Mastering

精通区块链开发技术

(美) 伊姆兰 · 巴希尔 著
王烈征 译

Blockchain

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。

北京市版权局著作权合同登记号 图字：01-2017-7182

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　　**字　　数：** 525 千字
版　　次： 2018 年 6 月第 1 版　　**印　　次：** 2018 年 6 月第 1 次印刷
印　　数： 1～3000
定　　价： 129.00 元

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，以帮助我们进一步了解读者的阅读喜好。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