区块链原理、设计与应用

作者：杨保华

区块链技术丛书

区块链原理、设计与应用

杨保华　陈昌　编著

ISBN：978-7-111-57782-9

本书纸版由机械工业出版社于2017年出版，电子版由华章分社（北京华章图文信息有限公司，北京奥维博世图书发行有限公司）全球范围内制作与发行。

版权所有，侵权必究

客服热线：+ 86-10-68995265

客服信箱：service@bbbvip.com

官方网址：www.hzmedia.com.cn

新浪微博 @华章数媒

微信公众号 华章电子书（微信号：hzebook）

目录

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

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

理论篇

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。

提示　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

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响的巧妙设计。

1.2　站在巨人的肩膀上

从上世纪80年代开始，数字货币技术就一直是研究的热门，前后经历了几代演进，比较典型的成果包括e-Cash、HashCash、B-money等。

1983年，David Chaum最早在论文《Blind Signature for Untraceable Payments》中提出了e-Cash，并于1989年创建了Digicash公司。e-Cash系统是首个匿名化的数字加密货币（anonymous cryptographic electronic money或electronic cash system），基于David Chaum自己发明的盲签名技术，曾被应用于部分银行的小额支付系统中。e-Cash依赖于一个中心化的中介机构，这导致它最终失败。

1997年，Adam Back发明了HashCash，来解决邮件系统中DoS攻击问题。HashCash首次提出用工作量证明（Proof of Work，PoW）机制来获取额度，该机制后来被随后出现的数字货币技术所采用。

1998年，Wei Dai提出了B-money，将PoW引入数字货币生成过程中。B-money同时是首个面向去中心化设计的数字货币。从概念上看B-money已经比较完善，但是很遗憾，其未能提出具体的设计实现。

上面这些数字货币都或多或少地依赖于一个第三方的信用担保系统。直到比特币的出现，将PoW与共识机制联系在一起，首次从实践意义上实现了一套去中心化的数字货币系统 。

比特币依托的分布式网络无需任何管理机构，自身通过数学和密码学原理来确保所有交易的成功进行，并且，比特币自身的价值通过背后的计算力进行背书。这也促使人们开始思考，在越来越数字化的世界中，应该如何发行货币，以及如何衡量价值。

目前，除了像比特币这样完全丢弃已有体系的分布式技术之外，仍然存在中心化代理模式的数字货币机制，包括类似PayPal这样的平台，通过跟已有的支付系统合作，代理完成交易。

现在还很难讲哪种模式将会成为日后的主流，未来甚至还可能出现更先进的技术。但毫无疑问，这些成果都为后来的数字货币设计提供了极具价值的参考；而站在巨人们肩膀上的比特币，必将在人类货币史上留下难以磨灭的印记。

1.3　了不起的社会学实验

1.比特币的诞生

2008年10月31日，一位化名Satoshi Nakamoto（中本聪）的人在metzdowd密码学邮件列表中提出了比特币（Bitcoin）的设计白皮书《Bitcoin：A Peer-to-Peer Electronic Cash System》，并在2009年公开了最初的实现代码。首个比特币于UTC时间2009年1月3日18：15：05生成。但比特币真正流行开来并被人们所关注则是至少两年以后了。

作为开源项目，比特币很快吸引了大量开发者的加入，目前的官方网站bitcoin.org提供了比特币相关的代码实现和各种工具软件。

除了精妙的设计理念外，比特币最为人津津乐道的一点是发明人“中本聪”到目前为止尚无法确认真实身份。也有人推测，“中本聪”背后可能不止一个人，而是一个团队。这些猜测都为比特币项目带来了不少传奇色彩。

2.比特币的意义和价值

直到今天，关于比特币的话题仍充满了不少争议。但大部分人应该都会认可，比特币是数字货币历史上，甚至整个金融历史上一次了不起的社会学实验。

比特币网络自2009年上线以来，在无人管理的情况下，已经在全球范围内7×24小时运行超过8年时间，成功处理了几百万笔交易，甚至支持过单笔1.5亿美元的交易。更为难得的是，比特币网络从未出现过重大的系统故障。

比特币网络目前由数千个核心节点参与构成，不需要任何中心化的支持机构参与，纯靠分布式机制支持了稳定上升的交易量。

比特币首次真正从实践意义上实现了安全可靠的去中心化数字货币机制，这也是它受到无数金融科技从业者热捧的根本原因。

作为一种概念货币，比特币主要希望解决已有货币系统面临的几个核心问题：

·被掌控在单一机构手中，容易被攻击；

·自身的价值无法保证，容易出现波动；

·无法匿名化交易，不够隐私。

在前文中曾探讨过，要实现一套去中心化的数字货币机制，最关键的是要建立一套可靠的交易记录系统，以及形成一套合理的货币发行机制。

这个交易记录系统要能准确、公正地记录发生过的每一笔交易，并且无法被恶意篡改。对比已有的银行系统，可以看出，现有的银行机制作为金融交易的第三方中介机构，有代价地提供了交易记录服务。如果参与交易的多方都完全相信银行的记录（数据库），就不存在信任问题。可是如果是更大范围（甚至跨多家银行）进行流通的货币呢？哪家银行的系统能提供完全可靠不中断的服务呢？唯一可能的方案是一套分布式账本。这个账本可以被所有用户自由访问，而且任何个体都无法对所记录的数据进行恶意篡改和控制。为了实现这样一个前所未有的账本系统，比特币网络巧妙地设计了区块链结构，提供了可靠、无法被恶意篡改的数字货币账本功能。

比特币网络中，货币的发行是通过比特币协议来规定的。货币总量受到控制，发行速度随时间自动进行调整。既然总量一定，那么单个比特币的价值会随着越来越多的经济实体认可比特币而水涨船高。发行速度的自动调整则避免出现通胀或者滞涨的情况。

另一方面，也要冷静地看到，作为社会学实验，比特币已经获得了巨大的成功，特别是基于区块链技术，已经出现了许多颇有价值的商业场景和创新技术。但这绝不意味着比特币自身必然能够进入未来的商业体系中。

3.更有价值的区块链技术

如果说比特币是影响力巨大的社会学实验，那么从比特币核心设计中提炼出来的区块链技术，则让大家看到了塑造更高效、更安全的未来商业网络的可能。

2014年开始，比特币背后的区块链技术开始逐渐受到大家关注，并进一步引发了分布式记账本 （distributed ledger）技术的革新浪潮。

实际上，人们很早就意识到，记账相关的技术对于资产（包括有形资产和无形资产）的管理（包括所有权和流通）十分关键；而去中心化或多中心化的分布式记账本技术，对于当前开放、多维化的商业模式意义重大。区块链的思想和结构，正是实现这种分布式记账本系统的一种极具可行潜力的技术。

区块链技术现在已经脱离比特币网络自身，在金融、贸易、征信、物联网、共享经济等诸多领域崭露头角。现在，除非特别指出是“比特币区块链”，否则当人们提到“区块链技术”时，往往所指已经与比特币没有什么必然联系了。

1.4　潜在的商业价值

商业行为的典型模式为：交易的多方通过协商和执行合约，完成交易过程。区块链擅长的正是在多方之间达成合约，并确保合约的顺利执行。

根据类别和应用场景不同，区块链所体现的特点和价值也不同。从技术角度一般认为，区块链具有如下特点：

·分布式容错性：分布式网络极其鲁棒，能够容忍部分节点的异常状态；

·不可篡改性：一致提交后的数据会一直存在，不可被销毁或修改；

·隐私保护性：密码学保证了数据隐私，即便数据泄露，也无法解析。

随之带来的业务可能包括如下特性：

·可信任性： 区块链技术可以提供天然可信的分布式账本平台，不需要额外第三方中介机构参与；

·降低成本： 跟传统技术相比，区块链技术可能需要的时间、人力和维护成本更少；

·增强安全： 区块链技术将有利于安全、可靠的审计管理和账目清算，减少犯罪风险。

区块链并非凭空诞生的新技术，而更像是技术演化到一定程度突破应用阈值后的产物，因此，其商业应用场景也跟促生其出现的环境息息相关。对于基于数字方式的交易行为，区块链技术能潜在地降低交易成本、加快交易速度，同时能提高安全性。能否最终带来成本的降低，将是一项技术能否得到深入应用的关键 。

所有跟信息、价值（包括货币、证券、专利、版权、数字商品、实际物品等）、信用等相关的交换过程，都将可能从区块链技术中得到启发或直接受益（见图1-1）。但这个过程绝不是一蹴而就的，可能需要较长时间的探索和论证。具体的商业应用案例可以参考本书后续的应用场景章节。

图1-1　区块链影响的交换过程

目前，区块链技术已经得到了众多金融机构和商业公司的关注，包括大量金融界和信息技术界的领军性企业和团体。典型企业组织如下（排名不分先后）：

·Visa国际组织；

·美国纳斯达克证券交易所（Nasdaq）；

·高盛投资银行（Goldman Sachs）；

·花旗银行（Citi Bank）；

·美国富国银行（Wells Fargo）；

·中国人民银行；

·中国浦发银行；

·日本三菱日联金融集团；

·瑞士联合银行；

·德意志银行；

·美国证券集中保管结算公司（DTCC）；

·全球同业银行金融电讯协会（SWIFT）；

·国际商业机器公司（IBM）；

·微软（Microsoft）；

·英特尔（Intel）；

·思科（Cisco）；

·埃森哲（Accenture）。

1.5　本章小结

区块链思想诞生于数字货币长达三十多年的发展过程中，它支持了首个试图自带信任、防篡改的分布式记账本——比特币网络。这也第一次让大家意识到，除了互联网这样的尽力而为（不保证可信）的基础设施外，基于区块链技术还将可能打造一个实现彼此信任的基础网络设施。

当然，从应用角度讲，比特币也只是基于区块链技术的一种金融应用。区块链技术其实还能带来更通用的计算能力和商业价值。本书后续章节将介绍更多的商业应用案例，并介绍开源界打造的区块链平台项目，包括“以太坊”和“超级账本”等项目。这些开源项目加速释放了区块链技术的威力，为更多更复杂的区块链应用场景提供了技术支持。

第2章　核心技术概览

运用之妙夺造化，存乎一心胜天工。

有人可能会遇到这样的问题：

·跨境商贸合作中签订的合同，怎么确保对方能严格遵守和及时执行？

·酒店宣称刚打捞上来的三文鱼，怎么追踪捕捞和运输过程中的时间和卫生？

·现代数字世界里，怎么证明你是谁？怎么证明某个资产属于你？

·经典囚徒困境中的两个人，怎样才能达成利益的最大化？

·宇宙不同文明之间的“黑暗森林”猜疑链，有没有可能被彻底打破？

这些看似很难解决的问题，在区块链的世界里已经有了初步的答案。本章将带领大家探索区块链的核心技术，包括其定义与原理、关键的问题等，还将探讨区块链技术的演化，并对未来发展的趋势进行展望。最后，对一些常见的认识误区进行了澄清。

2.1　定义与原理

1.定义

公认的最早关于区块链的描述性文献是中本聪所撰写的文章《Bitcoin：A Peer-to Peer Electronic Cach System》，但该文献重点在于讨论比特币系统，实际上并没有明确提出区块链的定义和概念，在其中指出，区块链是用于记录比特币交易账目历史的数据结构。

另外，Wikipedia上给出的定义中，将区块链类比为一种分布式数据库技术，通过维护数据块的链式结构，可以维持持续增长的、不可篡改的数据记录。

区块链技术最早的应用出现在比特币项目中。作为比特币背后的分布式记账平台，在无集中式管理的情况下，比特币网络稳定运行了八年时间，支持了海量的交易记录，并且从未出现严重的漏洞，这些都与巧妙的区块链结构分不开的。

区块链技术自身仍然在飞速发展中，目前相关规范和标准还在进一步成熟中。

2.基本原理

区块链的基本原理理解起来并不复杂。首先，区块链包括三个基本概念：

·交易 （transaction）：一次对账本的操作，导致账本状态的一次改变，如添加一条转账记录；

·区块 （block）：记录一段时间内发生的所有交易和状态结果，是对当前账本状态的一次共识；

·链 （chain）：由区块按照发生顺序串联而成，是整个账本状态变化的日志记录。

如果把区块链作为一个状态机，则每次交易就是试图改变一次状态，而每次共识生成的区块，就是参与者对于区块中交易导致状态改变的结果进行确认。

在实现上，首先假设存在一个分布式的数据记录账本，这个账本只允许添加、不允许删除。账本底层的基本结构是一个线性的链表，这也是其名字“区块链”的来源。链表由一个个“区块”串联组成（如图2-1所示），后继区块记录前导区块的哈希值（pre hash）。新的数据要加入，必须放到一个新的区块中。而这个块（以及块里的交易）是否合法，可以通过计算哈希值的方式快速检验出来。任意维护节点都可以提议一个新的合法区块，然而必须经过一定的共识机制来对最终选择的区块达成一致。

图2-1　区块链结构示例

3.以比特币为例理解区块链工作过程

以比特币网络为例，可以具体看其中如何使用了区块链技术。

首先，比特币客户端发起一项交易，广播到比特币网络中并等待确认。网络中的节点会将一些收到的等待确认的交易记录打包在一起（此外还要包括前一个区块头部的哈希值等信息），组成一个候选区块。然后，试图找到一个nonce串（随机串）放到区块里，使得候选区块的哈希结果满足一定条件（比如小于某个值）。这个nonce串的查找需要一定的时间去进行计算尝试。

一旦节点算出来满足条件的nonce串，这个区块在格式上就被认为是“合法”了，就可以尝试在网络中将它广播出去。其他节点收到候选区块，进行验证，发现确实符合约定条件了，就承认这个区块是一个合法的新区块，并添加到自己维护的区块链上。当大部分节点都将区块添加到自己维护的区块链结构上时，该区块被网络接受，区块中所包括的交易也就得到确认。

当然，在实现上还会有很多额外的细节。这里面比较关键的步骤有两个：一个是完成对一批交易的共识（创建区块结构）；一个是新的区块添加到区块链结构上，被大家认可，确保未来无法被篡改。

比特币的这种基于算力寻找nonce串的共识机制称为工作量证明 （Proof of Work，PoW）。目前，要让哈希结果满足一定条件，并无已知的快速启发式算法，只能进行尝试性的暴力计算。尝试的次数越多（工作量越大），算出来的概率越大。

通过调节对哈希结果的限制，比特币网络控制平均约10分钟产生一个合法区块。算出区块的节点将得到区块中所有交易的管理费和协议固定发放的奖励费（目前是12.5比特

币，每四年减半），这个计算新区块的过程俗称为挖矿。

读者可能会关心，比特币网络是任何人都可以加入的，如果网络中存在恶意节点单，能否进行恶意操作来对区块链中的记录进行篡改，从而破坏整个比特币网络系统。比如最简单的，故意不承认收到的别人产生的合法候选区块，或者干脆拒绝来自其他节点的交易等。

实际上，比特币网络中存在大量（据估计数千个）的维护节点，而且大部分节点都是正常工作的，默认都只承认所看到的最长的链结构。只要网络中不存在超过一半的节点提前勾结一起采取恶意行动，则最长的链将很大概率上成为最终合法的链。而且随着时间增加，这个概率会越来越大。例如，经过6个区块生成后，即便有一半的节点联合起来想颠覆被确认的结果，其概率也仅为（1/2）^{6}≈1.6%，即低于1/60的可能性。

当然，如果整个网络中大多数的节点都联合起来作恶，可以导致整个系统无法正常工作。要做到这一点，往往意味着付出很大的代价，跟通过作恶得到的收益相比，得不偿失。

提示　区块链结构与Git版本管理的有向无环图数据结构，在设计上有异曲同工之妙。

2.2　技术的演化与分类

区块链技术自比特币网络设计中被大家发掘关注，从最初服务数字货币系统，到今天在分布式账本场景下发挥着越来越大的技术潜力。

1.区块链的演化

比特币区块链已经支持了简单的脚本计算，但仅限于数字货币相关的处理。除了支持数字货币外，还可以将区块链上执行的处理过程进一步泛化，即提供智能合约（smart contract）。智能合约可以提供除了货币交易功能外更灵活的合约功能，执行更为复杂的操作。

这样，扩展之后的区块链已经超越了单纯数据记录的功能，实际上带有一点“智能计算”的意味；更进一步，还可以为区块链加入权限管理和高级编程语言支持等，实现更强大的、支持更多商用场景的分布式账本。

从计算特点上，可以看到现有区块链技术的三种典型演化场景，如表2-1所示。

表2-1　区块链技术的三种典型演化场景

2.区块链与分布式记账

记账技术历史悠久，古老的账本见图2-2。

图2-2　古老的账本

现代复式记账系统（double entry bookkeeping）由意大利数学家卢卡·帕西奥利于1494年在《Summa de arithmetica，geometrica，proportioni et proportionalità》一书中最早制定。复式记账法对每一笔账目同时记录来源和去向，首次将对账验证功能引入记账过程，提升了记账过程的可靠性。

从这个角度来看，区块链是首个自带对账功能的数字记账技术实现 。

更广泛地看，区块链属于一种去中心化的记录技术。参与到系统上的节点，可能不属于同一组织，彼此无需信任；区块链数据由所有节点共同维护，每个维护节点都能复制获得一份完整或部分记录的拷贝。

跟传统的记账技术相比，基于区块链的分布式账本应该包括如下特点：

·维护一条不断增长的链，只可能添加记录，而发生过的记录都不可篡改；

·去中心化，或者说多中心化，无需集中控制而能达成共识，实现上尽量采用分布式；

·通过密码学的机制来确保交易无法被抵赖和破坏，并尽量保护用户信息和记录的隐私性。

3.分类

根据参与者的不同，可以分为公开（public）链、联盟（consortium）链和私有（private）链。

·公有链 ，顾名思义，任何人都可以参与使用和维护，如比特币区块链，信息是完全公开的；

如果进一步引入许可机制，可以实现私有链和联盟链两种类型：

·私有链 ，由集中管理者进行管理限制，只有内部少数人可以使用，信息不公开；

·联盟链 则介于两者之间，由若干组织一起合作维护一条区块链，该区块链的使用必须是带有权限的限制访问，相关信息会得到保护，如供应链机构或银行联盟。

目前来看，公有链更容易吸引市场和媒体的眼球，但更多的商业价值会在联盟链和私有链上落地。

根据使用目的和场景的不同，又可以分为以数字货币为目的的货币链，以记录产权为目的的产权链，以众筹为目的的众筹链等，也有不局限特定应用场景的通用链。

现有大部分区块链实现都至少包括了网络层、共识层、智能合约和应用层等结构，联盟链实现往往还会引入一定的权限管理机制。

2.3　关键问题和挑战

从技术角度讲，区块链所涉及的领域比较繁杂，包括分布式系统、存储、密码学、心理学、经济学、博弈论、控制论、网络协议等，这也就意味着大量工程实践上的技术挑战。

下面列出了目前业内关注较多的一些技术话题。

1.抗抵赖与隐私保护

·怎么防止交易记录被篡改？

·怎么证明交易双方的身份？

·怎么保护交易双方的隐私？

密码学的发展为解决这些问题提供了不少手段。传统方案包括Hash算法、加解密算法、数字证书和签名（盲签名、环签名）等。

随着区块链技术的应用，新出现的需求将刺激密码学的进一步发展，包括更高效的随机数产生、更高强度的加密、更快速的加解密处理等。同时，量子计算等新技术的出现，也会带来更多的挑战，例如，RSA算法等目前商用的加密算法，在未来可能无法提供足够的安全性。

能否满足这些新的需求，将依赖于数学科学的进一步发展和新一代计算技术的突破。

2.分布式共识

这是个经典的技术难题，学术界和业界都已有大量的研究成果（包括Paxos、拜占庭系列算法等）。

问题的核心在于如何解决某个变更在分布式网络中得到一致的执行结果，是被参与多方都承认的，同时这个信息是被确定的，不可推翻的。

该问题在公开匿名场景下和带权限管理的场景下需求差异较大，从而导致了基于概率的算法和确定性算法两类思想。

最初，比特币区块链考虑的是公开匿名场景下的最坏保证。通过引入了“工作量证明”策略来规避少数人的恶意行为，并通过概率模型保证最后参与方共识到最长链。算法在核心思想上是基于经济利益的博弈，让恶意破坏的参与者损失经济利益，从而保证大部分人的合作。同时，确认必须经过多个区块的生成之后达成，从概率上进行保证。这类算法的主要问题在于效率的低下。类似算法还有以权益为抵押的PoS、DPoS和Casper等。

后来更多的区块链技术（如超级账本）在带权限管理的场景下，开始考虑支持更多的确定性的共识机制，包括经典的拜占庭算法等，可以解决快速确认的问题。

共识问题在很长一段时间内都将是极具学术价值的研究热点，核心的指标将包括容错的节点比例、决策收敛速度、出错后的恢复、动态特性等。PoW等基于概率的系列算法理论上允许少于一半的不合作节点，PBFT等确定性算法理论上则允许不超过1/3的不合作节点。

3.交易性能

虽然一般来说，区块链不适用于高频交易的场景，但由于金融系统的需求，业界目前十分关心如何提高区块链系统交易的吞吐量，同时降低交易的确认延迟。

目前，公开的比特币区块链只能支持平均每秒约7笔的吞吐量，一般认为对于大额交易来说，安全的交易确认时间为一个小时左右。以太坊区块链的吞吐量略高一些，但交易性能也被认为是较大的瓶颈。

提示　实际上，小额交易只要确认被广播到网络中并带有合适的交易服务费用，即有较大概率被最终打包。

区块链系统跟传统分布式系统不同，其处理性能很难通过单纯增加节点数来进行横向扩展。实际上，传统区块链系统的性能，在很大程度上取决于单个节点的处理能力。高性能、安全、稳定性、硬件辅助加解密能力，都将是考查节点性能的核心要素。

这种场景下，为了提高处理性能，一方面可以提升单个节点的性能（如采用高配置的硬件），同时设计优化的策略和算法；另外一方面试图将大量高频的交易放到链外来，只用区块链记录最终交易信息，如比特币社区提出的“闪电网络”等设计。类似地，侧链（side chain）、影子链（shadow chain）等思路在当前阶段也有一定的借鉴意义。类似设计可以将交易性能提升1～2个数量级。

此外，在联盟链的场景下，参与多方存在一定的信任前提和利益约束，可以采取更优化的设计，换来性能的提升。以超级账本Fabric项目为例，在普通虚拟机配置下，单客户端交易吞吐量可达几百次每秒（transactions per second，tps）；在有一定工程优化或硬件加速情况下可以达到每秒数千次的吞吐量。

客观地说，目前开源区块链系统已经可以满足不少应用场景的性能需求，但离大规模交易系统在峰值每秒数万笔的吞吐性能还有较大差距。

提示　据公开的数据，VISA系统的处理均值为2000tps，号称的峰值为56000tps；某金融支付系统的处理峰值超过了85000tps；某大型证券交易所号称的处理均（峰）值在80000tps左右。

4.扩展性

常见的分布式系统可以通过增加节点来横向扩展整个系统的处理能力。对于区块链网络系统来说，根据共识机制的不同，这个问题往往并非那么简单。

例如，对于比特币和以太坊区块链而言，网络中每个参与维护的核心节点都要保持一份完整的存储，并且进行智能合约的处理。此时，整个网络的总存储和计算能力取决于单个节点的能力。甚至当网络中节点数过多时，可能会因为一致性的达成过程延迟降低整个网络的性能。尤其在公有网络中，由于存在大量低性能处理节点，导致这个问题将更加明显。

要解决这个问题，根本上是放松对每个节点都必须参与完整处理的限制（当然，网络中节点要能合作完成完整的处理），这个思路已经在超级账本中得到应用；同时尽量减少核心层的处理工作。

在联盟链模式下，还可以专门采用高性能的节点作为核心节点，相对较弱的节点仅作为代理访问节点。

5.安全防护

区块链目前最热门的应用场景是金融相关的服务，安全自然是讨论最多、挑战最大的话题。区块链在设计上大量采用了现代成熟的密码学算法。但这是否就能确保其绝对安全呢？

世界上并没有绝对安全的系统。

系统是由人设计的，系统也是由人来运营的，只要有人参与的系统，就难免出现漏洞。如下几个方面是很难避免的。

首先是立法。对区块链系统如何进行监管？攻击区块链系统是否属于犯罪？攻击银行系统是要承担后果的。但是目前还没有任何法律保护区块链（特别是公有链）以及基于它的实现。

其次是软件实现的潜在漏洞。考虑到使用了几十年的OpenSSL还带着那么低级的漏洞（heart bleeding），而且是源代码完全开放的情况下，让人不禁对运行中的大量线上系统持谨慎态度。而对于金融系统来说，无论客户端还是平台侧，即便是很小的漏洞都可能造成难以估计的损失。

另外，公有区块链所有交易记录都是公开可见的，这意味着所有的交易即便被匿名化和加密处理，但总会在未来某天被破解。安全界一般认为，只要物理上可接触就不是彻底的安全。实际上，已有文献证明，比特币区块链的交易记录很大可能是能追踪到真实用户的。

作为一套完全分布式的系统，公有的区块链缺乏有效的调整机制。一旦运行起来，出现问题也难以修正。即使是让它变得更高效、更完善的修改，只要有部分既得利益者联合起来反对，就无法得到实施。比特币社区已经出现过多次类似的争论。

最后，运行在区块链上的智能合约应用可能是五花八门的，可能存在潜在的漏洞，必须有办法进行安全管控，在注册和运行前需要有合理的机制进行探测，以规避恶意代码的破坏。

2016年6月17日发生的“DAO系统漏洞被利用”事件，直接导致价值6000万美元的数字货币被利用者获取。尽管对于这件事情的反思还在进行中，但事实再次证明，目前基于区块链技术进行生产应用时，务必要细心谨慎地进行设计和验证。必要时，甚至要引入“形式化验证”和人工审核机制。

提示　可以参考著名黑客米特尼克所著的《反欺骗的艺术——世界传奇黑客的经历分享》，其中介绍了大量的实际社交工程欺骗场景。

6.数据库和存储系统

区块链网络中的大量信息需要写到文件和数据库中进行存储。

观察区块链的应用，大量的读写操作、Hash计算和验证操作，跟传统数据库的行为十分不同。当年，人们观察到互联网应用大量非事务性的查询操作，而设计了非关系型

（NoSQL）数据库。那么，针对区块链应用的这些特点，是否可以设计出一些特殊的针对性的数据库呢？

LevelDB、RocksDB等键值数据库，具备很高的随机写和顺序读、写性能，以及相对较差的随机读的性能，被广泛应用到了区块链信息存储中。但目前来看，面向区块链的数据库技术仍然是需要突破的技术难点之一，特别是如何支持更丰富语义的操作。

大胆预测，未来将可能出现更具针对性的“块数据库”（BlockDB），专门服务类似区块链这样的新型数据业务，其中每条记录将包括一个完整的区块信息，并天然地跟历史信息进行关联，一旦写入确认则无法修改。所有操作的最小单位将是一个块。为了实现这种结构，需要原生支持高效的签名和加解密处理。

7.集成和运营

即便大量企业系统准备迁移到区块链平台上，但在相当长的一段时间内，基于区块链的新业务系统必将与已有的中心化系统集成共存。

两种系统如何共存，如何分工，彼此的业务交易如何进行合理传递？出现故障如何排查和隔离？已有数据如何在不同系统之间进行迁移和灾备？区块链系统自身又该如何进行运营（如网络的设计选择、状态监控、灾备等）？

这些都是迫切要解决的实际问题。若解决不好，将是区块链技术落地的不小阻碍。

2.4　趋势与展望

关于区块链技术发展趋势的探讨和争论，自其诞生之日起就从未停息。或许，读者从计算技术的演变历史中能得到一些启发。计算技术的发展历史如图2-3所示。

图2-3　计算的历史

以云计算为代表的现代计算技术，其发展历史上有若干重要的时间点和事件：

·1969——ARPANet（Advanced Research Projects Agency Network）：现代互联网的前身，由美国高级研究计划署（Advanced Research Project Agency）提出，其使用NCP协议，核心缺陷之一是无法做到和个别计算机网络交流；

·1973——TCP/IP：Vinton.Cerf（文特·瑟夫）与Bob Karn（鲍勃·卡恩）共同开发出TCP模型，解决了NCP的缺陷；

·1982——Internet：TCP/IP正式成为规范，并被大规模应用，现代互联网诞生；

·1989——WWW：早期互联网的应用主要包括telnet、ftp、email等，Tim Berners-Lee（蒂姆·伯纳斯-李）设计的WWW协议成为互联网的杀手级应用，引爆了现代互联网，从那开始，互联网业务快速扩张；

·1999——Salesforce：互联网出现后，一度只能进行通信应用，但Salesforce开始以云的理念提供基于互联网的企业级服务；

·2006——AWS EC2：奠定了云计算的业界标杆，直到今天，竞争者们仍然在试图追赶AWS的脚步；

·2013——Cognitive：以IBM Watson为代表的认知计算开始进入商业领域，计算开始变得智能，进入“后云计算时代”。

从这个历史中能看出哪些端倪呢？

首先，技术领域也存在着周期律 。这个周期目前看是7～8年左右。或许正如人有“七年之痒”，技术也存在着七年这道坎，到了这道坎，要么自身突破迈过去，要么就被新的技术所取代。如果从比特币网络上线（2009年1月）算起，到今年正是在坎上。因此，现在正是相关技术进行突破的好时机。

提示　为何恰好是七年？7年按照产品周期来看基本是2～3个产品周期，所谓事不过三，经过2～3个产品周期也差不多该有个结论了。

其次，最早出现的未必是先驱 。创新固然很好，但过早播撒的种子，若没有合适的土壤，往往也难长大。技术创新与科研创新很不同的一点是，技术创新必须立足于需求，过早过晚都会错失良机。科研创新则要越早越好，比如20世纪出现的物理学巨匠们，超前的研究成果奠定了后续一百多年的科技革命的基础。

最后，事物的发展往往是延续的、长期的 。新生事物大都不是凭空蹦出来的，往往是解决了前辈未能解决的问题，或是出现了之前未曾出现过的场景。而且很多时候，新生事物的出现需要长期的孵化；坚持还是放弃，故事不断重复（见图2-4）。笔者认为，只要是朝着提高生产力的正确方向努力，迟早会有出现在舞台上的一天。

图2-4　坚持还是放弃

目前，区块链在数字货币领域（以比特币为代表）的应用已经相对成熟，而在智能合约和分布式账本方向尚处于初步实践阶段。但毫无疑问的是，区块链技术在已经落地的领域，确实带来了生产力提升。因此可以相信，随着相关技术的进一步发展，区块链技术必然会在更多的领域中大放异彩，特别是金融科技相关领域。

2.5　认识上的误区

目前，由于区块链自身仍是一种相对年轻的技术，不少人对区块链的认识还存在一些误区。下面是需要注意的一些问题：

首先，区块链不等于比特币 。虽说区块链的基本思想诞生于比特币的设计中，但发展到今日，比特币和区块链已经俨然成为了两个不太相关的技术。前者更侧重从数字货币角度发掘比特币的实验性意义；后者则从技术层面探讨和研究可能带来的商业系统价值，试图在更多的场景下释放智能合约和分布式账本带来的科技潜力。

其次，区块链不等于数据库 。虽然区块链也可以用来存储数据，但它要解决的核心问题是多方的互信问题。单纯从存储数据角度，它的效率可能不高，也不推荐把大量的原始数据放到区块链系统上。当然，现在已有的区块链系统中，数据库相关的技术十分关键，直接决定了区块链系统的吞吐性能。

最后，区块链并非一门万能的颠覆性技术 。作为融合多项已有技术而出现的新事物，区块链跟现有技术的关系是一脉相承的。它在解决多方合作和可信处理上向前多走了一步，但并不意味着它是万能的，更不会彻底颠覆已有的商业模式。很长一段时间里，区块链所适用的场景仍需不断摸索，并且跟已有系统也必然是长期合作共存的关系。

2.6　本章小结

本章剖析了区块链的相关核心技术，包括其定义、工作原理、技术分类、关键问题和认识上的误区等。通过本章的学习，读者可以对区块链的相关核心技术形成整体上的认识，并对区块链在整个信息科技产业中的位置和发展趋势形成更清晰的认知。

除了数字货币应用外，现在业界越来越看重区块链技术可能带来的面向商业应用场景的计算能力。开源社区发起的开放的“以太坊”和“超级账本”等项目，让用户可以使用它们来快速设计复杂的分布式账本应用。

有理由相信，随着更多商业应用场景的出现，区块链技术将在未来金融和信息技术等领域占据越来越重要的地位。

第3章　典型应用场景

科技创新，应用为王。

一项新技术能否最终落地普及，取决于很多影响因素。其中很关键的一点便是能否找到合适的应用场景。以比特币网络为代表的大规模数字货币系统，长时间自治运行，支持了传统金融系统都难以实现的全球范围即时可靠交易。这为区块链技术的应用潜力引发了无限遐想。如果未来基于区块链技术构造的商业价值网络成为现实，所有的交易都将高效完成且无法伪造；所有签署的合同都能按照约定严格执行。这将极大降低整个商业体系运转的成本，同时大大提高社会沟通协作的效率。从这个意义上讲，基于区

欢迎访问：电子书学习和下载网站（https://www.shgis.cn）
文档名称：《区块链原理、设计与应用》杨保华.epub
请登录 https://shgis.cn/post/1855.html 下载完整文档。
手机端请扫码查看: