的海绵，先来学习一下区块链的原理，感受一下它的魅力！

希望大家通过本书不仅能知其然，还能知其所以然。

徐宝龙

火币区块负责人

2017年1月28日

Preface 前言

本书原名《Nodejs 开发加密货币》，大部分已经通过网络免费分享（网络上仍有原文），正式出版的时候改成了现在的名字，部分章节也做了调整。写作本书的时候，“区块链”这个称呼并不流行，但讨论的内容实际上就是区块链技术。就在本书整理出版的时候，国家发布了《中国区块链技术和应用发展白皮书》，整个社区也接纳了“区块链”这个称谓，因此改为现在的名字。

“每一件与众不同的绝世好东西，其实都是以无比寂寞的勤奋为前提的，要么是血，要么是汗，要么是大把大把的曼妙青春好时光”。这是一位文笔非常好的朋友大学毕业后给我的留言。每每读到这句话，总能被感动。后来，与那位朋友聊天，我说你真有才，能把一句话说到人的内心深处，我若不是因为是个男人，一定美美地哭一场。他一听，十分感慨，告诉我他也是摘抄来的，还说只有经历过，才能被感动。

工匠精神人人推崇，但不是人人都能做到，环境往往起到了很大的作用。还是我的那位朋友，刚毕业的时候，他去了某机关报社，最初当记者，待遇优厚，后来做编辑，自在逍遥。这中间，他还经常写写书，一年下来，仅仅版税收入也非常可观。但是，最近几年好像不太好了，有一次聊天明显感觉到他的消极，问他怎么了，他说互联网抢了他们的饭碗。我说，那你就抢回来吧，化敌为友，借助互联网挣更多钱。他说试过了，没那么简单，几大文学网站，那么多作者，真正挣到钱的没有几个。偶尔火起来了，大部分都被平台分去了，有的甚至连版权都得不到。加之盗版猖獗，基本入不敷出。

听着他的话，我始终沉默，当初我也想不到出路，时代变迁，谁都无法阻拦。但是，这两年我有了方向，找到了可以彻底解决的办法，这也是我坚持分享这本书的内在动力。软件是给个人用的，开发者首先想到的自然是身边人，这是再正常不过的道理。这位朋友的问题就是亿书诞生的初衷，没有任何离奇的故事，都是满满的生活小节，这多少也有点工匠精神的情结吧。

当主动往版权保护和写作分享发力的时候，资源就源源不断地聚集到了我的面前。亿书，

这个去中心化的版权保护和知识直销系统（自出版平台）的操作过程大致是这样的：在经过一段时间的技术探索之后，2015 年，我把关于打造电子书版权保护项目的想法在网上和盘托出，吸引了很多小伙伴的关注，同时也证明了想法的可行性。接着，我用行动实践电子书写作和分享的全过程，并把亿书这个项目的真实源码作为分享的主要内容，边分享边开发，边打造团队，这中间提交了多个开源代码（本书多个实例便是其中一部分）。读者越来越多，团队日益壮大，仍有很多小伙伴在了解、考察和熟悉中。接下来，待亿书正式发布，就可以用亿书（软件）来继续分享亿书（源码）了。这就像 C/C++ 这样的编程语言可以用来开发自己，开发者也是使用者，自身不断循环完善。

亿书，以价值传播为目标，定位在协同创作和版权保护，从底层区块链版权协议到顶层客户端应用，完全自主开发，是国内少有的不依赖于比特币、以太坊等国外第三方平台的产品。新版产品提供了强大的扩展开发能力，基于亿书可轻松开发很多类型的去中心化应用，比如数字资产管理、财务结算与审计、交易存证与监控、电子商务、视频直播等。这仍然是从基础需求起步，步步搭建积木的思路和过程，与我通过写作本书体验产品需求，然后发展亿书的思路一样。这是工程学的基础，再厉害的天才也无法逾越。

亿书注定要成为价值传播领导者，开启数字出版新时代。

这是本什么样的书？

亿书是完全开放开源的项目，是一个完整的类比特币的区块链产品。本书基于该项目，完全以实用为目的，将开发实践贯穿始终，内容涉及开发区块链产品前端、后台和桌面应用的全过程。本书用开发的思维进行反复迭代，由浅入深，详细介绍了区块链技术相关理论知识、Node.js 前后台开发基础知识、加密签名技术、P2P 网络实现、共识算法等，能帮助初学者快速学习入门区块链技术，深入掌握 Node.js 编程开发技术，帮助区块链技术从业者、Web 开发者更深刻地理解相关概念和技术实现。

- ❑ 想找到关于如何开发一款真正的区块链产品（不只是调用某款加密货币 API）的图书吗？这可能是目前世界上第一本，也可能是唯一的一本。
- ❑ 想找到关于 Node.js 大型实践项目的图书吗？这可能是世界上少有的一本，也可能找不到第二本。
- ❑ 想找到亿书、Lisk 等基于 Crypti 的分支项目的详细开发文档吗？这一定是世界上唯一的一本。
- ❑ 想深入了解区块链的技术实现吗？看看本书，对于区块链、共识机制等各种概念的理解将会更加透彻。

- ❑ 想从事区块链（无论是比特币还是其他各类竞争币）的开发吗？Node.js 一定是无法回避的，这本书也必然无法错过。
- ❑ 想了解比特币的原理吗？这本书不仅告诉你其原理是什么，还会从技术的角度告诉你为什么，无论你是做技术还是做管理，本书都值得参考。

本书面向的读者

- ❑ 开发人员。本书涉及前端、后台的方方面面，无论是前端开发人员，还是后台开发者都可以学习参考。
- ❑ 架构师。区块链本身是分布式、云计算的典范，本书详细描述了一款区块链产品的架构设计，他们可以通过本书学习掌握区块链是如何基于 P2P 网络构建复杂的自适应系统的。
- ❑ 高校学生、教师、科研人员等。本书内容在网络上分享的过程中，已经有大学老师作为教参用在实际教学之中，本书从概念到代码实现，理论与实践结合紧密，深入浅出，适合系统研究学习区块链技术。
- ❑ 学习 Node.js 的读者。本书介绍了 Node.js 入门知识，包含了 Node.js 的技术原理和使用技巧，是一个完整的 Node.js 使用案例，有一定 JavaScript 基础的初中级读者，通过本书可以更深入的学习提高使用 Node.js 编码技能。
- ❑ 投资人，以及对比特币等区块链产品感兴趣的普通用户。本书力求语言朴实，书写过程中尽量避免晦涩的技术术语，在具体的编码之前，都要详细介绍相关概念，因此投资人和普通读者也可作为科普读物，从技术层面对加密货币等区块链相关产品有更进一步的认识。

本书内容

本书力图用最少的篇幅表述更丰富的内容，共分为五个部分，具体结构如下。

第一部分：了解区块链，共 4 章。详细讲述了区块链产品——加密货币的相关概念，用独特的技术视角，把加密货币的基本技术要素串联起来，同时在文中自然引导读者跳转阅读下面各个部分，实现理论到实践的过渡。

第二部分：Node.js 入门指南，共 4 章。详细介绍了 Node.js 入门知识，并通过一个具体项目完成对 Node.js 在区块链技术领域的调查和描述，整个部分也是项目架构设计必备的调研和技术选型阶段，是本书第一个完整的实践范例。

第三部分：源码解读，共 9 章。从架构设计的角度，层层剖析区块链的设计原理，深刻解读相关概念和技术。从项目设计的角度谋篇，第 9 章详细介绍了亿书白皮书的核心内容，明确了项目的需求，教读者如何着手研究区块链产品；第 10 章从项目入口程序出发，介绍了亿书项目的整体结构；第 11 ~ 17 章分别介绍了 P2P 网络、加密解密、签名和多重签名、区块链、共识机制等区块链核心内容，并给出了代码实现。

第四部分：开发实践，共 9 章。主要是对第二和第三部分的有益补充，把在这两个部分出现的技术难点抽取出来，集中介绍。仍然以亿书项目中涉及的实际项目为主，包含多个完整独立的小项目。第 18 ~ 19 章主要介绍了函数式编程等编程方法论；第 20 章，介绍了命令行工具的开发（含开源实例）；第 21 章总结了 `async` 的用法，解决了 Node.js 回调流程控制问题；第 22 ~ 23 章介绍了亿书官方网站的开发，对市面上的静态网站进行了总结，通过两个实例详细介绍了客户端的开发设计；第 24 章详细介绍了密码学技术；第 25 章介绍了时间戳、数据计算等更加细致的优化内容；第 26 章介绍了测试技术。

第五部分：附录。汇总了区块链的相关概念、常见词汇的中英文对照等内容。

本书的相关资源

本书分享的开源项目——亿书，仍在持续开发中，因此，当您在阅读本书源码的时候，核心代码库已经做了比较大的修改。所以，我将本书分享的源码锁定在了一个固定的版本里。有关亿书的相关资源如下：

❑ 亿书官网：<http://ebookchain.org>

❑ 亿书源码：<https://github.com/Ebookcoin/ebookcoin/tree/v0.1.3>

❑ 亿书白皮书：<http://ebookchain.org/ebookchain.pdf>

❑ 亿书官方 QQ 群：185046161

因水平所限，书中难免会有不足之处，为了方便大家交流，也为了弥补可能出现的不足，我在区块链俱乐部论坛上与本书配套设置了一个勘误版块，也会定期回答读者的问题，欢迎大家访问，地址如下：

<http://chainclub.org/>

实际上，亿书和本书都是开源的产物。非常欢迎有志于区块链研发的小伙伴参与进来，共同进步。

致谢

我是个极度不愿意重复的人，所以才会始终保持足够的热情来编写软件为自己服务。而

写文章恰恰需要反复推敲和修改，甚至推倒重来。自从 2016 年年初决定要撰写和分享本书中的系列文章，并从中汲取区块链的技术营养，我就做好了各种思想准备。为了防止退缩，我还在网络上公开许下承诺。但让我万万没有想到的是，战胜自己是如此艰巨。这段时间，我几度放弃，又重新开始。

很庆幸的是，在这个过程中，有一帮小伙伴们始终陪伴、支持和鼓励着我。

感谢科学技术文献出版社李沛副社长，他对知识传播领域的独到见解以及他推崇的“知识服务商”理念，让我很受启发。他受邀为本书作序，并给了我很多极为宝贵的意见和建议。“知识服务商”将会成为亿书未来发展的重要理念。亿书的新版本，从每一个细节都会体现这一思想，让每一个使用亿书的人从中受益，令知识的创造充满动力。

感谢出版社的编辑杨绣国老师，给了我极大的宽容和鼓励，她极为认真地帮我梳理和策划书的内容，协调各类资源。

感谢火币网徐宝龙，我们在亿书组织的区块链茶座上相识，一见如故，成了好朋友。他专注区块链行业，给我、给亿书提供了很多宝贵的意见和帮助。他不仅聪明，还非常勤奋，居然在大年初一的晚上给我发来了他为本书撰写的序言，让我感动不已。

感谢 CSDN 技术社区的编辑们，这是一群充满激情的活跃分子，在 @猫白 @红月 两位编辑的带领下，很快构建起多个开发技术知识库，在社区引起了强烈反响。她们支持本书，还邀请我与她们一起构建了区块链知识库。

感谢巴比特论坛的几个小伙伴。这些文章最先发布到巴比特论坛，巴比特的 @长铗、@miner、@等一轮残月、@萌大大等，几乎将这些文章篇篇都设为精华帖，跟踪进展，给予极大的关注和支持。

感谢 cnodejs.org 社区。这些文章后来陆续在 cnodejs.org 上同步发布。因为共同的爱好，我与社区很多 Node.js 技术大咖 (@i5ting @lc @Grape 等) 成了好友。他们对这些文章给予了充分的肯定和极大的支持，还主动帮我推荐和宣传，让我深受鼓舞。

感谢亿书社区的小伙伴们，比如 @Tailor @火鼎 @珍惜 @一 @Mojie @cyio @zbinlin 等，他们不仅支持我，有的还给我提供了内容。当然，还有很多其他小伙伴，这里就不一一列举了。

最后，感谢我的爱人和我可爱的儿子，谢谢你们的陪伴。

目 录 Contents

推荐序一	2.6 总结	12
推荐序二	2.7 参考	12
推荐序三		
前言		
第一部分 了解区块链		
第1章 加密货币就是货币		2
1.1 加密货币简史		2
1.2 什么是加密货币		3
1.3 加密货币就是货币		4
1.4 加密货币可靠吗		4
1.5 总结		6
1.6 参考		6
第2章 区块链，承载人类信用的基石		7
2.1 利益，现实世界的内在驱动力		7
2.2 信用，决定着利益转移的方向		7
2.3 未来趋势		9
2.4 应用场景		9
2.5 风险提示		11
	第3章 共识机制，可编程的利益转移规则	13
	3.1 机制，左右产品走向的根源	13
	3.2 PoW：工作量证明机制	14
	3.3 PoS：股权证明机制	15
	3.4 DPoS：授权股权证明机制	16
	3.5 亿书对 DPoS 机制的改进	17
	3.6 总结	17
	3.7 参考	18
	第4章 区块链架构设计	19
	4.1 基本概念	19
	4.2 架构图	20
	4.3 协议层	20
	4.4 扩展层	22
	4.5 应用层	22
	4.6 编程实现	23
	4.7 知识图谱	25
	4.8 总结	26

4.9 参考	27
--------------	----

第二部分 Node.js 入门指南

第5章 Node.js 在币圈流行么 30

5.1 Node.js 在开源社区很流行	30
5.2 Node.js 在币圈也同样流行	32
5.2.1 Github 自带搜索	32
5.2.2 自制查询工具	32
5.3 Github 上前 10 个应用的简介	34
5.4 结论	36
5.5 总结	36
5.6 参考	36

第6章 Node.js 让前端开发像 子弹飞一样 37

6.1 项目需求	37
6.2 技术选型	37
6.3 Node.js 简介	38
6.4 开发步骤	39
6.4.1 搭建环境	39
6.4.2 新建工程	40
6.4.3 前端组件	40
6.4.4 前端流程	42
6.4.5 学习 API	43
6.4.6 数据整理	44
6.4.7 D3.js 渲染	46
6.4.8 代码调试	48
6.4.9 部署发布	48
6.5 总结	51
6.6 参考	51

第7章 Node.js 让后台开发像前端 一样简单 53

7.1 需求	53
7.2 开发	54
7.2.1 安装 Express	54
7.2.2 创建简单应用	54
7.2.3 使用模板引擎	55
7.2.4 使用静态文件服务	55
7.2.5 后台请求 Github API	56
7.2.6 模块化重构	57
7.2.7 测试和部署	61
7.3 总结	61
7.4 参考	62

第8章 你必须知道的几个 Node.js 编码习惯 63

8.1 一切都是数据流	63
8.2 事事皆回调	65
8.3 异常要捕捉	67
8.4 总结	72
8.5 参考	73

第三部分 源码解读

第9章 亿书，一个面向未来的 自出版平台 76

9.1 亿书是什么	76
9.2 使用场景	76
9.3 主要特点	77
9.4 核心功能	77
9.5 技术架构	78

9.6 总结	79	第 13 章 地址	105
9.7 参考	79	13.1 源码、类图与流程图	105
第 10 章 入口程序 app.js 解读	80	13.2 解读	105
10.1 源码与类图	80	13.2.1 公共 API	107
10.2 解读	80	13.2.2 Hash 地址	109
10.2.1 配置处理	80	13.2.3 别名地址	110
10.2.2 异常捕捉	82	13.2.4 注册用户名	111
10.2.3 模块加载	83	13.2.5 联系人列表	113
10.3 总结	86	13.3 总结	115
第 11 章 一个精巧的 P2P 网络实现	88	13.4 参考	115
11.1 源码、类图与流程图	88	第 14 章 签名和多重签名	116
11.2 解读	89	14.1 源码	116
11.2.1 路由扩展	89	14.2 解读	116
11.2.2 节点路由	92	14.2.1 签名	116
11.2.3 节点保存	94	14.2.2 多重签名	120
11.3 总结	98	14.3 总结	125
11.4 参考	98	第 15 章 交易	126
第 12 章 加密和验证	99	15.1 源码与类图	126
12.1 源码、类图与流程图	99	15.2 解读	128
12.2 概念	101	15.2.1 交易的本质	128
12.2.1 私钥和公钥	101	15.2.2 交易的生命周期	129
12.2.2 加密货币地址	101	15.2.3 亿书的交易类型	129
12.2.3 加密过程	101	15.2.4 交易的基本流程	130
12.2.4 验证过程	102	15.2.5 转账交易分析	136
12.3 实践	102	15.3 总结	141
12.4 总结	104	15.4 参考	141
12.5 参考	104	第 16 章 区块链	142
		16.1 源码、类图与流程图	142