

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 and 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

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问: 北京大成律师事务所 韩光/邹晓东

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

前言

第1篇 基础理论与原理

| | |
|--------------------|----|
| 第1章 与区块链的第一次亲密接触 | 2 |
| 1.1 什么是区块链 | 2 |
| 1.1.1 区块链简介 | 2 |
| 1.1.2 区块链的链式结构 | 3 |
| 1.1.3 区块链上的区块常见数据 | 4 |
| 1.2 工作量证明机制 (PoW) | 6 |
| 1.2.1 区块链遭遇的问题 | 6 |
| 1.2.2 PoW 模型 | 8 |
| 1.2.3 PoW 为什么能防止篡改 | 9 |
| 1.3 权益证明机制 (PoS) | 11 |
| 1.3.1 什么是 PoS | 12 |
| 1.3.2 PoS 的优势与劣势 | 12 |
| 1.4 委托权益证明 (DPoS) | 12 |
| 1.5 权威证明 (PoA) | 13 |
| 1.6 区块链的应用 | 13 |
| 1.7 本章小结 | 13 |
| 第2章 去中心化应用——DApp | 15 |
| 2.1 DApp 简介 | 15 |
| 2.1.1 什么是 DApp | 15 |
| 2.1.2 DApp 网络组建过程 | 16 |
| 2.1.3 DApp 的优点 | 16 |
| 2.1.4 DApp 存在的问题 | 16 |
| 2.2 中心化与去中心化 | 17 |
| 2.2.1 身份验证 | 17 |
| 2.2.2 通信 | 17 |

| | | |
|--------------|-----------------|-----------|
| 2.2.3 | 数据交互 | 17 |
| 2.2.4 | 系统维护 | 18 |
| 2.3 | DApp 网络与通信 | 18 |
| 2.3.1 | P2P 网络与 WWW | 19 |
| 2.3.2 | P2P 网络拓扑结构类型 | 20 |
| 2.3.3 | 小结 | 21 |
| 2.4 | DApp 货币与中心化数据交互 | 22 |
| 2.4.1 | DApp 货币 | 22 |
| 2.4.2 | 中心化应用获取去中心化数据 | 22 |
| 2.4.3 | 去中心化应用获取中心化数据 | 22 |
| 2.5 | 常见的 DApp | 23 |
| 2.5.1 | 比特币 | 23 |
| 2.5.2 | 以太坊 | 23 |
| 2.5.3 | IPFS 存储系统 | 23 |
| 第 3 章 | 比特币那些事 | 25 |
| 3.1 | 比特币简介 | 25 |
| 3.1.1 | 比特币公钥与私钥 | 25 |
| 3.1.2 | 数字签名 | 26 |
| 3.2 | 椭圆曲线算法 | 26 |
| 3.2.1 | 群 | 26 |
| 3.2.2 | 椭圆曲线算法定义 | 28 |
| 3.2.3 | 椭圆曲线几何运算 | 29 |
| 3.2.4 | 椭圆曲线算法的代码实现 | 30 |
| 3.2.5 | 椭圆曲线加密与签名原理 | 37 |
| 3.3 | 比特币私钥、公钥与地址 | 39 |
| 3.3.1 | 从私钥到地址 | 39 |
| 3.3.2 | 公钥压缩 | 40 |
| 3.3.3 | 私钥格式 | 41 |
| 3.3.4 | 私钥与安全 | 41 |
| 3.4 | 比特币交易 | 44 |
| 3.4.1 | 交易简介 | 44 |
| 3.4.2 | 交易输出 | 44 |
| 3.4.3 | 交易输入 | 44 |
| 3.4.4 | 交易费 | 45 |
| 3.4.5 | 付款至公钥哈希 (P2PKH) | 45 |
| 3.4.6 | 多重签名与 P2SH | 46 |
| 3.5 | 比特币钱包 | 46 |
| 3.5.1 | 钱包简介 | 46 |

| | | |
|--------------|-------------------------|-----------|
| 3.5.2 | 生成助记词 | 47 |
| 3.5.3 | 从助记词生成种子 | 48 |
| 3.5.4 | 从种子生成 HD 钱包 | 48 |
| 3.5.5 | HD 钱包密钥路径 | 50 |
| 3.6 | 比特币相关资源 | 51 |
| 第 4 章 | 以太坊 | 52 |
| 4.1 | 以太坊简介 | 52 |
| 4.1.1 | 什么是以太坊 | 52 |
| 4.1.2 | 以太坊虚拟机 (EVM) | 53 |
| 4.1.3 | 以太坊智能合约与高级语言 | 53 |
| 4.1.4 | 以太币单位 | 54 |
| 4.1.5 | 以太坊发行版本与提案 | 54 |
| 4.2 | 以太坊账户 | 55 |
| 4.2.1 | 外部账户 | 55 |
| 4.2.2 | 合约账户 | 56 |
| 4.2.3 | 外部账户与合约账户的异同 | 56 |
| 4.3 | 以太坊交易 | 57 |
| 4.3.1 | gas、gasPrice 与 gasLimit | 57 |
| 4.3.2 | gasUsed 与交易花费 | 58 |
| 4.3.3 | 什么是以太坊交易与消息 | 58 |
| 4.4 | 以太坊网络 | 59 |
| 4.4.1 | 以太坊网络简介 | 59 |
| 4.4.2 | 以太坊与 Kademlia | 59 |
| 4.4.3 | 以太坊客户端 | 61 |
| 4.5 | 挖矿 | 62 |
| 4.5.1 | 什么是挖矿 | 62 |
| 4.5.2 | 挖矿奖励 | 62 |
| 4.5.3 | 以太坊区块 | 63 |
| 4.6 | GHOST 协议 | 64 |
| 4.6.1 | 区块时间 | 64 |
| 4.6.2 | 区块分叉 | 65 |
| 4.6.3 | 普通分叉带来的问题 | 66 |
| 4.6.4 | GHOST 协议的具体内容 | 67 |
| 4.7 | Ethash 算法之 DAG | 68 |
| 4.7.1 | 什么是 DAG | 68 |
| 4.7.2 | DAG 生成过程 | 69 |
| 4.7.3 | 为什么要使用 DAG | 69 |
| 4.8 | Ethash 算法 | 70 |

| | | |
|-------|-------------|----|
| 4.8.1 | Ethash 算法简介 | 70 |
| 4.8.2 | Ethash 算法流程 | 70 |
| 4.9 | 本章小结 | 71 |

第 2 篇 开发工具

| | | |
|-------|------------------------------|-----|
| 第 5 章 | 智能合约开发常用工具 | 74 |
| 5.1 | Git 简介 | 74 |
| 5.1.1 | Git 安装 | 74 |
| 5.1.2 | Git 常用命令 | 75 |
| 5.1.3 | Git 资源推荐 | 76 |
| 5.2 | Node.js 简介 | 76 |
| 5.2.1 | 什么是 Node.js | 76 |
| 5.2.2 | Node.js 安装 | 77 |
| 5.3 | NPM 简介 | 78 |
| 5.3.1 | npm config 命令 | 78 |
| 5.3.2 | NPM 与语义化版本 | 80 |
| 5.3.3 | npm install 命令 | 82 |
| 5.3.4 | NPM 镜像 | 83 |
| 5.3.5 | NPM 的其他常用命令 | 84 |
| 5.4 | webpack 简介 | 85 |
| 5.4.1 | 认识 webpack | 85 |
| 5.4.2 | webpack 首秀 | 85 |
| 5.4.3 | webpack 与 webpack-dev-server | 87 |
| 5.4.4 | webpack 常用功能与配置 | 90 |
| 5.4.5 | webpack 总结 | 92 |
| 5.5 | Postman 简介 | 92 |
| 5.5.1 | 认识 Postman | 93 |
| 5.5.2 | Postman 的简单用法 | 94 |
| 5.5.3 | Postman 脚本 | 95 |
| 5.6 | LevelDB 简介 | 96 |
| 5.6.1 | 认识 LevelDB | 96 |
| 5.6.2 | LevelDB 文件 | 97 |
| 5.6.3 | SST 结构与数据查找 | 99 |
| 第 6 章 | 以太坊私链神器——Ganache | 102 |
| 6.1 | Ganache 简介 | 102 |
| 6.1.1 | 什么是 Ganache | 102 |

| | | |
|-------|------------------------------|-----|
| 6.1.2 | ganache-cli 命令安装 | 103 |
| 6.1.3 | Ganache 图形界面 | 104 |
| 6.2 | Ganache 常见命令参数 | 106 |
| 6.2.1 | 挖矿时间 | 106 |
| 6.2.2 | 主机端口与网络 | 106 |
| 6.2.3 | gas 相关参数 | 106 |
| 6.2.4 | 其他参数 | 106 |
| 6.3 | Ganache 账户 | 107 |
| 6.3.1 | 能多给我点钱吗 | 107 |
| 6.3.2 | 能多给我几个账户吗 | 108 |
| 6.3.3 | 助记词相关参数 | 108 |
| 6.3.4 | 指定账户 | 108 |
| 6.3.5 | 锁定账户与解锁 | 109 |
| 6.4 | Ganache 与 JavaScript | 109 |
| 6.4.1 | 在工程中引用 Ganache 的 Provider | 109 |
| 6.4.2 | 在工程中启动 Ganache 的 Server | 110 |
| 6.4.3 | 配置工程中依赖的 Ganache | 111 |
| 6.5 | Ganache 交易相关 RPC 方法 | 112 |
| 6.5.1 | eth_sendTransaction 方法 | 113 |
| 6.5.2 | eth_getTransactionCount 方法 | 115 |
| 6.5.3 | eth_getTransactionReceipt 方法 | 116 |
| 6.5.4 | eth_getTransactionByHash 方法 | 116 |
| 6.5.5 | 交易相关的其他方法 | 117 |
| 6.6 | Ganache 账户相关 RPC 方法 | 117 |
| 6.6.1 | eth_accounts 方法 | 118 |
| 6.6.2 | eth_getBalance 方法 | 118 |
| 6.6.3 | eth_coinbase 方法 | 119 |
| 6.7 | Ganache 区块相关 RPC 方法 | 119 |
| 6.7.1 | eth_getBlockByHash 方法 | 119 |
| 6.7.2 | eth_getBlockByNumber 方法 | 122 |
| 6.7.3 | 其他相关方法 | 122 |
| 6.8 | Ganache 日志相关 RPC 方法 | 123 |
| 6.8.1 | eth_newFilter 方法 | 123 |
| 6.8.2 | eth_getFilterLogs 方法 | 124 |
| 6.8.3 | eth_getLogs 方法 | 125 |
| 6.8.4 | 其他关联方法 | 126 |
| 6.9 | Ganache 的其他 RPC 方法 | 127 |
| 6.9.1 | web3_clientVersion 方法 | 127 |

| | | |
|-----------------------------|-----------------------------|------------|
| 6.9.2 | net_version 方法 | 127 |
| 6.9.3 | eth_getCode 方法 | 128 |
| 6.9.4 | eth_sign 方法 | 129 |
| 第 7 章 以太坊官方客户端——Geth | | 130 |
| 7.1 | Geth 简介 | 130 |
| 7.1.1 | Geth 是什么 | 130 |
| 7.1.2 | Geth 安装 | 130 |
| 7.1.3 | Geth 相关目录 | 132 |
| 7.1.4 | Geth 相关工具 | 134 |
| 7.2 | Geth 子命令 | 134 |
| 7.2.1 | Geth 子命令概述 | 135 |
| 7.2.2 | Geth 子命令之 account | 136 |
| 7.2.3 | Geth 子命令之 console 与 attach | 137 |
| 7.2.4 | Geth 子命令之 copydb 与 removedb | 137 |
| 7.3 | Geth 启动参数 | 138 |
| 7.3.1 | Geth 数据同步模式 | 138 |
| 7.3.2 | Geth 网络相关参数 | 138 |
| 7.3.3 | Geth 以太坊相关参数 | 139 |
| 7.3.4 | Geth RPC 相关参数 | 140 |
| 7.3.5 | Geth 挖矿相关参数 | 141 |
| 7.3.6 | Geth ethash 算法参数 | 142 |
| 7.3.7 | Geth 交易池配置 | 142 |
| 7.3.8 | Geth 日志参数 | 145 |
| 7.3.9 | Geth 的其他参数 | 146 |
| 7.4 | Geth 启动实例 | 146 |
| 7.4.1 | Geth 启动单个节点 | 146 |
| 7.4.2 | Geth 启动多节点组网 | 148 |
| 7.5 | Geth 控制台与管理接口 | 149 |
| 7.5.1 | admin 模块 | 149 |
| 7.5.2 | debug 模块 | 150 |
| 7.5.3 | miner 模块 | 151 |
| 7.5.4 | personal 模块 | 152 |
| 7.5.5 | txpool 模块 | 153 |
| 7.6 | keystore 文件 | 153 |
| 7.6.1 | keystore 文件简介 | 153 |
| 7.6.2 | 从密钥到密钥文件 | 154 |
| 7.6.3 | 从密钥到密钥文件流程验证 | 155 |

| | |
|----------------------------------|-----|
| 第 8 章 以太坊钱包与浏览器 | 158 |
| 8.1 MetaMask 插件 | 158 |
| 8.1.1 MetaMask 简介 | 158 |
| 8.1.2 MetaMask 安装 | 159 |
| 8.1.3 第一次使用 MetaMask | 160 |
| 8.1.4 MetaMask 的连接配置 | 161 |
| 8.1.5 MetaMask 的其他配置 | 162 |
| 8.1.6 MetaMask 账户管理 | 163 |
| 8.1.7 MetaMask 交易 | 164 |
| 8.1.8 小结 | 165 |
| 8.2 Ethereum Wallet 钱包 | 166 |
| 8.2.1 Ethereum Wallet 简介 | 166 |
| 8.2.2 安装 Ethereum Wallet 与 Mist | 166 |
| 8.2.3 使用 Ethereum Wallet | 169 |
| 8.3 Mist 与 Ethereum Wallet | 170 |
| 8.3.1 Ethereum Wallet 与 Mist 的区别 | 171 |
| 8.3.2 Mist 的配置与使用 | 171 |
| 8.3.3 小结 | 172 |
| 8.4 MyEtherWallet 网页钱包 | 172 |
| 8.4.1 MyEtherWallet 简介 | 173 |
| 8.4.2 MyEtherWallet 合约交互 | 174 |
| 8.4.3 MyEtherWallet 离线交易 | 175 |
| 8.4.4 MyEtherWallet 的其他功能 | 177 |

第 3 篇 Solidity 与智能合约开发

| | |
|---------------------|-----|
| 第 9 章 Solidity 初遇 | 180 |
| 9.1 Solidity 简介 | 180 |
| 9.1.1 什么是 Solidity | 180 |
| 9.1.2 智能合约示例 | 181 |
| 9.1.3 Solidity 编译版本 | 182 |
| 9.2 Solidity 编辑器 | 182 |
| 9.2.1 Sublime 编辑器 | 182 |
| 9.2.2 Atom 编辑器 | 185 |
| 9.2.3 IDEA 编辑器 | 187 |
| 9.3 Remix 编辑器 | 188 |
| 9.3.1 Remix 简介 | 188 |

| | | |
|-----------------------------|-----------------------|------------|
| 9.3.2 | Remix 文件管理 | 189 |
| 9.3.3 | Remix 编辑面板与控制台 | 190 |
| 9.3.4 | Remix 编译与运行面板 | 191 |
| 9.3.5 | Remix 基本配置面板 | 193 |
| 9.3.6 | Remix 分析配置面板 | 194 |
| 9.4 | Solidity 常见概念 | 196 |
| 9.4.1 | 状态变量 | 196 |
| 9.4.2 | 局部变量 | 196 |
| 9.4.3 | Solidity 函数 | 197 |
| 9.4.4 | 返回多值 | 197 |
| 9.4.5 | 构造函数 | 198 |
| 9.4.6 | 异常 | 200 |
| 9.4.7 | Solidity 注释与文档 | 201 |
| 9.5 | Solidity 运算符 | 203 |
| 9.5.1 | Solidity 运算符简介 | 203 |
| 9.5.2 | Solidity 运算符注意事项 | 204 |
| 9.6 | Solidity 控制结构 | 205 |
| 9.6.1 | 控制结构简介 | 205 |
| 9.6.2 | 判断语句 | 205 |
| 9.6.3 | for 循环 | 206 |
| 9.6.4 | while 与 do...while 循环 | 206 |
| 9.6.5 | continue 与 break | 207 |
| 9.6.6 | 三目运算符 | 208 |
| 9.7 | 可见性修饰符 | 209 |
| 9.7.1 | public 修饰符 | 209 |
| 9.7.2 | internal 修饰符 | 210 |
| 9.7.3 | private 修饰符 | 213 |
| 9.7.4 | external 修饰符 | 214 |
| 9.8 | 函数其他修饰符 | 216 |
| 9.8.1 | constant 修饰符 | 216 |
| 9.8.2 | view 修饰符 | 217 |
| 9.8.3 | pure 修饰符 | 217 |
| 第 10 章 Solidity 数据类型 | | 219 |
| 10.1 | 数据类型简介 | 219 |
| 10.1.1 | 值类型 | 219 |
| 10.1.2 | 引用类型 | 220 |
| 10.1.3 | 小结 | 221 |
| 10.2 | Booleans 类型 | 221 |

| | | |
|---------------|------------------------|------------|
| 10.2.1 | Booleans 类型简介 | 221 |
| 10.2.2 | Booleans 类型支持的运算符 | 221 |
| 10.3 | Integers 类型 | 223 |
| 10.3.1 | Integers 类型简介 | 223 |
| 10.3.2 | Integers 类型支持的运算符 | 224 |
| 10.3.3 | Integers 整除问题 | 225 |
| 10.4 | 定点数类型 | 226 |
| 10.4.1 | 定点数类型简介 | 226 |
| 10.4.2 | 定点数类型支持的运算符 | 227 |
| 10.5 | 字面量 | 227 |
| 10.5.1 | 字符串字面量 | 227 |
| 10.5.2 | 十六进制字面量 | 229 |
| 10.5.3 | 有理数字面量 | 230 |
| 10.6 | Enum 类型 | 231 |
| 10.6.1 | 枚举类型简介 | 231 |
| 10.6.2 | 枚举类型实例 | 231 |
| 10.7 | mapping 类型 | 232 |
| 10.7.1 | mapping 类型简介 | 232 |
| 10.7.2 | mapping 类型实例 | 232 |
| 10.8 | struct 类型 | 233 |
| 第 11 章 | Solidity 数据类型进阶 | 235 |
| 11.1 | Solidity 固定大小字节数组 | 235 |
| 11.1.1 | 固定大小字节数组类型 | 235 |
| 11.1.2 | 固定大小字节数组支持的运算符 | 236 |
| 11.1.3 | 固定大小字节数组的成员 | 236 |
| 11.1.4 | 固定大小字节数组与字符串 | 237 |
| 11.1.5 | 固定大小字节数组之间的转换 | 240 |
| 11.1.6 | 小结 | 241 |
| 11.2 | Solidity 动态大小字节数组 | 242 |
| 11.2.1 | 动态大小字节数组简介 | 242 |
| 11.2.2 | 创建动态大小字节数组 | 242 |
| 11.2.3 | 动态大小字节数组成员 | 243 |
| 11.2.4 | 字节数组间的转换 | 245 |
| 11.2.5 | 小结 | 247 |
| 11.3 | Solidity 数组 | 247 |
| 11.3.1 | 固定长度数组 | 248 |
| 11.3.2 | 动态长度数组 | 249 |
| 11.3.3 | 二维数组 | 250 |

| | | |
|-------------------------------|------------------------------|------------|
| 11.3.4 | 小结 | 251 |
| 11.4 | 以太坊地址类型 | 251 |
| 11.4.1 | 地址简介 | 252 |
| 11.4.2 | transfer、send 与 balance | 254 |
| 11.4.3 | call、callcode 与 delegatecall | 255 |
| 11.5 | 函数类型 | 257 |
| 11.5.1 | 函数类型简介 | 258 |
| 11.5.2 | 函数签名 | 258 |
| 11.5.3 | 函数类型实例 | 260 |
| 11.6 | 数据类型转换 | 262 |
| 11.6.1 | 隐式转换 | 262 |
| 11.6.2 | 显式转换 | 263 |
| 11.6.3 | var 关键字 | 264 |
| 11.7 | delete 运算符 | 265 |
| 11.7.1 | delete 与常见类型 | 265 |
| 11.7.2 | delete 与数组 | 266 |
| 11.7.3 | delete 与 mapping | 267 |
| 11.7.4 | delete 与 struct | 267 |
| 11.8 | 本章小结 | 268 |
| 第 12 章 Solidity 开发智能合约 | | 270 |
| 12.1 | 智能合约简介 | 270 |
| 12.1.1 | 智能合约的概念 | 270 |
| 12.1.2 | EVM 结构与数据 | 271 |
| 12.1.3 | 智能合约执行 | 271 |
| 12.2 | 事件与日志简介 | 272 |
| 12.2.1 | 事件简介 | 272 |
| 12.2.2 | 事件主题 | 272 |
| 12.2.3 | 事件与日志 | 274 |
| 12.3 | Solidity 中的单位后缀 | 276 |
| 12.3.1 | 以太币单位 | 276 |
| 12.3.2 | 时间单位 | 277 |
| 12.4 | 区块与交易属性 | 279 |
| 12.4.1 | 区块的相关属性 | 279 |
| 12.4.2 | 消息的相关属性 | 281 |
| 12.4.3 | 交易的相关属性 | 282 |
| 12.5 | 错误处理函数 | 283 |
| 12.5.1 | assert 函数 | 283 |
| 12.5.2 | require 函数 | 283 |