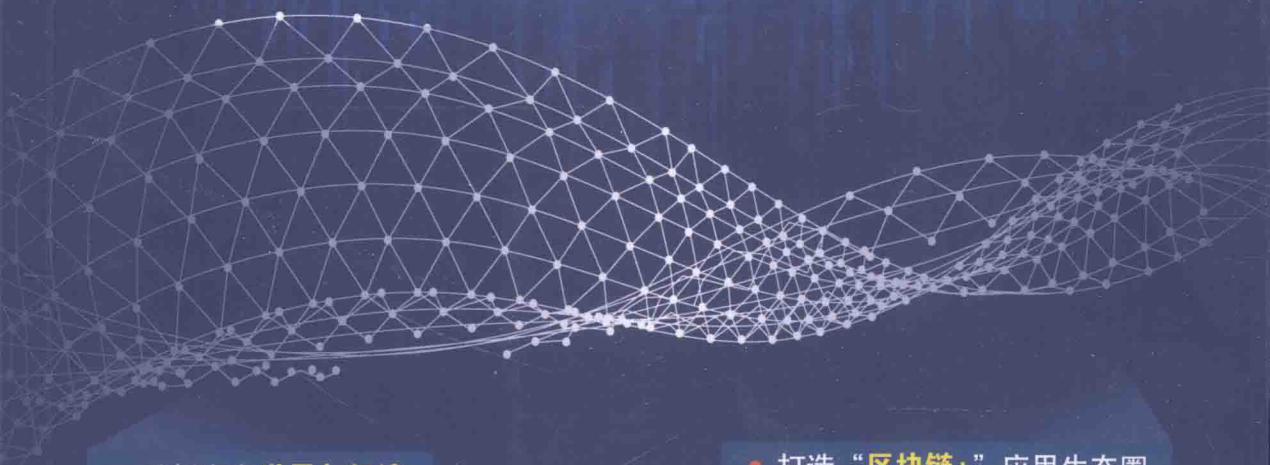
青岛“链湾”区块链系列丛书

• 描绘社会信用新蓝图

区块链技术原理及底层架构

The Principle and Bottom Architecture of Block Chain Technology

陈东敏 主编
郭 峰 广 红 副主编



• 重新定义世界与经济

• 打造“区块链+”应用生态圈

• 构建全球区块链中心

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

青岛“链湾”区块链系列丛书

区块链技术原理及底层架构

陈东敏　主　编
郭　峰　广　红　副主编

北京航空航天大学出版社

图书在版编目(CIP)数据

区块链技术原理及底层架构 / 陈东敏主编. -- 北京 : 北京航空航天大学出版社, 2017.4

ISBN 978-7-5124-2375-6

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(2017)第 063237 号

区块链技术原理及底层架构

陈东敏 主 编

郭 峰 广 红 副主编

责任编辑 杨 昕

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(邮编 100191) http://www.buaapress.com.cn

发行部电话:(010)82317024 传真:(010)82328026

读者信箱: emsbook@buaacm.com.cn 邮购电话:(010)82316936

北京泽宇印刷有限公司印装 各地书店经销

*

开本:710×1 000 1/16 印张:10 字数:138 千字

2017 年 5 月第 1 版 2017 年 5 月第 1 次印刷

ISBN 978-7-5124-2375-6 定价:45.00 元

编 委 会

主　　编：陈东敏

副 主 编：郭　峰　广　红

参编人员：（按汉语拼音排序）

陈海峰　陈　润　高登攀　高　炎

纪文峰　蒋　海　李　军　李少恒

廖　逸　马　刚　马　蓉　王大崑

杨　廉　杨　勇　于　潇　曾强生

翟海滨

参编单位：（按汉语拼音排序）

百灵科技

北京大学创新研究院

布比网络

点亮资本

国际大学创新联盟

金股链科技

青岛区块链研究院

数链科技

物链科技
中国科学院计算所
众签科技

合作单位：中关村区块链产业联盟
万向区块链实验室
中国分布式总账基础协议联盟
赛尔网络

序

近年来兴起的区块链技术是继互联网、无线通信、云计算、大数据之后计算和网络技术的又一颠覆性创新，正在引起一场新的技术变革和产业变革。区块链技术是由分布式数据存储、点对点传输、共识机制、加密算法等计算机技术交汇(Convergence)而形成的一种可用于信任传递、分布和管理价值(如货币)等与诚信关联的各种交易过程和结果的信息网络应用技术。区块链去中心化的数据结构和智能合约的基本功能使得该技术具有彻底颠覆传统金融行业和价值交易体系的巨大潜力，因此受到全球金融行业和各国政府的高度关注。虽然，区块链技术起源于数字货币的诞生，但随着人们对区块链认识的不断提升和对该技术的不断拓展，区块链的应用远远超出数字货币管理的范畴，并已延伸到各类价值和商品的交易、传输中，比如供应链管理、保险业、医疗信息、工业 4.0、知识产权管理、社会福利保障、政府和社会诚信体系的维护等。可以预言，区块链技术在各个领域的成功应用，将从根本上影响和改变社会成员、企事业机构和政府的行为。

作为新兴产业，区块链在多种场景的应用中将替代多种传统服务业。这些传统行业因广泛涉及民生和社会发展，受到各种法规的管控和监督。区块链产业的发展必然会挑战现有的法规和制度。加速区块链产业的发展，一方面需要政府的积极参与，引领产业发展生态环境的建设，有序地开放市场，建立开放的监督和管理机制；另一方面需要开发区块链技术和应用的各种新创企业加强自律和社会责任感，严格把控产品和服务的可靠性、安全性和实效性，不失信于用户和市场。建立行业协会和产业标准，要坚持营造开放和公平竞争的市场环境，要对加速发展新兴行业起到积极的推动作用。

中国在区块链的底层技术上已经形成了具有国际竞争力的自主专利技

术，应用区块链的新创技术公司更如雨后春笋般层出不穷，已经覆盖多个领域。各地政府高度重视区块链技术的落地和发展，纷纷出台扶持政策。如同互联网技术的发展，中国在区块链的核心技术和应用技术的开发上将走在世界前列。青岛“链湾”区块链系列丛书将系统地介绍区块链技术的发展史，我国自主研发的区块链的核心技术，以及区块链技术在金融服务业、医疗健康、供应链管理、食品溯源等多个领域的应用方案和案例。这套丛书的编写和出版旨在促进区块链技术产业知识的传播、人才的培养，加速区块链产业在中国的发展，提升中国在全球的竞争力。

北京大学创新研究院教授
青岛区块链研究院院长
陈东敏
2017 年 3 月

前　言

自2014年以来，区块链技术就受到广泛关注，其应用领域已从比特币延伸到金融科技、数字资产交易、供应链管理、物联网与互联网应用等多个领域，且有可能引发新一轮的技术创新和产业变革。很多业内专家、学者认为，“互联网＋区块链”能让人类用技术手段低成本地解决信任传递难题，将从根本上改变人类几千年来的交易模式，使人类社会的运作更加高效简单。

但是，任何创新技术的发展都有其发展规律。我们先回顾一下最近两年来区块链（包括比特币）业内发生的几件大事。

比特币“监守自盗”事件。2015年1月1日，日本《读卖新闻》头版惊曝一条内幕，曾是世界最大比特币交易平台的Mt.Gox所遗失的99%的比特币源自内部系统操纵，而不是来自外部的黑客攻击。《读卖新闻》指出，在Mt.Gox遗失的总计65万枚比特币中，仅有7 000枚是外部黑客攻击所致。其实，比特币“监守自盗”问题在圈内早已不是新闻。比特币的发展，从早期的技术极客开始到金融爱好者关注，逐步从一个理想化的技术社区演变成一个投机者、洗钱者的天堂，更像是一个21世纪互联网版的加利福尼亚淘金潮。

2016年6月的The DAO事件。The DAO全称为Decentralized Autonomous Organization，即去中心化的自治组织，是基于以太坊区块链智能合约平台的一个众筹基金项目。其设想是，每个众筹参与者按照出资数额（以太币）获得相应的DAO代币后即具有审查项目和投票表决的权利，其中投票权重与出资额相关。该组织不到一个月的时间，就成功地从约1万名参与者中募集到超过1亿美元的资金。然而，2016年6月17日下午，The DAO智能合约平台遭遇黑客攻击，数千万美元的用户资金被盗。几经周

折，以太坊平台通过被称为软分叉和硬分叉的技术手段，将所有在被攻击期间的相关交易做无效处理，并把所有筹集的资金退还给众筹人，The DAO项目就此解散、终结。

2016年11月，高盛、桑坦德银行、JP摩根等退出R3联盟。R3是一家总部位于纽约的区块链创业公司，由其发起的R3区块链联盟已吸引了80多家世界巨头银行和金融机构的参与。R3的产品是分布式账本应用平台Corda，目前已开源供免费使用。就在Corda推出后不久，JP摩根又推出了一个其称之为Juno的分布式加密账本原型。R3总经理查理·库珀说过，虽然Corda是一个分布式账本平台，但它绝对不是一个传统的区块链平台。为了适应监管、隐私和延展性问题，R3必须做出改变，Corda必须适应金融服务行业的具体需求。关于高盛等退出R3联盟的原因，虽然没有官方的正式解释，但显而易见，“技术意识形态”之争是主要因素。

以上事件表面看似相互独立无关，却反映出区块链发展过程中一些共性的问题。

一是如何摒弃意识形态对技术发展的干扰。

区块链领域一直存在着去中心化和中心化的理念之争，很多人推崇百分之百地去中心化，并把百分之百去中心化列为区块链的最重要属性。The DAO项目虽然已经终结，但由此引起的争论远没有结束。以太坊团队对事件的应急处理，无论是软分叉还是硬分叉，其本质均为中心化的做法。也就是说，在百分之百去中心的The DAO平台之外，还存在一个“上帝”，这个上帝就是以太坊团队。其实，如果思考一下人类历史和我们的现实生活就会发现，百分之百地去中心化和单一中心化是问题的两个极端，是理想化的产物。大部分的应用场景需要的可能既不是百分之百去中心化，也不是单一中心化，而是适度去中心化的多中心机制。早在互联网发展初期，类似的争论就曾出现过。1995年前后，通信网络的发展曾面临两种路线的选择：一种是基于传统电信思维模式的中心化路线，即以ATM（异步交换模式）协议为

代表的宽带综合业务路线，另一种是新型的、去中心化的路线，即以 TCP/IP 协议为代表的互联网路线。这一争论延续了五年，最后实践给出了结论：ATM 逐渐消亡，TCP/IP 则扩张到了全世界。当然，虽然提倡去中心化，但互联网本质上也并不是百分之百地去中心，而是存在多个中心的自治系统。

二是要遵循技术发展的演进规律。

基于密码学的分布式算法及协议，需要对其长期的安全性进行定期审核、测试与升级，这包括系统的安全和终端的安全，这样才能有效预防由于新技术的出现和计算能力的大幅提高对安全体系带来的威胁，以及程序员作恶和程序员出错带来的安全漏洞。互联网发展的经验告诉我们，任何一个成功的互联网应用，都要经历一个小步快跑、迅速迭代升级的过程。在此过程中，瑕疵与漏洞被不断地完善与修补，随着功能及规模的扩展，应用系统逐步稳定。因此，发展初期，区块链从金融科技外围的痛点应用切入，快速迭代发展，这是区块链发展无法回避的路径。

值得庆幸的是，经过这两三年的市场培育，区块链在国内取得了扎实的进步，逐渐形成了以底层技术为支撑、以中间层为衔接、以应用层为市场突破点的区块链生态体系。部分底层技术平台与应用类项目已实现落地：2015 年 12 月中国第一个区块链开发平台“布比区块链”上线运营；2016 年 3 月万向区块链实验室发布“万云区块链的云平台”；2016 年 3 月阳光保险联手布比推出基于区块链技术的“阳光贝”积分产品，这是除代币应用之外中国的第一个区块链示范应用；2016 年 4 月格格积分平台上线，推出中国首个资产型的区块链积分平台；2016 年 8 月作为综合区块链数字资产平台的布萌上线，目前，布萌已广泛地应用在商业积分、游戏币、预付卡、电子券、保险卡单、证券化资产等各个领域，截止到 2017 年 3 月 12 日，布萌平台已拥有超过 900 万终端用户。

布比区块链从一开始就摒弃了百分之百去中心化的意识形态思维，以多中心化信任为核心，并在实践中不断探索创新，逐步充实壮大。布比团队

源自中国科学院计算所，自2012年就开始从事区块链与数字资产的研究，目前已经拥有数十项核心专利技术。布比的产品定位是提供商业级的区块链基础设施服务，一是打造企业级区块链平台，二是在其上构建具有高扩展性的应用业务支撑系统。

本书由布比工程师团队纂写，内容涵盖了区块链技术的基本原理、布比区块链底层架构与开发指南，以及实际应用案例。期望本书的出版能为有志于区块链应用开发的技术人员提供帮助。由于时间仓促，书中难免出现遗漏与错误，敬请各位区块链爱好者、技术人员和专家指正，大家一起努力，共同探索创新，为推动区块链在国内的发展作出贡献。

点亮资本合伙人
中关村区块链产业联盟副理事长
郭峰
2017年3月

目　　录

第 4 章　布萌区块链数字资产网络开发指南

第 1 章

区块链技术原理

1.1 区块链和区块链技术的涵义

截至目前，很多人都听说过区块链的概念，至少对其作为账本的作用有所了解。随着人们对区块链认知程度的加深，已经逐渐开始明白，区块链本身就是一种强大的技术。本章从区块链的基本概念开始介绍。

区块链(Blockchain)技术的产生发展离不开比特币，首先是因为随着比特币的诞生，作为比特币底层技术的区块链技术才得以公之于众；其次，因为比特币是截至目前区块链技术中最为人知的应用案例。比特币的概念由中本聪(Satoshi Nakamoto)在2008年发表的论文 *Bitcoin: A Peer-to-Peer Electronic Cash System* 中首次提出。在论文中，中本聪将区块链技术作为构建比特币数据结构及交易体系的基础技术，将比特币打造为一种数字货币和在线支付系统，利用加密技术实现资金转移，而不再依赖于中央银行。比特币使用公钥地址来发送和接收比特币，并进行交易记录，从而实现个人身份信息的匿名。交易确认的过程则需要用户贡献算力，共同对交易进行共识确认从而将交易记录到全网公开账本中。用户可以利用计算机、手机等来发送或接收比特币，并选择交易费用。现有过万种加密数字货币(未来币、点点币、莱特币、狗狗币等)，但比特币约占所有加密数字货币市值的90%。

比特币的区块链是为比特币体系的设计而定制的，因此比特币的区块链技术并不等于区块链技术。区块链技术应该是可以有更多种形态、更多

种体系、更多种用途、更多种规格的技术，其概念可以定义如下：区块链是一个去中心化的分布式数据库，该数据库由一串使用密码学方法产生的数据区块有序链接而成，区块中包含有一定时间内产生的无法被篡改的数据记录信息。

如图 1.1 所示，区块中包含数据记录、当前区块根 Hash、前一区块根 Hash、时间戳以及其他信息。数据记录的类型可以根据场景决定，比如为资产交易记录、资产发行记录、清算记录、智能合约记录甚至物联网数据记录等。数据记录在存储过程中，通常组织为树形逻辑结构，比如 Merkle 树，而区块根 Hash 实际就是数据记录树的根节点 Hash，是根据数据记录树自下而上通过 SHA－256 等 Hash 算法逐步计算得出的。时间戳为区块的生成时间。其他信息包括区块签名信息、随机值等信息，也可根据具体应用场景灵活定义。

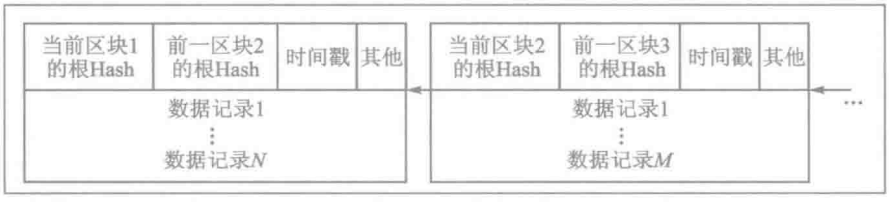


图 1.1　区块链结构示意图

区块链技术是多种技术整合的结果，包括密码学、数学、经济学、网络科学等。这些技术以特定方式组合在一起，形成了一种新的去中心化数据记录与存储体系，并对存储数据的区块打上时间戳使其形成一个连续的、前后关联的诚实数据记录存储结构。其最终目的是建立一个保证诚实的数据系统，可将其称为能够保证系统诚实的分布式数据库。在这个系统中，只有系统本身是值得信任的，所以数据记录、存储与更新规则是为建立人们对区块链系统的信任而设计的。诚实意味着系统可以被信任，这是商业活动和应用推广的前提，所以区块链技术已经被很多领域的主流机构看中。因为有