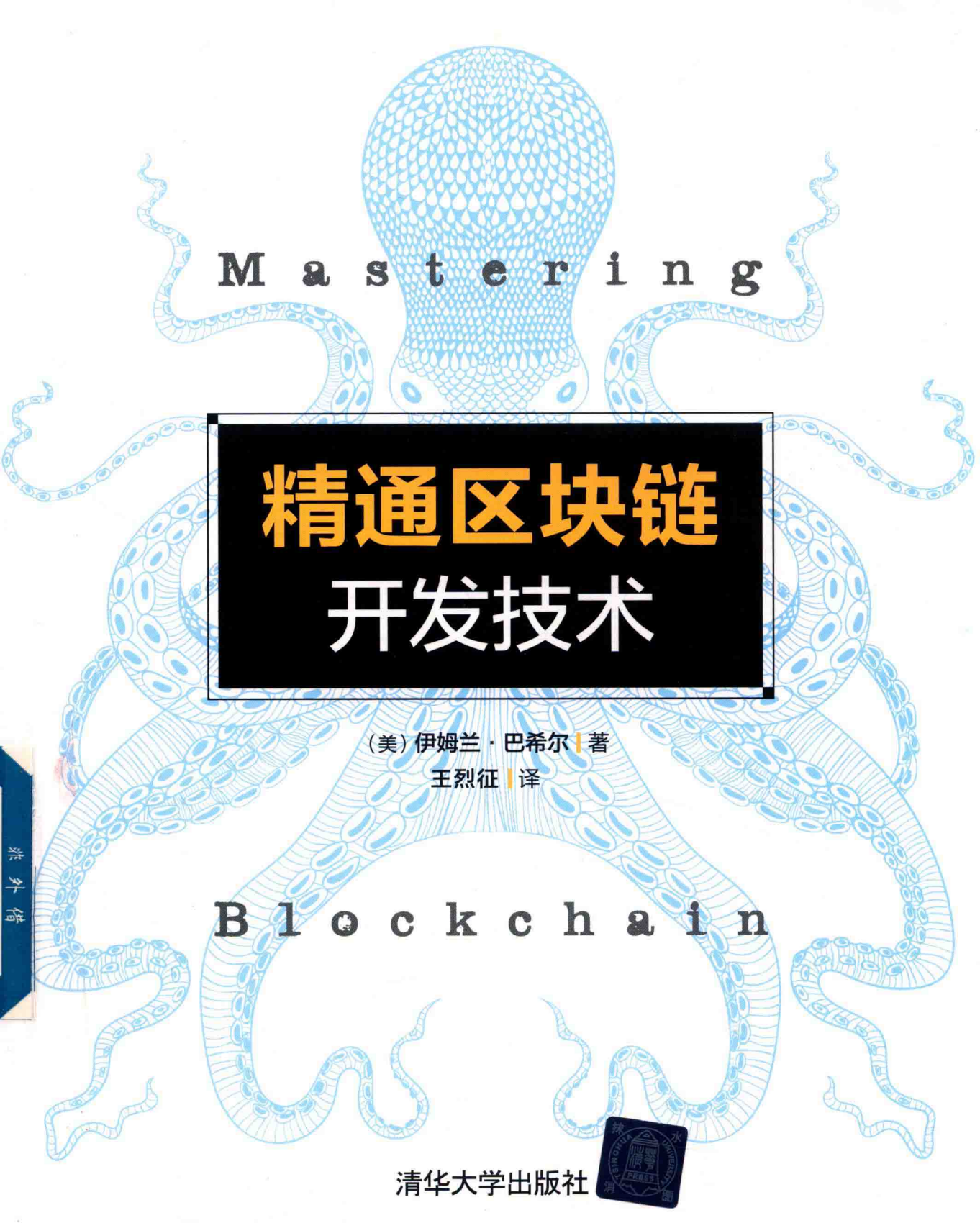




M a s t e r i n g

精通区块链
开发技术

(美) 伊姆兰·巴希尔 | 著
王烈征 | 译

B l o c k c h a i n

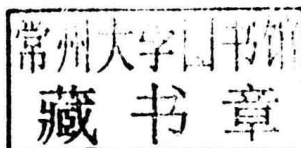
清华大学出版社



精通区块链开发技术

(美) 伊姆兰·巴希尔 著

王烈征 译



清华大学出版社

北 京

内 容 简 介

本书详细阐述了与区块链开发相关的基本解决方案,主要包括区块链、去中心化、密码学和基本技术、比特币、替代币、智能合约、以太坊、超级账本等内容。此外,本书还提供了相应的示例、代码,以帮助读者进一步理解相关方案的实现过程。

本书适合作为高等院校计算机及相关专业的教材和教学参考书,也可作为相关开发人员的自学教材和参考手册。

Copyright © Packt Publishing 2017. First published in the English language under the title

Mastering Blockchain.

Simplified Chinese-language edition © 2018 by Tsinghua University Press. All rights reserved.

本书中文简体字版由 Packt Publishing 授权清华大学出版社独家出版。未经出版者书面许可,不得以任何方式复制或抄袭本书内容。

北京市版权局著作权合同登记号 图字: 01-2017-7182

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话: 010-62782989 13701121933

图书在版编目(CIP)数据

精通区块链开发技术/(美)伊姆兰·巴希尔(Imran Bashir)著;王烈征译. —北京:清华大学出版社, 2018

书名原文: Mastering Blockchain

ISBN 978-7-302-49983-1

I. ①精… II. ①伊… ②王… III. ①电子商务-支付方式-研究 IV. ①F713.361.3

中国版本图书馆CIP数据核字(2018)第069053号

责任编辑: 贾小红

封面设计: 刘超

版式设计: 魏远

责任校对: 马子杰

责任印制: 丛怀宇

出版发行: 清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址: 北京清华大学学研大厦A座 邮 编: 100084

社总机: 010-62770175 邮 购: 010-62786544

投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn

印装者: 三河市君旺印务有限公司

经 销: 全国新华书店

开 本: 185mm×230mm 印 张: 25.5

版 次: 2018年6月第1版

印 数: 1~3000

定 价: 129.00元

字 数: 525千字

印 次: 2018年6月第1次印刷

产品编号: 077465-01

译者序

在阅读本书之前，相信读者已对区块链及其巨大的发展潜力有所耳闻。

2008年，随着比特币的出现，当今世界步入一个全新的概念中，并很有可能引发全社会的变革，同时对各行各业产生深远的影响，其中包括（但不仅限于）金融业、政府部门以及媒体。一些人把区块链描述为一场革命，而另一种思想学派则认为，这将是一种进化，且需要许多年才能从区块链获得实际利益。这在某种程度上是正确的，但我认为变革已经开始了；世界上许多大型机构已经开始用区块链技术来证明这一概念，因为其颠覆性潜力已经得到充分的承认。然而，一些组织仍处于初步探索阶段，但随着技术的成熟，预计将会更快地取得进展。

本书详细阐述了与区块链开发相关的基本解决方案，主要包括区块链、去中心化、密码学和基本技术、比特币、智能合约、以太坊、超级账本等内容。此外，本书还提供了相应的示例、代码，以帮助读者进一步理解相关方案的实现过程。

在本书的翻译过程中，除王烈征之外，黄立臣、周建娟、李秋霞、程晓磊、于鑫睿、张博、刘祎、张骞、李垚、张颖、张弢、刘君、李强、沈旻、李伟、李娇娇、翟露洋、刘洋、蔡辉、王福会、杨崇珉、刘璋、刘晓雪、张华臻等人也参与了本书的翻译工作，在此一并表示感谢。

限于译者的水平，译文中难免有错误和不妥之处，恳请广大读者批评指正。

译者

前 言

本书将全面介绍区块链技术的理论和实践，涵盖了充分理解区块链技术的全部内容。在阅读完本书后，读者将能够深入了解区块链技术的内部工作原理，并具备开发区块链应用程序的能力。本书包含了与区块链技术相关的所有主题，涉及密码学、加密货币、比特币、以太坊，以及用于区块链开发的各种平台和工具。

在阅读本书之前，建议读者具备一定的计算机科学知识和基本的编程经验，但若无经验也并不妨碍读者的学习进程，相关背景知识在书中均有所介绍。

本书内容

第1章介绍了基于区块链技术的分布式计算的基本概念，包括区块链的历史、定义、特性、类型和优点，以及区块链技术的核心内容——共识机制。

第2章介绍了去中心化的概念及其与区块链技术的关系。除此之外，还讨论了相关方法和平台，进而可对处理过程或系统执行去中心化操作。

第3章介绍了密码学的理论基础，这也是全面了解区块链技术的必要条件，其中包括公钥和私钥加密等概念及其应用实例。最后，本章还对金融市场进行了简要介绍，在金融领域，许多有趣的用例均可实现于区块链技术中。

第4章主要讨论比特币，这也是第一个最大的区块链。本章详细介绍了与比特币加密有关的技术概念。

第5章讨论了比特币出现之后的其他替代加密货币，包括各种代币示例、属性以及开发和实现方式。

第6章深入讨论了智能合约，介绍了智能合约的历史、定义、李嘉图合约、Oracle 定义，以及智能合约的理论知识。

第7章详细介绍了以太坊区块链的设计和架构，包括与以太坊区块链相关的各种技术概念，并深入分析了该平台的基本原理、特性和组件。

第8章考查了一个详细的示例，并使用以太坊区块链开发去中心化的应用程序和智能合约。除此之外，本章还讨论了 Solidity 语言和各种相关工具。

第 9 章介绍了 Linux 的超级账本项目，其中包含了不同的区块链项目。

第 10 章介绍了可替代的区块链解决方案和平台，同时还阐述了可替代区块链的技术细节和特性。

第 11 章探讨了区块链技术在其他领域的应用，包括物联网、政府部门、媒体和金融等行业。

第 12 章考查了区块链技术所面临的一些挑战性问题及其解决方案。

第 13 章讨论与区块链技术的现状、项目和研究工作相关的信息。此外，还提出了一些针对区块链技术现状的预测观点。

准备工作

本书中的所有示例都是在 Ubuntu16.04.1 LTS (Xenial) 上进行开发的。因此，建议读者使用 Ubuntu 系统。但这并不意味着排除了其他操作系统，例如 Windows 或 Linux，但相关示例，尤其是与安装相关的操作步骤，可能需要进行相应的更改。

与密码学相关的示例使用 OpenSSL 1.0.2g 1 Mar 2016 命令行工具进行开发。

以太坊的 Solidity 示例则通过 Browser Solidity 予以实现，读者可访问 <https://ethereum.github.io/browser-solidity/> 获取在线资源。

以太坊的 homestead 版本可用于开发相关应用示例，在本书编写时，这也是以太坊的最新版本，读者可访问 <https://www.ethereum.org/> 进行下载。

与物联网相关的示例可通过 Raspberry Pi 工具包进行开发。特别地，可采用 Raspberry Pi 3 Model B V 1.2 创建物联网硬件示例。Node.js V7.2.1 和 npm V3.10.10 则用于下载相关的数据包，并针对物联网示例运行 Node.js 服务器。

Truffle 框架用于智能合约的部署操作，读者可访问 <http://truffleframework.com/> 进行下载。

适用读者

本书适用于希望深入了解区块链技术的读者。另外，本书也可用作区块链应用程序开发人员的参考工具书，同时也可作为区块链技术和加密货币相关课程的教学参考书，以及各种考试和认证的学习资源。

本书约定

代码块通过下列方式设置：

```
function difference(uint x) returns (uint y)
{
    z=x-5;
    y=z;
}
```

代码中的重点内容则采用黑体表示：

```
function difference(uint x) returns (uint y)
{
    z=x-5;
    y=z;
}
```

命令行输入或输出如下所示：

```
$ geth --datadir .ethereum/PrivateNet/ --networkid 786 --rpc --
rpccorsdomain 'http://192.168.0.17:9900'
```



图标表示较为重要的说明事项。



图标则表示提示信息和操作技巧。

读者反馈和客户支持

欢迎读者对本书提出建议或意见，以帮助我们进一步解读者的阅读喜好。反馈意见对于我们来说十分重要，以便改进我们日后的工作。对此，读者可向 feedback@packtpub.com 发送邮件，并以书名作为邮件标题。若读者针对某项技术具有专家级的见解，抑或计划撰写书籍或完善某部著作的出版工作，则可访问 www.packtpub.com/authors。

我们将为每一位本书读者竭诚服务。

资源下载

读者可访问 <http://www.packtpub.com> 并通过个人账户下载示例代码文件。另外，可访问 <http://www.packtpub.com/support>，注册成功后，我们将以电子邮件的方式将相关文件发与读者。

读者可根据下列步骤下载代码文件：

- ☐ 通过个人电子邮件地址和密码登录并注册我们的网站。
- ☐ 选择 SUPPORT 选项卡。
- ☐ 单击 Code Downloads & Errata。
- ☐ 在 Search 文本框中输入书名。
- ☐ 选择本书对应的代码文件。
- ☐ 从下拉菜单中选择本书的购买方式。
- ☐ 单击 Code Download。

当文件下载完毕后，确保使用下列最新版本软件解压文件夹：

- ☐ Windows 系统下的 WinRAR/7-Zip。
- ☐ Mac 系统下的 Zipeg/iZip/UnRarX。
- ☐ Linux 系统下的 7-Zip/PeaZip。

另外，读者还可访问 GitHub 获取本书的代码包，对应网址为 <https://github.com/PacktPublishing/Mastering-Blockchain>。此外，读者还可访问 <https://github.com/PacktPublishing/> 以了解丰富的代码和视频资源。

读者可访问 https://www.packtpub.com/sites/default/files/downloads/MasteringBlockchain_ColorImages.pdf 下载本书的彩色图像，以方便读者对比某些输出结果。

勘误表

尽管我们在最大程度上做到尽善尽美，但错误依然在所难免。如果读者发现谬误之处，无论是文字错误抑或是代码错误，还望不吝赐教。对于其他读者以及本书的再版工作，这将具有十分重要的意义。对此，读者可访问 <http://www.packtpub.com/submit-errata>，选取对

应书籍，单击 Errata Submission Form 超链接，并输入相关问题的详细内容。经确认后，填写内容将被提交至网站，或添加至现有勘误表中（位于该书籍的 Errata 部分）。

另外，读者还可访问 <http://www.packtpub.com/books/content/support> 查看之前的勘误表。在搜索框中输入书名后，所需信息将显示于 Errata 项中。

版权须知

一直以来，互联网上的版权问题从未间断，Packt 出版社对此类问题异常重视。若读者在互联网上发现本书任意形式的副本，请告知网络地址或网站名称，我们将对此予以处理。

关于盗版问题，读者可发送邮件至 copyright@packtpub.com。

对于作者的爱护，我们表示衷心的感谢，并将于日后向读者呈现更为精彩的作品。

问题解答

若读者对本书有任何疑问，均可发送邮件至 questions@packtpub.com，我们将竭诚为您服务。

目 录

第 1 章 区块链	1
1.1 分布式系统	2
1.1.1 CAP 定理	3
1.1.2 拜占庭将军问题	4
1.1.3 一致性	4
1.2 区块链发展史	5
1.2.1 电子现金	6
1.2.2 电子现金的概念	6
1.3 区块链简介	8
1.3.1 区块链技术的各种定义	9
1.3.2 区块链中的一般元素	10
1.3.3 区块链特性	11
1.3.4 区块链技术应用	13
1.3.5 区块链发展层次	13
1.4 区块链类型	14
1.4.1 公有区块链	14
1.4.2 私有区块链	14
1.4.3 半私有区块链	15
1.4.4 侧链技术	15
1.4.5 许可账本	15
1.4.6 分布式账本	15
1.4.7 共享账本	15
1.4.8 全私有和专有区块链	15
1.4.9 标记化区块链	16
1.4.10 无代币区块链	16
1.4.11 区块链中的共识	16
1.5 CAP 定理和区块链	18

1.6	区块链的优点和局限性	18
1.7	区块链技术的限制和挑战	19
1.8	本章小结	20
第2章	去中心化	21
2.1	基于区块链的去中心化	21
2.2	去中心化方法	23
2.2.1	非中介化	23
2.2.2	竞争	23
2.3	去中心化流程	24
2.4	区块链和完整的生态圈去中心化操作	25
2.4.1	存储	25
2.4.2	通信	26
2.4.3	计算	27
2.5	智能合约	28
2.6	去中心化组织	28
2.7	去中心化自治组织	29
2.8	去中心化自治企业	29
2.9	去中心化自治社会	30
2.10	去中心化应用程序	30
2.10.1	去中心化应用程序的需求条件	30
2.10.2	DAPP 操作	31
2.11	去中心化平台	31
2.12	本章小结	32
第3章	密码学和基本技术	33
3.1	简介	33
3.1.1	数学知识	33
3.1.2	密码学	35
3.1.3	保密性	35
3.1.4	完整性	35
3.1.5	认证	35
3.1.6	不可否认性	36

3.1.7 问责制	36
3.2 密码原语	37
3.2.1 对称加密	38
3.2.2 块密码	39
3.2.3 数据加密标准	42
3.2.4 高级加密标准 (AES)	42
3.3 非对称加密	45
3.3.1 整数分解	47
3.3.2 离散对数	47
3.3.3 椭圆曲线	47
3.4 公钥和私钥	48
3.4.1 RSA	48
3.4.2 离散对数问题	54
3.4.3 密码原语	62
3.4.4 哈希函数	62
3.4.5 椭圆曲线数字签名算法 (ECDSA)	71
3.5 金融市场和交易	76
3.5.1 交易	77
3.5.2 交易所	77
3.5.3 交易的生命周期	78
3.5.4 订单预期者	79
3.5.5 市场操控	79
3.6 本章小结	79
第 4 章 比特币	81
4.1 比特币概述	82
4.1.1 比特币的概念	83
4.1.2 密钥和地址	83
4.1.3 比特币中的公钥	84
4.1.4 比特币中的私钥	84
4.1.5 比特币货币单位	85
4.1.6 Base58Check 编码	85

4.1.7 虚地址	86
4.2 交易/事务	87
4.2.1 交易的生命周期	87
4.2.2 交易的结构	87
4.2.3 交易类型	90
4.3 区块链	94
4.3.1 区块链结构	94
4.3.2 区块头结构	94
4.3.3 创始区块	96
4.3.4 比特币网络	103
4.3.5 钱包	109
4.4 比特币支付	112
4.4.1 比特币投资和比特币交易	113
4.4.2 比特币安装	114
4.4.3 比特币编程和命令行接口	120
4.4.4 比特币改进协议 (BIP)	120
4.5 本章小结	121
第 5 章 替代币	123
5.1 理论基础	125
5.1.1 工作量证明的替代方案	125
5.1.2 难度调整和目标重定位算法	128
5.2 比特币中的限制条件	130
5.2.1 隐私和匿名性	130
5.2.2 比特币上的扩展协议	131
5.2.3 替代币的开发	133
5.3 域名币	135
5.4 莱特币	140
5.5 素数币	142
5.5.1 素数币交易	143
5.5.2 挖掘规则	144
5.6 Zcash	145

5.6.1	Zcash 交易	146
5.6.2	挖掘规则	147
5.6.3	GPU 挖掘	150
5.7	本章小结	152
第 6 章	智能合约	153
6.1	发展历史	153
6.2	定义	153
6.3	李嘉图合约	155
6.3.1	智能合约模板	158
6.3.2	Oracle.....	159
6.3.3	Smart Oracle	160
6.3.4	在区块链上发布智能合约	160
6.3.5	DAO.....	161
6.4	本章小结	161
第 7 章	以太坊	163
7.1	简介	163
7.1.1	以太坊客户端和发布	163
7.1.2	以太坊栈	164
7.2	以太坊区块链	164
7.2.1	货币 (ETH 和 ETC)	165
7.2.2	分叉	165
7.2.3	gas.....	166
7.2.4	共识机制	166
7.2.5	世界状态	167
7.2.6	交易	168
7.2.7	合约生成型交易	170
7.2.8	消息调用型交易	171
7.3	以太坊区块链中的元素	172
7.3.1	以太坊虚拟机	172
7.3.2	执行环境	173
7.3.3	操作码及其含义	176

7.4	预编译合同	182
7.4.1	椭圆曲线公钥恢复函数	182
7.4.2	SHA256 位哈希函数	182
7.4.3	RIPEMD160 位哈希函数	182
7.4.4	恒等函数	182
7.5	账户	183
7.6	区块	183
7.6.1	区块头	184
7.6.2	创始区块	185
7.6.3	交易收据	186
7.6.4	交易验证和执行	186
7.6.5	区块验证机制	187
7.7	Ether	189
7.7.1	gas	189
7.7.2	费用标准	190
7.8	消息	190
7.9	挖掘	191
7.9.1	Ethash	192
7.9.2	CPU 挖掘	192
7.9.3	GPU 挖掘	193
7.9.4	挖掘设备	194
7.10	客户端和矿工	196
7.11	贸易与投资	204
7.12	黄皮书	205
7.13	以太坊网络	206
7.13.1	MainNet	206
7.13.2	TestNet	206
7.13.3	专用网络	206
7.14	所支持的协议	207
7.15	以太坊应用程序	208
7.16	可扩展性和安全问题	208
7.17	本章小结	208

第 8 章 以太坊开发	211
8.1 配置开发环境	211
8.1.1 TestNet (Ropsten)	211
8.1.2 配置 PrivateNet	212
8.1.3 启动私有网络	214
8.1.4 在 PrivateNet 上运行 Mist	218
8.1.5 利用 Mist 部署合约	219
8.2 开发工具和客户端	223
8.2.1 开发语言	224
8.2.2 编译器	224
8.2.3 工具和库	228
8.2.4 EthereumJS	230
8.2.5 合约的开发和部署	231
8.3 Solidity 语言	231
8.3.1 值类型	232
8.3.2 字面值	233
8.3.3 枚举值	234
8.3.4 函数类型	234
8.3.5 引用类型	234
8.3.6 映射	235
8.3.7 全局变量	236
8.3.8 控制结构	236
8.4 引入 Web3	241
8.4.1 POST 请求	247
8.4.2 HTML 和 JavaScript 前端	248
8.4.3 开发框架	255
8.5 本章小结	281
第 9 章 超级账本	283
9.1 项目	283
9.1.1 Fabric	283
9.1.2 Sawtooth lake	283

9.1.3	Iroha.....	284
9.1.4	Blockchain explorer.....	284
9.1.5	Fabric 链式工具.....	284
9.1.6	Fabric SDK Py.....	284
9.1.7	Corda	285
9.2	超级账本协议.....	285
9.2.1	参考架构.....	285
9.2.2	需求条件.....	286
9.2.3	隐私和保密性.....	286
9.2.4	身份.....	287
9.2.5	可审核性.....	287
9.2.6	互操作性.....	287
9.2.7	可移植性.....	287
9.3	Fabric.....	287
9.4	Hyperledger Fabric.....	288
9.4.1	Fabric 体系结构.....	288
9.4.2	Fabric 组件.....	291
9.5	Sawtooth lake.....	293
9.5.1	PoET.....	293
9.5.2	交易族.....	293
9.5.3	Sawtooth 中的共识机制.....	295
9.5.4	开发环境.....	295
9.6	Corda.....	298
9.6.1	体系结构.....	299
9.6.2	组件.....	300
9.6.3	开发环境.....	302
9.7	本章小结.....	303
第 10 章	替代区块链方案.....	305
10.1	区块链.....	305
10.2	平台.....	318
10.2.1	BlockApps.....	318