以太坊
智能合约开发实战

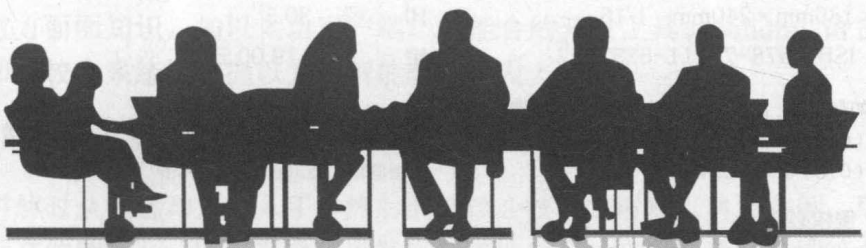
唐盛彬◎编著

资深区块链开发工程师的经验总结，业内7位大咖点评并推荐
从概念、原理、核心技术和应用4个维度，系统介绍以太坊智能合约开发
注重实战，详解100余个智能合约开发示例和2个项目实战案例

机械工业出版社
China Machine Press

以太坊
智能合约开发实战

唐盛彬◎编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

以太坊智能合约开发实战 / 唐盛彬编著. —北京：机械工业出版社，2019.4

ISBN 978-7-111-62371-7

Ⅰ. 以… Ⅱ. 唐… 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057440号

本书从区块链的概念、原理、核心技术和应用四个方面，系统地介绍了以太坊区块链开发的相关知识。其中，重点介绍了以太坊的相关概念和原理、以太坊客户端Geth、以太坊常用智能合约开发工具、Solidity语言和智能合约开发等内容，并介绍了众筹合约和代币合约两个项目实战案例，可以让读者对智能合约开发的整体流程有一个全面的了解。另外，书中结合示例对web3.js的相关知识也做了详细介绍，以帮助读者更好地理解和利用以太坊的相关数据。

本书共17章，分为4篇，涵盖的主要内容有区块链的概念、原理与底层技术；以太坊的相关概念与原理；以太坊相关协议；以太坊客户端Geth；以太坊智能合约的其他常用工具与客户端；Solidity语言的基本概念与数据类型；使用Solidity进行以太坊智能合约开发；通过web3.js与以太坊区块链数据进行交互；众筹智能合约与代币智能合约项目实战案例。

本书内容丰富，讲解通俗易懂，案例典型，实用性强，特别适合区块链技术爱好者和智能合约开发的相关从业人员阅读，也适合区块链底层研究人员阅读。另外，本书还适合区块链培训机构作为相关课程的培训教材。

以太坊智能合约开发实战

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：欧振旭 李华君　　责任校对：姚志娟

印　　刷：中国电影出版社印刷厂　　版　　次：2019 年 4 月第 1 版第 1 次印刷

开　　本：186mm × 240mm 1/16　　印　　张：30.5

书　　号：ISBN 978-7-111-62371-7　　定　　价：119.00 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

前言

区块链技术是当下炙手可热的应用技术。甚至与区块链相关的一些名词，比如数字货币、去中心化应用、比特币和以太坊等也是开发人员经常提及的热门话题，即便不是计算机相关行业的人也可能有所耳闻。而智能合约的出现让人们意识到，区块链技术除了数字货币之外还有更广阔的应用空间。就现阶段而言，要实现智能合约的落地应用，最普及的方式就是通过以太坊智能合约而实现，它有不断完善的生态，也有一些具体的落地项目。可以预见，以太坊智能合约开发技术在未来会有更多的落地应用开花结果。

当前，以太坊区块链的开发还处在一个起步阶段，很多生态还不是很完善，相关工具、库，甚至开发语言本身都还处在不断地迭代之中，而且相关学习资料也比较少。这种情形和当年 Android 开发在国内刚起步时一样。笔者作为一个区块链技术的探索者正行走在这条道路上，觉得有必要把自己的一些经验和心得体会进行总结并集结成册，以帮助那些对区块链技术感兴趣的人，让他们少走一些弯路。这便是笔者写作本书的初衷。

本书主要介绍了利用 Solidity 语言开发以太坊智能合约的相关知识。书中涵盖了区块链与以太坊智能合约的基本原理；智能合约开发环境的搭建；各种开发、集成与测试工具的介绍，以及 Solidity 语言的详细介绍等。相信通过阅读本书，读者能较为系统地掌握以太坊智能合约开发的核心技术与要点。

本书特色

1. 内容全面、系统

本书从区块链的概念、原理、核心技术和应用四个方面展开讲解，涵盖以太坊智能合约开发的方方面面知识，如以太坊客户端、智能合约开发工具、Solidity 语言等，读者通过一本书即可较为系统地掌握以太坊智能合约开发。

2. 讲解由浅入深，循序渐进

本书讲解时从概念和原理入手，然后剖析核心技术，再辅以典型实例，尽量让前文的讲解作为后文的铺垫，一步步带领读者循序渐进地学习。这样的章节安排符合读者的学习和认知规律，学习梯度比较平滑，学习效果更好。

3. 原理与实践相结合

笔者深信，只有通过动手实践，才能加深对知识的理解，所以书中不仅介绍了区块链和以太坊智能合约的相关概念和原理，而且还给出了实现方法和步骤，这样可以让读者真正学以致用，适应职场的要求。

4. 一图胜千言，配合大量图示讲解

本书涉及的概念和基本原理比较多，这些概念和原理比较抽象。为了便于读者直观地理解这些知识，笔者绘制了大量的流程图和原理图帮助读者学习。真可谓一图胜千言，用文字不容易讲解清楚的内容，一幅图就可以直观地展现出来。

5. 案例典型，步骤详细，代码翔实

本书注重内容的实用性，重要的知识点都配合实例进行讲解，而且在最后两章介绍了众筹和代币智能合约开发两个项目案例。书中在讲解这些实例和案例时都给出了详细的操作步骤和实现代码，并对关键代码做了详细的注释，便于读者理解。

本书内容

本书共 17 章，分为 4 篇。

第1篇　基础理论与原理篇（第1~4章）

第 1 章与区块链的第一次亲密接触，主要介绍了区块链的概念和原理，并介绍了区块链中的工作量证明机制、权益证明机制和委托权益证明等内容。

第 2 章去中心化应用——DApp，主要介绍了 DApp 的概念及其优缺点，还介绍了 DApp 如何和中心化应用进行通信。

第 3 章比特币那些事，主要介绍了比特币的公钥格式、私钥格式、私钥的生成和从私钥获取公钥的方法，并介绍了如何从公钥获取地址，以及测试比特币账户碰撞等。

第 4 章以太坊，主要介绍了以太坊涉及的基本概念和原理，如以太坊账户、以太坊交易、挖矿、GHOST 协议、DAG 算法和 Ethash 算法等。

第2篇　开发工具（第5~8章）

第 5 章智能合约开发常用工具，主要介绍了在以太坊智能合约开发过程中会用到的一些工具，如 Git 版本管理工具、Node.js 和 NPM 等。

第 6 章以太坊私链神器——Ganache，主要介绍了在以太坊智能合约开发中需要使用的 Ganache 工具。其中，重点介绍了 Ganache 的图形界面、命令行工具、常用命令和参数，以及如何在项目中使用 Ganache。

第 7 章以太坊官方客户端——Geth，主要介绍了 Geth 的启动命令和参数，借此认识以太坊的各个协议内容。

第 8 章以太坊钱包与浏览器，主要介绍了 MetaMask 浏览器插件的用法。MetaMask 也可以看做是一个轻钱包，可以在开发者构建 Web 应用和以太坊区块链交互时提供帮助。

第3篇　Solidity与智能合约开发（第9~14章）

第 9 章 Solidity 初遇，主要介绍了 Solidity 语言常用开发工具的安装与配置，并对 Solidity 语言的基本概念，如状态变量和局部变量做了详细介绍，另外还对 Solidity 中的运算符、控制结构和函数的常见修饰符（如 payable、view、pure 等）做了必要讲解。

第 10 章 Solidity 数据类型，主要介绍了 Solidity 的数据类型及其应用，如整型中包含的具体类型、各种字面量类型、枚举类型、结构体类型及 mapping 类型等。

第 11 章 Solidity 数据类型进阶，主要介绍了 Solidity 的一些更加复杂的数据类型，如固定大小字节数组、动态大小字节数组、地址类型、函数类型等，另外还介绍了不同数据类型之间隐式转换与显式转换的方法，以及 delete 操作应用于各个数据类型等。

第 12 章 Solidity 开发智能合约，主要介绍了使用 Solidity 开发以太坊智能合约的相关内容，涵盖 EVM 结构和数据、事件与日志、全局以太币和时间单位后缀、区块与交易的全局属性、错误处理函数、数学与 Hash 函数、ABI 编码和特殊类型函数等。

第 13 章 Solidity 开发智能合约进阶，介绍了 Solidity 和智能合约开发的进阶知识，涵盖 Solidity 数据位置与赋值、函数修改器、合约继承，以及 Solidity 的库、编译与编码风格等。

第 14 章通过 web3.js 与以太坊进行交互，主要介绍了如何使用 web3.js 与以太坊智能合约进行交互，给出了 web3.js 和账户、合约、ABI 及 IBAN 交互的多个实例。

第4篇　项目案例实战（第15~17章）

第 15 章工程化项目开发利器——Truffle，主要介绍了如何使用 Truffle 初始化项目、配置 Truffle、编译合约，以及执行部署和测试等。

第 16 章项目流程与众筹实战案例，主要介绍了一个众筹项目案例的实现过程，涉及项目的初始化、目录结构、本地测试及部署环境搭建等相关内容。

第 17 章以太坊代币标准与 ERC20 代币案例，主要介绍了以太坊代币的相关内容，涉及 ERC20 的标准接口和扩展接口，并给出了一个 ERC20 代币实例，还对 ERC20 标准代币的扩展做了介绍。

配书资源及获取方式

本书涉及的源代码等配书资源需要读者自行下载。请登录华章公司的网站 www.hzbook.com，搜索到本书，然后单击“资料下载”按钮，单击页面上的“配书资源”

下载链接即可下载。

本书读者对象

- 区块链技术爱好者；
- 区块链底层开发人员；
- 以太坊智能合约开发初学者；
- 想要系统了解智能合约开发的人员；
- 区块链 DApp 应用开发人员；
- 各类转行做区块链开发的程序员；
- 其他对区块链感兴趣的人员；
- 计算机和金融专业的学生；
- 区块链开发的培训班学员。

售后服务

因受笔者水平所限，加之成书时间较短，本书可能还有疏漏和不当之处，敬请读者指正。读者在阅读本书的过程中若有疑问，请发 E-mail 到 hzbook2017@163.com 和编辑部取得联系。

编著者

目录

第 2 篇 开发工具

第 3 篇　Solidity 与智能合约开发