新时代
科技
新物种

BLOCKCHAIN +
INTELLIGENT SOCIAL ADVANCED
AND SCENARIO APPLICATION

区块链+
智能社会进阶与场景应用

申 丹 著

区块链+金融、征信、保险、能源、医疗、版权、物联网、农业、公益、社交
全方位讲述区块链在各个领域中的应用

清華大學出版社

新时代
科技
新物种

区块链+
智能社会进阶与场景应用

申 丹 著

清華大學出版社
北京

内 容 简 介

继大数据、工业4.0之后，区块链作为一种新的时代趋势出现了。区块链这一热点与大数据、工业4.0、物联网等呈现相融相生的局面。不过，由于区块链目前还处于概念性阶段，应用层面比较少。因此这一热点能够像工业4.0一样，可能会持续5～10年。

本书逻辑层次清晰，案例新颖。为了让读者更好地看到“区块链+”的实际应用，本书讲述了区块链+金融、区块链+征信、区块链+保险、区块链+能源、区块链+医疗、区块链+版权、区块链+物联网、区块链+农业、区块链+公益、区块链+社交等方面的内容，全方位讲述了区块链在各个领域中的应用，同时还对区块链未来的发展趋势做了分析和预测。

本书内容通俗易懂，涉及面广泛，适合金融领域相关工作人员、数字货币相关工作人员、区块链研究者和开发者、各领域企业领导高管以及对区块链感兴趣的其他人群阅读。

图书在版编目（CIP）数据

区块链+：智能社会进阶与场景应用 / 申丹著. —北京：清华大学出版社，2019
（新时代·科技新物种）
ISBN 978-7-302-51850-1

Ⅰ. ①区… Ⅱ. ①申… Ⅲ. ①电子商务－支付方式－基本知识 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 284322 号

责任编辑： 刘 洋
封面设计： 徐 超
版式设计： 方加青
责任校对： 王荣静
责任印制： 杨 艳

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： 三河市国英印务有限公司
经 销： 全国新华书店
开 本： 170mm×240mm **印 张：** 13.75 **字 数：** 202 千字
版 次： 2019 年 4 月第 1 版 **印 次：** 2019 年 4 月第 1 次印刷
定 价： 59.00 元

产品编号：081268-01

前言
Preface

2008年，中本聪在自己的文章《比特币：一种点对点的电子现金系统》中，第一次提到了区块链这一名词，不过，在那个时候，区块链还只是作为比特币的一种底层技术而存在。2016年，知名投资银行高盛发布的一份报告称，区块链已经做好了颠覆整个世界的准备。正是这份报告让我们对区块链有了更加深刻的了解。

如今，在时代不断进步的影响下，区块链开始突破原有的限制而被广泛应用到金融、征信、保险、版权、能源、医疗、物联网、农业、公益、社交等多个领域，从而形成了极具影响力的“区块链+”模式。区块链的应用价值获得了广泛认可，基于此，世界各国政府也意识到了区块链的巨大潜力，纷纷出台与该项技术有关的政策和规划。要知道，对于一项全新的技术而言，政府的政策和规划具有无与伦比的推动力。

2016年1月20日，中国人民银行数字货币研讨会正式召开，在此次大会上，中央银行相关负责人宣布我国在数字货币方面取得的阶段性成果，同时还表示他们正在积极探索数字货币的发行；同年12月20日，中国inTech数字货币联盟及FinTech研究院正式筹建；2017年2月，中国人民银行利用区块链对数字票据交易平台进行深入研究，其旗下的数

字货币研究所也在 2017 年上半年挂牌成立。

除此之外，各大行业巨头也在积极布局区块链。例如，百度进军消费金融，开发出一个名为 BaaS 的区块链云计算平台；阿里巴巴旗下的蚂蚁金服着重研发生产级底层技术，专注项目落地；腾讯致力于打造垂直行业应用的生态平台；京东发力商品防伪溯源以及物流追踪，希望为消费者提供更加安全放心的商品。

上面提到的案例还只是区块链应用案例中的一小部分，由此可见，区块链的普及程度正在一点点提高，这也意味着，区块链在各个领域所发挥的作用也会越来越大。然而，对于与区块链相关的从业人员而言，区块链也许既是机遇也是挑战。

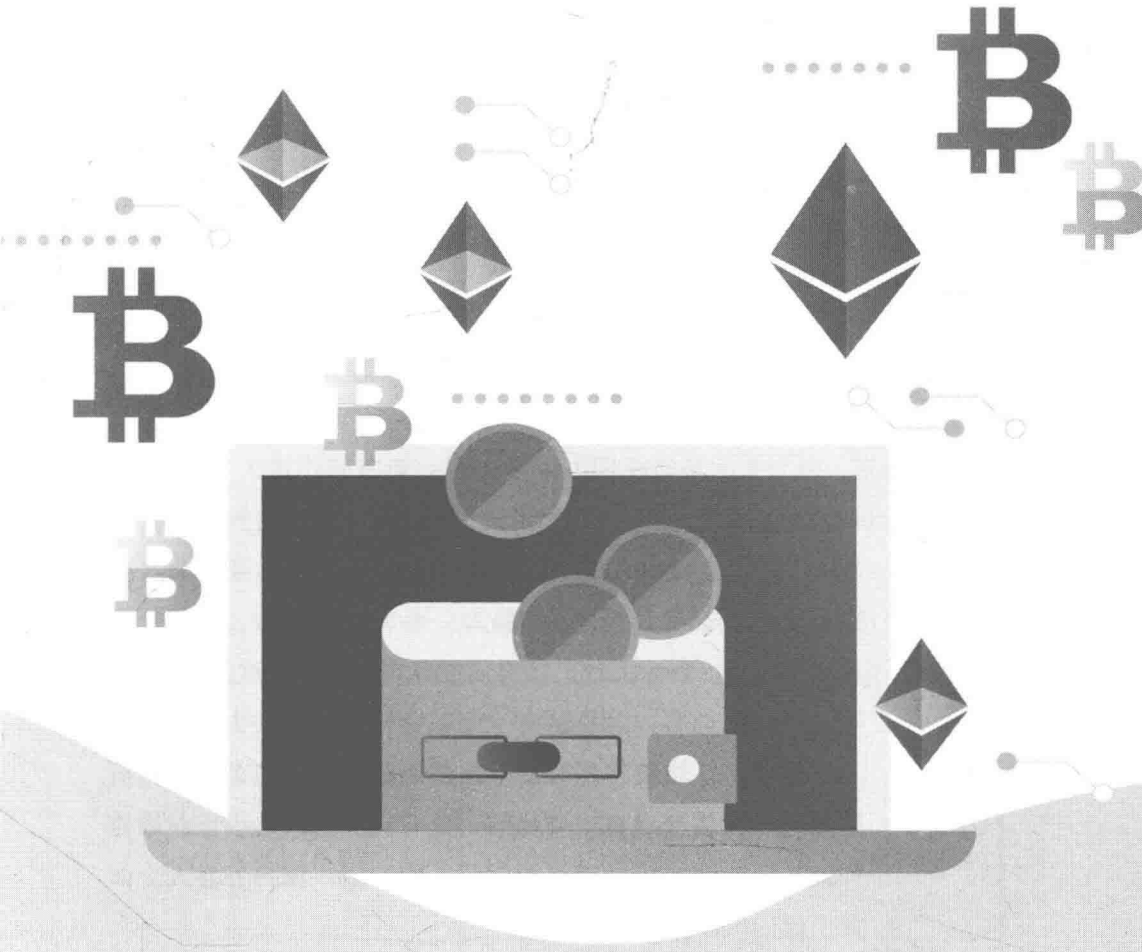
为了更好地平衡二者之间的关系，我们必须要找到一些行之有效的办法，并制定出比较完善的策略。但是，从目前的情况来看，大部分人都不是非常了解区块链，只知道这是一项新的技术，可以对各个领域产生影响，因此也就很难找到区块链技术与应用更好结合的解决方法，并制定出切实可行的策略。

本书正好抓住了这些不足，为读者传授详细的区块链知识和全面的区块链应用，从而使读者对区块链有更加深入的了解。

本书中不仅有与区块链相关的各种理论知识，还有各种各样的经典案例以及大量的精美图表，可谓是实现了真正意义上的图文并茂。除此以外，本书的文字内容也力求诙谐幽默、浅显直白，目的就是要让读者能在轻松愉快的氛围中感受到区块链的魅力。

可以想象，在这个不断发展的时代，如果不及时充实自己的话，很可能会落后于别人，因此我们必须要把握机会，提升素质，通过对本书的学习，读者可以迅速了解区块链，并将其应用到实践当中，相信对于广大读者而言，阅读本书的学习之旅定会是一段非常完美的体验。

目录
Contents



第 1 章
区块链技术的原理与特征

若要提及当下的大热门，“区块链”一定名列前茅，而且在多数专家看来，它还将会创造未来。那么，区块链到底是什么呢？其实，它就是一种特殊的分布式数据库。在很早之前，市场上就已经出现了分布式数据库这类的产品。不过，相比而言，区块链有一个革命性特征——去中心化。具体来讲，区块链将所有的数据都储存在独立的个人计算机网络中，使其变成去中心化的、分布式的结构。也正是因为如此，区块链才可以拥有如此巨大的价值，获得各界人士如此广泛的关注。

1.1 从数据和效果两个维度来看区块链技术原理

区块链最初是由中本聪设计出来的一种独具特色的数据库技术，该技术是以密码学中的椭圆曲线数字签名算法为基础来实现去中心化的 P2P 系统设计。很多人认为，区块链只能在比特币上发挥作用，但事实却并非如此。从目前的情况来看，区块链的含义似乎已经变得多种多样，例如，数据结构、数据库、数据库技术等。而无论是哪一种含义，都与比特币没有必然的联系。

1.1.1　数据：区块链是一种分布式数据库

如果从数据的角度来看，区块链应该是一种分布式数据库，而这里所说的“分布式”则主要体现为数据的分布式储存，对此可以从以下两个方面进行详细说明。

（1）大家必须知道，区块链储存的基本单元是区块，在链式结构的助力下，新增的区块都知道自己的前一个区块是什么，而且可以一直追溯到根。此外，哈希值为区块链提供了标识，链式结构又将业务产生的轨迹保留了下来。因此，在有新交易增加的时候，链式结构就可以根据区块的标识和前面的记录对新交易进行校验，进而保证区块的数据不会轻易被篡改，具体如图 1-1 所示。

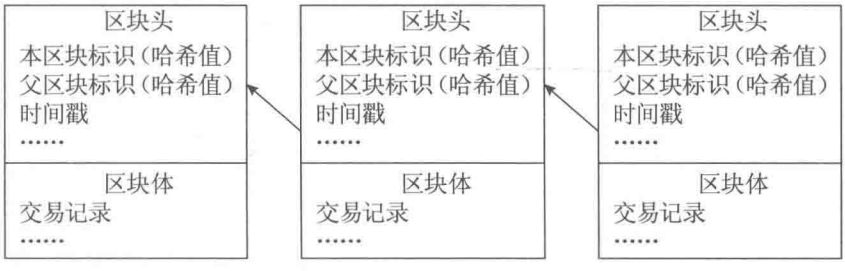


图 1-1　数据的分布式储存

当然，在传统的数据库设计中，与之相类似的模式也经常会被采用，例如，拉链表模式。在拉链表模式下，数据的每一次更新都会被追加，交易历史（例如，起始时间、是否生效、失效时间等）也会被完整地保存下来。区块链在该模式的基础上，加入了哈希、时间戳等新技能，以此来保证链条的准确性和完整性。

（2）既然区块链以分布式的方式来储存数据，那就必须要解决存储时分布式一致性的问题，在解决这一问题的时候，区块链的前身比特币采用了工作量证明的方法。那么，何谓工作量证明呢？具体来说，就是通过工作获得成果，然后再用成果证明已经付出的努力。

对此，很多人可能有所不解，为什么一定要用工作量来证明，难道就没有其他办法了吗？实际上，自从区块链与比特币分离以后，上述问题就被归结为共识问题了，而工作量证明也成为了达成共识的一种方式。

实际上，除了工作量证明以外，权益证明、实用拜占庭容错也是达成共识的方式。其中，权益证明是一种通过业务规则达成共识的方式；实用拜占庭容错是一种通过技术规则达成共识的方式。

这里还需要介绍一个知识点，区块链可以分为三种类型——公有链、私有链、联盟链。在公有链和私有链上，达成共识的最主要方式就是工作量证明，而且这一方式在短期内不会被轻易取代。但是在联盟链上，完全可以根据实际情况，创造出一些新的方式达成共识，以便更好、更有效地解决分布式数据存储的一致性问题。

总而言之，区块链可以实现全球数据的分布式储存，也正是因为如此，它才变成了一个巨大的数据库。在这个数据库当中，任何企业、机构、个人都可以完成数据储存，而且根本不需要担心自己的数据会被删除或者篡改。

1.1.2 效果：记录时间先后的、不可篡改的、可信任的数据库

如果我们想建立一个可以在世界范围内使用的数据库，那么就会面临三个亟待解决的棘手问题。

（1）如何让数据库既能储存海量的数据，又能记录这些数据产生的时间？

（2）如何保证存储在数据库当中的数据不被篡改？

（3）如何使数据库变得可信任，进而确保我们在无实名的背景下也不会上当受骗？

自从区块链出现以后，上述三个问题便不再像之前一样那么棘手，似乎已经有了解决的可能。之所以这样说，主要是因为如果从效果的角度来看，区块链可以生成一个记录时间先后的、不可篡改的、可信任的数据库。

为了生成一个这样的数据库，区块链做了不少努力。首先，创新数据库的结构，将数据库中的数据分成不同的区块；其次，通过特定的信息，把区块链接到上一个区块的后面；最后，让区块以前后顺连的方式形成一条链，从而呈现出一套完整的数据。

在区块链当中，数据以电子记录的形式被永久储存下来，区块的主要作用就是储存这些电子记录，其生成遵循着严格的时间顺序。具体而言，每一个区块都会将自己被创建期间的交易活动记录下来，把全部区块汇总在一起就可以形成一个记录合集。

另外，不同区块链的区块结构可能会有所不同，但基本上都被分为区块头和区块体两个部分。区块头的作用是链接到前面的区块并保证区块链数据库的完整性；区块体的作用是储存与交易有关的所有记录。一般来说，区块结构有以下两个非常关键的特点。

第一，每一个区块上记录的都是上一个区块形成之后、该区块被创建前发生的交易活动。

第二，通常情况下，只要新区块完成记录并被加入到区块链的最后，那么记录在这个新区块上的交易信息以及数据就不可以被删除或者篡改。

上述所提到的第一个特点为区块链数据库的完整性提供了有力保障，使其变得可以被信任。第二个特点为区块链数据库的严谨性提供了有力保障，使其变得不可以被随意篡改。也正是因为有了这两个特点的助力，区块链数据库才可以发挥如此巨大的作用。

那么，何谓区块链数据库呢？顾名思义，以“区块链 +”的方式形成的数据库就被称为区块链数据库。在储存数据的时候，区块链数据库有自己的一套模式，如图 1-2 所示。

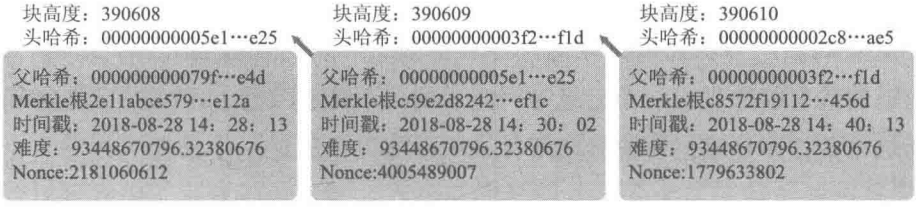


图 1-2　区块链数据库储存数据的模式

因为每一个区块头都包含了前一个区块的“交易信息压缩值”，所以，把开始的第一个区块，到当前最近的区块连接起来就形成了长链。又因为如果不知道前一区块的“交易信息压缩值”就不能继续生成当前区块，所以，每个区块必须要严格按照时间顺序跟随在前一个区块之后。

在这种模式下，储存在区块链数据库中的数据就可以有非常明确的产生时间，各自的先后顺序也十分的清晰明确。但应该知道的是，区块链数据库是以区块链为基础的，最后还要归结到区块链上。因此，与区块链数据库储存数据的模式相比，区块链的基本结构也同样重要。

在《区块链：互联网金融的终局》当中，有这样一段话：“人们把一段时间内生成的信息（包括数据或代码）打包成一个区块，盖上时间戳，与上一个区块衔接在一起，每下一个区块的页首都包含了上一个区块的索引数据，然后再在本页中写入新的信息，从而形成新的区块，首尾相连，最终形成了区块链。”

该段话深刻阐明了区块链的基本结构，而这一结构还有一个不得不提的最大创新点——“区块链＝时间戳”。“区块链”的结构可以保证区块链的完整性，从第一个区块开始，一直到生成当前区块为止，区块链上储存了与交易有关的所有数据。

不仅如此，在区块链的帮助下，区块链数据库中的任何数据都可以被查询，也可以被追本溯源，这样的话，无论是企业，还是机构，抑或是个人，都可以对这些数据进行验证，从而保证数据的真实性和有效性。

除了区块链的基本结构以外，区块链数据库的最大创新点也是“区块链＝时间戳”。区块链数据库可以在储存数据的过程中为每一个区块都盖上时间戳，以表示数据是在这个时间被记录到区块当中的。

上述做法不仅可以证明数据的储存顺序，还可以确保数据没有被篡改，更重要的是，可以大幅度地提升区块链数据库的可信任度。由此看来，区块链的确有能力生成一个记录时间先后的、不可篡改的、可信任的数据库，而这个数据库便是区块链数据库。