区块链2.0

区块链精学书丛

赵其刚 陆斌 赵其国 编著

以太坊应用开发指南

一本书让你读懂区块链；

全面讲解以太坊技术原理、应用开发与核心创新；

深度解析经典应用案例“虚拟币”、众筹、去中心化自治组织等

智能合约的开发、编译、部署与应用。

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

区块链2.0

以太坊应用开发指南

赵其刚 陆斌 赵其国 编著

人民邮电出版社

北京

图书在版编目（CIP）数据

区块链2.0 : 以太坊应用开发指南 / 赵其刚, 陆斌, 赵其国编著. -- 北京 : 人民邮电出版社, 2018.7
ISBN 978-7-115-48483-3

Ⅰ. ①区… Ⅱ. ①赵… ②陆… ③赵… Ⅲ. ①电子商务－支付方式－研究 Ⅳ. ①F713.36

中国版本图书馆CIP数据核字(2018)第095142号

内 容 提 要

本书主要介绍区块链第二代技术主导平台“以太坊”的应用开发方法。第 1 章主要讲解区块链的概念、发展历程、区块链的应用本质及思维模式；第 2 章主要讲解以太坊的技术原理、体系及其他重要基本概念；第 3 章主要讲解以太坊的安装、网络的配置及应用开发环境的搭建；第 4 章主要讲解以太坊应用开发的接口方式；第 5 章主要讲解以太坊的核心创新——智能合约的开发、编译、部署与应用；第 6～8 章主要讲解以太坊的经典应用案例、众筹的技术特征及去中心化自治组织等智能合约的创建思路、原理与源码。

本书主要面向有志于从事区块链研究，特别是以太坊应用开发的相关技术人员、管理人员及兴趣爱好者，同时可作为本科生、硕士研究生等学生学习与研究区块链技术的参考书籍。

◆ 编　　著　赵其刚　陆　斌　赵其国
责任编辑　李　莎
责任印制　马振武

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷

◆ 开本：700×1000　1/16
印张：15.25
字数：194 千字　　2018 年 7 月第 1 版
印数：1 – 2 500 册　　2018 年 7 月河北第 1 次印刷

定价：59.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

前言 PREFACE

当我第一次听到“区块链”这个词的时候，非常好奇怎么会有这么一个古怪的名字。在查阅相关资料，了解这个词背后的含义时，我也仅有如下模糊的印象：区块链是比特币背后的一种技术，相较于“人工智能”“深度学习”“大数据”“工业4.0”等目前流行的新技术，这是很让人费解的一个技术概念。

2017年年初，在四川奥游创世科技公司的推动下，我们研究院和奥游公司合作成立了“区块链技术研究中心”，开始了我们团队对区块链技术的深入研究。在推进区块链技术研发的过程中，我们深感国内有关区块链实践资料的匮乏，目前市场上可见的区块链书籍多以概念、理论为主，而网络上所查找的资料又过于零碎。为指导研究中心技术人员的技术开发工作，同时也为了帮助广大区块链技术研究“新人”避免一进入这个领域就迷失在繁杂、新奇的技术术语中，我们觉得很有必要把我们所知道的，以及我们实践所得的各种区块链项目开发经验进行系统总结，帮助技术人员快速熟悉区块链技术概念并展开相关的应用开发。我们以此为动力开始了本书的编写。

在区块链技术资料的分析研究中，有几个问题一直在我的脑中萦绕：“我们为什么需要区块链？”“区块链的本质是什么？”“区块链适用于哪些地方？”对这几个问题的正确理解无疑有助于人们消除对区块链的过度追捧，并能在适当的时间、适当的场景选用合适的区块链解决方案，既

不轻忽其意义，又不盲目认为其无所不能。

“区块链绝对不是为计算效率而生。”这是应用区块链的一大禁忌。基于P2P网络，大盘的网络节点保存同一份数据，执行同样的运算，而且浪费大量电力去解与计算结果几乎毫无关系的数学难题，这其实是低效的甚至是浪费的。因此，如果想追求高效计算的场景和计算成本极度敏感的场景，看到区块链还是绕道而行吧。

但为什么需要区块链呢？要回答这个问题，可以从了解区块链的技术体系开始。以代表着当前区块链先进技术架构与体系的区块链二代技术——以太坊为例：以太坊通过6层技术体系，以非对称加解密、散列计算为基础，确保同一网络的区块数据的唯一性、一致性与不易篡改性；以P2P协议为基础，在没有中心化平台的参与及在节点自由进出的环境下，实现网络中所有节点数据的同步和相互服务，并确保不依赖于中心平台网络的可靠性与稳定性；通过复杂和高成本的共识与激励机制，保证新封装进链的区块数据的唯一性与高可靠性。

以太坊通过这么多复杂技术、机制的集中应用，采用如此高昂的计算代价究竟解决了什么问题呢？分析以太坊基础网络各层技术方案，我们似乎可以得到这个答案：以太坊基础网络所集中解决的问题，是不依赖于垄断、权威的第三方平台，在高度崇尚开放的互联网环境下的“信任”问题。

“信任”是什么？在现实社会中，人与人、人与组织、组织与组织、人与社会、人与国家，每天人们都在为这复杂的“信任”网络努力工作，花费了大量的时间、金钱与精力，可以说“信任”是人类社会关系运行最重要的基础和最昂贵的东西之一。

互联网是一个什么样的世界呢？万物互联、从未谋面、瞬息参与。在传统模式的互联网世界，人和物之间直接建立“信任”是非常困难的，因此，长期以来仍需依赖线下世界的权威、官方、品牌来背书。这种在互联

试读结束：需要全本请在线购买： www.ertongbook.com

世界必须借助第三方平台来建立信任的模式，实质上通过互联网的“放大”效应变相地加剧了这些中心化平台的垄断、封闭与不均衡。这种状态实质上与互联网崇尚开放的精神背道而驰。回归互联网原旨精神，在不依赖第三方平台的条件下，区块链正在力图解决互联社会关系中的“信任”问题。这让互联网不再单单是一个可自由传递“信息”的网络，而成为一个可以自由承载“信任”及“价值”传递的平台。

在信息技术的应用历史中，长期以来人们都聚焦于一个问题——效率。无论是各类信息系统，还是当前的“物联网”“大数据”“人工智能”，其核心都专注于提升人们的“生产力”。而区块链则是在关注另一个重大课题：在开放的互联网社会中，在不依赖于第三方平台的条件下，如何构建可信的社会关系。

基于这个认识，我们团队对区块链作了一个定义：区块链是互联世界构建信任的技术基础设施。这里“互联世界”指明了区块链应用的环境是正蓬勃发展的互联网社会，特别是在不依赖于垄断、权威、封闭的第三方中心化平台下开放的互联网社会关系，“信任”是区块链旨在解决的核心课题，“技术基础设施”则是区块链的本质属性。

有了如上的定义与认识，将不难推导出区块链可以应用的领域：以“信任”为基础，反垄断、反封闭、反权威，需要开放，要求规则透明、智能运行的社会关系管理，即可通过区块链在互联网中映射，从而在互联网世界重构人类社会中已形成的各种社会关系，如经济合约、经济组织关系和社会组织关系等。

基于这些应用领域的项目的共同特点是需要有高度透明的运行机制、正确无误的智能执行、消费者的广泛参与及自由进出等。区块链，作为一种可以解决互联网世界可信社会关系的技术基础设施，正可以满足这些应用领域的需求，因而区块链也正展示其光明的应用前景和可观的社会经济价值。

因而，本书在系统阐释区块链二代技术——以太坊开发原理及方法的同时，也重点介绍几个基于智能合约的应用案例。为帮助广大读者全面了解区块链及其应用，我们特作以下说明。

（1）关于比特币、以太币等“虚拟币”。目前我国政府已明文规定“虚拟币”不具有法定货币的地位，因此，通过智能合约构建的无价值依托的“虚拟币”不得从事以人民币为对手的交易活动。使用智能合约以实体或数字资产为价值依托所创建的“虚拟币”，仅是实体或数字资产在区块链网络中的价值“符号”代表，其价值载体必须是实体或数字资产本身。

（2）关于股权众筹。本书仅介绍区块链当中的众筹智能合约的技术方法，包括技术方案、代码原理等，不涉及其相关的金融应用。在实际应用中，如果项目涉及股权众筹融资，是必须要得到相关监管部门批准的，但据我们所知，目前市场上还未有一家获得此牌照。因而，若项目涉及实际的金融应用，敬请留意国家关于股权众筹的相关政策法规。

成都高新信息技术研究院

赵其刚　博士

2017年9月18日

目录 CONTENTS

2 以太坊工作原理与基础

CHAPTER

3 以太坊安装与开发环境配置

CHAPTER

4 以太坊应用接口

CHAPTER

试读结束：需要全本请在线购买： www.ertongbook.com

5 智能合约编码、部署与应用 CHAPTER

CHAPTER 6

智能合约“虚拟币”创建

7 众筹智能合约设计

CHAPTER 7

8 去中心化自治组织

CHAPTER

1 区块链概论

CHAPTER

数字经济之父唐塔普斯科特（Don Tapscott）提出“不是机器人，不是大数据，甚至不是人工智能，而是区块链将引发人类第四次工业革命，并重新定义互联网甚至人类社会”。

1.1 区块链概念及应用

尽管“区块链”很像是在2016年由于比特币在世界范围内引起剧烈争议而突然产生的一个技术术语，但实际上，区块链从技术理论的提出，到今天的区块链2.0，已经历二十多年的发展。

1.1.1 ▷ 区块链发展历程

早在1991年，斯图尔特·哈伯（Stuart Haber）和史葛托尔内塔（W. Scott Stornetta）就在论坛中提出了关于区块的加密保护链产品。之后，分别由罗斯安德森（Ross J. Anderson）与布鲁斯·施奈尔（Bruce Schneier）、凯尔西（John Kelsey）在1996年和1998年发表相关产品。尼克·萨博（Nick Szabo）在1998年进行了“虚拟币”分散化的机制研究，他将其命名为比特金。2000年，斯特凡·康斯特（Stefan Konst）发表了加密保护链的统一理论，并提出了一整套实施方案。

2008年爆发全球金融危机，当时有人用“中本聪”的化名发表了一篇论文，描述了“比特币”的产生模式。2009年，比特币诞生，其到2140年将达到2 100万个的总量上限，现在被挖出的比特币总量已经超过1 200万个。目前各国政府对待比特币的政策区别较大，在我国比特币不具有法定货币的地位，只是一种特定的虚拟商品。它对社会的贡献和价值主要在于其通过实践验证了其背后的支撑技术——区块链。

2014年，维塔利克·布特瑞（Vitalik Buterin）、加文伍德（Gavin Wood）和杰夫瑞·威尔克（Jeffrey Wilcke）开始开发下一代区块链平

试读结束：需要全本请在线购买： www.ertongbook.com