区块链

数据通信性能优化

李　皎◎著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

区块链数据通信性能优化

李　皎◎著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书重点讲述了区块链数据通信性能的优化问题。从提升数据通信的效率、确保传输的可靠性、改善服务的公平性3个方面进行了阐述，在节点通信能力、信任度、权值、服务请求优先级等多个影响因素的约束下，先从通信拓扑结构和通信机制的角度优化通信性能，构建了多连接并发通信树模型，再针对不同的应用需求和场景，提出了多个区块链数据通信算法，对区块链通信性能进行优化。具体包括考虑节点信任度的区块链通信算法、考虑权值的多因子区块链通信算法、考虑节点失效的区块链通信算法和考虑节点服务优先级的区块链通信算法，并且通过理论证明和仿真实验对算法的正确性和有效性进行了验证。

本书适合区块链技术研究领域的学者，以及进行区块链技术应用和实践的研究、开发人员学习参考。

图书在版编目（CIP）数据

区块链数据通信性能优化/李皎著. —北京：电子工业出版社，2019.1

ISBN 978-7-121-31743-9

Ⅰ. ①区… Ⅱ. ①李… Ⅲ. ①电子商务－支付方式－研究 Ⅳ. ①F713.361.3

中国版本图书馆CIP数据核字（2018）第218278号

策划编辑：朱雨萌
责任编辑：朱雨萌　　特约编辑：刘　炯
印　　刷：三河市兴达印务有限公司
装　　订：三河市兴达印务有限公司
出版发行：电子工业出版社
　　　　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：720×1 000　1/16　印张：12.5　字数：200千字
版　　次：2019年1月第1版
印　　次：2019年1月第1次印刷
定　　价：49.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：（010）88254750。

前　言

随着经济全球化的持续发展，企业向着跨地域、跨国界方向发展，企业数据分布式管理成为必然趋势。企业数据量日益增长，传统的集中式数据管理导致中心节点负荷重，容易引起中心节点故障而出现全网瘫痪现象。企业越来越倾向于根据实际业务需求将数据分布式存储在各个站点。然而，数据分布式存储带来站点间数据协作交互困难、通信效率低、可靠性差等问题，严重影响着企业获取数据的响应速度和时效性。企业寻求一种更有效的方式解决分布式数据管理所面临的问题。区块链（Blockchain）是支撑管理信息系统发展的新兴信息技术之一，它为分布式数据的存储、验证、传递和交流提供了一种解决方案。

近年来，区块链技术受到人们的关注，区块链在各个行业的巨大潜力被逐步挖掘，区块链的研究和应用呈现迅猛的发展势态。区块链技术具有去中心化、数据不可伪造、不可篡改、去信任化、低运营成本的特点，使其在数字货币、金融证券、资产管理、交易支付领域凸显广阔的应用前景。与强烈的市场应用需求相比，区块链的基础理论研究相对滞后。各大学术检索机构的搜索关键词为“区块链”的文献并不多，可见区块链技术作为新技术，还处于萌芽阶段，其基础理论需要进一步完善。目前，比特币区块链交易确认共识达成的时间周期为 10 分钟左右，其处理业务能力只有每秒 8 笔，这显然不适合大规模交易频繁的商业级应用。如何缩短交易验证时间、提高交易验证效率，这些都是影响区块链应用推广的重要因素。因此采用何种方法有效组织节点进行交易验证，以达到缩短区块数据交易确

认时间，提高区块链业务处理能力是区块链研究领域的关键问题之一。本书重点解决区块链交易验证中数据通信性能优化问题。

区块链从本质上讲是一种去中心化的 P2P 计算模式。作者从 2005 年开始研究 P2P 通信算法，已经进行了 10 余年。在陕西省自然科学基金、陕西省科技攻关项目、陕西省教育厅专项科技计划的资助下，对 P2P 通信算法的网络拓扑结构、通信机制、通信影响因子、通信树构造进行了深入的研究。而近两年兴起的区块链技术正是采用 P2P 网络结构，长期研究的 P2P 通信算法可为区块链交易验证提供路由选择策略，为区块链技术实施落地提供理论参考。早在 2008 年已经有比特币，然而区块链技术是近两年才真正被重视起来的。作者在 2015 年较早关注区块链技术，读博期间重点研究区块链数据通信。本书正是这些研究工作的一个小结。

本书重点讨论区块链数据传输性能优化问题，分为 6 章。第 1 章对区块链技术进行概述，通过对比特币区块链交易验证流程分析，提出区块链数据通信所要解决的问题。第 2 章从通信拓扑结构和通信机制的角度出发，构建了适合区块链数据传输的模型。第 3 章分析了区块链通信影响因子并给出节点通信连接数、节点信任度、服务请求优先级、权值的表示方法及度量方法，为后续区块链通信算法研究奠定基础。第 4 章从提升数据通信的效率、确保传输的可靠性、改善服务的公平性三方面进行研究，在节点通信能力、节点信任度、权值、服务请求优先级等多个影响因素的约束下，提出了不同的区块链数据通信性能优化策略，包括考虑节点通信连接数的区块链通信算法，考虑节点信任度的区块链通信算法，考虑权值的多因子区块链通信算法和考虑节点服务优先级的区块链通信算法。第 5 章针对区块链节点失效这一特例，研究了考虑节点失效的区块链通信算法。第 6 章总结了全书的内容，对有待进一步研究的问题进行了展望。

在本书完成的过程中，得到了梁工谦教授、刘天时教授的指导与帮助，

他们对本书的内容提出了很多宝贵的意见，在此表示衷心的感谢。本书由西安石油大学优秀学术著作出版基金资助出版。

由于作者水平有限，书中所存不妥之处，敬请专家和读者批评指正。

作者

2018 年 6 月

目　录

第 1 章 区块链技术概述

1.1 区块链发展历程

1.1.1 区块链的起源

近年来，比特币的底层技术——区块链受到人们的关注，区块链的研究和应用呈现迅猛的发展势态。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网上的创新应用模式。区块链的本质是一种去中心化的点对点（Peer to Peer，P2P）计算模式。运用区块链技术，可使节点在没有中心机构参与的情况下实现信息的自由交流与协作。当前互联网提供给人们的主要是信息服务，在这种模式下，信息是以数据形式存在的，难以体现信息最为宝贵的价值和信用本质，而区块链技术从架构上将信息的价值和信用本质，以一种全新的方式规划，实现从当前的信息互联网向价值互联网的转变，将彻底改变互联网的现有形态。区块链技术在金融、证券、全球化支付、物品交易等方面凸显出广阔的应用前景。然而区块链的基础技术研究仍然滞后，在各大学术检索机构搜索关键词“区块链”，查到的文献并不多，可见区块链技术作为新技术，还处于萌芽阶段。

区块链和比特币密切相关，大多数人知道区块链是从比特币开始的，比特币是众多区块链应用中的一种实现，是基于互联网的，属于区块链中的公有链，而区块链是支撑比特币交易的底层技术。比特币系统是区块链技术第一个典型的应用实例，比特币的概念最初是在2008年由中本聪在一

篇文章《比特币：一种点对点的电子现金系统》中提出的[1]。比特币是一种虚拟的电子货币系统，它不依靠传统支付方式中的第三方金融机构，直接在交易双方之间完成支付，通过随机散列对所有交易加上时间戳，并通过工作量证明的方式保证交易的不可篡改性。比特币与法定货币不同，没有特定的货币发行方，它是通过特定的算法产生的，其数量有限，目前仅有 2100 万个[2]。比特币具有匿名性、身份隐藏、全球范围均可兑现、价格看涨等特点[3]。有人认为比特币是黑客犯罪的帮凶，2017 年 5 月勒索病毒 WannaCrypt 将比特币推上风口浪尖，长期以来，比特币的存在与发展备受争议，存在法律地位不明确性、不易监管等问题。虽然在 2016 年，比特币的主要创始人 Mike Hearn 宣布比特币是一个失败的项目，而近年来，作为比特币底层架构的区块链技术受到政府、资本市场和科技巨头公司的追捧[4]。

1.1.2　区块链构建价值互联网

在人类的文明中，信息的呈现方式多样化、丰富化，信息的传递方式经历了文本、图片、音频、视频的发展过程，香农以比特为单位将信息量化，从而方便了信息的传输。互联网的出现解决了信息的高效传播、自由分享的问题。然而，在以银联卡、信用卡、网银、移动终端支付为代表的电子货币新的应用背景下，人们不局限于在网络上传输信息，价值的传递越来越受到人们的重视。

现在，互联网主要负责信息的传输（主要包括文本、图片、音频、视频），而引入电子货币后，货币是有价值的，而且是有归属权的，这就涉及一个问题，使用何种技术传输具有价值的信息。就像传输控制协议/互联网络协议（Transmission Control Protocol/Internet Protocol，TCP/IP）是现有 Internet 的底层网络协议一样，区块链正是超脱比特币成为支持价值传输的

新技术。区块链将构建一个价值互联网。在互联网上发邮件，一封邮件可以转发给多个人，可以零成本复制。而在价值互联网中进行支付，钱只能点对点地付给唯一特定的人，即必须保证价值交换的唯一性。由于互联网是基于信息传输的网络，而价值互联网实现的是价值的传递[5]，因此信息可以无限复制，而价值交换传递具有唯一性。另外，从网络结构来看，现有互联网信息存储有中央服务器的概念，信息传输大多依赖于中心节点，而在价值互联网中，价值传递是点对点直接支付的。价值互联网中各个节点记录的账目信息，引入了时间戳概念，为账目信息增加了时间轴的维度，保证了账目信息的可追溯性。现有互联网提供了一个信息交互的平台，这种平台是基于信息服务的，而未来价值互联网将提供一个基于电子货币支付和交易的便捷、可信、低成本的交易平台，这种平台是基于价值和信用服务的[6~8]。

表 1-1 从网络结构、传输内容、数据存储、特征、网络协议、应用场景等方面对信息互联网和价值互联网进行了比较。

表 1-1　信息互联网与价值互联网比较

	信息互联网	价值互联网
网络结构	有中心节点	P2P
传输内容	信息	具有价值、归属权的数据
数据存储	集中式存储	按时间轴分布式存储
特征	信息可多次复制转发	价值交换唯一性
网络协议	TCP/IP	区块链
应用场景	获取网络信息，交流互动	比特币、证券交易、电子货币支付

总之，为了传播信息，人们从文字开始，最终创造了现在的互联网，完成了信息的高效快捷传递和分享；为了传输价值，人们从电子货币开始，必然会创造一个与现有信息互联网同等重要的价值互联网。区块链技术的出现正好构建了价值互联网的底层技术。在未来社会，互联网可分为信息互联网与价值互联网，互联网将承担信息传递和价值传输的双重责任。

1.1.3　区块链发展的三个阶段

有人将区块链技术分为 1.0、2.0、3.0 三个阶段，区块链 1.0 以 2008 年比特币在区块链上发行为标志。随着以太坊智能合约区块链被发明、设计，进入区块链 2.0 时代，称为智能合约时代。智能合约区块链能够自动执行事先约定好的合约条款的计算机程序。智能合约要执行，资产必须数字化[9]，这就需要给每个设备装上传感器[10,11]，变成智能资产。有了智能合约，不需要依靠中介机构来帮助建立信任，仅靠一段代码、一个算法来解决信任问题[12]。区块链 3.0 将超越货币、金融市场以外的应用，将区块链技术引入社会管理[13,14]、医疗健康[15,16]、科学、文化和艺术等方面[17,18]。图 1-1 显示了区块链技术经历的三个发展阶段。

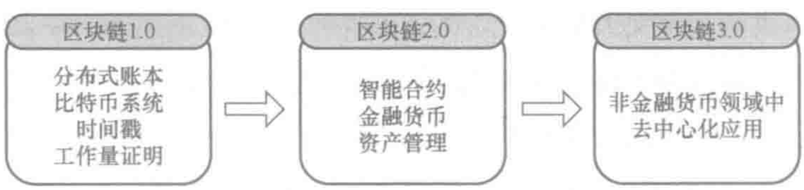

图 1-1　区块链技术经历的三个发展阶段

1.1.4　区块链的国内外研究现状

2015 年，区块链成了美国创投中获得融资最高的板块，突破 10 亿美元。美国纳斯达克于 2015 年 12 月率先推出基于区块链技术的证券交易平台 Linq，成为金融证券市场去中心化趋势的重要里程碑。在 2017 年华盛顿区块链峰会上，美国政府将区块链技术应用到各个政府部门，帮助提高工作效率，并推动本国经济发展。2016 年 1 月，英国政府发布了《分布式账本技术：超越区块链》报告，报告中提到，英国联邦政府正在探索区块链技

术，并且分析了区块链应用于传统金融行业的潜力[19]。考虑到区块链可减少欺诈、腐败、错误的发生，并改变办事依赖于纸张的流程，在物品所有权和知识产权保护方面有着巨大的潜力，它将重新定义政府与公民之间在数据共享、透明度及信任方面的关系[20]。2018 年 1 月，美国国务院鼓励使用区块链技术，通过提高政府与企业之间的合作透明度，能够处理公共采购资金流程本身的资金腐败、欺诈或挪用和效率低下问题。2018 年 6 月，美韩政府加强第四次工业革命合作，携手三星、微软推动区块链技术的应用，他们将通过区块链所提供的防篡改账本技术，进一步构建更透明、开放的全球互联网。

在我国，2016 年 12 月，国务院印发了《“十三五”国家信息化规划》，其中首次写入区块链技术。周小川在 2016 年 2 月和 2017 年 3 月曾几次谈到数字货币和区块链技术对未来支付业务造成的巨大改变，其影响力将难以想象，并部署重要力量研究区块链在数字货币中的应用模式。2016 年 10 月，中国工业和信息化部发布了《中国区块链技术和应用发展白皮书》。该白皮书总结了国内外区块链发展的现状和趋势，分析了包含金融、供应链、文化娱乐、智能制造、社会公益、教育就业等多个应用场景的技术应用，指出了区块链的核心技术路线，以及未来区块链技术标准化的方向和进程。专家指出了区块链技术在 84 个行业的应用潜力，而国内外区块链行业标准尚属空白，行业发展自成体系，呈现碎片化，行业应用存在盲目性，不利于区块链技术的应用及发展[21]。另外，国家政策也推动着区块链标准的发展。2017 年 5 月，在中国工业和信息化部的指导下，中国区块链技术和产业发展论坛公布了《区块链和分布式账本技术参考架构》，这是首个在政府指导下的国内区块链标准。区块链的标准化为区块链技术在各个行业的应用和发展提供了规范和指导，促进解决区块链的关键技术问题。2017 年 9 月，中华人民共和国中央人民政府网站新闻报道了中国拥有世界上最大的互联网应用市场，因而区块链产业具备走在世界前列的众多有利条件。2017 年，

区块链逐渐进入“政府主导模式”，不仅从国家层面重视区块链的发展，而且多个省份、自治区、直辖市发布了区块链部署应用的指导意见。2018 年 5 月，中国工业和信息化部发布了《2018 中国区块链产业白皮书》，深入分析了中国区块链技术在金融领域和实体经济领域的应用落地情况，系统阐述了中国区块链产业发展的六大特点和六大趋势。

科技巨头也纷纷聚焦区块链。以太坊（Ethereum）是一个源码公开、全球开放的区块链平台，它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用[22]。超级账本（Hyperledger）是 Linux 基金会于 2015 年 11 月发起的推进区块链数字技术和交易验证的开源项目，目标是让成员共同合作，共建开放平台，满足来自多个不同行业的各种用户，并简化业务流程。2017 年 4 月，全球科技巨头三星电子发布了一个基于区块链的 B2B 数字化商业区块链平台，名为 Nexledger，它能够提供大规模实时交易，检测控制信息，并对区块数据按条件隔离，以保障数据的安全性。三星电子同时也展示了基于区块链的数字认证和数字支付服务。IBM 互联部门发布了区块链网络软件 Hyperledger Fabric 1.0，它是一款基于 Linux 架构开发、具有企业应用价值的软件，可以帮助开发者建立、运行和管理一个企业级的区块链网络[23,24]。

世界经济论坛创始人克劳斯·施瓦布说，自蒸汽机、电和计算机发明以来，迎来了第四次工业革命——数字革命，而区块链技术就是第四次工业革命的成果[25]。“经济数学之父”唐塔普斯科特说，区块链是第二代互联网，将对现有互联网产生深刻改变[26]。区块链技术是继蒸汽机、电力、互联网之后，下一代颠覆性的核心技术。如果说蒸汽机解放了生产力，电力满足了生活基本需求，互联网改变了信息传递方式，那么区块链将解决价值传输过程中的信任问题。总之，区块链技术在各个行业的巨大的应用前景和潜能得到政府、资本市场、科技巨头的普遍追捧与认可。有人称 2017 年为区块链元年，全球都在研究区块链技术在各个行业的应用潜力和可行性[27]。