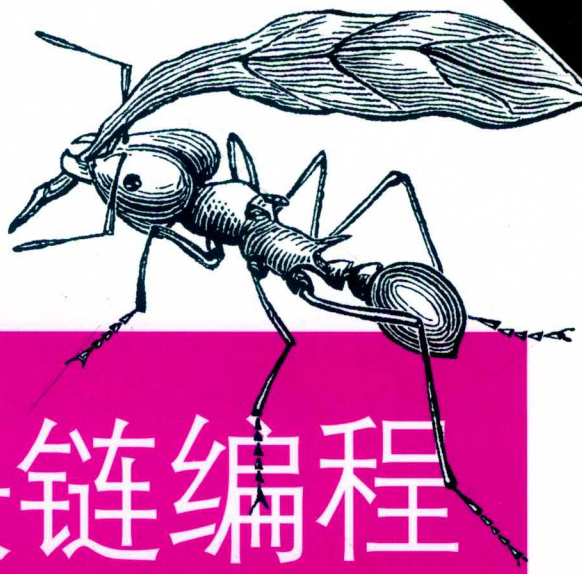
O'REILLY®

原书第2版

HZ BOOKS
华章IT



精通区块链编程

加密货币原理、方法和应用开发

Mastering Bitcoin: Programming the Open Blockchain

[希] Andreas M. Antonopoulos 著
郭理靖 李国鹏 李卓 译
乔延宏 邵周 Higer 审校

机械工业出版社
China Machine Press

精通区块链编程：加密货币原理、方法和应用开发（原书第 2 版）

Mastering Bitcoin: Programming the Open Blockchain, Second Edition

[希] 安德烈亚斯·M. 安东波罗斯
(Andreas M. Antonopoulos) 著
郭理靖　李国鹏　李卓 译
乔延宏　邵周　Higer 审校

Beijing · Boston · Farnham · Sebastopol · Tokyo　O'REILLY®

O'Reilly Media, Inc. 授权机械工业出版社出版

机械工业出版社

图书在版编目（CIP）数据

精通区块链编程：加密货币原理、方法和应用开发（原书第 2 版）/（希）安德烈亚斯·M. 安东波罗斯著；郭理靖，李国鹏，李卓译 . —北京：机械工业出版社，2019.5
（O'Reilly 精品图书系列）
书名原文：Mastering Bitcoin: Programming the Open Blockchain, Second Edition
ISBN 978-7-111-62605-3

I. 精… II. ①安… ②郭… ③李… ④李… III. 电子商务－支付方式－研究
IV. F713.361.3

中国版本图书馆 CIP 数据核字（2019）第 081091 号

北京市版权局著作权合同登记
图字：01-2018-2528 号

书　　名 / 精通区块链编程：加密货币原理、方法和应用开发（原书第 2 版）
书　　号 / ISBN 978-7-111-62605-3
责任编辑 / 陈佳媛
封面设计 / Randy Comer，张健
出版发行 / 机械工业出版社
地　　址 / 北京市西城区百万庄大街 22 号（邮政编码 100037）
印　　刷 / 北京市荣盛彩色印刷有限公司
开　　本 / 178 毫米 ×233 毫米　16 开本　21.5 印张
版　　次 / 2019 年 5 月第 1 版　2019 年 5 月第 1 次印刷
定　　价 / 119.00 元（册）

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
购书热线：(010)68326294
投稿热线：(010)88379604
读者信箱：hzit@hzbook.com

O'Reilly Media, Inc. 介绍

O'Reilly Media 通过图书、杂志、在线服务、调查研究和会议等方式传播创新知识。自 1978 年开始，O'Reilly 一直都是前沿发展的见证者和推动者。超级极客们正在开创着未来，而我们关注真正重要的技术趋势——通过放大那些“细微的信号”来刺激社会对新科技的应用。作为技术社区中活跃的参与者，O'Reilly 的发展充满了对创新的倡导、创造和发扬光大。

O'Reilly 为软件开发人员带来革命性的“动物书”；创建第一个商业网站（GNN）；组织了影响深远的开放源代码峰会，以至于开源软件运动以此命名；创立了《Make》杂志，从而成为 DIY 革命的主要先锋；公司一如既往地通过多种形式缔结信息与人的纽带。O'Reilly 的会议和峰会集聚了众多超级极客和高瞻远瞩的商业领袖，共同描绘出开创新产业的革命性思想。作为技术人士获取信息的选择，O'Reilly 现在还将先锋专家的知识传递给普通的计算机用户。无论是通过书籍出版，在线服务或者面授课程，每一项 O'Reilly 的产品都反映了公司不可动摇的理念——信息是激发创新的力量。

业界评论

“O'Reilly Radar 博客有口皆碑。”

——Wired

“O'Reilly 凭借一系列（真希望当初我也想到了）非凡想法建立了数百万美元的业务。”

——Business 2.0

“O'Reilly Conference 是聚集关键思想领袖的绝对典范。”

——CRN

“一本 O'Reilly 的书就代表一个有用、有前途、需要学习的主题。”

——Irish Times

“Tim 是位特立独行的商人，他不光放眼于最长远、最广阔的视野并且切实地按照 Yogi Berra 的建议去做了：‘如果你在路上遇到岔路口，走小路（岔路）。’回顾过去 Tim 似乎每一次都选择了小路，而且有几次都是一闪即逝的机会，尽管大路也不错。”

——Linux Journal

本书赞誉

我羡慕那些能直接看懂区块链源代码的程序员——他们能感受到区块链的创世之美，而我只能粗浅地理解。我强迫自己反复看比特币 / 以太坊的白皮书，于工作于兴趣，我都希望能够从源头了解区块链，但我不是程序员，只看白皮书，无法深入，更谈不上系统。

恰好碰到本书的出版，读之大有裨益，即使看不懂书中的代码也不要紧，它能帮你建立对区块链的系统性了解。正如纳·斯·穆勒所说“几乎所有新颖和惊人的思索都受到过有系统的粗浅的思想的启发”，更何况此书一点也不粗浅，它生动透彻，不只是适合有志于区块链领域的程序员阅读，也适合我们这种希望对区块链的思想有系统性深入了解的人读，因此郑重推荐。

——西门柳上，容铭投资合伙人，《正在爆发的互联网革命》作者

在我看来，区块链是门杂学，也是件独一无二的艺术品，它巧妙地融合了很多已有的技术，通过密码朋克的精神把自由主义极客紧紧绑到了一起。

这也是我很喜欢和区块链领域开发者打交道的原因，这是一群有着强烈共识并愿意用行动去推动变革的人。这本书会向你阐述这套系统背后的技术、经济和心理逻辑。

——阿秋（刘婧雅），回向基金合伙人

区块链技术的出现，标志人类社会进入了信用记账的阶段，这是社会经济发展的一个里程碑，也是金融科技发展和数字社会的新台阶。区块链的概念最早出现于 2008 年问世的比特币白皮书中，成为比特币产出、记录、流通的基础协议和技术应用。尽管比特币一直以来饱受争议，但其所应用的区块链技术给我们带来的是信用和价值的传递。本书从比特币的基础技术概念、应用、用户和场景解析入门，深入浅出地剖析了区块链行业发展的基础逻辑，具有极强的实操性和指导性。特别适合区块链行业从业者、爱好者作为入门读物。

——Hana Zhang，DAEX Blockchain 合伙人，多家交易平台投资人

译者序

郎咸平说：比特币白给我都不要。

巴菲特说：比特币是泡沫，不是一种能够生产价值的资产。

紫色的股说：为什么说比特币是典型的泡沫？

也有人说，区块链是最伟大的发明，堪比互联网。

那么，比特币到底是什么？难道我们能做的就是人云亦云？

如何能有自己的独立判断？

每个人都有自己的“全知遮蔽”，就像每个人都看不见自己的后脑勺一样。在自己的视野内，在自己的舒适区，如鱼得水，但就是这种感觉最容易让人觉得“自己以为的”就是客观事实。

正确的态度是研究明白，之后才有资格做判断。

本书就能够帮助你全面了解比特币，同时理解其他数字货币。

在翻译过程中得到了 higer（区块链研究社社长）的支持和鼓励，特此致谢。

以下朋友对本书做出了巨大贡献。

菜菜子：翻译了英文版序言、第 2 版更新说明、词汇表、附录 B 等章节。

柴春燕和格林怪物：负责翻译附录 D。

Robbie_ 英语翻译：第 4 章审校。

吴迪：第 5 章和第 9 章审校。

格林怪物：第 6 章审校。

阿龙：第 7 章和第 11 章审校。

阮立志和冯锦炜：第 10 章审校。

琳：第 12 章审校。

黄豆：封面、封底、扉页以及其他内容审校。

由于时间原因和个人能力原因，初稿中有许多格式和理解错误。以上各位朋友在审校过程中修正了初稿中的许多错误，在此深表感谢。

即便如此，当前版本还可能存在部分错误，欢迎读者在 GitHub 上提交勘误，也可以发至邮箱：yuntianming@aliyun.com

译者

2019 年 5 月

推荐序

2008年比特币诞生，它原本只是密码学极客们的一个玩物，没想到慢慢席卷全球。在2008年以前还没有人能够成功地研发出运行良好的数字货币，直到比特币问世；另外，作为比特币的底层技术，区块链在此之前也是无人提及。那么区块链到底有什么魔力，能让整个世界为之疯狂呢？

相信很多初学者都有这样的疑问。我也曾带着这样的困惑翻阅了大量的书籍，然后才有了比较全面的认识。2010年从中科院毕业以来，我一直在农行软件开发中心工作，平时做的主要是一些传统银行核心系统的研发，有时候会觉得枯燥。特别是，2013年互联网金融爆发，直接冲击了银行的传统业务。我并非觉得压力大，而是看到了机会。

那个时候银行业正处于变革的关口，大量的员工和我一样看到了这样的机会，选择出走寻求更好的待遇。正犹豫不决是否要像他们一样选择离开的时候，我看到单位内部的一封邮件里提到了关于研究区块链技术方面的文字。我自身对新技术有狂热，经过一番思量，2016年6月我给总经理发了一封邮件，正式决定从当时枯燥的工作岗位上“出走”，选择进入一个全新的领域，虽然我仍在银行业，但我觉得在一个大的平台上，或许有更好更多的资源让我学习这些新东西。

这是故事的开始，也是区块链研究社（建立之初叫作“区块链研习社”）成立的发端。正是得益于这样的机会，我当时有幸参加了大量的区块链会议，并接触到业内顶尖的区块链专家，从而耳濡目染地慢慢深入。我当时意识到这个群体还很小，整个社会对区块链的了解还远远不够，虽然以前有很多布道者也曾尝试推动区块链技术在国内的发展，但是我决定做一件不太一样的事情——建立一个区块链的学习社群，让所有爱好者能够在这里获得最贴心的区块链知识服务，并形成一个强有力的群体，创造更大的价值和影响力。因此，2017年1月，区块链研习社成立，这是国内最早的区块链学习社群，目前整个群体人数近3000。对于这个社群，我把它当成一份事业来做，至少要做20年。

在带着大家学习的过程中，很多人都会问我一个问题：“从何入手？”我深知理论的学习总是非常必要的，武装了大脑之后才能更好地践行，于是我推荐大家看书学习。而这

里首推的就是本书，可以说它是学习区块链的入门首选，是宝典级的区块链书籍。只不过，比特币经历了几年的发展，也开始出现一些变化，比如进行了隔离见证升级，也分叉出了一个全新的币种BCC，因此第1版的书籍很多地方可能需要更新。

本书译者乔延宏也是我们区块链研究社的核心成员，他多年来都在打磨一个叫作“认知学习法”的学习方法，并尝试将其应用到各种新领域知识的学习当中，效果颇为显著。为此，他还专门成立了一个品牌，叫作“云天明”，希望将此方法传递给更多的人。使用该方法，他快速掌握了区块链知识，并在网络上撰写了30多万字的文章，同时担任本书的第一译者。

刚开始的时候他只是一味地进行翻译，在有限的渠道进行推广，为了坚持，他基本上每天都在进行翻译工作，从而形成了初稿。对于他这种过人的毅力，我非常佩服。不过我觉得，我们应该做一件更有价值的事情——将这些翻译进行充分校订并形成阅读体验良好的中文电子书籍和纸质书籍，供全国的区块链爱好者学习，为我们的国家，为这个世界，更好地普及区块链知识。

为了全力促成此事，我又从人才济济的区块链研究社内部挑选了大量的精英配合乔延宏的翻译和校订工作，这个团队历经多个日夜的苦思琢磨和仔细推敲，最终促成了本书中文版的问世。

相信本书会成为你最好的入门书籍，即便你有了一定的基础，偶尔翻一翻都会有不一样的收获。

现在将这把钥匙送给你，一起打开区块链世界的大门，共创美好的未来吧！

Higer（区块链研究社社长）

2017年11月12日

目录