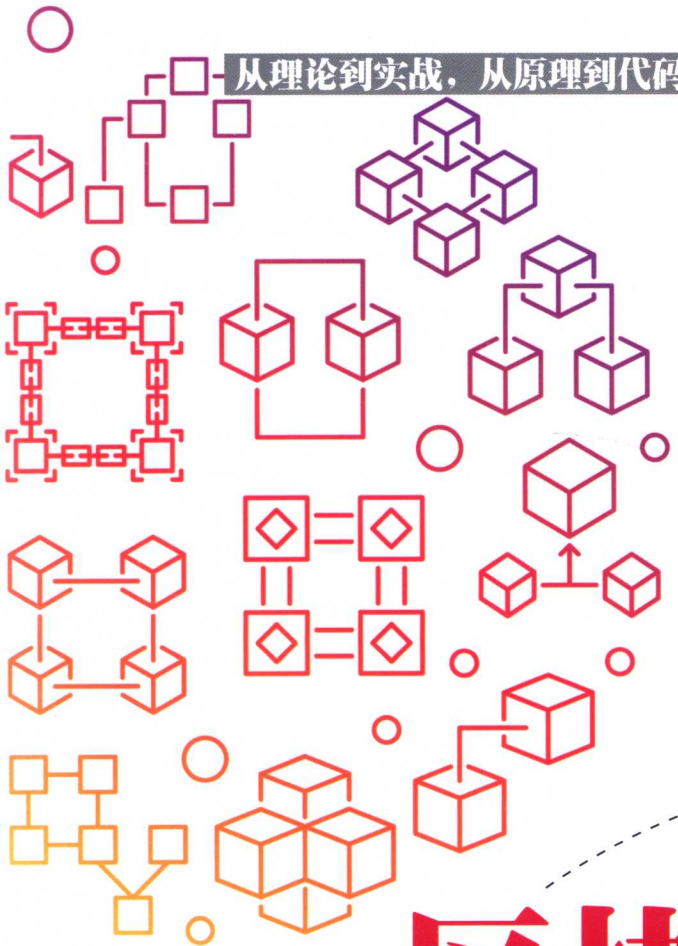
从理论到实战，从原理到代码，一本书搞定区块链的底层技术



陈人通◎编著

# 区块链开发

## 从入门到精通

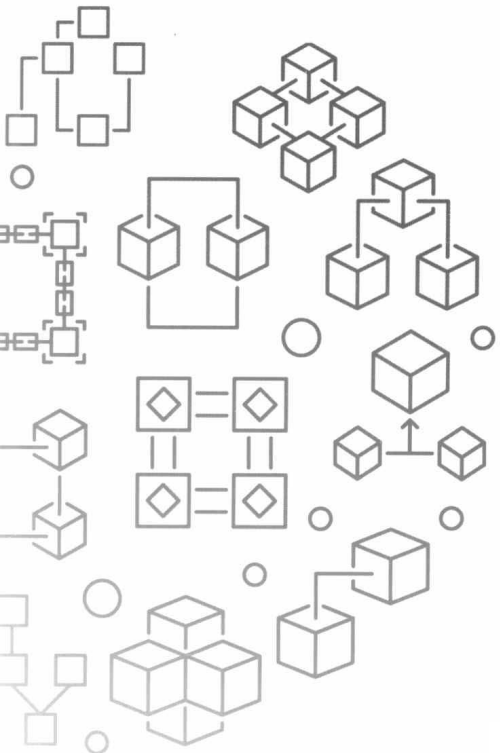
### 以太坊+超级账本

**范围广**
涵盖数字货币、以太坊及超级账本等三大应用

**容易学**
用大量的图片、图示来详解区块链的实现原理

**很有用**
详解区块链核心技术，细致剖析两大开发案例

中国水利水电出版社
www.waterpub.com.cn



# 区块链开发从入门到精通

## 以太坊+超级账本

陈人通◎编著

中国水利水电出版社
www.waterpub.com.cn
·北京·

## 内 容 提 要

《区块链开发从入门到精通 以太坊+超级账本》系统讲述了区块链原理、技术与应用，全书分三大部分：区块链思想以及去中心化应用、区块链技术在去中心化数字货币系统中的应用、区块链热议话题与区块链技术的典型应用场景；区块链的核心技术——密码算法和共识算法；最后一部分系统介绍了区块链的应用开发平台——以太坊和超级账本，包括以太坊项目的主要设计及如何用 Solidity 语言创建能够部署到以太坊平台的智能合约应用、后起之秀超级账本项目（尤其是 Fabric 子项目）的设计以及如何在 Fabric 超级账本项目上搭建和运行区块链网络。

《区块链开发从入门到精通 以太坊+超级账本》内容由浅入深、遵循区块链技术的发展规律，从区块链的思想缘起，到技术应用与发展趋势，剖析实际落地案例，探究区块链价值及未来发展趋势，帮助读者快速步入区块链应用新时代。

《区块链开发从入门到精通 以太坊+超级账本》适合想要了解区块链技术但没有基础的新手读者，也适合以太坊智能合约开发人员或者超级账本链码开发人员使用，亦可作为互联网金融研究员、互联网创业者、数字货币爱好者及各类程序员学习区块链技术的参考用书。

**图书在版编目（CIP）数据**

区块链开发从入门到精通 ：以太坊+超级账本 / 陈人通编著. —北京：中国水利水电出版社, 2019.11

ISBN 978-7-5170-7744-2

Ⅰ. ①区… Ⅱ. ①陈… 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（2019）第 112859 号

| | |
|---|---|
| 书　　名 | 区块链开发从入门到精通　以太坊+超级账本<br>QUKUAILIAN KAIFA CONG RUMEN DAO JINGTONG YITAIFANG+CHAOJI ZHANGBEN |
| 作　　者 | 陈人通　编著 |
| 出版发行 | 中国水利水电出版社<br>（北京市海淀区玉渊潭南路 1 号 D 座　100038）<br>网址：www.waterpub.com.cn<br>E-mail：zhiboshangshu@163.com<br>电话：（010）62572966-2205/2266/2201（营销中心） |
| 经　　售 | 北京科水图书销售中心（零售）<br>电话：（010）88383994、63202643、68545874<br>全国各地新华书店和相关出版物销售网点 |
| 排　　版 | 北京智博尚书文化传媒有限公司 |
| 印　　刷 | 三河市龙大印装有限公司 |
| 规　　格 | 170mm×230mm　16 开本　20.25 印张　373 千字　1 插页 |
| 版　　次 | 2019 年 11 月第 1 版　2019 年 11 月第 1 次印刷 |
| 印　　数 | 0001—5000 册 |
| 定　　价 | 79.80 元 |

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

# 前　言

区块链技术是近几年随着比特币系统（一个去中心化加密数字货币系统的典型代表）的兴起而被炒得火热的一项新技术，在最初出现的时候，区块链技术仅仅是用来解决比特币系统中分布式交易记账的问题。

对大部分人来说，“区块链技术”可能只是一个新名词而已，但是对那些善于思考的专家或学者来说，将区块链技术从比特币系统中“提炼出来”后可以作为一种全新分布式架构技术的底层框架，而一些较为明朗的专业人士则认为区块链技术不仅仅是一项技术，在它的设计中体现出来的是一种新的经济贸易方式、新的消费理念和新的组织结构形式。

一些对区块链技术有大胆想法的人，也将他们的想法付诸了实践，这也就导致了一些区块链技术的应用如雨后春笋般被开发出来，例如，同比特币系统极其相似的莱特币系统、零币系统、达世币系统，实现了智能合约的部署与运行的以太坊平台，以及实现了用户应用链码的部署与运行的超级账本平台等。

笔者从2010年就开始接触和了解比特币系统，2014年比特币系统名声大噪，笔者也更加关注比特币系统的发展，尤其是其核心——区块链技术。在2015年以及之后的几年，类似于以太坊和超级账本等基于区块链技术开发的应用逐渐变多，不同于比特币系统只用于数字货币收支的单一功能，这些应用提供给开发人员的更像是应用的开发和运行平台。

为了对区块链技术进行更深入的讲解，本书不仅着眼于它的最初使用场景——去中心化加密数字货币系统，还重点分析了区块链技术中用到的密码算法和共识算法，在书的后半部分，对以太坊和超级账本的介绍各占两章，重点包括它们相比于之前的典型区块链技术应用在设计上有什么突出的地方，以及如何通过智能合约和用户应用链码开发出去中心化应用。

## 本书特色

- 内容详略得当

区块链涉及的技术很多，到底哪些该讲，哪些不该讲，需要慎重对待。本书集中讲解了区块链开发必备的技术，有些相关度不高、应用场景不多的技术就一笔带过，让读者用最短的时间掌握最有用的技术。

- 代码展示齐全

在本书中，涉及代码编写的部分均给出了详细的代码及解释，这对于读者理

解书中的案例非常有帮助。

- 图片资源丰富

相比于冗长的文字而言，一张优美的图片不仅能起到辅助说明的作用，还能消除读者内心中对阅读的抵触情绪。不可否认书中文字部分非常多，但是在必要的位置都插入了图片进行内容展示。

## 本书读者对象

- 互联网金融研究人员
- 各类程序员
- 互联网创业者
- 区块链技术开发者
- 数字货币爱好者

## 本书源文件下载

本书提供代码源文件，有需要的读者可以关注右侧的微信公众号（人人都是程序猿），然后输入“QKL77442”，并发送到公众号后台，即可获取本书资源的下载链接，然后将此链接复制到计算机浏览器的地址栏中，根据提示下载即可。

## 作者简介

陈人通，资深产品经理、经济管理博士、著名经济学家、数字货币领域领航人实践者、数字货币领域权威专家，多年来致力于区块链产品开发、金融投资与区块链行业研究。现任爱普科技董事长、北斗集团董事局执行总裁、世界海外学人投资联盟机构轮席主席、中国鸿途投资发展有限公司董事局执行主席、世界海外学人投资联盟机构大中华区首席投资顾问、经济管理领域领航人、EMBA 企业家总裁班客座教授。

## 致谢

本书能够顺利出版，是作者、编辑和所有审校人员共同努力的结果，在此表示深深地感谢。同时，祝福所有读者在职场一帆风顺。

编 者

# 目 录

# 第1章　区块链思想以及去中心化应用

区块链（Blockchain）思想源于当初被炒得沸沸扬扬的比特币（Bitcoin）开源项目。比特币项目博采百家之长，可以在其中找到来自数字货币、密码学、博弈论以及分布式系统等诸多领域的相关理论。在下一章，我们会重点讲解区块链思想是如何从比特币中诞生的，但是在本章，我们将目标放在区块链本身。

在比特币之后，又出现了一些以区块链技术作为核心支撑结构的所谓去中心化应用（Decentralized Application，DApp），正是由于这些DApp的出现，区块链技术才取得了许多令人瞩目的创新成果。从1.4节开始，我们将介绍去中心化的应用。

## 1.1　从记账角度理解区块链

比特币系统率先引进了区块链的思想，为的是通过区块链记录过去发生的每一笔转账交易。记录这些交易信息有用吗？非常有用！除了奖励给“矿工”（负责将多个独立的交易写入区块链整体中）的比特币是新创造出来的外，历史发行的比特币的数量是固定的，记录每一笔交易的交易信息就是为了保证比特币数量的固定。区块链数据是不容易被修改的，强制修改了区块链中的交易信息就相当于变更了设定的比特币数量，这会对比特币系统的稳定运行造成影响。

在深入探索区块链技术之前，对区块链技术本身有一个比较清晰的理解是非常重要的，相信对于大多数人而言，“区块链”是一个比较陌生的词汇。既然使用区块链的目的是记录过去发生的每一笔转账交易（至少早期的区块链是为此而设计的），那么本节就通过一个简单的记账例子来解释区块链，从而消除读者们对于区块链技术的陌生感。

在集体计划经济时代，所有人都生活在他所属于的一个群体中，例如，乡镇合作社，一般每一个群体中都有一个账本用于记录这个群体的财政收支，并且也

会有一个专职的账房管理员来看管这个账本。账房先生的工作简单来说就是在账本上记录整个团队中平时的收入和支出情况，例如，农村里集体购买农具的记账可以算作是一笔支出，将集体的粮食卖出后所获得的经济收益可以算作是一笔收入，这样的管理员与账本之间的关系如图 1-1 所示。


图 1-1 原始的一个管理员记账方式

这样由一个人负责记账的缺点是当账目出错，在其他人都没有余力去承担起监督账目的工作时，等到年末或月底结算的时候，哪怕是管理员只有一笔账目没有正确记录或者有人提出了反对的意见，都需要重新核对并确认每一笔账目，这是一件非常麻烦的事情。由此看来，这个管理员最期望出现的理想情况应该是所有人都对账目没有异议。

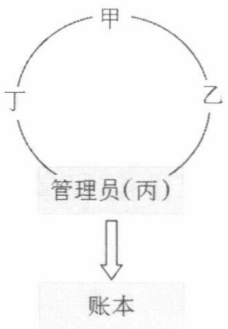



图 1-2 多个管理员轮流记账的方式

针对一人记账容易出错的问题，也许将账本从一人专门管理升级为多人轮流管理是一个比较不错的做法，假设一共有甲、乙、丙、丁四人轮流来做管理员，那么这样的管理员与账本之间的关系如图 1-2 所示。

在运行机制上，多人轮流管理账本相对于专人专管账本是有很大的进步性。首先，账本在多人手里流转，之前的人所记录的账目可以在短时间内让接下来的一个人检查，这样可以尽量避免错误的发生；其次，节省了人力资源（没有了专门的账房管理员）。

但是时间一长，这样的方式也可能会暴露一些弊端。试想一下，如果一个群体中存在有私心的人，那么他拿到账本以后很可能会为自己创造一笔“隐形”的收入，措施也很简单，销毁这部分账目就行了。一个人如此，那么其他的人在看到他的“成果”之后也很有可能效仿。这也就是多人轮流管理账本的弊端所在，这种做法不能确保公正性。

之所以多人轮流管理账本存在这样的一个弊端，是因为账本只有一个，这一个账本遭到破坏就不能再对账本查证了。那我们很自然地想，让这些管理员每人管理一个账本不就行了？对，这是一个不错的办法。此时的管理员与账本之间的关系如图 1-3 所示。

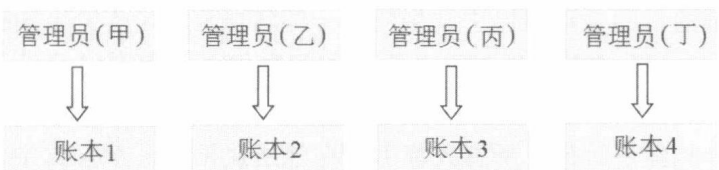



图 1-3 多个管理员分别记账的方式

如果真采用了这样的记账方式，那么相当于多找了几个专职的管理员，这是非常不划算的，因为支出的人力成本实在太大了。以上所说的这些都不是区块链的真正记账方式，那么区块链中的记账方式是怎么样的呢？假设这些管理员每人都有一个账本，他们要做的只是每天随机选一个人在他的账本上记账，第二天其他人从他的账本中抄录记账数据并核对是否有误，然后再随机选出另一个人来记录这一天的财政支出情况，第三天其他人再从这个人的账本中抄录记账数据并核对是否有误，以此类推。此时的管理员与账本之间的关系如图1-4 所示。

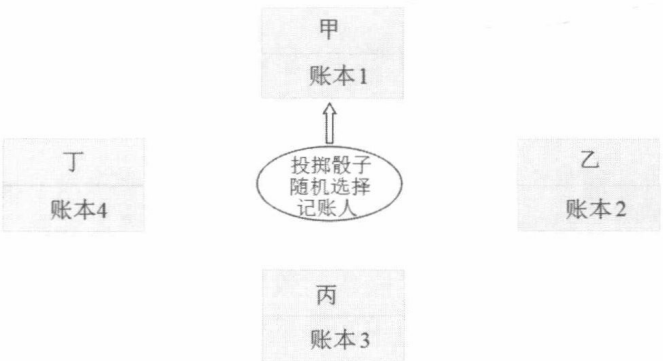



图 1-4　区块链式的记账方式

观察图 1-4，不得不说这的确是一个非常不错的方法，某天轮到某人记账时，他还会像最初的专职管理员一样获得一份额外的兼职收入，同时他也无法篡改记账数据，因为其他人也在掌握着账本。

区块链中的“矿工”就相当于账本管理员。矿工们接收全网的交易信息，并每 10 分钟参与一次全网的解题选拔，计算机硬件水平高的矿工会相对于其他竞赛选手更快地解得正确答案，这时他就有权利将这一时间段的全网交易信息（可能有很多的交易）打包成一个区块并填入整体的区块链中，作为矿工的劳务费，他会得到一些奖励（比特币系统中的奖励就是一定数量的比特币，以太坊中的奖励就是一定数量的以太币）。而矿工们将一段时间内的交易信息打包到区块链中的行为就被通俗地称为“挖矿”。

## 1.2　区块链技术的典型成分

区块链技术毕竟是利用计算机技术实现的一种全新的记账方式，所以说区块链技术就是一系列计算机技术的结晶。无论区块链技术怎么演化，使用区块

链技术实现的应用主要包括网络通信、区块链账本、共识机制和密码算法这四部分。这一节，我们来看一下这四部分主要在区块链技术应用中扮演了什么样的角色。

另外，不排除一些新兴的区块链技术应用中包括身份验证或权限管理等其他的组成部分，但上述这四部分是无论在什么样的区块链技术应用中都明显存在的。

### 1.2.1 网络通信

上一小节介绍了记账方式的演变，之所以先介绍这些内容是因为区块链技术在本质上就是实现了一种记账方法，它是用一种特定的格式（就像 Excel 或 Word 中的排版格式一样）将记录的数据存储在计算机上。与账本有关的参与者使用一种客户端软件参与到账本的维护中。例如，在上一小节的例子中，甲、乙、丙和丁四人通过掷骰子的方法确定当天的记账人，他们每人都需要安装一个客户端软件，这个软件上存储了账本的数据，当天的记账人要更新账本数据并广而告之给其他客户端软件的用户。除了他们四个人之外，其他的村民也要安装这个客户端软件，除了存储账本数据外，这个软件还具有资金收入和支出的功能，用于完成交易。

这个客户端软件是分布式的，运行在不同的设备上，通常将运行中的客户端软件称为“节点”。这些节点运行后，会通过一种拓扑关系连接彼此相近的节点。例如，甲能连接到乙和丙，乙能连接到丙和丁，那么通过乙，甲也能连接到丁（如图 1-5 所示），以此类推，通过这样的拓扑关系，大家就形成了一张网，某个人发送了一条信息（如交易信息），那么立马消息就会传到全部节点上。这就像是转发头条新闻一样，新闻从主编那里出来，一传十，十传百，很快大家就都知道这个头条新闻了。

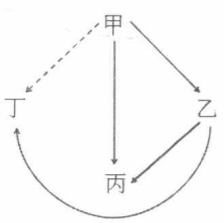



图 1-5 甲、乙、丙、丁之间的拓扑关系

这样，我们就能明白区块链的客户端应用软件运行在一个分布式的网络环境中，确切地说是一个P2P（Peer to Peer，点对点）的网络架构。这样一来，应

用开发者就需要考虑，在分布式的网络结构中无法加入一个中心服务器的情况下，应用该采取一种什么样的协议来完成节点之间的信息传递，从而达到摆脱对中心服务器中介作用的依赖。除了完成节点之间快速的信息传递的功能外，协议的另一个重要功能就是快速地发现节点。

为什么在节点之间快速地传递信息非常重要？因为在没有中心服务器作为中介的情况下，用户想要同步数据，只能在临近节点那里快速拷贝，这相当于把临近节点当成了服务器对待，能否及时拷贝并传递到网络中的所有节点取决于节点之间信息传递的速度是否足够快。

快速地在节点间同步数据允许某一节点向与之相连的节点发送数据请求来下载最新的数据，这就是区块链网络中时时更新已有账本数据的一种方式。及时地更新账本数据是非常有必要的。通过这种方式，网络中的每一个节点都会在某一个时刻达成数据上的一致。

快速地发现节点也非常重要，在中心服务器存在的时候，所有节点应该在启动后主动连接到服务器，但是中心服务器不存在的时候，所有节点在启动后应该快速搜索邻近的节点是否在线，如果在线就要构成连接，连接到其他节点才是与网络发生交互的前提。

### 1.2.2　区块链账本

如上所述，所有的节点都保存有一份账本数据，并通过网络从其他节点那里更新账本数据，我们暂且称这个账本为区块链账本。区块链账本的数据主体是网络中发生的每一笔交易。那么区块链账本中记录数据的格式是什么样的呢？

形象地说，区块链就是“区块+链”。其中所谓的“区块”就是指数据块的意思，每一个数据块中都记录了一段时间内发生的交易的信息，交易的数量或多或少。所谓的“链”就是指区块之间通过某种方式链接起来，从而形成一条单向无环链。图 1-6 展示了区块链结构的链接方式。

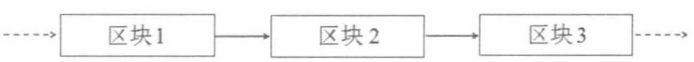



图 1-6　区块链简单示意图

如图 1-6 所示，区块链最显著的特征就是区块之间的链接是有向无环的。

区块链中区块的产生速度要根据实际情况进行设置。例如，上一小节介绍的甲、乙、丙、丁四人按照投掷骰子的方法确定这一天谁记账，那么他们使用的这个区块链账本应该是每一天产生一个区块，在这个区块中，也许昨天没有发