HZ BOOKS
华章IT

**HiBlock社区官方出品，4位区块链技术专家联合撰写**

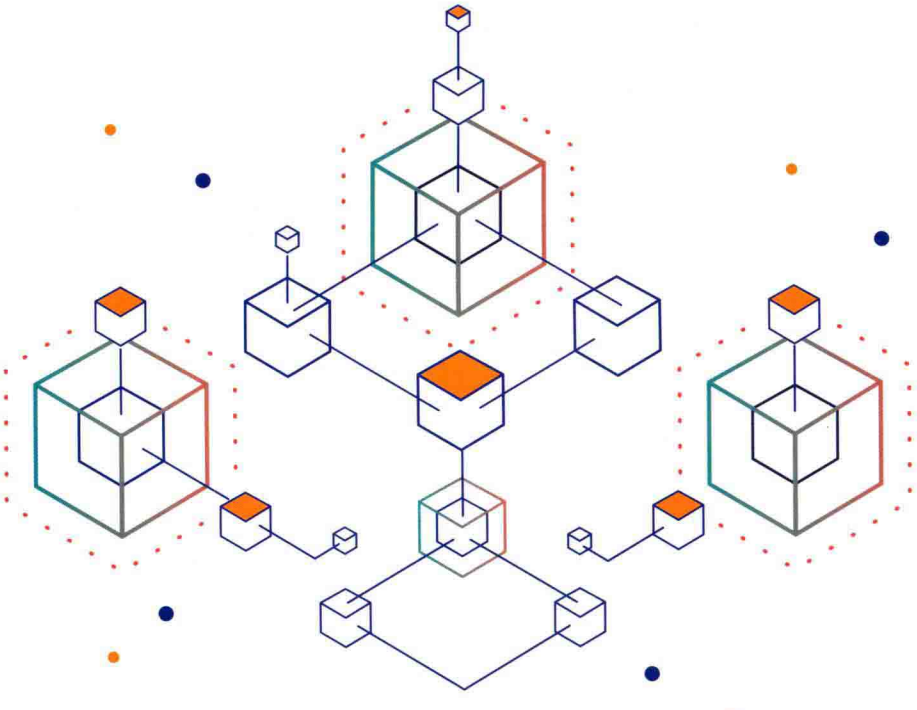
从开发工具与生态、编程语言（Solidity）、编写方法、优秀实践、以太坊虚拟机、合约安全、软件工程、DApp开发等维度全景呈现以太坊智能合约开发

区块链技术丛书

DIVING DEEP INTO ETHEREUM SMART CONTRACT DEVELOPMENT

# 深入以太坊智能合约开发

杨镇 姜信宝 朱智胜 盖方宇◎著



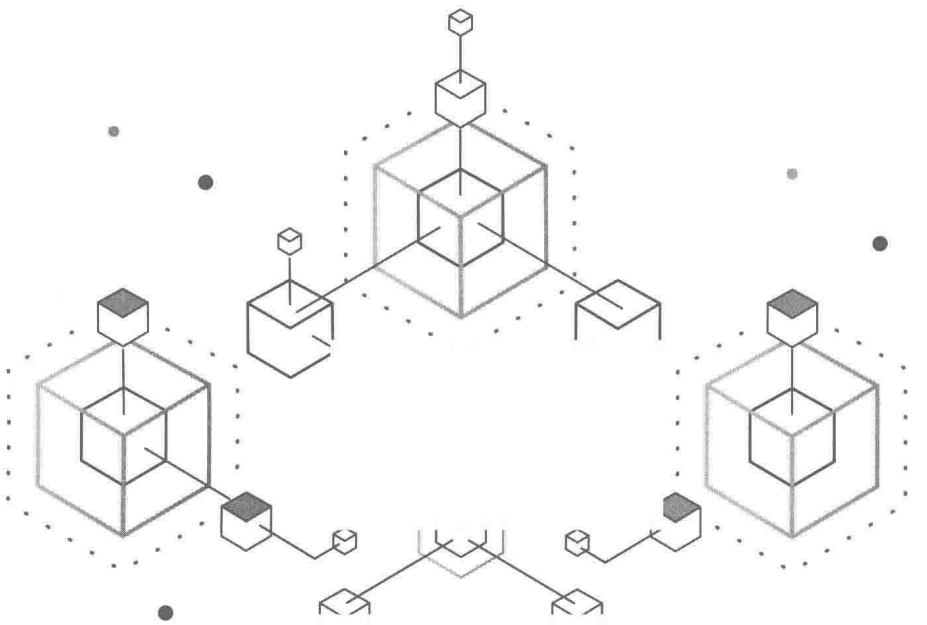
机械工业出版社
China Machine Press

区块链
技术丛书

DIVING DEEP INTO ETHEREUM
SMART CONTRACT DEVELOPMENT

# 深入以太坊智能合约开发

杨镇 姜信宝 朱智胜 盖方宇 ◎ 等



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

深入以太坊智能合约开发 / 杨镇等著 . —北京：机械工业出版社，2019.4
（区块链技术丛书）

ISBN 978-7-111-62372-4

I. 深… II. 杨… III. 电子商务 - 支付方式 - 程序设计 IV. ① F713.361.3 ② TP311.1

中国版本图书馆 CIP 数据核字（2019）第 055852 号

# 深入以太坊智能合约开发

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：孙海亮　　责任校对：李秋荣
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2019 年 4 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：25
书　　号：ISBN 978-7-111-62372-4　　定　　价：99.00 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　　读者信箱：hzit@hzbook.com

华章IT
HZBOOKS | Information Technology

# *Foreword* 推荐序

以太坊开启了一个新的时代，诞生了基于公链的各种智能合约，为互联网信息的 Token 化提供了有效的基础设施。我相信在不久的将来，我们可以通过区块链技术和其他密码学技术来 Token 化和我相关的全部信息，包括“我是谁（我的各种身份标示）”“我有什么（各种价值和权益）”和“我做过什么（我和不同系统、其他人之间的发生过的逻辑）”。有转让价值的信息可以作为区块链 Token 存在，并自动进入一个高效开放的市场。全部的 Token 都可以作为系统集成点，来集成不同的服务，为现有的互联网增加集成能力。

期待着 Tokenise Everything 的那一天，我可以带着 Token 化的社交关系使用 NoFacbook 应用来点赞使用 NoWeChat 应用的朋友的朋友圈，然后语音呼叫几个使用 NoTwitter 的朋友，大家一起约个饭。

期待着 Tokenise Everything 的那一天，我可以对着手机吼一声“重新优化我的投资组合”，手机就会根据我的 Token 了解我的消费习惯、收入情况、家庭情况、社交关系、工作状况等等各种 Token 化的信息，结合我现有的各种 Token 化的投资和高效开放的市场内的各种产品，一个原子化交易同时调用 100 多份智能合约，帮我完成一个只适合我的投资组合。

期待着 Tokenise Everything 的那一天，每个人的手机都是一个完全按照个人定制的集成平台，再也没有复制、粘贴、登录、跳转等步骤。简单提一个要求，手机自动调用多个服务，通过 Token 将这些服务系统集成在一起，一个动作直接完成用户需求。

上述这些的实现，很多都要依赖于智能合约，本书很好地介绍了公链智能合约的基本概念和进阶开发技巧，对于区块链有兴趣的开发人员来说，是一本很好的入门书籍，值得推荐。

——张中南 AlphaWallet 联合创始人 &CEO

# 赞　誉 Praise

本书深入浅出地介绍了区块链 2.0 时代的代表作品——以太坊。全书分为准备篇、基础篇、进阶篇、实战篇，从以太坊的发展历程、基本概念开篇，逐渐深入到 Solidity 智能合约开发语言、以太坊虚拟机等核心内容，既适合初次涉及区块链领域的读者进行概念了解，也适合相关领域的开发者进行以太坊核心技术的学习。本书还对多个通用智能合约进行了源码级分析，着重解读了智能合约安全编码，为想要基于以太坊进行 DApp 开发的读者提供了丰富的开发示例，同时强调了开发过程中必须要注意的安全事项，避免开发者由于缺乏开发安全合约的思维而产生安全隐患。所以说，本书是一本不可不读的书籍。

——戎佳磊 go-ethereum 开发者

我们（EthFans.org）以前在做技术内容的时候，常有面临一些困扰：一方面，以太坊的技术说明文档，尤其是比较前沿的技术说明和开发工具说明，都是用英文写的；另一方面，虽然有不少从事技术翻译的人，但是其中少有一线开发人员，故难免在技术关键点上出现“失之毫厘谬以千里”的情况。

会出现这样的情况，说到底还是因为缺乏一本足够专业和深入的本土入门书籍。这本书一要能讲清楚以太坊底层的运行原理；二要能深入解读 EVM 中的各种方法；三要介绍适合上手的开发工具；四要对合约开发中常见的问题做出说明并提供解决方案。

从我有限的翻译经历和技术理解来看，本书已明确提供了这些内容，并且跟上了最新的技术发展趋势，所以足可称为以太坊中文社区的一座里程碑。

——阿剑 EthFans

相较于比特币，以太坊提供了一套内部图灵完备的脚本语言和虚拟机以供用户来构建任何可以精确定义的智能合约和业务交易。以太坊的出现是区块链领域一次伟大的技术

革新，无论从科研、技术落地还是应用的角度看，都给予广大爱好者启发与帮助。截至2018年年末，以太坊拥有区块链领域最为庞大的开发者社区，同时也获得了最多的关注度，其与IPFS星际文件系统的技术搭配，也被应用于诸多去中心化应用之中。本书便是对以太坊及其智能合约进行了全面且深度的讲解，从入门到进阶再到实战逐层展开。通过阅读本书，读者在短时间内快速掌握核心知识，上手项目。喜爱以太坊技术的读者万不可错过。

——戴嘉乐《IPFS原理与实践》作者

# 前　言 *Preface*

## 为什么要写这本书

笔者其实并不是开源软件的早期拥趸，而是一名在企业 IT 服务领域工作了 16 年的老程序员。大概在 2016 年下半年，因为工作需要，笔者开始研究区块链，开始考虑在企业业务中使用这种所谓的“新技术”。不过因为当时的企业级区块链方面还没有可用的技术平台（Fabric 还不成熟），所以最终没有在具体业务中使用区块链。但也是由于这次对区块链技术的学习，笔者发现了区块链技术的潜力，尤其是发现了以太坊这个项目的潜力，这使笔者受到了很大的触动，笔者感觉自己有可能基于对技术的理解和钻研精神，在这个新领域中获得超出过往十余年所取得的成绩。

笔者在 2017 年用业余时间翻译了以太坊官网的 Homestead 文档，没有用任何翻译软件，完全是自己读原文来将其译为中文的；而后参与了 HiBlock 社区组织的 Solidity 官方文档的中译项目，并很快成为项目的管理员，对中译版做了很多的校订工作，这也是以太坊社区官方的中文版本（以太坊官网上的 Solidity 文档中有对应的链接）。之后就是《以太坊黄皮书》(*Ethereum Yellow Paper*)。《以太坊黄皮书》就是以太坊协议的技术说明文档，里边记载了以太坊协议的几乎全部细节，包括以太坊虚拟机的具体设计。这是一份难得的、经过实践检验的高质量技术文档，对学习以太坊，乃至其他区块链技术都有很高的参考价值。同时《以太坊黄皮书》也是所有以太坊客户端的理论和实现基础。目前业内几乎所有智能合约平台都或多或少地“借鉴”了《以太坊黄皮书》中的设计。

笔者从 2018 年 4 月下旬开始对《以太坊黄皮书》的中文版（最初由猿哥和高天露译）的全文进行独立的校订和增补更新（结合英文拜占庭版本的更新，也没有用翻译软件），到 5 月初最终完成。至此，结合 Solidity 文档中的相关细节，可以说笔者已经掌握了与以太坊协议以及 Solidity 智能合约开发相关的方方面面的知识。在开始写作本书的时候，笔者已经对以太坊协议和智能合约技术有了很深的理解。

## 本书主要内容

本书分为四大部分。

第一部分为准备篇，简单地介绍了以太坊及其相关基本概念，并讲解了以太坊的基本交互和基础工具的使用。

第二部分为基础篇，详细讲解了智能合约开发语言 Solidity 的所有语法和编写合约的基本方法，同时也介绍了对编译器的使用以及 Solidity 集成开发工具的使用。

第三部分为进阶篇，详细讲解了以太坊协议的细节和以太坊协议的核心——以太坊虚拟机的实现原理和相关设计；讲解了用于以太坊虚拟机函数调用的应用二进制编码的细节；对目前最有价值的公共基础合约库 OpenZeppelin-Solidity 的所有源码进行了详细解读；为智能合约安全开发提供了经验性的详细指南。

第四部分为实战篇，结合若干 DApp 实例，讲解了如何基于智能合约来构造可用的去中心化应用程序。

附录中则包含了对以太坊协议中涉及的部分基础算法、以太坊虚拟机的费用设计和指令设计的介绍，以及对 Solidity 内联汇编的简单介绍，可以作为我们进行智能合约开发的参考资料。

如果你是一名了解以太坊基础知识和相关工具使用方法的开发者，那么可以直接从第二或第三部分开始学习。但如果你是一名初学者，或者对以太坊的基本概念和工具还没有了解，请按照本书编排的顺序从第 1 章开始学习。

## 本书尝试实现的目标

本书将尝试引导智能合约开发者深入理解下面的一些问题。

**（1）认识到 Solidity 并不简单**

Solidity 是一种结合了 C++、Python 和 JavaScript 语言创造出来的为智能合约开发而定制的语言，它在事实上简化了智能合约的开发，是一种上手很容易、对初学者“很友好的”开发语言。只要用户稍有编程经验，就可以很快写出一些简单的智能合约。

不过，这种看起来“很简单的”语言，其实并不简单，因为有太多不那么直观的因素会影响 Solidity 程序的运行；而大部分开发者也许并不那么理解智能合约的运行环境——以太坊虚拟机（EVM）——其中存在各种各样的技术细节和各种各样的“大坑小坑”。比如，private 函数和 public 函数在调用时到底有什么不同？仅仅是可见性吗？比如，数据在内存和存储中的结构有什么区别？为什么可以对存储中的动态数组使用 push 和 pop，而对内存中的就不行？比如，fallback 函数是如何运作的？它真的不能接收参数，也不能有返回值吗？比如，transfer、send 和带 value 的 call 有什么区别？又比如，EVM 中复杂的费用设计（尤其是存储的使用费）和 gas 返还机制是如何影响合约的 gas 消耗（也就是运行费用）的？

显然，这些问题并不是我们学习传统的编程语言就可以了解到的，所以对于大多数初学者来讲，这些细节很可能会妨碍他们真正掌握合约开发或者影响他们处理一些相对复杂的逻辑的能力。所以让智能合约开发者真正搞懂 Solidity 与其他开发语言的区别是首要工作。

**（2）不要重复造轮子**

与我们在其他所谓传统软件开发中看到的工程特性一样，在智能合约开发中同样存在“重复造轮子”的问题。同样的基础功能或者非常接近的基础功能，被程序员反复编写，犯各种各样的小错误，这种情况在智能合约开发的初学者中同样普遍存在。那么有没有已经被证明是很好用的、很安全的“轮子”呢？这也是笔者希望给智能合约开发者讲解和普及的一个重要内容。因为笔者从刚刚入行时就非常重视可复用的代码和设计模式，所以学会使用那些经过反复审计的、反复优化的可复用代码，在笔者看来也是非常重要的。

**（3）智能合约并非绝对安全**

这个问题的答案已经众所周知。其实自以太坊诞生以来，各种各样的合约漏洞、安全问题已经多次出现在技术社区，乃至公众视野中。所以合约安全问题早已不是小众的话题。笔者认真搜集并整理了目前智能合约开发中已知的几乎所有合约级别的漏洞或者可能遭受的攻击，希望广大的合约开发者能真正理解这些问题产生的原因并知道相应规避方法。这无论是对开发者本身还是对实际业务安全都极其关键。

**（4）智能合约开发离不开软件工程**

任何软件项目都脱离不了软件工程上的一些基础理论和最佳实践，智能合约开发也不例外。当然，因为智能合约运行环境的特殊性，智能合约开发项目从工程特点上讲与传统软件工程有很大区别。最主要的就是智能合约代码一旦部署就无法更改了，这使我们已经习以为常的冷热修补式的工程实践再无应用可能。我们必须要结合智能合约本身的特性来安排工程活动。笔者也将结合自己 15 年以上的工程经验和对智能合约开发的深入理解为智能合约开发者讲解智能合约开发项目中需要注意的方方面面。

**（5）本书中还有什么**

在以太坊协议中，智能合约的本质就是 EVM 字节码加上合约状态数据所组成的所谓“自主对象（autonomous object）”。所以，内联汇编是我们的终极武器。了解了内联汇编，就知道了智能合约到底都能做什么，不能做什么；因为不管我们用什么高级语言来写智能合约，最终都是要反映为 EVM 字节码的，也就是 EVM 汇编指令，它们就是以太坊智能合约的全部能力。同时，了解 EVM 指令也是进行终极 gas 优化的基础。这些相对高级的话题，也是笔者希望能让更多智能合约开发者了解的。不过这些话题都被编排在附录中，供学有余力的开发者参考。

**（6）写在最后**

与学习其他技术一样，学习智能合约开发是一个艰苦的、需要积累的过程，没有人能一夜之间成为专家。笔者只是希望能将自己学习以太坊和智能合约的大部分收获更快、更有效地传授给后来者，让更多同行真正理解和掌握智能合约开发的要点，但这也同样需要

学习者投入一定的时间和精力。

这是一本给那些和笔者一样关注细节、希望扎扎实实打好基础、讨厌低质量的快餐式学习的同行们打造的，能真正帮助他们提高对智能合约的理解，帮助他们尽快从入门到精通的智能合约开发方面的书。

在开始有写书念头的时候，笔者就很幸运地获得了3位朋友（姜信宝、朱智胜和盖方宇）的支持，并收到了机械工业出版社华章分社的邀请，于是我们4人开始了本书的编写工作。编写工作当然很艰苦，大家都是利用业余时间进行的，所以前后大概经历了5个月的时间。

我们希望本书为以太坊开发者或希望学习以太坊智能合约开发的开发者提供一套系统的、完整的学习和参考资料，帮助他们快速认识、理解和掌握基于以太坊和Solidity语言来进行智能合约开发，乃至DApp开发的实践。本书的附录也可以作为以太坊技术细节的参考手册。

## 本书的特色

本书囊括了开发者基于以太坊平台进行智能合约开发所需要的所有知识细节，由浅入深地讲解了以太坊智能合约开发的方方面面。

本书的基础篇介绍了以太坊智能合约开发语言Solidity的几乎所有语法和语言特性细节，既可以按编排顺序逐步学习，也可以作为工具手册随时查阅。而进阶篇详细介绍了以太坊协议和以太坊虚拟机的原理和相关细节，并对大量经过社区设计、优化的合约源代码进行了详细解读，可以帮助开发者在知其然的基础上知其所以然；同时，进阶篇中也包含了对目前已知的所有针对智能合约的攻击方式的详细介绍和基于智能合约进行工程实践的经验总结，这些都是不可多得的优秀技术资料，有极高的参考价值。

此外，本书的实战篇中还为开发者提供了完整的DApp开发实例，可以帮助开发者快速上手构建基于以太坊智能合约的新一代去中心化应用程序。

本书的附录中则包含了对以太坊虚拟机的费用设计、指令设计以及Solidity内联汇编的介绍，可以作为开发者更深入学习、研究智能合约开发的参考资料。

到本书截稿时，国内还没有一本同类书籍能够像本书一样覆盖以太坊智能合约开发的几乎全部细节，并具有同等的讲解深度和广度。

## 读者对象

本书内容的安排由浅入深，即使没有智能合约开发经验的开发者也可以学习参考。不过，由于本书中并未包括对区块链技术基础（比如分布式网络、密码学等）的详细介绍，需要读者对相关基础知识有一定的了解。

本书适用于以下几类读者：

- 有高级语言（如 C++、Java、Python 等）开发经验的开发者；
- 有计算机软件及相关专业本科及以上学历，且正在从事软件开发工作的开发者；
- 有计算机软件及相关专业本科及以上学历的在校生或应届毕业生；
- 其他有计算机专业基础知识（如数据结构和算法、分布式网络、密码学等），且希望从事智能合约开发的开发者。

## 勘误和支持

由于作者们的水平有限，加之编写时间仓促，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。为此，笔者特意创建一个在线支持与应急方案的二级站点 http://book.blendercn.org。你可以将书中的错误发布在 Bug 勘误表页面中，同时如果你遇到任何问题，也可以访问 Q&A 页面，笔者将尽量在线上为你提供最满意的解答。书中的全部源文件可以从上述二级站点下载，笔者也会将相应的功能更新及时发布出来。如果你有更多的宝贵意见，欢迎发送邮件至邮箱 rivers.yang@icloud.com，期待能够得到你的反馈。

## 致谢

首先要感谢伟大的 Vitalik Buterin 和 Gavin Wood 博士创造了以太坊平台；感谢来自全世界的开源贡献者们将以太坊生态发展丰富到目前的状态；感谢以太坊社区为全球开发者提供的高质量文档和相关资料。本书是站在巨人的肩膀上完成的。

其次要感谢 3 位合作者对本书的付出：其中，盖方宇编写了第 1 章、第 3 章和第 5 章，朱智胜编写了第 2 章和第 11 章，姜信宝编写了第 6 章和第 12 章。没有你们的努力，本书是不可能在这么短的时间内完成的。

感谢机械工业出版社华章分社的编辑杨福川和孙海亮，在这近半年的时间中始终支持笔者和 3 位合作者的编写工作，你们的鼓励和帮助使我们能顺利完成全部书稿。

最后要感谢笔者的父母和笔者的夫人提供的支持。

谨以本书献给笔者最亲爱的家人，以及所有热爱开源、热爱以太坊的朋友们！

杨镇

# Contents 目　录

## 第二部分　基础篇