HZ BOOKS
华章IT

区块链技术丛书

以全方位视角，结合生活化的示例与图表生动讲解，从技术、应用到系统设计

涵盖区块链底层技术、典型业务场景设计、主流框架与应用，并手把手教你从零构建区块链系统（微链）

白话区块链

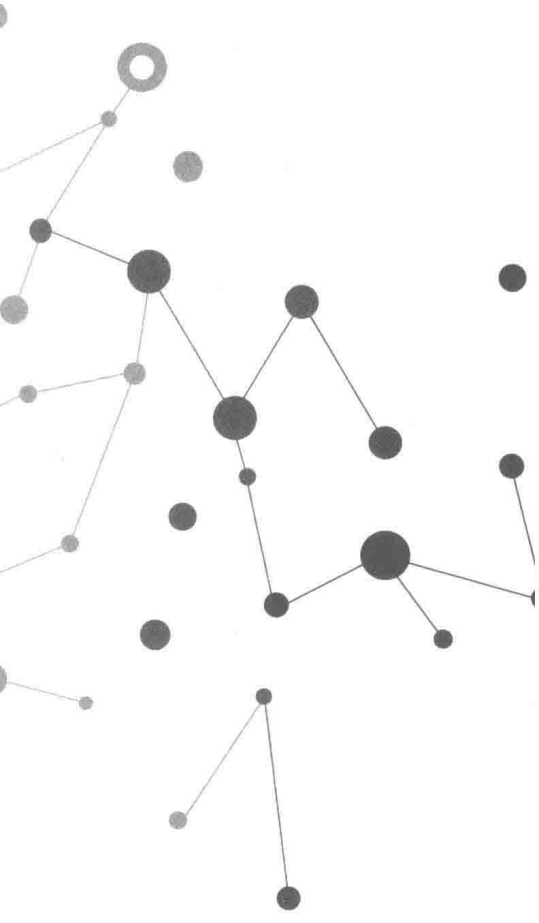
蒋勇 文延 嘉文 著

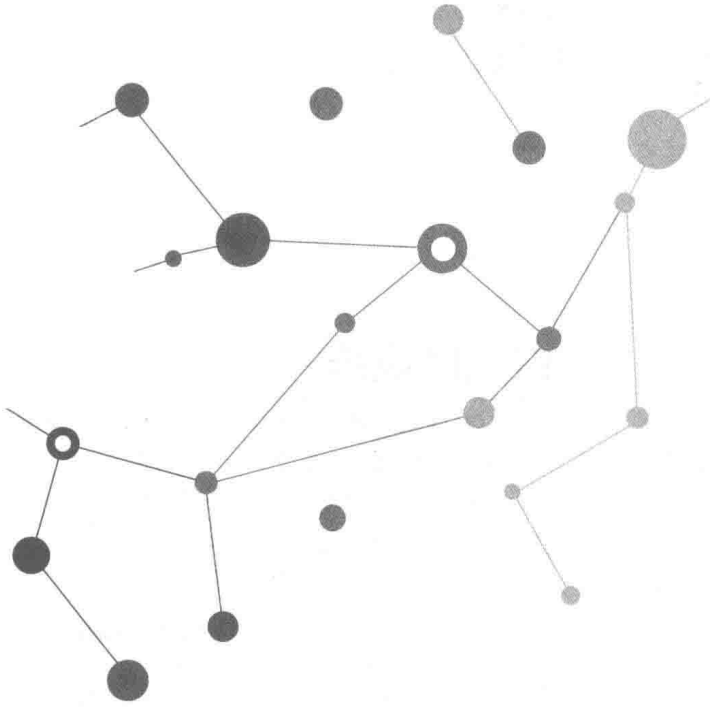
机械工业出版社
China Machine Press

区块链
技术丛书

白话区块链

蒋勇 文延 嘉文 著





机械工业出版社
China Machine Press

图书在版编目（CIP）数据

白话区块链 / 蒋勇，文延，嘉文著 . —北京：机械工业出版社，2017.10
（区块链技术丛书）

ISBN 978-7-111-58298-4

I. 白… II. ①蒋… ②文… ③嘉… III. 分布式计算机系统 - 研究 IV. TP338.8

中国版本图书馆 CIP 数据核字（2017）第 256191 号

白话区块链

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：缪 杰 高婧雅 责任校对：殷 虹
印 刷：北京市荣盛彩色印刷有限公司 版 次：2017 年 11 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：15.5
书 号：ISBN 978-7-111-58298-4 定 价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzit@hzbook.com

Reviewer 技术审校

韩璐，毕业于北京工业大学计算机科学与技术专业，现任大型金融机构信息安全架构师，深度参与互联网金融信息安全建设，对手机银行、网上银行等金融交易安全设计富于经验。从 2014 年开始关注区块链和数字货币，具有数字货币交易经验，同时也热衷于研究学习区块链技术原理，结合现任工作方向思考比特币、以太坊、零币等区块链技术安全特点及优势，也曾参与区块链相关项目。她是一个区块链及数字货币的爱好者，也是去中心化思想的支持者。

前　言 Preface

为什么要写这本书

想要写一本综合介绍区块链的书，这个想法是从2016年年底开始有的。一直以来，关于这方面的资料比较少，能够找到的资料，或着眼于经济金融方面的发展远景，或着重介绍区块链的发展历史，或阐述纯技术化的内容，读来总是有一种意犹未尽的感觉。而身边的朋友或对区块链完全陌生，或是有很多误解，还有些朋友甚至简单地认为区块链就等于比特币。笔者也曾多次在一些类似读书会的场合对区块链进行较为通俗的介绍，然而很多感兴趣的朋友来自银行、投融资等行业，他们并非都有完备的计算机知识背景，当然也不乏一些希望从事区块链技术开发的程序员。然而即便是用了自认为很通俗的文字和语言来介绍，也难以在短短的一两个小时内讲清楚，对于各种名词术语、各种新鲜概念，每当他们希望我推荐一些资料的时候，我都很头疼。对于一个还没有广为人知的事物，大家的求知欲是很强烈的，并不满足于囫囵吞枣地了解概念，但也不喜欢去啃枯燥深入的技术文字，他们只是希望能有一个系统化的介绍，白话点的，通俗些的，能把每个点都讲到，把技术原理、应用场景、发展历史、当前现状等都贯穿起来。鉴于此，写这么一本书的想法就愈发强烈了。

我自2012年由比特币开始关注区块链技术，一直只在一个小范围的技术圈内进行讨论交流，每每为理解了一个技术概念而欣喜不已。区块链技术绝不仅仅代表一种数字货币，某种程度上，与其说是一门技术不如说是一类思想或者价值观。比特币把区块链技术带入了世人的眼中，以一种“货币”的身份降临，着实带来了不少的神秘感，其带来的理念为后来者所发扬光大，闪电网络、比特股、以太坊、超级账本等，不断冒出各种新的理念和产品，它们都是为了解决某一特定问题以及应用到更多领域而发展起来的。区块链技术的各种特点（分布式、可信任、不可篡改、智能合约等），在与传统技术领域结合的过程中，一定会显示出巨大的优势。事实上这两年区块链技术的发展可以说是势如破竹，相当迅猛，国内外都开始有大

量的机构或者企业投入研究，力图能够抓住这未来的一缕阳光。

这一切，都要从全面了解区块链开始。

本书将呈现给读者一个全方位的视角，从技术到应用以及未来展望，以通俗的语言阐述区块链的各个技术点，力求给读者一个通透的讲解，并希望能抛砖引玉，引导读者拓展出新颖而有价值的思路。

本书特色

从章节安排来说，本书从比特币开始，到区块链技术的骨骼（密码算法）和灵魂（共识算法），再到目前知名的系统，最后到从零开始构建一个微型区块链系统。读者的学习是一个由生到熟的渐进过程，对区块链完全陌生的读者，可以先从章节中的非专业技术部分读起，对于已经有一定基础的读者，可以从中挑选感兴趣的内容。

从内容安排来说，除了概念与原理的介绍之外，更多的是各种示例以及图表，以大量示例介绍比特币的源码编译、以太坊智能合约的开发部署、超级账本 Fabric 的配置使用、模拟比特币的微型区块链系统的设计实现等。阐述中会使用各种示意图，形象、直观地帮助读者理解各个概念和过程。

行文风格方面，力求白话通俗，避免枯燥感，使阅读体验更好。

读者对象

- ❑ 希望进行区块链开发的程序员。
- ❑ 希望投资或参与区块链项目的人员。
- ❑ 对区块链感兴趣的爱好者。

如何阅读本书

第 1 章　介绍区块链的技术组成，并以比特币为例介绍各种基础技术原理。

第 2 章　综合介绍目前的各种区块链应用，为后面的技术介绍铺垫场景。

第 3 章　介绍现代密码算法在区块链中的作用。

第 4 章　介绍各种网络共识算法。

第 5 章　介绍区块链的链内外互联扩展技术。

第 6 章　详细介绍以太坊的技术结构以及智能合约开发。

第 7 章　详细介绍超级账本项目以及 Fabric 的配置使用。

第 8 章　详细介绍如何从零开始设计一个微型区块链系统（简称微链）。

第 9 章　介绍目前出现的各种区块链技术问题。

勘误和支持

由于笔者水平有限，编写时间仓促，书中难免会出现一些错误或者不准确的地方，恳请读者批评指正。如果你有更多的宝贵意见，欢迎通过微信或邮件进行讨论。你可以通过微信 Cshen003、微博 @ 行者 C 神，或者发送邮件到邮箱 tnix_blockchain@outlook.com 联系到我，我会尽量给出满意的解答，期待能够得到你们的真挚反馈，在技术之路上互勉共进。

致谢

感谢我的作者伙伴——文延和嘉文，他们在工作之余，挤出宝贵的时间为本书贡献了他们对区块链技术的深入理解以及应用的展望分析，他们的专业和敬业令我感到钦佩。

感谢韩璐女士为本书做的审核工作，为书稿的内容质量付出了辛勤的劳动。

感谢比特币社区、以太坊社区、超级账本社区以及巴比特论坛各位技术专家，每次阅读他们的技术文章都让我有所收获，本书也多处引用了他们的观点和思想。

感谢中本聪，是他带来了区块链！

特别致谢

最后，感谢父母从小对我的培养，他们为我创造了良好的学习环境并培养了我爱好读书的习惯，这个习惯将伴随我终生并使我受益匪浅。因为工作和写书，牺牲了很多陪伴家人的时间，所以我更要感谢太太王晓英长期以来对我的默默支持，以及女儿 Cindy 对我工作的理解。

谨以此书献给我最亲爱的家人，多年以来帮助、支持我的朋友们，以及众多热爱区块链技术的朋友们！

蒋　勇

Contents 目　录

第 1 章 Chapter 1

初识区块链

本章我们将从区块链的原理及分类、技术组成、技术特点等出发来初步介绍区块链的概念，并通过分析比特币的结构让大家对区块链有一个感性的认识。比特币作为区块链技术的第一个应用，它的原理设计影响深远。

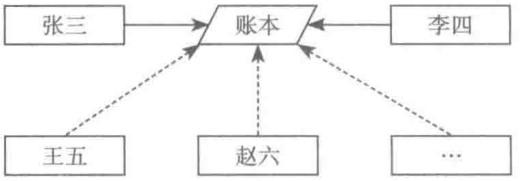
1.1 例说区块链

1.1.1 从一本账本说起

早些时候，农村一般都会有个账房先生，村里人出个工或者买卖些种子肥料等，都会依靠这个账房先生来记账，大部分情况下其他人也没有查账的习惯，那个账本基本就是这个账房先生保管着，到了年底，村长会根据账本余额购置些琐碎物件给村里人发发，一直以来也都是相安无事，谁也没有怀疑账本会有什么问题。账房先生因为承担着替大家记账的任务，因此不用出去干活出工，额外会有些补贴，仅此一点，倒也是让一些人羡慕不已。下图便是当时账本的记账权图示：

终于有一天，有个人无意中发现了账房先生的那本账。看了下账面，发现数字不对，最关键的是支出、收入、余额居然不能平衡。对不上，这可不行，立即报告给其他人，结果大家都不干了，这还得了。经过一番讨论，大家决定，轮流来记账，这个月张三，下个月李四，大家轮着来，防止账本被一个人拿在手里。于是，账本的记账权发生了如下图所

示的变化：



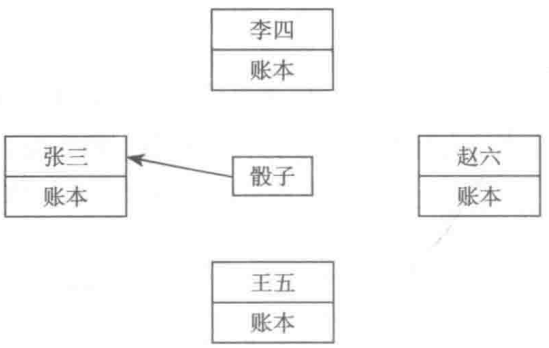
通过上图我们可以看到，村里的账本由大家轮流来保管记账了，一切又相安无事了，直到某一天，李四想要挪用村里的公款，可是他又怕这个事情被后来记账的人发现，怎么办呢？李四决定烧掉账本的一部分内容，这样别人就查不出来了，回头只要告诉大家这是不小心碰到蜡烛，别人也没什么办法。

果然，出了这个事情以后，大家也无可奈何。可是紧接着，赵六也说不小心碰到蜡烛了；王五说不小心掉水里；张三说被狗啃了……终于大家决定坐下来重新讨论这个问题。经过一番争论，大家决定启用一种新的记账方法：每个人都拥有一本自己的账本，任何一个人改动了账本都必须要告知所有其他人，其他人会在自己的账本上同样地记上一笔，如果有人发现新改动的账目不对，可以拒绝接受，到了最后，以大多数人都一致的账目表示为准。

果然，使用了这个办法后，很长一段时间内都没有发生过账本问题，即便是有人真的不小心损坏了一部分账本的内容，只要找到其他的人去重新复制一份来就行了。

然而，这种做法还是有问题，时间长了，有人就偷懒了，不愿意这么麻烦地记账，就希望别人记好账后，自己拿过来核对一下，没问题就直接抄一遍。这下记账记得最勤的人就有意见了。最终大家开会决定，每天早上掷骰子，根据点数决定谁来记当天的账，其他人只要核对一下，没问题就复制过来。

我们可以看到，在这个时候，账本的记账权变成了这样：



通过上图，我们可以看到，经历了几次风雨之后，大家终于还是决定共同来记账，这样是比较安全的做法，也不怕账本损坏丢失了。后来大家还决定，每天被掷到要记账的人，能获得一些奖励，从当天的记账总额中划出一定奖励的比例。

实际上，最后大家决定的做法，就是区块链中记账方法的雏形了，接下来我们就来了

解一下区块链的技术理念。

1.1.2　区块链技术理念

区块链在本质上就是一种记账方法，当然了，并不是通过人来记账的，而是通过一种软件，我们暂且简称为区块链客户端。以上面的例子来说，张三、李四、王五、赵六等人，就相当于一个个的区块链客户端软件，它们运行在不同的设备上，彼此之间独立工作。通常我们把运行中的客户端软件称为“节点”。这些节点运行后，彼此之间会认识一下。它们彼此之间是这样认识的：张三认识李四也认识王五，赵六联系到了张三，让张三把他认识的人的联系方式发给自己，这样赵六也认识了李四和王五，通过这样的方式，大家就形成了一张网，有什么事只要招呼一声，立马消息就会传遍整个网络节点。这种方式跟新闻转发差不多，不需要依靠某一个人，大家就能互通消息了，在区块链软件的结构中，这种互相通信的功能称为“网络路由”。

在这个网络中，每个节点都维护着自己的一个账本，账本中记录着网络中发生的一笔笔账务。具体是什么样的账务呢？这得看具体是什么样的功能网络。区块链技术属于一种技术方法，可以用来实现各种不同的业务功能，小到如上例中的日常记账，大到各种复杂的商业合约，等等，记录的数据也就不同了。网络中的节点是独立记账的，可是记账的内容要保持彼此一致。所用的方法就是设定一个游戏规则，通过这个规则选出一个记账的节点，就如上例中的掷骰子。在区块链系统中，这个所谓的“掷骰子”称为“共识算法”，就是一种大家都遵守的筛选方案，我们可以先这么简单地理解。选出一个节点后，则一段时间内的账务数据都以这个节点记录的为准，这个节点记录后会把数据广播出去，告诉其他的节点，其他节点只需要通过网络来接收新的数据，接收后各自根据自己现有的账本验证一下能不能接得上，有没有不匹配和不规范的，如果都符合要求，就存储到自己的账本中。

在有些系统中，会考虑到被骰子投中的节点的劳动付出，毕竟它要负责整理数据，验证数据，打包数据，还要再广而告之，这个活还是挺辛苦的。于是会设计一种激励机制，负责打包数据的那个节点可以获得系统的奖励，这个奖励类似于论坛积分，站在软件技术的角度，就是一个数据。这个数据可以视为奖金，有时候大家会很积极地去争取那个奖金，于是就希望骰子能投中自己，有些区块链系统在这个环节会设计出一种带有竞争的机制，让各个节点去抢，谁能抢到这个机会谁就能获得打包数据的权力并且同时获得这笔奖励，在这种情况下，我们会形象地将这个竞争的过程称为“挖矿”。

那么，话又说回来了，我们将一个个运行客户端称为节点，那到底怎么标记不同的使用者呢？也是通过用户名注册吗？实则不然。在区块链系统中，这个地方的设计很有意思，是通过一种密码算法来实现的，具体来说是通过一种叫公开密钥算法的机制来实现的。我们知道，对于一种密码算法来说，无论算法过程是什么样的，都会有一个密钥。而公开密钥算法拥有一对（也就是两个）密钥，跟虎符一样，是彼此配合使用的，可以互相用来加解

密。其中一个叫私钥，另外一个叫公钥，公钥可以公开给别人，私钥要自己保管好。在区块链系统中，公钥就是用来用户身份识别的，一般不会直接使用公钥，因为不容易让人记住。公钥往往都比较长，实际处理的时候都会进行转换，比如取得公钥的最后 20 个字节或者经过一系列更复杂的转换，最后得到一个称为“地址”的转换结果，这个“地址”就能代表一个用户。

为什么在区块链系统中要用这么一个奇怪的用户身份表示方法呢？似乎看起来除了有些创意外，也没特别的用处。这里我们就得再介绍下这个公开密钥算法的特别能力。之前提到说这种算法有两个密钥，那么这两个密钥是怎么配合工作的呢？我们来简单说明一下：用公钥加密的数据必须用对应的私钥来解密，而用私钥加密（通常称为“签名”）的数据必须用对应的公钥来解密。这个特点可是能发挥很大用处的，就如上述的例子中，如果张三要发送给李四一张支票，那怎么传送呢？就这么发过去，会被那个记账的人拿到，风险可就大了。于是张三想了一个办法，他在支票上用李四的公钥加了个密，然后再签上自己的名字（使用自己的私钥签名），这个时候其他人就算拿到支票也没用，因为只有李四才有自己的私钥，也只有李四才能解开这张支票来使用。这种功能设计在区块链系统中称为“脚本系统”。

现在我们知道了，区块链的技术理念，其实就是大家共同来参与记账，通过一种规则不断地选出账务打包者，其他节点接收验证，并且每个用户都有一对密钥表示自己，通过脚本系统的功能实现在公共网络中定向发送有价值的数据。

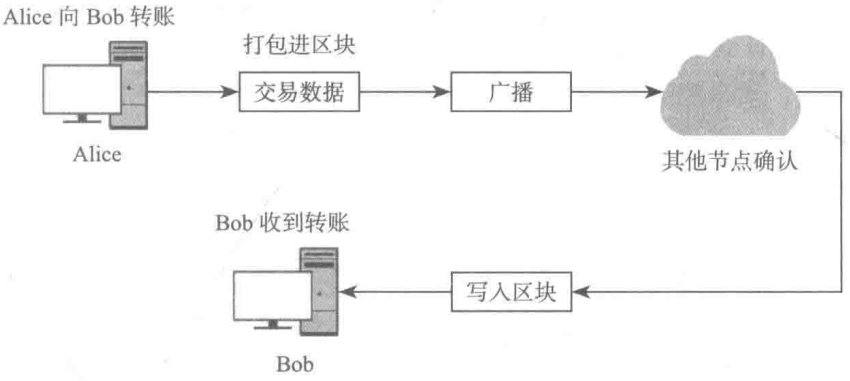
1.1.3 一般工作流程

通过上面的例子，相信读者朋友对区块链已经有了基本认识。区块链系统有很多种，第一个应用区块链技术的软件就是比特币，事实上区块链的概念就是比特币带出来的。到现在为止，已经出现了相当多的基于区块链技术的衍生系统，比如闪电网络、公证通、以太坊、超级账本项目等。每一类系统都有自己的特点，例如汽车设计，有的设计成跑车，有的设计成运输车，有的设计成商务车，但是有一点，无论是什么类型的车，它的工作方式或者说工作流程都是类似的，在本质上它们都是同一类技术结构的产物。在这一小节，我们从一般性的角度阐述一下区块链系统的工作流程，为了便于说明，我们会选取一些场景例子。

我们先来看一个转账交易的流程。转账交易本质上就是发送一笔数据，这个数据可以表示为资产，也可以表示为订单或者其他各种形式的数据，我们看一下下面的图示。

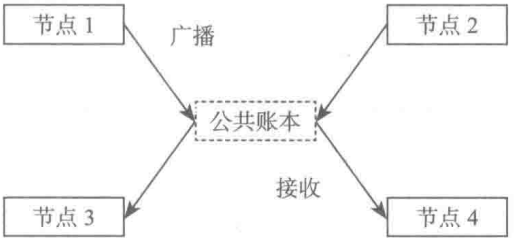
从图中我们可以看到，整个数据的发送过程其实还是很简单的，数据发送出去后，会被打包进区块，然后广播出去给所有的节点确认，确认没有问题后就写入到各自的本地区块链账本中，当网络中的大多数节点都确认写入后，这个转账过程就算是完成了。有朋友可能会问，在这种分布式的网络中，怎么能知道是被大多数节点确认写入了呢？这里并没有什么服务器登记呀？这个问题我们先留着，在下面讲到区块链分类的时候会有详细的解

释，大家可以先思考一下。



这个工作流程图是有代表性的，其他各种系统都是在这个基础上进行衍生和扩展。比如有些会增加身份认证功能，以确保只有符合身份验证的用户才能发送数据；有些则扩展交易数据的表达能力，不但能用来表示一般的交易转账，还能表示更复杂的商业逻辑。各种应用很多，但是万变不离其宗。

实际上，说一千道一万，整个区块链网络，就是大家共同来维护一份公共账本。注意了，这个公共账本是一个逻辑上的概念，每个节点各自都是独立维护自己账本数据的，而所谓的公共账本，是说各自的账本要保持一致，保持一致的部分就是公共账本，我们看下图示：



如图所示，有些节点在广播新的数据，有些节点在接收数据，大家共同维护一个账本，确保达成一致。区块链技术其实就是围绕如何保持数据的一致、如何让这个公共账本的数据不被篡改来展开的。为了解决这些问题，区块链技术拥有一套技术栈，我们通过以下章节来阐述。

1.2　区块链技术栈

区块链本身只是一种数据的记录格式，就像我们平常使用的 Excel 表格、Word 文档一样，按照一定的格式将我们的数据存储在电脑上。与传统的记录格式不同的是，区块链是将产生的数据按照一定的时间间隔，分成一个个的数据块记录，然后再根据数据块的先后关系串联起来，也就是所谓的区块链了。按照这种规则，沿着时间线不断增加新的区块，