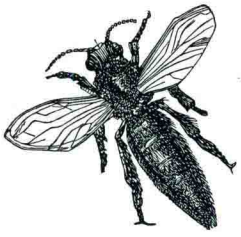
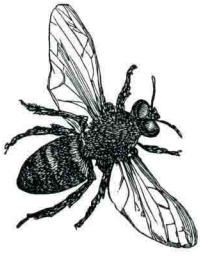
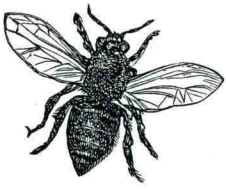
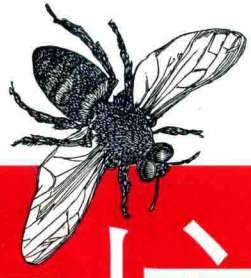
O'REILLY®

HZ BOOKS
华章IT









精通以太坊

开发智能合约和去中心化应用

Mastering Ethereum: Building Smart Contracts and DApps

[希] Andreas M. Antonopoulos,
[英] Dr. Gavin Wood 著
喻勇 杨镇 阿剑 任露露 Elisa Jiang 译
EthFans社区 审校

工业出版社
Machine Press

精通以太坊：开发智能合约和去中心化应用

Mastering Ethereum: Building Smart Contracts and DApps

[希]安德烈亚斯·M. 安东波罗斯(Andreas M. Antonopoulos)
[英] 加文·伍德(Gavin Wood) 著
喻勇 杨镇 阿剑 任露露 Elisa Jiang 译
EthFans 社区 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

精通以太坊：开发智能合约和去中心化应用 /（希）安德烈亚斯·M. 安东波罗斯等著；喻勇等译 . —北京：机械工业出版社，2019.4

（O'Reilly 精品图书系列）

书名原文：Mastering Ethereum: Building Smart Contracts and DApps

ISBN 978-7-111-62492-9

I. 精… II. ①安… ②喻… 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 066640 号

北京市版权局著作权合同登记

图字：01-2019-1171 号

书　　名 / 精通以太坊：开发智能合约和去中心化应用

书　　号 / ISBN 978-7-111-62492-9

责任编辑 / 曲　熠

封面设计 / Karen Montgomery，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 / 三河市宏图印务有限公司

开　　本 / 178 毫米 ×233 毫米　16 开本　23.75 印张

版　　次 / 2019 年 5 月第 1 版　2019 年 5 月第 1 次印刷

定　　价 / 129.00 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

“这是一本非常全面的指南，从区块链的基础知识，到最新的智能合约编程实践，而且两位作者都是区块链领域的知名布道师。”

——Manuel Araoz，Zeppelin CTO

“《*Mastering Bitcoin*》是一本经典的参考书，它使更多的普通人理解了比特币和区块链技术；本书实现了同样的目的，让以太坊和世界计算机的概念变得普及。”

——Lane Rettig，以太坊核心开发人员

“如果你尝试开发自己的 DApp，本书绝对是最好的入门图书！如果你对去中心化网络以及如何构建去中心化的应用程序感兴趣，Andreas 和 Gavin 的这本书为你提供了全面的指南。”

——Taylor Gerring，区块链研究所执行董事

“我有幸阅读了 Andreas 和 Gavin 的这本新书，不得不说，我对它的广度、深度和可读性感到惊讶。它囊括了一切：以太坊的精彩历史、椭圆曲线的数学解释、Solidity 教程，以及关于代币和 ICO 的法律讨论。它有足够的深度，可以作为教学参考资料；同时也有很好的可读性，即使只有初步的数学知识，也能够轻松读懂。在阅读了关于密码学的几个章节后，我觉得我对许多底层密码学概念有了更为扎实的理解。无论你是研究人员、开发者、经理、律师、学生或任何对以太坊技术未来发展方向感兴趣的人，我都强烈建议你将这本书置于自己的书架上。”

——Alex van de Sande，以太坊基金会设计师

“本书将成为未来的必读书，因为以太坊将像 TCP/IP 一样无处不在。它将成为去中心化的基础设施，推动技术的发展和繁荣。”

——Hudson Jameson，以太坊基金会社区组织者

“无论你是想要初步了解，还是尝试深入学习，本书对于关注以太坊的人来说都是一本完美的书。Gavin 熟悉以太坊内部的技术细节，Andreas 善于化繁为简，这本书充分发扬了两方面的优势。我多么希望在刚开始接触以太坊时，就能够读到这本书。”

——Taylor Monahan，MyCrypto 创始人兼首席执行官

推荐序一

区块链技术在最近几年时间里不但获得了大量的媒体关注，其本身的发展速度可能也超出了所有人的想象。人们使用区块链技术不仅仅是因为其技术发展带来的比较竞争优势，而是更多地考虑到这种技术对社区治理和经济生产带来的深刻变革。如果说能源和信息主导了前几次的工业革命，我相信区块链技术也会深深地改变我们生活的这个世界。

谈到区块链技术，一般人首先想到的就是比特币。但是不得不说，比特币无论是在创新的广度还是深度上都和以太坊有差距。从比特币时代开始，人们开始大量关注密码学的实用及落地问题，过去十年密码学的发展超过了以往任何时代，那种繁荣程度让人很难相信过去这只是一个只有少数科学家才关注的领域。椭圆曲线、哈希算法、零知识证明等诸多概念都在区块链的世界里得到了非常切实的实践，共识机制的探讨也如火如荼，与之前图灵奖获得者 Lamport 的寂寞形成了巨大的反差。但这可能只是一个开始，以太坊开启了区块链 2.0 的大门，为区块链提供了实用的计算模型，不但打开了人们对区块链应用的巨大想象空间，也在过去几年的实践当中极大地推动了很多计算机基础科学的进步。比如，智能合约的出现使得形式化验证技术大放异彩，虽然这项技术在理论上并不算新，但在智能合约广泛应用之前并没有什么像样的应用场景。它原本只有非常小规模的应用，在航天或者军工等尖端领域并不能形成广泛的通用技术。但由于智能合约本身传递的价值非常高，又执行在一个不那么可信的环境中，且执行过程是对所有参与者透明的，就使得原本在传统软件业中很微小的瑕疵都能产生灾难性的后果。正是这种严苛的应用场景推动了诸如形式化验证技术的蓬勃发展。再比如，与编程语言相关的虚拟机技术和编译技术，以前都是少数技术极客或者计算机科学家的事。智能合约运行在一个巨大的分布式计算机中，而以前的大部分编程语言也好，虚拟机设计也好，隐含的假设都是在单个计算机系统中运行。因此，出现大量为智能合约设计的新语言和新虚拟机就不足为奇了。我们要看到这种真实需求与理论实践的巨大差异，回想一下科学发展的历史，就会发现有很多类似情形，比如蒸汽机发明之后所带来的工业变革推动了控制理论的建立。也有很多原本在理论上可行的东西终于找到了现实中对应的模型，就好比非

欧几何找到了相对论。不仅仅是类似于零知识证明这样的革命性技术在快速演化，对于技术极客来说，在这个领域中的创新所遇到的唯一限制就是自己的想象力。

我们还不能简单地把以太坊理解为技术的集合。毕竟它拥有全球最大的区块链技术社区，总共大约有35万开发者，而这一数字还在快速增长。以太坊社区处在区块链技术发展的核心位置，即使新技术不是来自这个社区的实践，也会和这个社区产生非常良性的互动。如果我们不能理解这一点，就不能把握区块链发展的方向。目前很多独立的项目，其核心成员都是在以太坊社区做过重要贡献的人。从另外一个角度来说，以太坊是区块链2.0，在区块链1.0——比特币的基础上已前进一步，我们有理由相信，未来的区块链3.0，也就是下一代的革命性技术是来自以太坊社区的。在区块链技术的整个发展过程中，我们看到了技术社区所展现出的巨大生命力，全世界的技术极客热情地投入到共同建设区块链技术的体系当中，而且获得了广泛的商业支持，形成了可持续发展的共赢模式。以太坊社区的开放和包容促进了这种欣欣向荣的局面进一步发展。区块链技术不是一门具体的技术，也不是几种技术简单地拼凑在一起形成的解决方案，而是一个体系非常庞大的技术群落，技术之间相互影响、相互促进。只有在非常强有力的社区的支持下才能形成完整的生态体系，以太坊的技术专业分工的多元社区是我们目前看到的这些技术产生的土壤，这样的土壤也会孕育出更多让人期待的技术创新。

最后，我要说人类对“Trustless”的力量一无所知。大航海时代，人类不仅仅拓展了自己的疆域，对这个世界的认知的改变才是更为重要的。如果我们没有意识到地球是圆的，那么就不会有环球航行，更不会有新的天文观测手段，不会有通过天文观测实现的光速测量方法，也不会有后来的人造卫星等。可能这一切最初的起点就是由于我们纠正了原来局限的认知。只要我们认识到地球是圆的就会有这么多改变，那么我们意识到区块链技术所带来的Trustless体系后，是不是会改变更多？推导出质能方程是一回事，造出核电厂是另一回事。让人改变认知是非常困难的，这也是区块链技术拓展边界的障碍，这个技术太颠覆人们的常识，至少在信任关系上，需要漫长的过程才能获得人类社会的广泛认可。Trustless的力量是无穷的，是我们追求的星辰大海。

程显峰

火币集团CTO

推荐序二

区块链充满魔力，它给我们所在的网络世界带来了非常特别的改变，其本质是——通过数学降低人类的信任成本。

我算是很早就用比特币进行交易的人，由于过去十多年都在安全 / 黑客领域，早期的比特币仅仅作为我用于特殊领域的交易媒介。对于当时的我来说，觉得这很方便，居然有一种支付方式是匿名的，是大家形成共识的。而这种支付方式并不存在中心化监管，是一种去中心化支付方式，底层是数学，是严谨的算法，在这些之上是独特的经济模型，激励着这个网络的发展。这种共识机制被命名为 PoW（Proof of Work），通过消耗大量算力，促进了比特币的价值发展，保证了整个网络的安全稳定。

以太坊借鉴了 PoW 这种共识机制，并有自己在共识机制上的独特发展路线，其中很大的原因在于以太坊本身的定位——在其网络基础上可以快速构建应用，我们称之为去中心化应用（DApp）。DApp 的核心是智能合约，而智能合约运行在一个叫作 EVM 的虚拟机上。可以看到一个分层架构世界的出现。随着这个世界的发展，许多安全问题也在陆续出现，由于我的身份，这是我深入这个世界的最直接驱动力。所幸的是，这些安全事件都未能摧毁以太坊，但却屡次让我们意识到安全是必选项、底线、基础设施。

这个世界的进化出自无数天才之手，站在我的角度来看，如果想做好安全，离不开对方方面面的深入了解。我很乐意看到优秀书籍的出现，包括我有幸作序的这本。希望更多技术人员能沉下心来，探索与创造属于这个世界的特别的东西。我也希望通过自己微薄的力量，给这个世界带来更多的安全感。

余弦

慢雾科技联合创始人

译者序

以太坊和几乎所有数字货币，在过去两年中都经历了过山车一般的暴涨和暴跌。就像是20年前的互联网泡沫，任何技术的发展都要经历这样一个“吹尽黄沙始见金”的过程。

我在2018年冬天去捷克首都布拉格参加了第五届以太坊开发者大会。令人欣慰的是，在整个数字货币市场极为萧条的情况下，大会吸引了超过3000名来自世界各地的开发者和技术爱好者，以太坊在熊市中仍旧维持着顽强的生命力和极高的活跃度，参会的每一位开发者都对区块链技术在未来的广阔应用场景充满信心。在这些五彩缤纷的技术背后，体现的是极客对技术和改变世界的追求，对自由的渴望和向往。

本书的作者之一AA[译注1]是数字货币领域著名的布道师，作为承担过同样工作的人，我深知“布道”对于一项新技术的普及和推广的重要性。我本人对比特币和区块链的认知，绝大部分都来源于AA的那本《*Mastering Bitcoin*》。当得知AA要写一本关于以太坊的著作时，我立刻迸发了要翻译这本书的念头，但是我也深知，翻译是一项非常辛苦甚至还可能“吃力不讨好”的工作，尤其是我这样一个区块链初学者，一不小心就会搞砸一本好书。

幸运的是，在翻译的过程中，我得到了多位好友的帮助，他们帮我分担了部分翻译工作，并解答了我在技术上的一些疑惑。这本书的第1、2、3、5、6、7、10章由我翻译完成，第11、14章和附录A、B由阿剑翻译完成，第8、12章由任露露翻译完成，第9、13章的EVM部分由杨镇翻译完成，第4、13章的gas部分和术语速查由Elisa Jiang翻译完成，吕国宁在翻译过程中提供了技术指导。团队的全体成员共同完成了译稿的润色和校对工作，最后由我统稿。

在此，我向参与本书翻译和校对工作的几位好友表示诚挚的感谢。同时，我也要感谢机械工业出版社对我们的信任，以及在翻译和出版过程中给予的帮助。

喻勇

2019年2月28日

译注1：技术社区对本书作者Andreas Antonopoulos的昵称。

译者简介

喻勇

在技术圈驰骋多年，曾担任过微软技术布道师，VMware Cloud Foundry 生态建设负责人，并有幸引领了国内容器技术的创业浪潮。目前赋闲在家，翻译图书，学习新知。

杨镇

资深软件工程师、区块链布道师，17 年从业经验，对以太坊黄皮书中文版进行了独立校订和增补，是 Solidity 官方文档翻译项目管理员，《深入以太坊智能合约开发》一书作者。

阿剑

EthFans 主编、译者，曾翻译过区块链相关文章共计十万余字。经济学学士，哲学爱好者，古典自由主义者，读书人。

任露露

元熵科技技术总监，Firestack 技术社区联合创始人，R3 CordaLedger Contributor，公链项目 Zilliqa Java SDK 作者，对区块链和微服务技术有深入理解和实践。喜欢养猫。

Elisa Jiang

语言爱好者，2015 年开始着迷以太坊，随后长期为 EthFans 社区输出各类文献的中文译本，累计翻译、校对数百篇文章。

目录