# 从零开始学区块链

## 数字货币与互联网金融新格局

黄振东◎编著

互联网改变了世界，但你要知道，区块链正在改变互联网！

比特币　挖矿挖出的『美元』

数字货币　不需要印钞机的钞票

智能合约　可以自动执行的合同

R3 CEV　全球大银行建造的朋友圈

DAO　导致以太坊分家的『史上最强众筹』

清華大學出版社

# 从零开始学区块链

## 数字货币与互联网金融新格局

黄振东◎编著

清華大學出版社
北　京

## 内 容 简 介

本书紧密结合社会发展的最新前沿科技，介绍了金融科技领域颠覆性的应用技术——区块链技术的发展历程和现状，重点介绍了掩藏在区块链神秘面纱之下的技术原理和一些重要的基础性技术模块，引领读者深入区块链成熟应用比特币的运作流程；同时对区块链的技术原理做了进一步的探究，使读者对于区块链的运行流程、数据解读等有所了解。在此基础上，本书介绍了区块链在数字货币领域的典型应用，通过阅读读者可以穿透数千种数字货币的迷雾，洞悉数字货币的区块链本质。

此外，本书还介绍了区块链在金融行业的两大重量级应用：R3 CEV联盟、超级账本项目。在金融行业之外，重点介绍了以智能合约为主要特色的全球性应用——以太坊网络，以及在以太坊基础上开发的红极一时却又“黯然退隐”的The DAO项目。通过对这些重量级应用的介绍，为读者全面展示了区块链所具有的重塑世界的潜能。

本书以全球化的视角紧盯国际前沿商业实践，定位高端，专业性强，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发展的创业者，还可以作为各类想了解区块链技术的大专院校学生的参考资料。



**图书在版编目（CIP）数据**

从零开始学区块链：数字货币与互联网金融新格局 / 黄振东编著. — 北京：清华大学出版社，2017

ISBN 978-7-302-46670-3

Ⅰ. ①从… Ⅱ. ①黄… Ⅲ. ①电子商务—电子支付—支付方式—研究②互联网络—应用—金融—研究 Ⅳ. ①F713.361.3②F830.49

中国版本图书馆 CIP 数据核字（2017）第 036018 号

**责任编辑：** 张立红
**封面设计：** 邱晓俐
**版式设计：** 方加青
**责任校对：** 郭熙凤
**责任印制：** 王静怡

**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：** 三河市金元印装有限公司
**经　　销：** 全国新华书店
**开　　本：** 170mm×240mm　　**印　　张：** 18.25　　**字　　数：** 253 千字
**版　　次：** 2017 年 5 月第 1 版　　**印　　次：** 2017 年 5 月第 1 次印刷
**定　　价：** 65.00 元

产品编号：073316-01

# 前言

忽如一夜春风来，“区块链”这个名词传遍大江南北，上至庙堂之高，下到江湖之远，从大学教授、专家学者，到中国人民银行的政府官员，更不用说得风气之先的互联网从业者，以及金融行业的分析师和投资人，甚至是炒股的普通股民都在不断地说起这个词，一些A股上市公司的股票也因为沾上了区块链的一点边，而不断出现涨停板……区块链，似乎成为新世界的一把钥匙，谁掌握了它，谁就可以率先打开新世界的大门。

但是，“区块链”究竟是什么？它背后的原理又是什么？它到底能用来做些什么？为什么这么多的人对它如此看好？对于很多人来说，这些问题仿佛一层朦胧的面纱，遮掩着区块链的美丽容颜。为此，本书试图引领广大读者深入区块链的世界，揭开区块链的神秘面纱，让读者对区块链的前世今生、技术原理和商业应用都有深入的了解，体会到区块链的创新之美，成为区块链领域的明白人。

令人欣慰的是，区块链这一技术，目前在全球范围内都还处于向各个方向探索的过程中，而且由于中国互联网行业的飞速发展，以及相关从业人员对区块链各个环节的深度投入，中国在区块链行业已经产生了众多的产品和业务。当然，更应该承认，区块链是由国外的软件开发人员基于互联网思维提炼出来的新的商业应用，欧美对区块链已经有了多年的理论积累和实践经验，他们在许多方面还是先行一步。为此，本书很多内容直

接采用欧美第一手的资料和信息，精心加工成为符合中文习惯的区块链知识。另外，区块链是一项前沿的金融科技，本书也非常注重时效性，尽可能选用最新的案例、数据和资料。在写作方式上，本书采用了大量的图表，行文朴实自然，读者可以自如阅读，轻松掌握一种全新的科技应用。区块链打开了一片广阔的空间，处处充满了值得探索的未知事物，但本书并没有追求大而全，而是选取区块链领域最经典的专题进行深度探究，有助于读者对区块链的本质深入了解，“一念通，路路通。”

因受作者水平所限，本书难免存有疏漏和不当之处，敬请指正。

## 本书特色

### 1. 内容新颖、重点突出，符合人们对新生事物的认知规律

本书介绍了当前最新的金融科技应用——区块链，这是一项非常前沿的技术，目前仍然处在发展和探索的过程中。因此本书的内容紧紧抓住时代的脉搏，帮助读者建立面向未来的知识储备，在新生事物开始影响人们生活的过程中占据主动。本书从案例切入，重点讲述了区块链的技术原理，令读者“知其然，知其所以然”，符合人类认识新事物的规律。

### 2. 行文朴实自然，通俗易懂，便于各水平的人们阅读

本书采用朴实、自然的语言介绍区块链的各种知识、原理，在兼顾专业性、准确性的前提下，尽量做到行文通俗易懂，以便于各个水平的读者阅读，让读者可以读懂，并获得知识的积累。

### 3. 专业化配合图形化，将抽象事物形象化

本书在介绍一些枯燥、冗长的知识点时，充分尊重读者的思维习惯，用大量的图示来补充说明文字内容，通过这种方式使原本专业性很强的知识和信息或者某一个业务流程，转变为可读性更强的图片，将抽象事物形象化，使读者更易理解。

## 本书内容及体系结构

### 第1章 区块链概览

本章从现实生活中出现的区块链相关新闻开始，介绍了区块链对社会生活方方面面带来的改变和影响，说明了区块链的定义，对区块链的发展历程和当前的发展现状进行了介绍，为读者建立了区块链的感性认知。

### 第2章 区块链技术初探

本章从区块链技术最成熟的应用——比特币切入，深入介绍了比特币的原理；在此基础上，引入了区块链的系统框架结构，然后分别介绍了在区块链系统框架中处于基础地位的组成模块——分布式网络以及共识机制；最后介绍了区块链的三种类型。本章带领读者对区块链技术进行初步的探究。

### 第3章 区块链技术基础

本章在第2章的基础上，进一步深入探讨区块链的技术原理，详细介绍了区块链的数据结构、区块链的数据加密和降维过程，以及加密所用到的椭圆曲线加密算法，令读者对区块链的深层技术有深入了解。随后，本章介绍了区块链的运行流程，以及怎样对区块链的数据进行解读。总的来说，本章全面介绍了构建区块链的基础性技术模块。

### 第4章 区块链与数字货币

本章着重介绍了区块链在数字货币领域的应用，这也是目前区块链应用最成熟、范围最广的商业领域。本章从数千种数字货币中选择了各具特色的四种：莱特币、瑞波币、狗狗币和点点币，对它们分别做了介绍。通过对四种不同的数字货币的介绍，读者可以对区块链在数字货币的应用获得全面的了解。

### 第5章 区块链在金融行业的应用

本章聚焦于区块链在金融行业的应用情况，选取了两个典型案例：R3 CEV和超级账本项目，分别介绍了这两个项目的创立和发展情况，以及区

块链原理在这两个项目当中的应用情况，帮助读者充分理解区块链在金融行业的应用优势和前景。

第6章　以太坊与DAO

本章介绍了区块链除比特币之外的另一个全球性应用：以太坊，以及在以太坊基础上曾经红极一时的去中心化自治组织DAO，通过本章的介绍，读者可以进一步了解智能合约在区块链上的应用前景。

## 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
- 从事区块链研究的专家学者
- 大专院校金融或互联网科技等相关专业的学生
- 其他对区块链有兴趣爱好的各类人员

## 关于作者

本书由黄振东组织编写，同时参与编写的还有吕琨、李慧敏、黄维、金宝花、梁岳、张驰、孙景瑞、苗泽、李涛、刘帅、景建荣、胡雅楠、焦帅伟、李信、王宁、鲍洁、艾海波、张昆。

# 目录

第1章

# 区块链概览

人类认知事物的客观过程，总是先远观其整体，后深入事物的内部结构进行探究，外观其形，内究其理，内外结合，然后可以明道。因此，面对区块链这样一个绝大多数人都很陌生的概念，我们的目光当然首先要从它的外部入手，获得整体性认知，知道它是什么、怎么来的、可以做什么。

## 1.1 区块链：下一个趋势

如果纠缠于过去和现在，我们将失去未来。

——（英）温斯顿·丘吉尔

人类跨过二十一世纪的第一个10年之后，互联网的大潮席卷了整个地球，在地球的每一个角落，有人的地方就可以连上互联网，获得与其他人的联系。互联网填平了不同人群之间存在的信息鸿沟，让“地球村”成为现实。在这轮大潮中，以Google、Facebook、国内的BAT等为代表的企业，抓住了互联网趋势，成为时代的弄潮儿。它们的成功也让人们不断思考：下一个趋势是什么？

从2015年上半年以来，“区块链”（Blockchain）成了投资界、金融行业、上市公司等业态中高密度出现的一个词汇，从国内到国外，与区块链相关的新闻频繁出现在媒体聚光灯下，从证券分析师、企业高管到政府官员，纷纷发表对区块链的溢美之词，在业内人士看来，只要掌握了区块链，就掌握了打开未来30年财富之门的钥匙。

### 1.1.1 商业银行积极参与

2015年9月29日，全球13家顶级银行，包括汇丰银行、德意志银行等共同加入了由一家初创公司所领导的组织，宣布加入的另外11家银行是：

花旗银行、美国银行、摩根士丹利、德国商业银行、法国兴业银行、瑞典北欧斯安银行、纽约梅隆银行、三菱UFJ金融集团、澳大利亚国民银行、加拿大皇家银行和多伦多道明银行。领导这一组织的初创公司名为R3 CEV，总部设在美国纽约。据其介绍，R3 CEV公司将会利用区块链技术作为框架，研发银行业区块链技术开发行业标准及应用，致力于建立银行业区块链组织。这种巨大的反差充分展示了区块链在银行业的潜在力量。

而此前的9月15日，已经有9家银行签署了R3 CEV的初创协议，包括巴克莱银行、西班牙毕尔巴鄂比斯开银行、澳大利亚联邦银行、瑞士信贷银行、高盛集团、摩根大通集团、苏格兰皇家银行、美国道富银行、瑞银集团。到2015年12月17日，R3 CEV组织宣布共有42家银行机构加入了其团队。这些银行都是成立数十年甚至数百年的传统银行，但却不约而同选择加入R3 CEV组织，这说明全球商业银行对于区块链在金融层面即将带来的革命都相当重视。

这一趋势也影响到了中国的相关机构和企业。

2015年10月，首届全球区块链峰会“区块链——新经济蓝图”在上海举办，共有来自中国央行金融研究所、央行征信中心、上海证券交易所、上海陆家嘴国际金融资产交易市场股份有限公司（陆金所）、德勤会计事务所等全球约200位行业专业人士参加，涉及银行、支付、证券、大宗商品等金融行业及其他对区块链技术应用前景有兴趣的人士。本次会议主办方为万向区块链实验室（WanXiang Blockchain Labs），会议上举行了区块链技术投资基金成立仪式，由中国万向控股有限公司设立一只5000万美元的专门投资于有商业前景的区块链应用技术项目的基金，用于在全球范围内投资区块链商业应用相关的各类项目。

区块链在商业银行业内首先形成了广泛的认同和参与，是有其根本原因的。首先是互联网金融对传统银行业带来了巨大的冲击，商业银行认识到了金融技术（Fintech）的力量。其次，目前大多数互联网金融产品在本质上只是传统金融的电子化，信用创造的方式并没有改变。具体地说，在

当前商业模式和社会组织架构下，价值创造和交换活动都需要一个集中的制度体系（如政府信用背书）和机构体系（如银行、支付机构等）来建立信用，否则陌生人之间无法获取信任而发生交易。区块链技术从根本上改变了这种中心化的信用创造方式，运用一套基于共识的数学算法，在机器之间建立“信任”网络，可以让交易双方在无须借助第三方信用中介的条件下开展经济活动，从而实现全球低成本的价值转移。

虽然区块链给商业银行的传统金融业务带来了冲击，但参与R3 CEV组织的这些金融巨头真正感兴趣的是通过区块链技术对传统的商业银行业务进行自我革新，提升经营效率并缩减成本。区块链以去中心化的模式，可以大大简化金融服务流程，大幅缩短交易时间、降低交易成本。更重要的是，面对激烈的市场竞争，各商业银行都希望通过参与区块链在商业银行领域标准的制订占领市场先机，争取更大的业务份额以保持利润。可见，商业银行拥抱区块链技术最主要的动力是对传统的中心化银行系统的优化和革新，将区块链技术作为改造银行后台、优化基础架构的工具，从而提升自身竞争力，在未来的发展中不被新技术浪潮吞没。

目前商业银行基于区块链的应用领域主要有：（1）点对点交易。如基于P2P的跨境支付和汇款、贸易结算以及证券、期货、金融衍生品合约的交易等。（2）登记。区块链具有可信、可追溯的特点，因此，可作为可靠的数据库来记录交易的各种来源信息，应用于存储客户身份资料及交易记录，达到反洗钱的目的。（3）确权。利用区块链不可篡改的特点，对诸如土地所有权、股权等财产的真实性进行验证和转移等。（4）智能合约。由系统自动检测合约编码是否具备生效的条件，一旦满足了预先设定的程序，合同即自动执行，比如自动付息、分红等。

除了加入前述的R3 CEV等组织外，国际上许多大型银行也采用了多种形式在区块链领域开展探索。一是商业银行成立内部的区块链实验室，比如花旗银行、瑞银集团、纽约梅隆银行等已相继成立研发实验室，重点围绕支付、数字货币和结算模式等方面测试区块链的应用，有的还扩大到