区块链2.0实战

以太坊+Solidity编程从入门到精通

黄振东◎著

不做区块链知识碎片的搬运工，成为知识体系应用的区块链大咖！

系统： 囊括区块链4个层次、12个模块、100+个知识点
专业： 5年区块链研究经验，紧盯全球主流区块链开发
深入： 从宏观到微观，从总体到局部，深度解码硬核知识
前沿： 超过40组官方推荐源代码，借鉴主流通用编程案例

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

区块链2.0实战

以太坊+Solidity编程从入门到精通

黄振东◎著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

网络上的各种区块链知识虽然很多，但难以构成体系，本书根据读者的需求，以完整的体系介绍了当前主流的区块链技术。本书从总体出发，介绍了区块链的发展历程、典型应用、在社会生活各方面的应用前景，并进一步深入基础技术层面，详细介绍了区块链技术的各个组成部分，最后介绍了区块链 2.0——以太坊的发展情况和开发编程，引导读者由远及近、从感性到理性、从原理到实践，建立起全面的区块链知识体系，逐步深入地掌握区块链技术，并具备应用以太坊编程语言开发分布式应用程序的初步能力。

本书以全球化的眼光专注于区块链技术的体系搭建，定位高端、专业性强、内容全面、便于实操，既适合金融行业的投资人员研究和掌握区块链的技术与商业价值，也适合想在区块链领域有所发展的创业者学习，还可以作为编程开发人员的参考资料，同时适合想了解区块链技术的大专院校学生作为学习资料。

图书在版编目（CIP）数据

区块链 2.0 实战：以太坊+Solidity 编程从入门到精通 / 黄振东著. —北京：电子工业出版社，2018.10

ISBN 978-7-121-34877-8

Ⅰ. ①区… Ⅱ. ①黄… Ⅲ. ①电子商务－支付方式 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 184612 号

策划编辑：徐　岩
责任编辑：张　毅　　特约编辑：田学清
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：720×1000　1/16　　印张：22.5　　字数：468 千字
版　　次：2018 年 10 月第 1 版
印　　次：2018 年 10 月第 1 次印刷
定　　价：78.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件到 dbqq@phei. com.cn。

本书咨询联系方式：（010）57565805。

前言

从2017年下半年以来，区块链技术在全世界掀起了又一轮高潮，无论是金融行业的从业人员、投资专家，还是普通的股民，甚至从未接触过金融科技的人士，在网络、移动终端上都能感受到区块链的热浪。2018年春节期间，不眠不休的“三点钟投资群”再次点燃了许多人的热情。更不用说各种虚拟货币的币值剧烈波动，吸引了大量的资金投入进来。在全社会各个阶层的人们越来越多地投入区块链领域时，各个国家和地区也在加强对区块链的监管，比如中国央行等7部委在2017年9月4日专门出台政策规范区块链领域的融资乱象，2018年1月中国央行再次强化对区块链领域虚拟货币的监管政策。进入2018年中期，区块链带给全社会的热潮逐渐退去，虚拟货币的币值也逐步向价值回归，在这一轮炒作过去之后，区块链留给我们的更多的是思考和行动。

毋庸讳言，区块链技术是一种具备强大生命力的、可以改变现有商业规则的新技术。在一波又一波的热潮洗礼下，许多人了解到区块链的一些特点，如去中心化、分布式账本、不对称加密及无法篡改等，也能说出一些基本道理。但是如果再深入思考：到底什么是区块链技术？它的技术架构和技术体系是怎样的？面对这样体系化的问题，人们如果仅凭自己从社交媒体上获得的关于区块链的碎片式知识，那么显然是难以回答的，进而也难以在认知上建立起体系化的区块链知识结构。

另外，从2009年1月比特币的首次出现到现在，区块链技术进入人类社会已经过去了近10年，这期间虽然有所曲折，但区块链技术在全球总的发展态势还是在向人们生活的各个层面不断深入。以软件版本进行类比，区块链已经走过了1.0阶段，区块链2.0也已经成为很多从业人士的日常工作内容，区块链

3.0 正在向普通人走来。在这样一个时点上，如果想要了解区块链，除从原理和基础知识方面来掌握以外，更重要的还是要进入操作层面，从区块链 2.0 的以太坊应用开发入手，在具体实践中获得对于区块链的全新认知。正如古语有云：纸上得来终觉浅，绝知此事要躬行。

从这一角度出发，本书首先选择了“体系化的知识结构”和“可操作性的开发指南”两个层面，为读者构建了区块链的知识体系，包括区块链的总体架构、发展历程、系统构造、基础技术等方面的内容，让读者对于区块链技术建立一个从宏观到微观的总体结构性认知；然后引领读者转入对区块链 2.0——以太坊的深入了解过程，在区块链公有知识的基础上认识以太坊的独特之处，并由此进入对以太坊主流语言 Solidity 的介绍，在了解了 Solidity 语言的基础知识之后，以鲜活的编程实践引导读者灵活运用 Solidity 语言开发出自己需要的区块链分布式应用（DApp）。

区块链是一项前沿的金融科技，为此，本书坚持全球化的视野，很多内容直接采用欧美区块链行业的信息，在编程开发的案例中也选用更新日期最近的开发案例，突出地展示了本书注重时效性、紧盯科技前沿的鲜明特点。在写作方式上，本书采用了大量的图表，以图文并茂的方式增强可读性；全书行文朴实自然，力求表述准确，让读者可以清晰地掌握区块链这种具备较强数理特性的技术。

总之，关于区块链，我们已经讨论了很多，现在是时候进入操作阶段了。

因受作者水平和成书时间所限，本书难免存在疏漏和不当之处，敬请指正。

本书特色

1. 内容全面、结构清晰，有助于读者建立对区块链的系统性认知体系

本书系统而全面地介绍了区块链技术的知识体系，从宏观到微观、从总体到局部、从感性认知到理性知识，有利于读者建立全面的区块链知识体系，不再局限于碎片式阅读产生的点状知识图，符合人们从浅层学习提升到深入思考的要求。

2. 行文朴实自然、表述准确，有利于促进读者对区块链技术的理解

本书介绍的区块链知识体系、原理，以及采用以太坊编程开发的内容都采用朴实自然的语言，在兼顾专业性、准确性的前提下，尽量做到行文通俗易懂，以便于读者阅读和理解，提升对于区块链的掌握水平。

3. 充分使用图表方式，将抽象事物形象化

由于区块链技术是一种数理性较强的技术，因此本书在介绍一些过于专业的知识点时，使用大量的图表来补充说明，通过这种方式使原本专业性很强的知识或信息转变为清晰、易理解的内容，增强了本书的可读性。

本书内容及体系结构

第 1 章　区块链基础

本章从宏观方面对区块链技术进行“空间扫描”，为读者呈现了区块链技术的总体图像，解释了区块链的定义，回顾了区块链技术在全球的发展历程和现状，着重介绍了区块链在中国的发展现状及发展前景。

第 2 章　区块链的商业价值

本章以区块链在国内商业环境下的 5 个典型行业——银行业、电子商务、法律行业、影音娱乐和媒体行业、医疗行业的商业价值，分析了区块链对于解决当前这些行业“痛点”、提升效率的价值，点明了区块链的商业价值。

第 3 章　区块链技术原理

本章首先介绍了区块链技术最成熟应用——比特币的技术原理、组成部分和运行机制，由此提炼并引申介绍了区块链的技术原理、系统框架、分布式网络等基础原理。

第 4 章　区块链共识机制

本章介绍了区块链技术最重要的运行机制——共识机制，并逐一介绍了当前主流的 3 种共识机制的详细情况。此外，还介绍了区块链在不同规模等级下

的 3 种区块链类型，以及各自的应用案例。

第 5 章　区块链数据结构

本章介绍了区块链的数据结构、区块链技术所依赖的核心算法——哈希算法，并深入介绍了区块链不对称加密所用的椭圆曲线加密算法，在此基础上介绍了区块链的运行机制，以及怎样对区块中的数据进行解读。

第 6 章　以太坊

前 5 章为读者搭建了区块链技术的总体了解和完整体系，从第 6 章开始将深入区块链 2.0 的世界，对以太坊区块链进行深入的讲解。本章介绍了以太坊的创立和发展过程，并着重介绍了以太坊的各项技术原理。

第 7 章　以太坊应用开发基础

为了促进读者对于以太坊的实践应用，本章聚焦于介绍以太坊应用开发基础，主要介绍了 5 种常见的以太坊应用开发环境，对每种应用开发环境则介绍了其搭建的具体操作过程。另外，本章还引入了对主流以太坊编程语言——Solidity 语言的初步介绍。

第 8 章　Solidity 开发基础

本章介绍了 Solidity 语言的各种基础知识，为读者应用 Solidity 语言进行分布式应用开发打下了坚实的基础。主要介绍了 Solidity 语言的 17 种数据类型和 10 种控制结构，还着重介绍了以太坊合约和 Solidity 汇编过程，其中以太坊合约是区块链分布式应用（DApp）的核心要素。

第 9 章　采用 Solidity 语言开发以太坊游戏

本章介绍了一个采用 Solidity 语言开发以太坊游戏的案例，以此来引导读者灵活应用 Solidity 语言的各种基础元素开发自己的应用程序。其中介绍了以太坊游戏的特点、开发准备，还介绍了以太坊游戏 Influence 的代码框架，并对其主要源代码进行了分析和解读。

本书读者对象

- 从事区块链项目投资的各类投资机构从业人员。
- 希望进行区块链应用开发的软件开发人员。
- 希望利用区块链开发创新业务的金融机构从业人员。
- 大专院校金融或互联网科技等相关专业的学生。
- 从事区块链研究的专家学者。
- 其他对区块链感兴趣的各类人员。

目 录

chapter ONE

第1章

区块链基础

区块链已经成为全球范围内的热点。许多人可能被周围环境所影响，看到了大量的资金、人才、信息和资源在向区块链领域集中，或者从社交媒体上感受到了区块链领域追求发展的急切氛围，但是对于什么是区块链这样的基础性认知反而并不清晰。在此，我们先对区块链领域进行一次“空间扫描”，建立起对区块链领域的总体认识。

1.1 什么是区块链

2018年，距离2008年的全球金融危机已经过去了10年。10年以来，随着科技的发展，以互联网、人工智能（Artificial Intelligence，AI）为代表的金融科技（FinTech）蓬勃发展，人类似乎找到了避免全球金融危机的新方法。但是很多专家预计，只要以银行为中心节点的金融体系架构没有发生根本性的转变，危机仍将在未来某个时点再度前来，尽管我们可以有更多的应对之道。

探寻全球金融危机产生的根源，人们逐渐认识到：中心化的全球金融环境是危机产生的根源，只有从根源上解决危机产生的机制，才能够真正引领人类的发展进入新的阶段。在这方面，2009年伴随着比特币而诞生的区块链技术成为人类新金融、新发展的基础性思维，它彻底颠覆了金融系统数百年来固有的