HZ BOOKS
华章IT

区块链
技术丛书

清华五道口
互联网金融丛书

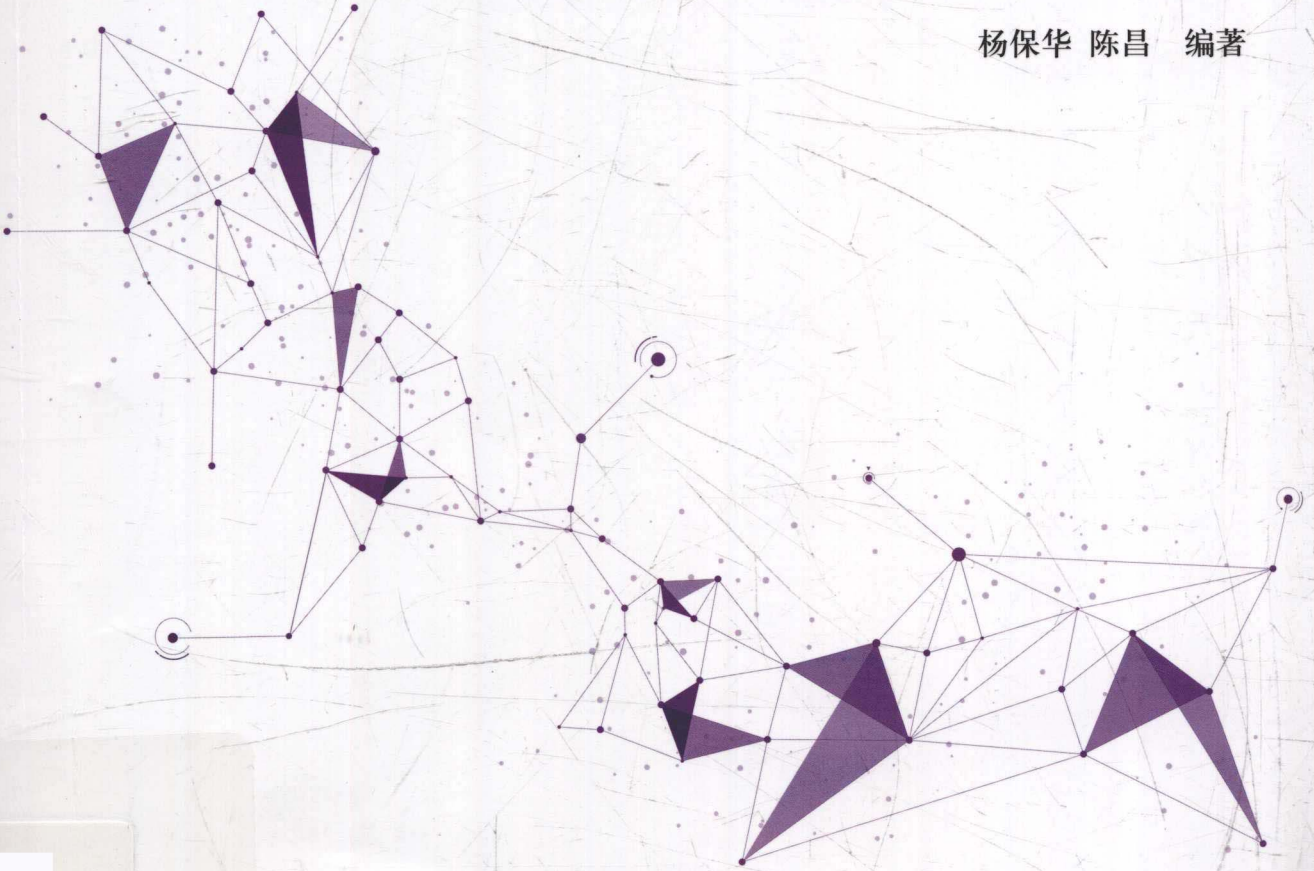
超级账本核心设计和开发者撰写，区块链开发落地专业指南。

由浅入深，详细讲解超级账本Fabric 1.0架构设计与应用开发。

区块链

原理、设计与应用

杨保华 陈昌 编著



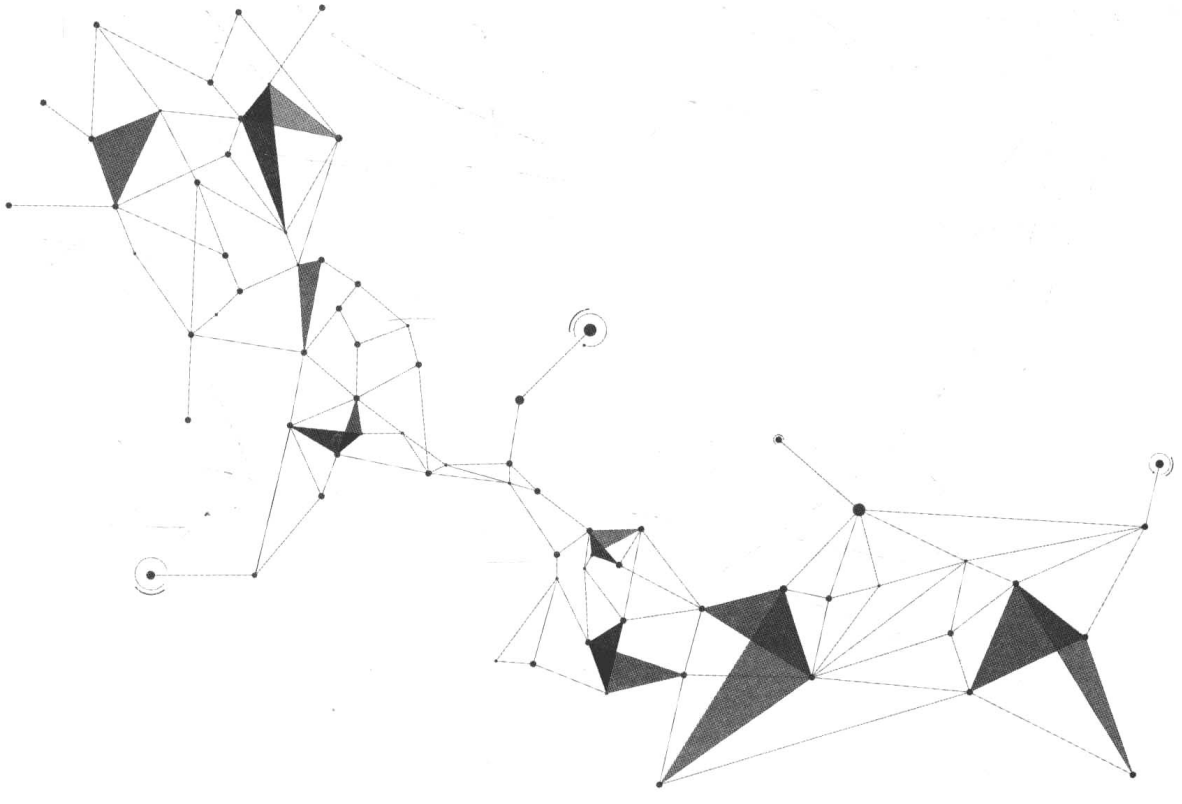
机械工业出版社
China Machine Press

区块链
技术丛书

区块链

原理、设计与应用

杨保华 陈昌 编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

区块链原理、设计与应用 / 杨保华，陈昌编著 . —北京：机械工业出版社，2017.8
（区块链技术丛书）

ISBN 978-7-111-57782-9

I. 区… II. ①杨… ②陈… III. 电子商务 – 支付方式 – 研究 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2017）第 197360 号

区块链原理、设计与应用

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：吴 怡 责任校对：李秋荣
印 刷：北京市荣盛彩色印刷有限公司 版 次：2017 年 8 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：23
书 号：ISBN 978-7-111-57782-9 定 价：89.00 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

Preface 序　言

金融是人类文明发展过程中经济运行的基础，自诞生起，金融领域就伴随经济发展的阶段和商业模式的变迁不断涌现出先进的技术手段，这些都大大提升了社会和经济的运转效率。从延续了近千年的纸质记账，到二十世纪的电子化交易，再到影响现在及未来的互联网、大数据、人工智能和区块链，金融行业和金融科技领域始终以开放的姿态迎接新技术和新变化，并不断进行自我革新和升华。

区块链技术是金融科技领域当下最受人关注的方向之一。区块链作为一个新兴技术，具备去中心化、防篡改、可追溯等众多金融领域十分需要的特点。它可以实现多方场景下开放、扁平化的全新合作信任模型，而这些都为实现更高效的资源配置，更具体地说是金融交易，提供了有效的技术手段。在可见的未来，区块链技术将为人类商业社会的快速发展带来更多发展机遇和成长空间。

区块链技术在金融领域的实际应用之一——新型数字货币，被认为具备了变革整个金融行业的潜力，引发了国内外广泛的研究讨论和实践。英国央行已在研发利用分布式账本技术的下一代支付系统。中国人民银行也组建了数字货币研究所，深入研究数字货币相关的技术和监管课题。国际货币基金组织也公开认可区块链技术在清算和结算方面的独特优势。

清华五道口金融学院始终密切关注和积极开展金融行业及区块链相关领域的学术与研究，于 2012 年成立互联网金融实验室，专注于互联网金融和金融科技领域的研究、开发与孵化，并联合国内外众多的创新型企业和研究机构，一起开展数字资产和区块链相关的课题和项目。

当然，创新技术的发展和落地往往难以一蹴而就。我们应该认识到，区块链技术目前仍处于早期阶段，在支撑大规模商业应用场景上还存在不少挑战，例如如何在不影响业务运行的前提下，将区块链系统融合到已有的业务系统；如何让区块链系统的处理性能满足金融交易的苛刻需求；如何设计基于区块链的全新业务运营框架，并对其实现有效的监管。这些都是非常值得进一步探索的课题。

在此之际，很欣喜地看到有这样一本系统讲解区块链技术及实践的书籍出版。与其他介绍区块链的图书不同，本书并没有局限在阐述区块链的思想、概念和应用场景等理论知识层面，而是进一步从实现角度剖析了区块链平台的架构、设计，并提供了大量一手的开发实践案例，特别是全球区块链领域首屈一指的开源项目——超级账本。这些都将帮助读者更深刻

地理解和掌握区块链技术的核心原理与应用方法。

本书作者在技术体系的经验和视野 、创新意识、国际化合作等方面都展现出了作为金融科技专家的综合素养，让我们对中国金融业进入下一个全新的发展阶段的人才储备充满了信心。我们愿意跟作者们一起，共同关注、共同努力于中国金融科技的未来。

廖理，教授，博士生导师，清华大学五道口金融学院

2017 年 8 月于清华五道口

Preface 前　言

区块链和机器学习被誉为未来十年内最有可能提高人类社会生产力的两大创新科技。如果说机器学习的兴起依赖于新型芯片技术的发展，那么区块链技术的出现，则是来自商业、金融、信息、安全等多个领域众多科技成果和业务创新的共同推动。

比特币网络自横空出世，以前所未有的新型理念支持了前所未有的交易模式；以太坊项目站在前人肩膀上，引入图灵完备的智能合约机制，进一步释放了区块链技术的应用威力；众多商业、科技巨头，集合来自大型企业的应用需求和最先进的技术成果，打造出支持权限管理的联盟式分布式账本平台——超级账本……开源技术从未如今天这样，对各行各业都产生着极为深远的影响。本书在剖析区块链核心技术时，正是以这些开源项目（特别是超级账本 Fabric 项目）为具体实现进行讲解，力图探索其核心思想，展现其设计精华，剖析其应用特性。

我们在写作中秉承了由浅入深、由理论到实践的思想，将全书分为两大部分：理论篇和实践篇。前三章介绍了区块链技术的由来、核心思想及典型的应用场景。第 4 ~ 5 章重点介绍了区块链技术中大量出现的分布式系统技术和密码学安全技术。第 6 ~ 8 章分别介绍了区块链领域的三个典型开源项目：比特币、以太坊和超级账本。第 9 ~ 11 章以超级账本 Fabric 项目为例，具体讲解了安装部署、配置管理，以及使用 Fabric CA 进行证书管理的实践经验。第 12 章重点剖析了超级账本 Fabric 项目的核心架构设计。第 13 章介绍了区块链应用开发的相关技巧和示例。最后，本书还就热门的“区块链即服务”平台进行了介绍，并讲解应用超级账本 Cello 项目构建区块链服务和管理平台的相关经验和知识。

相信读者在阅读完本书后，在深入理解区块链核心概念和原理的同时，对于区块链和分布式账本领域最新的技术和典型设计实现也能了然于心，可以更加高效地开发基于区块链平台的分布式应用。

在本书长达两年时间的编写过程中，得到了来自家人、同事以及开源社区开发者和技术爱好者的众多支持和鼓励，在此表示感谢！

最后，希望本书能为推动区块链技术的进步和开源文化的普及做出一点微薄的贡献！

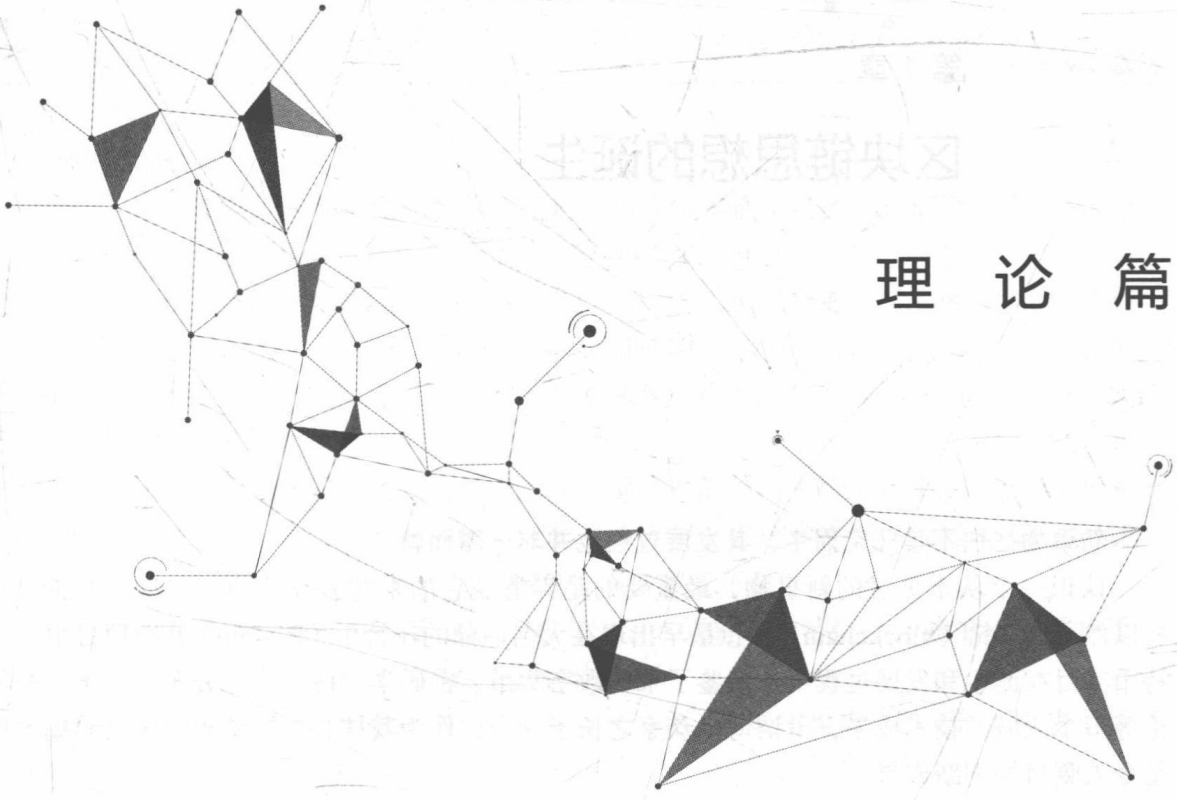
作者

2017 年 8 月于北京

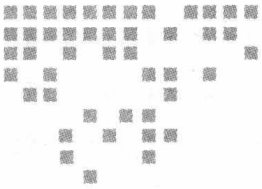
目　录 *Contents*

实 践 篇

附 录



理 论 篇



Chapter 1 第 1 章

区块链思想的诞生

新事物往往不是凭空而生，其发展过程也并非一蹴而就。

认识一个从未见过的新事物，最重要的是弄清楚它的来龙去脉，知其出身，方能知其所以然。区块链（blockchain）思想最早出现在大名鼎鼎的比特币（Bitcoin）开源项目中。比特币项目在诞生和发展过程中，借鉴了来自数字货币、密码学、博弈论、分布式系统、控制论等多个领域的技术成果，可谓博采众家之长于一身，作为其核心支撑结构的区块链技术更是令人瞩目的创新成果。

本章将从数字货币的历史讲起，简要介绍区块链思想诞生的摇篮——比特币项目的诞生和发展过程，并初步剖析区块链技术带来的潜在商业价值。通过阅读本章内容，读者可以了解区块链技术产生的背景、原因，以及在诸多商业应用场景中的潜在价值。

1.1 从实体货币到数字货币

区块链最初的思想诞生于无数先哲对于用数字货币替代实体货币的探讨和设计中。

1. 货币的历史演化

众所周知，货币是人类文明发展过程中的一大发明。其最重要的职能包括价值尺度、流通手段、贮藏手段等。很难想象离开了货币，现代社会庞大而复杂的经济和金融体系如何保持运转。也正是因为它如此重要，货币的设计和发行机制是关系到国计民生的大事。

历史上，在自然和人为因素的干预下，货币的形态经历了多个阶段的演化，包括实物货币、金属货币、代用货币、信用货币、电子货币、数字货币等。近代以前相当长的一段时间里，货币的形态一直是以实体的形式存在，可统称为“实体货币”。计算机诞生后，为货

币的虚拟化提供了可能性。

同时，货币自身的价值依托也不断发生演化，从最早的实物价值、发行方信用价值，直到今天的对科学技术和信息系统（包括算法、数学、密码学、软件等）的信任价值。

中国最早关于货币的确切记载“夏后以玄币”，出现在恒宽的《盐铁论·错币》。

2. 纸币的缺陷

理论上，一般等价物都可以作为货币使用。当今世界最常见的货币制度是纸币本位制，因为纸质货币既方便携带、不易仿制，又相对容易辨伪。

或许有人会认为信用卡等电子方式相对于纸币等货币形式使用起来更为方便。确实，信用卡在某些场景下会更为便捷，但它依赖背后的集中式支付体系，一旦碰到支付系统故障、断网、缺乏支付终端等情况，信用卡就无法使用。另外，货币形式相对电子支付方式还可以提供更好的匿名性。

目前，无论是货币形式，还是信用卡形式，都需要额外的支持机构（例如银行）来完成生产、分发、管理等操作。中心化的结构固然易于管理，但也带来了额外成本和安全风险。诸如伪造、信用卡诈骗、盗刷、转账骗局等安全事件屡见不鲜。

很显然，如果能实现一种数字货币，既有货币方便易用的特性，又能消除纸质货币的缺陷，无疑将极大提高社会整体经济活动的运作效率。

让我们来对比一下现有的数字货币（以比特币为例）和现实生活中的纸币，两者的优劣见表 1-1。

表 1-1　数字货币和纸币的对比

属性	分　析	优势方
便携	大部分场景（特别是较大数额支付时）下数字货币将具备更好的便携性	数字货币
防伪	两者各有千秋，但数字货币整体上会略胜一筹。纸币依靠的是各种设计（纸张、油墨、暗纹、夹层等）上的精巧，数字货币依靠的则是密码学上的保障。事实上，纸币的伪造时有发生，但数字货币的伪造目前还无法实现	数字货币
辨伪	纸币即使依托验钞机等专用设备仍会有误判情况，数字货币依靠密码学易于校验	数字货币
匿名	通常情况下，两者都能提供很好的匿名性。但都无法防御有意的追踪	持平
交易	对纸币来说，谁持有纸币谁就是合法拥有者，交易通过纸币自身的转移即可完成，无法复制。对数字货币来说则复杂得多，因为任何数字物品都是可以被复制的，但数字形式也意味着转移成本会更低。总体上看，两者适用不同的情景	持平
资源	通常情况下，纸币的生产成本要远低于面额。数字货币消耗资源的计算则复杂得多。以比特币为例，最坏情况下可能需要消耗接近甚至超过面值的电能	纸币
发行	纸币的发行需要第三方机构的参与，数字货币则通过分布式算法来完成发行。在人类历史上，通胀和通缩往往是不合理地发行货币造成的，而数字货币尚缺乏大规模验证，还有待观察	持平

可见，数字货币并非在所有领域都优于已有的货币形式。要比较两者的优劣应该针对具体情况具体分析。不带前提地鼓吹数字货币并不是一种科学和严谨的态度。实际上，仔细观察数字货币的应用情况就会发现，虽然以比特币为代表的数字货币已在众多领域得到应用，但目前还没有任何一种数字货币能完全替代已有货币。

另外，虽然当前的数字货币“实验”已经取得了巨大成功，但局限也很明显：其依赖的区块链和分布式账本技术还缺乏大规模场景的考验；系统的性能和安全性还有待提升；资源的消耗还过高等。这些问题的解决，有待金融科技的进一步发展。

注意 严格来讲，货币（money）不等于现金或通货（cash/currency），货币的含义范围更广。

3.“去中心化”的技术难关

虽然数字货币带来的预期优势可能很美好，但要设计和实现一套能经得住实用考验的数字货币并非易事。

现实生活中常用的纸币具备良好的可转移性，可以相对容易地完成价值的交割。但是对于数字货币来说，数字化内容容易被复制，数字货币持有人可以将同一份货币发给多个接收者，这种攻击称为“双重支付攻击”（double-spend）”。

也许有人会想到，银行中的货币实际上也是数字化的，因为通过电子账号里面的数字记录了客户的资产。说的没错，有人称这种电子货币模式为“数字货币 1.0”，它实际上依赖于一个前提：假定存在一个安全可靠的第三方记账机构负责记账，这个机构负责所有的担保环节，最终完成交易。

中心化控制下，数字货币的实现相对容易。但是，很多时候很难找到一个安全可靠的第三方记账机构来充当这个中心管控的角色。

例如，发生贸易的两国可能缺乏足够的外汇储备用以支付；汇率的变化等导致双方对合同有不同意见；网络上的匿名双方进行直接买卖而不通过电子商务平台；交易的两个机构彼此互不信任，找不到双方都认可的第三方担保；使用第三方担保系统，但某些时候可能无法连接；第三方的系统可能会出现故障或受到篡改攻击……

这个时候，就只有实现去中心化（de-centralized）或多中心化（multi-centralized）的数字货币系统。在“去中心化”的场景下，实现数字货币存在如下几个难题：

- 货币的防伪：谁来负责对货币的真伪进行鉴定；
- 货币的交易：如何确保货币从一方安全转移到另外一方；
- 避免双重支付：如何避免同一份货币支付给多个接收者。

可见，在不存在第三方记账机构的情况下，实现一个数字货币系统的挑战着实不小。能否通过技术创新来解决这个难题呢？

众多金融专家、科研人员向着这个方向不懈努力了数十年，创造出了许多具有深远影