HZ BOOKS 华章IT

[PACKT] PUBLISHING

前微软高级技术布道者撰写，Solidity初学者指南

既涵盖Solidity编程的核心概念，又详细讲解智能合约开发、部署、调试的相关技术及工具，帮你从头开始构建以太坊和区块链智能合约

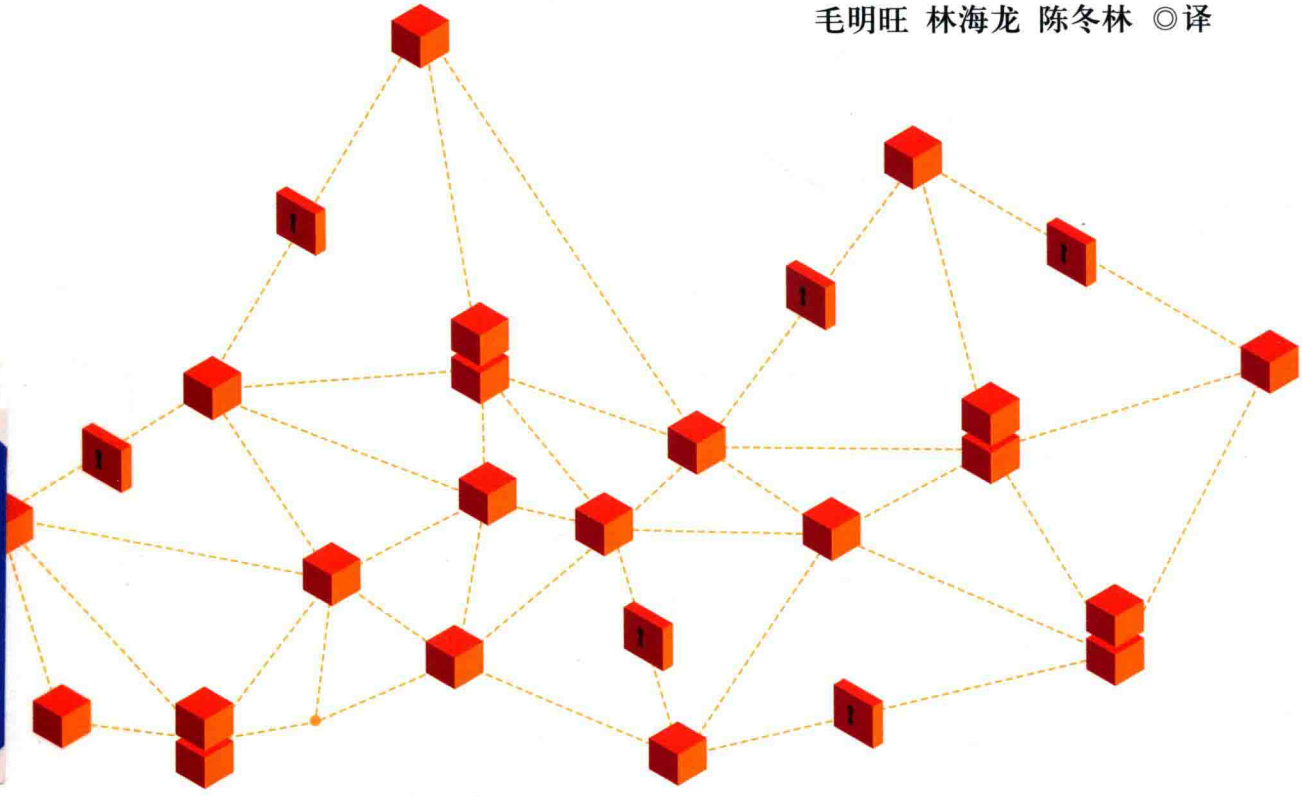
区块链技术丛书

SOLIDITY
PROGRAMMING ESSENTIALS

Solidity编程

构建以太坊和区块链智能合约的初学者指南

[印] 瑞提什·莫迪（Ritesh Modi）◎著
毛明旺 林海龙 陈冬林 ◎译



非外借

机械工业出版社
China Machine Press

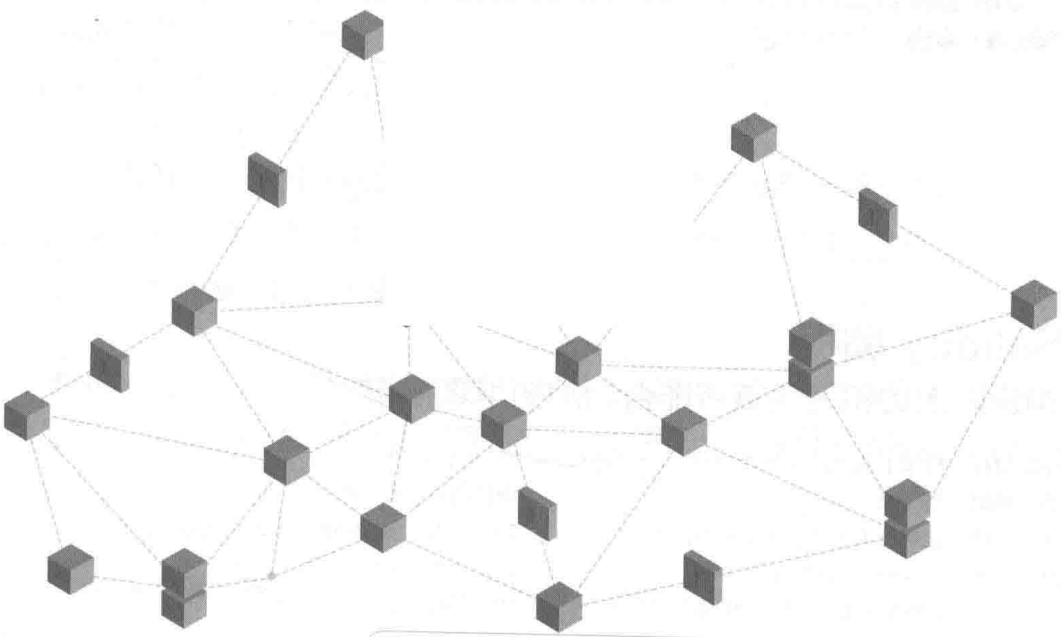
区块链
技术丛书

SOLIDITY
PROGRAMMING ESSENTIALS

Solidity编程

构建以太坊和区块链智能合约的初学者指南

[印]瑞提什·莫迪（Ritesh Modi）◎著
毛明旺 林海龙 陈冬林 ◎译



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Solidity 编程：构建以太坊和区块链智能合约的初学者指南 /（印）瑞提什·莫迪（Ritesh Modi）著；毛明旺，林海龙，陈冬林译 . —北京：机械工业出版社，2019.1
（区块链技术丛书）
书名原文：Solidity Programming Essentials

ISBN 978-7-111-61600-9

I. S… II. ①瑞… ②毛… ③林… ④陈… III. 电子商务－支付方式－程序设计
IV. ①F713.361.3 ②TP311.1

中国版本图书馆 CIP 数据核字（2018）第 287840 号

本书版权登记号：图字 01-2018-6833

Solidity 编程

构建以太坊和区块链智能合约的初学者指南

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：刘 锋 责任校对：殷 虹
印 刷：北京市荣盛彩色印刷有限公司 版 次：2019 年 1 月第 1 版第 1 次印刷
开 本：186mm×240mm 1/16 印 张：12.5
书 号：ISBN 978-7-111-61600-9 定 价：59.00 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 88379649 68995259 读者信箱：hzit@hzbook.com

The Translator's Words 译 者 序

本书从各个方面介绍了如何构建以太坊的智能合约，书中首先介绍了区块链、以太坊和智能合约的核心概念，比如密码学、以太币、gas、区块链和以太坊的架构、以太坊节点、以太坊账户、交易、区块、合约等，随后介绍了安装以太坊和Solidity的一系列工具和环境。

本书各章的主题相对独立，方便时间有限的读者直接钻研感兴趣的章节。对于初学者，我们建议通读本书，在对以太坊、智能合约和Solidity有了一定了解以后，再对某些章节进行详细研究。

Solidity是以太坊官方推荐的智能合约高级编程语言，这门语言受到了C++、Python和JavaScript语言的影响，设计的目的是使程序能在以太坊虚拟机（EVM）上运行。

本书一方面从概念上介绍了Solidity编程语言，比如从以太坊虚拟机、合约、Solidity语法和数据结构等方面进行了阐述，另一方面从编写智能合约的角度进行了阐述，比如创建合约、合约组合、封装、继承、多态、方法覆盖、抽象合约、接口、函数、修改器、fallback函数、异常、事件等诸多方面。最后，介绍了智能合约的测试和调试工具。

本书的几位译者完全是凭借着对区块链和以太坊的热爱以及在中文社区推广以太坊智能合约开发的一腔热情在业余时间完成了本书的翻译工作。由于自身知识和能力所限，翻译中出现不足甚至谬误在所难免，欢迎各位读者批评指正。

希望这本书能够帮助读者通过学习以太坊 Solidity，学习智能合约开发，进入区块链的技术世界！

译者

2018 年 10 月

Preface 前　言

我不太确定上次大量听说关于政府、组织、社区和个人的技术的讨论是什么时候。区块链是一种正在世界各地各种组织中进行详细讨论和辩论的技术。区块链不仅仅是一种有限影响我们生活的技术，而是对我们的生活产生了广泛的影响。不远的将来，区块链将会触及我们生活的方方面面——支付账单，与任何组织进行交易，获得工资，身份认证，教育结果，活动等。这只是开始，我们刚开始了解去中心化的含义及其影响。

我已经在区块链领域工作了很长一段时间，并且一直是加密货币投资者。我是一名技术专家，对比特币非常着迷，因为它架构奇特。我从未遇到过这样优越的思维过程和架构，它不仅解决了经济和社会问题，而且解决了一些技术上未解决的问题，如拜占庭式的一般问题和容错。它在很大程度上解决了分布式计算的问题。

以太坊以几乎相似的方式搭建，当第一次听到并经历智能合约时，我很敬畏。智能合约是在区块链上部署去中心化应用程序并通过自定义逻辑、策略和规则轻松扩展的最大创新之一。

在编写这本书时我心怀愉悦，并真诚地希望你也喜欢阅读和实施 Solidity。

我介绍了很多我的 Solidity 经验，并尽我所能阐述清楚，希望这本书能让你成为更好的 Solidity 开发人员和优秀的程序员。

如果有哪些我可以做的，能够更好地改善你对这本书的体验，我洗耳恭听！

本书目的读者

为了更好地阅读本书的内容，需要计算和编程的基本概念和知识。如果你觉得自己没有这方面的知识，可以通过快速阅读针对初学者的编程书籍来满足基本要求。本书主要面向使用区块链为最终客户和雇主提供高级服务的区块链架构师、开发人员、顾问和 IT 工程师。如果你想在以太坊上编写智能合约解决方案，那么本书对你来说非常理想。如果你已经拥有一些 JavaScript 经验，那么可以帮助你加快学习速度。

本书主要内容

第 1 章介绍区块链的基本原理、术语和行话、优势、尝试解决的问题以及行业相关性。本章将详细解释重要的概念和架构，还将介绍以太坊特有的概念。在本章中，将讨论有关其外部拥有的账户、合约账户、gas 和以太币等概念。以太坊主要基于密码学，你将了解用于创建交易和账户的散列、加解密算法。本章还将详细解释如何创建交易和账户，如何为每笔交易支付 gas，消息调用和交易之间的差异，以及代码存储和状态管理细节。

第 2 章将指导你使用以太坊平台创建私有区块链。以太坊生态系统中的另一个重要工具是 ganache-cli。本章还将介绍如何安装 ganache-cli 并使用它来部署 Solidity 合约，如何安装 Solidity 并使用它来编译 Solidity 合约。你还将安装 Mist，

这是一个钱包，可以与私有链进行交互。Mist 用于创建新账户，部署并使用合约。本章也将介绍交易中的挖矿。Remix 是创建 Solidity 合约的绝佳工具。

第 3 章开始 Solidity 之旅。在本章中，你将通过了解不同版本以及如何使用预编译指令来学习 Solidity 基础知识。本章的另一个重要方面是如何构建智能合约，将从使用重要结构（如状态变量、函数、常量函数、事件、修改器、fallback、枚举和结构体）方面深入讨论智能合约布局。本章讨论并实现任何编程语言中最重要的元素——数据类型和变量，既有简单数据类型也有复杂数据类型，既有值类型也有引用类型，既有存储类型也有内存类型，我们会使用示例说明所有这些变量类型。

第 4 章提供与区块和交易相关的全局函数和变量、与地址和合约相关的全局函数和变量的实现及使用细节。在一系列智能合约开发时，可以非常方便地使用这些内容。

第 5 章教你如何使用 if ... else 和 switch 语句编写具有条件逻辑的合约和函数。循环是任何语言的重要组成部分，Solidity 提供了 while 和 for 循环用于遍历数组。本章给出了循环的示例和实现。必须根据一定的条件中断循环，并根据其他条件继续循环。

第 6 章是本书的核心章节。从这章开始，你将编写真正的智能合约。本章将会讨论如何编写智能合约，如何定义和实现合约，如何使用 new 关键字和已知地址等不同机制创建和部署合约。Solidity 提供了丰富的面向对象机制，本章将深入研究面向对象的概念和实现，如继承、多继承、声明抽象类和接口，以及为抽象函数和接口提供实现方法。

第 7 章展示了如何实现接受输入和返回输出的基本函数，以及仅输出现有状态而不更改状态和修改器的函数。修改器有助于在 Solidity 中更好地组织代码，

并有助于提高合约的安全性和重用合约中的代码。fallback 函数是重要的结构，在函数调用与任何现有函数签名不匹配时执行。对于将以太币发送到合约的情况，实现 fallback 函数也很重要。为了便于理解，将使用示例讨论和实现修改器和 fallback 函数。

第 8 章从合约开发的角度来看是非常重要的。如果出现错误和异常，应将以太币返回给调用者。本章将使用较新的 Solidity 结构（如 assert、require 和 revert）深入解释和实现异常处理，还将讨论 hrow 语句。事件和日志记录有助于理解合约和函数的执行，本章将展示和解释事件和日志的实现。

第 9 章涵盖了 Truffle 的基础知识，你将理解它的概念，创建一个项目并理解项目结构，修改它的配置，通过一个示例了解编写、测试、部署和迁移合约的整个生命周期。测试合约和编写合约一样重要。Truffle 提供了测试框架，但还应该编写测试用例。本章将讨论单元测试的基础知识，使用 Solidity 编写单元测试，并对智能合约执行单元测试。通过创建交易并验证其结果来执行单元测试，本章将展示编写和执行单元测试的细节。

第 10 章将使用 Remix 和事件等多种工具展示如何解决和调试故障。本章将介绍如何逐行执行代码，检查每行代码执行后的状态，并相应地更改合约代码。

阅读本书的前提条件

本书假定你具有编程的基本知识，理想情况下应具备任意脚本语言的背景。本书的大部分内容需要连接互联网和使用浏览器。有些部分需要一台机器来部署区块链特定的工具和实用程序，可以使用云端或本地部署的物理机器或虚拟机器。

下载示例代码

本书的示例代码可以从 http://www.packtpub.com 通过个人账号下载，也可以访问华章图书官网 http://www.hzbook.com，通过注册并登录个人账号下载。

审校者简介 *About the reviewer*

Pablo Ruiz 在过去的十多年中始终接触前沿技术，参与了数十款技术产品的创造。2008 年，他深入参与了移动游戏和应用的创造；之后，他作为顾问在数字空间领域参与了很多项目。2015 ～ 2016 年，他曾担任拉美地区最著名的风险投资基金之一的总监，并为公司从零开始创建了自有的金融科技生态系统。2018 年，在活跃参与了数个 ICO 项目之后，他加入 Polymath 成为副总裁并领导研发了第一个基于以太坊的符合监管要求的证券代币发行平台。

Contents 目　录

第 1 章 Chapter 1

区块链、以太坊和智能合约

最近十多年来，科技和机器计算的生态系统发生了重大的变化。技术创新在多个领域影响显著，从**物联网**（IoT）到**人工智能**（AI），再到区块链（BlockChain），它们中的每一个都具有颠覆产业的力量。当前区块链已经成为最具有颠覆性的技术之一，它将潜在地改变各个行业，并将催生新的业务模式，很多行业将发生巨变。然而，区块链并不是一个全新的技术，它在过去数年间，一直在缓慢而持续地成长。区块链的突然爆发，是由于我们开始越来越多地思考去中心化和分布式应用的问题，它恰好是目前的系统架构转向不可篡改的分布式数据库的一个方案。

在第 1 章中，你将快速学习和理解一些简单的、基础性的区块链和以太坊的知识。我们也会讨论使区块链和以太坊得以运行的重要概念。同时，我们也将简要地涉及智能合约，以及如何使用 Solidity 编写智能合约。

需要注意的是，本章只会简单地介绍一些重要的区块链概念，并没有对其

进行展开叙述，否则单单介绍概念，恐怕就需要一本书才能讲完。因为以太坊是区块链技术的实现，所以，本书中这两个词会互换使用。

1.1 什么是区块链

区块链实质上是一个去中心化、分布式的数据库或账本，具有下列典型特征：

- **去中心化**：简单来说，在网络上一个或多个服务器瘫痪的情况下，应用或服务仍然能够持续地运行，这就是去中心化。服务和应用部署在网络上后，尽管每个服务器都有一份数据和执行程序的副本，但是没有任何一个服务器能够绝对控制数据和程序的执行过程。
- **分布式**：网络上的每个服务器或节点都互相连接在一起，服务器之间是多对多连接，而不是一对一或一对多连接。
- **数据库**：指的是存储持久化数据、用户能够及时从任何地点进行访问的地方。数据库的基本功能是数据存储和检索，同时也提供了一些管理功能，以方便高效地管理数据，如：数据导入和导出，数据备份和恢复。
- **账本**：这是一个会计专业术语。你也可以认为它是一个专门存储和检索数据的地方。账本对银行业而言很有用处。例如，Tom 在他的银行账户上存入了 100 美元，对银行而言，需要在账本上计入一笔贷方金额。未来的某一天，Tom 取回了 25 美元，银行不会直接把 100 美元修改成 75 美元，而是在同一个账本上，新增一笔借方金额 25 美元。从这个例子中可以看出，账本是一种特殊的数据存储方式，它不允许修改历史数据，要改变账户的余额只能通过新增和追加记录来实现。区块链是与账本存在共同特征的数据库，新的数据只能通过追加的方式进行存储，没有任何修改历史数据的可能。这里非常关键的一点就是理解只能通过新增记