人气经济学家
全面解读
**区块链实用**技术！

Blockchain
Technology

一本书搞懂

# 区块链
## 技术应用

董超　主编

## 解密区块链，重构金融与经济世界

区块链技术已成为时下热点
各商业巨头正陆续试水区块链技术应用

**区块链即一群认同并遵守这个规则的人共同记录连续信息的过程**

全国百佳图书出版单位
化学工业出版社

Blockchain
Technology

一本书搞懂

# 区块链
## 技术应用

董超　主编

化学工业出版社
·北　京·

《一本书搞懂区块链技术应用》通过图解、图示，用更为浅显易懂的语言和实例解释了什么是区块链、区块链的发展、区块链技术、区块链应用领域、区块链的安全防范五个方面的内容，区块链已经成为金融科技的底层技术，区块链革命将重塑经济世界！

《一本书搞懂区块链技术应用》内容涵盖面广，实用性强，图表为主，可供对区块链内容感兴趣的有识之士借鉴与参考。

**图书在版编目（CIP）数据**

一本书搞懂区块链技术应用/董超主编. —北京：化学工业出版社，2018.4

ISBN 978-7-122-31640-0

Ⅰ.①一… Ⅱ.①董… 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041329号

责任编辑：陈　蕾　　装帧设计：尹琳琳
责任校对：边　涛

出版发行：化学工业出版社（北京市东城区青年湖南街13号　邮政编码100011）
印　　装：三河市延风印装有限公司
710mm×1000mm　1/16　印张10　字数177千字　　2018年5月北京第1版第1次印刷

购书咨询：010-64518888（传真：010-64519686）　售后服务：010-64518899
网　　址：http://www.cip.com.cn
凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定　　价：49.80元

# 前言
PREFACE

区块链技术在国内已经成为了金融界的宠儿，已经成为时下的一个热门话题。

区块链是一种将数据用区块的形式记录，并利用分布式的方式存储、传输和证明的方法。以记账为例，所有的系统背后都有一个数据库，可以把数据库看成是一个大账本，一般情况下，谁拥有系统，谁就有记账的权利。因此当消费者在淘宝上购买一件产品时，阿里就记上一笔。但在区块链系统中，多个机构可同时参与记账。在不需要中介机构的情况下，区块链技术解决了账本数据的真实性、不可篡改性和扩展性问题。

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

目前国际上没有统一的清算中心，因为没有一家组织或机构能够获得公信力的背书，取得不同金融机构的信任。而借助区块链分布式账本技术的优势，则解决了交易的真实性和可靠性问题。

区块链有着广阔的应用前景，但它也存在着自身的局限性。区块链要想真正实现价值的互联互通，必须要解决底层技术、业务以及数据的标准化问题。除此之外，区块链还面临着性能、容量、安全性、可扩展性等一系列技术方面的挑战。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域，将为云计算、大数据、移动互联网等新一代信息技术的发展带来新的机遇，有能力引发新一轮的技术创新和产业变革。

《一本书搞懂区块链技术应用》由安德互联数据服务有限公司总裁、资深架构师、大数据分析师董超主编，安德互联数据服务有限公司副总裁、资深数据分析师、前贵阳大数据交易所会员部总监卢桂林，以及傅冬晓、周翔、叶坚镇、王浩鹏、骆相松、李军、李辉、张海雷、陈超、孙小平、匡仲潇、李旭升、王建伟、

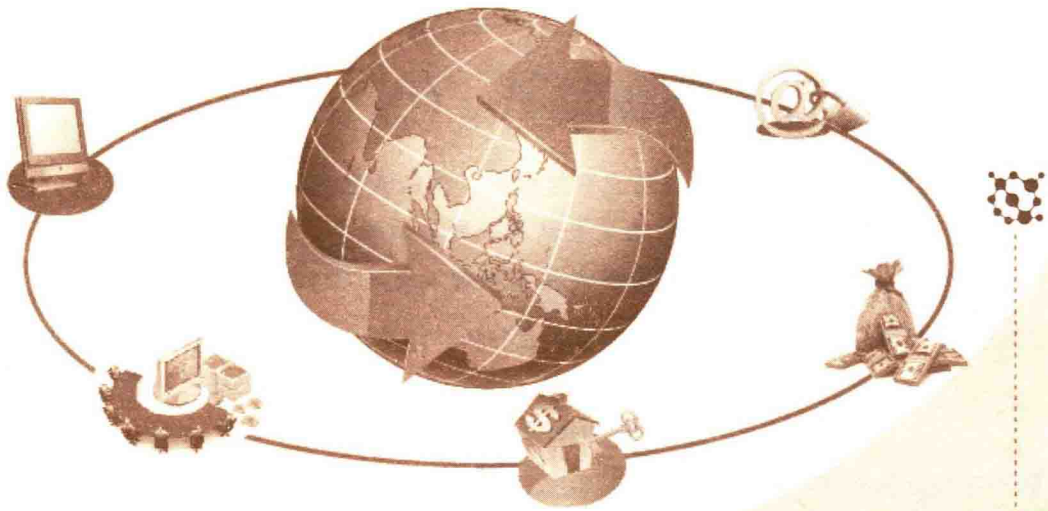
刘春海、郑时勇、刘俊、何春华、黄美、赵慧敏、冯永华参与了本书的编写工作，阿里巴巴高级技术专家崔亮、小米科技广告部资深研发工程师冀康、58赶集集团商业技术部副总监邓柱中参与了本书的审定工作，全书由董超和卢桂林统稿审核完成。在此，对他们一并表示感谢！

同时，由于作者水平所限，不足之处敬请读者指正。

编　者

# 目录
CONTENTS

目前，区块链应用已从单一的数字货币应用延伸到金融服务、供应链管理、文化娱乐、智能制造、社会公益、教育就业等多个领域，有可能引发新一轮的技术创新和产业变革。





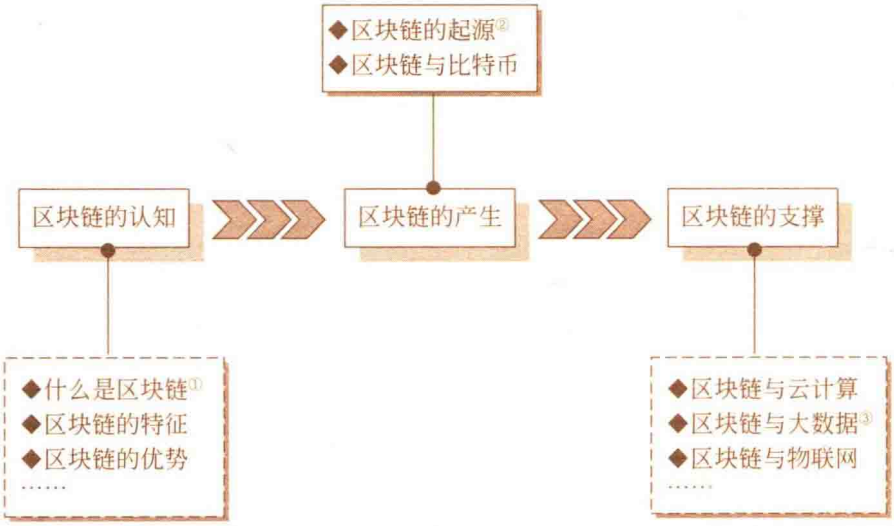
# 第一章 区块链概述

## 导言

近两年来，从美国硅谷到华尔街，从北京中关村到上海陆家嘴，从各国央行到国内外各大商业银行，区块链成为讨论的热点，风险投资和产业界也纷纷加大投入力度，“区块链+”应用创新正在成为引领发展的动力。

## 阅读指引

自2014年以来，区块链研究愈演愈烈，全球竞相发展区块链技术。区块链不仅仅是继互联网之后最具颠覆性的技术革命，它还有可能和大数据、移动互联网、云计算等新技术掀起人类历史上的第四次产业革命。




图示说明：

① 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

② 区块链起源于中本聪创建的比特币，比特币依靠于区块链这项技术完美的运行着，没有主导机构，做到了去中心化，使得大家开始研究比特币运行原理，发现了区块链。

③ 大数据具备海量数据存储技术和灵活高效的分析技术，极大提升区块链数据的价值和使用空间。

# 第一节　区块链的认知

## 一、什么是区块链

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

### 1. 狭义含义

狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。如图 1-1 所示。

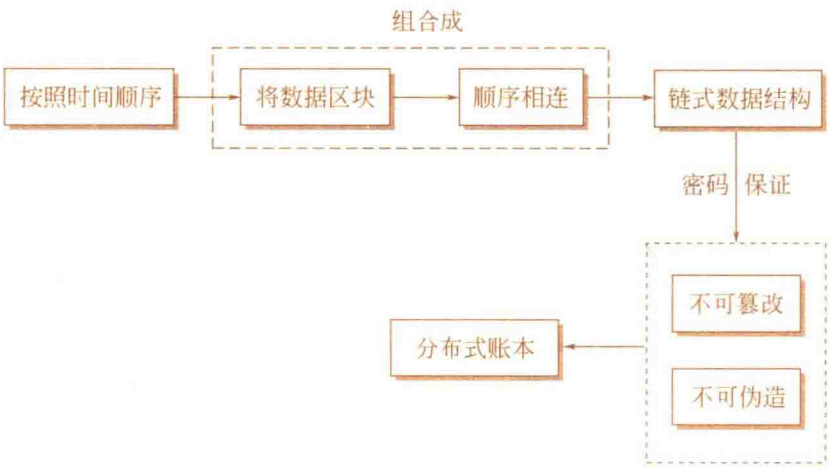



图 1-1　区块链的狭义含义

### 2. 广义含义

广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。如图 1-2 所示。


图 1-2　区块链的广义含义

## 二、区块链的特征

区块链具有如图 1-3 所示的特征。

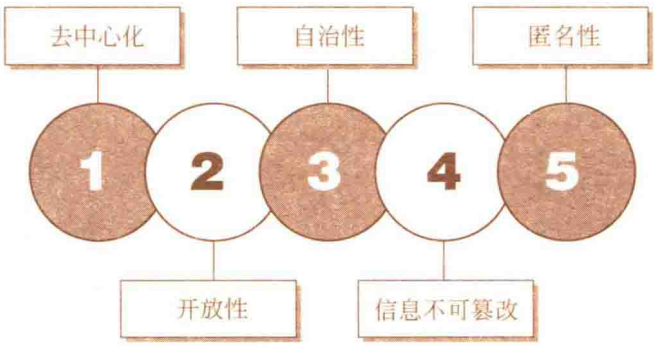



图 1-3　区块链的特征

### 1. 去中心化

区块链由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。

### 2. 开放性

系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

### 3. 自治性

区块链采用基于协商一致的规范和协议（比如一套公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全地交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

### 4. 信息不可篡改

一旦信息经过验证并添加至区块链，就会永久地存储起来，除非能够同时控制住系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

### 5. 匿名性

由于节点之间的交换遵循固定的算法，其数据交互是无需信任的（区块链中的程序规则会自行判断活动是否有效），因此交易对手无须通过公开身份的方式让对方对自己产生信任，对信用的累积非常有帮助。

## 三、区块链的优势

区块链的基本思想是建立一个基于网络的公共账本（数据区块），每一个区块包含了一次网络交易的信息。

由网络中所有参与的用户共同在账本上记账与核账，所有的数据都是公开透明的，且可用于验证信息的有效性。这样，不需要中心服务器作为信任中介，就能在技术层面保证信息的真实性和不可篡改性。

相比于传统的中心化方案，区块链技术主要有如图1-4所示的三个优点。

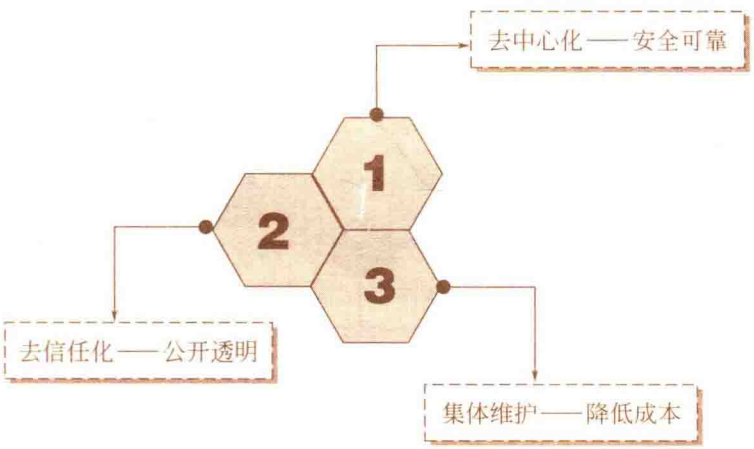



图1-4　区块链的优势

1. 去中心化——安全可靠

与传统网络系统对比，区块链最大特性是去中心化。在区块链系统中，整个网络没有中心化的硬件或者管理机构，任意节点之间的权利和义务都是均等的，所有的节点都有能力去用计算能力投票，从而保证了得到承认的结果是过半数节点公认的结果。即使遭受严重的黑客攻击，只要黑客控制的节点数不超过全球节点总数的一半，系统就依然能正常运行，数据也不会被篡改。

2. 去信任化——公开透明

传统的交易建立在信任的基础之上，尽管信任中介获取了大量信息，但是从中流出的、披露的信息却极为有限，导致大量数据被浪费和隐藏。参与区块链系统的每个节点之间进行数据交换则无需互相信任。

在区块链系统中，因为整个系统的运作规则是透明的，所有的数据内容也是公开的，因此在系统指定的规则范围和时间范围内，节点之间不能也无法相互欺骗。

3. 集体维护——降低成本

在中心化网络体系下，系统的维护和经营依赖于数据中心等平台的运维和经营，成本不可省略。

区块链则构建了一整套协议机制，系统中的数据块由整个系统中所有具有维护功能的节点来共同维护。这些具有维护功能的节点是任何人都可以参与的，每一个节点在参与记录的同时也来验证其他节点记录结果的正确性，维护效率提高，成本降低。

## 四、区块链的分类

区块链目前分为三类，如图1-5所示。

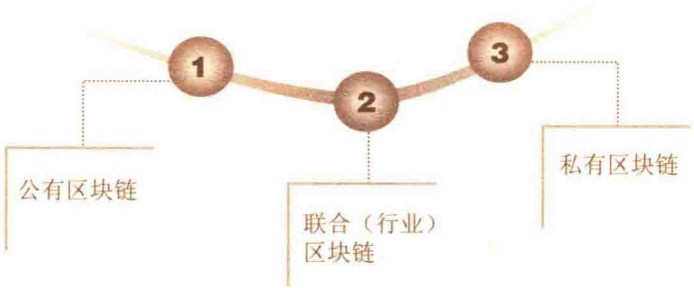



图1-5　区块链的类型

### 1. 公有区块链

公有区块链是指世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。公有区块链是最早的区块链，也是目前应用最广泛的区块链，各大Bitcoins系列的虚拟数字货币均基于公有区块链，世界上有且仅有一条该币种对应的区块链。公有区块链的特点如图1-6所示。

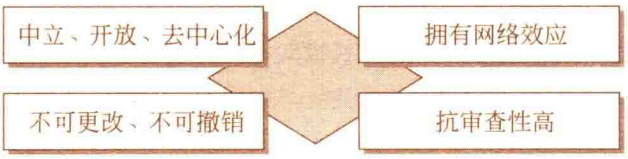



图1-6　公有区块链的特点

### 2. 联合（行业）区块链

行业区块链是由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不过问记账过程（本质上还是托管记账，只是变成分布式记账，预选节点的多少、如何决定每个块的记账者成为该区块链的主要风险点），其他任何人可以通过该区块链开放的API进行限定查询。

### 3. 私有区块链

私有区块链仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限，本链与其他的分布式存储方案没有太大区别。私有区块链具有如图1-7所示的特点。


图1-7　私有区块链的特点

## 五、区块链的意义

区块链的意义可从以下三个方面来看。

1.学术意义

在无信任的环境下，在整个网络中的任意节点建立起共识机制，而无需担心数据被篡改。

2.应用意义

数据库从集中式纵向扩展向分布式横向扩展发展。纵向扩展就是通过添加内存、存储和CPU，增强单台机器的性能，这种纵向扩展会遇到吞吐量瓶颈等问题。分布式数据库通过横向扩展，提升了吞吐量和计算效率，也开启了大数据时代。分布式数据库主要分为以Storm为代表的流数据库、Hadoop为代表的批处理数据库、以Spark为代表的内存数据库，和以Neo4j为代表的图形数据库。

**一点通**

区块链的意义在于，增加了一个分支，基于时间轴的分布式数据库。

3.战略意义

基于创建信任的机器，促进价值的全球流动。如果说基于TCP/IP的第一代互联网实现了信息的全球流动，像WWW和HTTP协议，区块链就是把各个机构和个人，映射到虚拟世界，基于数学这种人类文明的最大公约数，汇集世界上不同人群、不同权利群体的共识，实现了价值或者说资产的全球实时流动。

## 六、区块链系统的核心优势

区块链体系结构的核心优势包括如图1-8所示的内容。

- 任何节点都可以创建交易，在经过一段时间的确认之后，就可以合理地确认该交易是否为有效，区块链可有效地防止双花问题的发生
- 对于试图重写或者修改交易记录而言，它的成本是非常高的
- 区块链实现了两种记录，即交易以及区块。交易是被存储在区块链上的实际数据，而区块则是记录确认某些交易是在何时，以及以何种顺序成为区块链数据库的一部分

图1-8　区块链系统的核心优势