区块链技术丛书

白话区块链

蒋勇 文延 嘉文 著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

白话区块链

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：高婧雅　　责任校对：
印　　刷：　　版次：2017 年 11 月第 1 版第 1 次印刷
开　　本：186mm×240mm　1/16　　印张：
书　　号：ISBN 978-7-111-　　定价：　.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：hzjsj@hzbook.com

前　言

为什么要写这本书

想要写一本综合介绍区块链方面的书，这个想法是从去年年底开始有的，一直以来，关于这方面的资料都很少，能够找到的资料，或着眼于经济金融方面的发展远景，或着重介绍发展历史，或阐述纯技术化的内容，读来总是有一种意犹未尽的感觉，而身边的朋友或对区块链完全陌生，或是有很多误解，还有些朋友甚至简单的认为区块链就等于比特币，笔者也曾多次在一些读书会类似的场合进行些较为通俗的介绍，然而各行各业的朋友们，并非都有完备的计算机知识背景，很多感兴趣的朋友都来自银行、企业财务、人力资源、公务员、投融资等行业，当然也不乏一些希望进入区块链技术开发的程序员。然而即便是用了自认为很通俗的文字和语言来介绍，也难以在短短的一两个小时内讲清楚，各种名词术语、各种新鲜概念，每当他们希望我推荐一些资料的时候，我都很头疼，对于一个还没有广为人知的事物，大家的求知欲是很强烈的，并不满足于囫囵吞枣了解个概念，但也不喜欢去啃枯燥深入的技术文字，他们只是希望能有那么一个系统化的介绍，白话点的，通俗些的，能把每个点都能讲到些，不但是技术原理，还有应用场景、发展历史、当前现状等，都能贯穿起来。鉴于此，想要成这么一本书的想法就愈发强烈了。

自从 2012 年从比特币开始关注区块链技术，一直都只是在一个小范围内的技术圈内进行讨论交流，每每为理解了一个技术概念而欣喜不已，区块链技术绝不仅仅是代表一种数字货币，某种程度上，与其说是一门技术不如说是一类思想或者说是一类价值观，当年比特币的问世把区块链这个火种带入了世人的眼中，以一种“货币”的身份降临，着实带来了不少的神秘感，其带来的理念为后来者所发扬光大，闪电网络、比特股、以太坊、超级账本等，不断冒出各种新的理念和产品，它们都是为了解决某一特定问题以及应用到更多领域而发展起来的，区块链技术的各种特点，分布式、可信任、不可篡改、智能合约等，在与传统技术领域结合的过程中，一定会爆发出巨大的优势，事实上这两年区块链技术的发展可以说是势如破竹，相当的迅猛，国内外都开始有大量的机构或者企业投入研究，力图能够抓住这未来的一米阳光。

这一切，都要从我们全面的了解区块链开始。

本书将给读者一个全方位的视角，从技术到应用以及未来展望，以一个通俗的角度，阐述区块链方面的各个技术点，力求给读者一个通透的理解，并希望能抛砖引玉，为读者拓展

出新颖而有价值的思路。

本书特色

从章节的排序来说，本书由浅入深的从比特币开始，到区块链技术的骨骼（密码算法）和灵魂（共识算法），再到目前知名的系统介绍，到最后从零开始构建一个微型区块链系统，给读者一个由生到熟的渐进过程，对于完全陌生的读者，可以先从章节中的非专业技术部分读起，对于已经有一定基础的读者，可以从中挑选感兴趣的内容。

从内容安排上来说，除了概念原理的介绍，更多的是各种示例以及图表，本书包含不少的示例介绍如比特币的源码编译、以太坊智能合约的开发部署、超级账本 Fabric 的配置使用、模拟比特币的微型区块链系统的设计实现等，阐述过程会使用各种示意图，以形象而直观的方式帮助读者理解各个概念和过程。

行文风格方面，力求白话通俗，避免读者在阅读过程中理解技术概念时的枯燥感，使阅读体验更加舒服一些。

读者对象

- 希望转入区块链开发的程序员
- 希望投资或参与区块链项目的人员
- 对区块链感兴趣的爱好者

如何阅读本书

第 1 章 本书的开篇，介绍了区块链的技术组成，并以比特币为例介绍了各个基础技术原理

第 2 章 综合介绍了目前的各种区块链应用，为后面的技术介绍铺垫场景

第 3 章 介绍了现代密码算法在区块链中的作用

第 4 章 介绍了各种网络共识算法

第 5 章 介绍了区块链的链内外互联扩展技术

第 6 章 详细介绍了以太坊的技术结构以及智能合约开发

第 7 章 详细介绍超级账本项目以及 Fabric 的配置使用

第 8 章 详细介绍如何从零开始设计一个微型区块链系统

第 9 章 介绍了目前出现的各种区块链技术问题

勘误和支持

由于笔者水平有限，编写时间仓促，书中难免会出现一些错误或者不准确的地方，恳请读者批评指正。如果您有更多的宝贵意见，欢迎通过微信或邮件进行讨论。你可以通过微信Cshen003、微博@行者 C 神，或者发送邮件到邮箱 tnix_blockchain@outlook.com 联系到我，我会尽量为读者给出满意的解答，期待能够得到你们的真挚反馈，在技术之路上互勉共进。

致谢

感谢我的作者伙伴——文延和嘉文，他们在工作之余，挤出宝贵的时间为本书贡献了他们对区块链技术的深入理解以及应用的展望分析，他们的专业和敬业令我感到钦佩。

感谢韩璐女士为本书书稿做的审核工作，为本书的内容质量付出了辛勤的劳动。

感谢比特币社区、以太坊社区、超级账本社区以及巴比特论坛各位技术专家的技术文章，每次阅读都有收获，本书也多处引用了他们的观点和思想。

感谢机械工业出版社华章公司的编辑高婧雅，在写作技巧以及内容安排上始终给出恰当的指导，她的编辑效率和敬业精神令我十分钦佩，她的鼓励和帮助引导我们顺利完成全部书稿。

感谢中本聪，是他带来了区块链！

特别致谢

最后，因为工作和写书，牺牲了很多陪伴家人的时间。感谢父母从小对我的培养，他们为我创造了良好的学习环境并培养了我爱好读书的习惯，这个习惯将伴随我终生并受益匪浅。更要感谢我太太王晓英长期以来对我的默默支持，以及女儿 Cindy 对我工作的理解。

谨以此书献给我最亲爱的家人，多年以来帮助、支持我的朋友们，以及众多热爱区块链技术的朋友们！

蒋 勇

目录

第 9 章 潜在的问题 265

后记：区块链与可编程社会 284