



中国区块链技术与产业发展报告

(2017)

邢春晓 张桂刚 主 编

清华大学出版社



邢春晓 张桂刚 主编

中国区块链技术与产业发展报告 (2017)

清华大学出版社
北京

内 容 简 介

区块链技术是未来信用的基石,目前,全球多数国家以及著名企业均开始了这一领域的研究。未来5~10年将是区块链蓬勃发展的时机,市场需求巨大。本书介绍了区块链的常用关键技术,梳理了区块链的技术架构。同时,本书结合各种具体案例,对区块链在医疗、金融、物流、慈善、征信等各个领域的可能应用进行了详尽分析。本书将帮助广大读者理解和掌握区块链的具体应用。本书面向各个层次的读者,既具有专业性,也具有普适性,适合各个层次读者使用。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

中国区块链技术与产业发展报告. 2017/邢春晓,张桂刚主编. —北京:清华大学出版社,2018
ISBN 978-7-302-49834-6

I. ①中… II. ①邢… ②张… III. ①电子商务—支付方式—研究报告—中国
IV. ①F713.361.3

中国版本图书馆 CIP 数据核字(2018)第 042852 号

责任编辑:王 芳

封面设计:常雪影

责任校对:焦丽丽

责任印制:沈 露

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课件下载: <http://www.tup.com.cn>, 010-62795954

印 装 者:三河市铭诚印务有限公司

经 销:全国新华书店

开 本:185mm×260mm 印 张:10.75

字 数:171千字

版 次:2018年7月第1版

印 次:2018年7月第1次印刷

定 价:99.00元

产品编号:075054-01

编 写 者

主 编 邢春晓(清华大学)

张桂刚(中国科学院自动化研究所)

编写人

第 1 章 张跃冬 郭川(中国互联网络信息中心)

李永军(北京东方亿思知识产权代理有限公司)

第 2 章 张桂刚(中国科学院自动化研究所)

刘建伟(清华大学)

第 3 章 王宝兴(中金云金融(北京)大数据科技股份有限公司)

胡鸿雁 付永贵(中央财经大学)

唐长春 陈银玲(北京丰瑞祥信息技术有限公司)

蒋平友 杨灵江 黄小刚 李思远(广东区块链应用技术研究有限公司)

林大鹏(中关村区块链产业联盟秘书处)

朱义(清华大学)

黄喆(中国电信北京研究院)

张红 高海逵(上海快贝网络技术有限公司)

鲁静(远光软件股份有限公司)

范金刚 郭艳来(北京世纪互联宽带数据中心有限公司)

李清(北京太一云科技有限公司)

李军(布比(北京)网络技术有限公司)

唐文剑(安永(中国)企业咨询有限公司北京分公司)

- 第4章 郭峰 高炎(点亮投资管理(上海)有限公司)
李军 刘柱(布比(北京)网络技术有限公司)
李清(北京太一云科技有限公司)
王立仁(北京人民汇金科技有限公司)
- 第5章 许杰(清华大学)

审稿人

- 第1章 邢春晓(清华大学)
- 第2章 邹均(海纳云计算有限公司)
- 第3章 朱建明(中央财经大学)
- 第4、5章 蔡维德(北京航空航天大学)



本书系统地总结了区块链技术兴起的背景、动态、关键技术、典型应用场景和案例、产业链和生态圈、发展趋势、问题与建议等诸多内容。

区块链技术以其分布式、可追溯、安全可信等特征,有望成为价值互联网的基础协议,正在吸引着政府、企业及技术开发者和创业者等各方关注的目光。正如 2015 年《经济学人》封面标题文章《信任的机器》所言,“区块链技术不仅将彻底改变金融行业,还将成为全球跨国信用的基石,并最终深刻改变人类社会的结构。”区块链技术已经开始应用在金融、政府、医疗、能源、交通、电商、司法、艺术等众多领域,而这个名单还在延展……

在背景与动态部分,本书讨论了区块链的发展历程、技术特点、应用场景、区块链技术的局限性、在国内外推广的现状和标准化进程,提出了包括搭建区块链测试平台、研究区块链底层协议、设计基于区块链的典型应用模式和推进区块链标准化等诸多思考和建议。

区块链技术部分讨论了区块链研究的缘起、涉及的关键技术、区块链模型、数据安全与隐私保护以及区块链技术标准体系构想。

在区块链典型应用部分讨论了区块链与金融、医疗、政府、能源、产权交易、电子商务、慈善及物联网技术相结合的 8 类应用场景和案例,包含了作者基于现有应用提炼的模型描述和场景分析。

区块链产业链和生态圈部分讨论了国内外区块链产业的主要参与者,以及有关区块链产业创新孵化和投资的现状和建议。

区块链发展趋势与建议部分指出了区块链热点问题与技术发展趋

势,并对中国区块链的发展提出了包括做好技术及人才储备工作、积极参与区块链国际标准制定和加强对区块链产业发展的引导和监管等建议。

编写组

2018年1月

C

ONTENTS

目录

第 1 章 背景与动态	1
1.1 区块链的定义	2
1.2 区块链发展历程	3
1.2.1 数字货币时期	3
1.2.2 比特币时期	3
1.2.3 区块链时期	4
1.3 区块链技术的特点	5
1.4 区块链技术的延伸	6
1.5 区块链技术的应用场景	7
1.6 区块链技术的局限性	8
1.7 区块链技术在国外的推广	10
1.8 区块链技术在国外的推广	11
1.8.1 R3 区块链联盟	11
1.8.2 超级账本区块链联盟	11
1.8.3 布局区块链产业的科技巨头	12
1.9 区块链技术的标准化	13
1.10 区块链技术的总结和思考	14
第 2 章 区块链技术	16
2.1 区块链技术研究缘由	17
2.1.1 区块链用例描述：比特币	18
2.1.2 为什么要研究区块及区块链	22

2.1.3	区块链需要研究哪些关键技术	23
2.2	区块链模型	25
2.3	数据存储层关键技术	28
2.3.1	分布式文件系统	28
2.3.2	分布式数据库	30
2.3.3	数据区块	31
2.3.4	链式结构	32
2.3.5	Merkle 树	33
2.4	网络通信层关键技术	34
2.4.1	P2P 网络	34
2.4.2	连接方式	35
2.4.3	传播机制	36
2.4.4	共识机制	38
2.4.5	验证机制	38
2.4.6	其他	38
2.5	数据安全性与隐私保护关键技术	39
2.5.1	时间戳	39
2.5.2	哈希函数	39
2.5.3	数据加密	40
2.5.4	数字签名	43
2.5.5	零知识证明	44
2.5.6	区块链安全体系	45
2.5.7	隐私保护机制	46
2.5.8	隐私保护算法	47
2.5.9	区块链隐私保护体系	49
2.6	共识层关键技术	49
2.6.1	工作量证明	50
2.6.2	权益证明	50
2.6.3	股份授权证明	51
2.6.4	拜占庭容错共识机制	52
2.6.5	其他	52

2.7	应用组件层关键技术	52
2.7.1	发行机制	53
2.7.2	分配机制	53
2.7.3	区块链 2.0 核心智能合约衍生的核心组件	54
2.7.4	区块链 3.0 衍生的复杂的可编程资产	54
2.8	区块链应用层	56
2.8.1	区块链 1.0 系列应用	56
2.8.2	区块链 2.0 系列应用	56
2.8.3	区块链 3.0 系列应用	56
2.9	区块链与现代技术融合	56
2.9.1	区块链与云计算技术的结合	57
2.9.2	区块链与大数据技术的结合	57
2.9.3	区块链与现代加密技术的结合	57
2.9.4	区块链与物联网技术的结合	58
2.9.5	区块链与现代通信技术的结合	58
2.9.6	区块链与深度学习为代表的机器学习智能技术的结合	58
2.10	区块链技术标准	59
第 3 章	区块链典型应用	62
3.1	金融与区块链	62
3.1.1	概况	62
3.1.2	银行支付清算区块链应用模型	65
3.1.3	金融证券区块链应用模型	68
3.1.4	保险区块链应用模型	71
3.1.5	供应链金融区块链应用模型	75
3.1.6	纳斯达克 Linq 区块链应用分析	79
3.1.7	区块链金融案例——BitShares 分析	81
3.1.8	R3 区块链联盟	83
3.1.9	区块链的首次币发行	84
3.2	健康医疗与区块链	85

3.2.1	健康医疗区块链应用现状	86
3.2.2	国外健康医疗区块链分析的应用	86
3.2.3	区块链技术提升传统医疗信息系统效率	88
3.2.4	区块链在区域化医疗卫生方面的应用	89
3.2.5	健康医疗区块链的发展趋势	90
3.3	政府与区块链	91
3.3.1	在公共部门应用区块链技术的优势	91
3.3.2	政府等公共部门应用区块链技术的领域和现状	92
3.3.3	政府在区块链技术和产业发展中所能发挥的 作用	95
3.4	区块链与物联网	97
3.4.1	行业痛点	97
3.4.2	基于区块链的解决思路	97
3.4.3	应用场景	100
3.4.4	区块链技术在物联网环境下的演进	104
3.5	能源与区块链	104
3.5.1	行业现状	104
3.5.2	行业痛点	106
3.5.3	基于区块链的解决方案	107
3.5.4	区块链解决方案的优势和价值	120
3.6	区块链与产权交易	120
3.7	电子商务与区块链	122
3.7.1	行业痛点	122
3.7.2	基于区块链的解决思路	123
3.7.3	应用场景	123
3.8	慈善与区块链	125
3.8.1	我国慈善事业的发展历程	125
3.8.2	国内慈善事业的现状及存在的问题	126
3.8.3	区块链技术对于发展慈善事业的意义	129
3.8.4	区块链在慈善领域的应用案例	131
3.9	其他	132

第 4 章 区块链 IT 产业链和生态系统	134
4.1 概述	134
4.1.1 基础技术层	135
4.1.2 中间平台层	135
4.1.3 应用服务层	136
4.2 主力参与者	138
4.2.1 太一云科技	138
4.2.2 布比区块链	139
4.2.3 人民汇金	141
4.2.4 微软区块链服务	141
4.2.5 PDX 公司	142
4.2.6 银链科技	142
4.2.7 小蚁区块链	142
4.2.8 云象区块链	142
4.2.9 维优区块链	143
4.2.10 Waves 区块链平台	143
4.2.11 唯链	143
4.2.12 北航链	143
4.2.13 赞赏	144
4.2.14 物链	144
4.2.15 金股链	145
4.2.16 数链	145
4.3 区块链的创新孵化与投资	146
4.3.1 区块链投资现状	146
4.3.2 投资建议	147
4.3.3 区块链创新孵化	147
第 5 章 区块链发展趋势与建议	151
5.1 区块链发展现状与趋势	151
5.1.1 区块链发展现状	151

5.1.2	区块链发展趋势	151
5.2	区块链热点问题与技术发展趋势	152
5.2.1	区块链热点问题	152
5.2.2	技术创新滞后阻碍产业发展进程	152
5.2.3	企业级应用需要逾越的障碍较多	153
5.2.4	信息安全体系亟待建立	153
5.2.5	区块链技术发展趋势	154
5.3	中国区块链发展战略与建议	154
5.3.1	区块链基础研究的发展战略与建议	154
5.3.2	区块链产业的发展战略与建议	155
	参考文献	156

1

第 1 章

背景与动态

随着以比特币(Bitcoin)为代表的数字货币的崛起,其底层支撑技术架构——区块链(Blockchain)凭借去中心化、数据不可篡改等特点,吸引了多国政府部门、金融机构及互联网巨头公司的广泛关注,逐渐成为当前学术界和产业界的热点课题。

区块链技术的迅猛发展首先引起金融机构的广泛关注:美国全国证券交易商协会自动报价表(National Association of Securities Dealers Automated Quotations, NASDAQ, 纳斯达克)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里程碑。同时,摩根大通集团(JP Morgan)、高盛集团(Goldman Sachs)等 42 家大型金融机构组建成立区块链联盟,提出了全球汇款网络的实时结算清算框架协议。此外,中国人民银行也召开数字货币研讨会,探讨了采用区块链技术发行虚拟货币的可行性,以提高金融业务的效率、便利性和透明度。

2015 年 10 月,如图 1.1 所示,《经济学人》(*The Economist*)封面文章《信任的机器》所言,“区块链技术不仅将彻底改变金融行业,还将成为全球跨国信用的基石,并最终深刻改变人类社会的结构。”



图 1.1 2015 年 10 月《经济学人》封面

1.1 区块链的定义

狭义来讲,区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证不可篡改和不可伪造的分布式账本。

广义来讲,区块链技术是利用块链式数据结构来验证与存储数据,利用分布式节点共识算法来生成和更新数据,利用密码学的方式保证数据传输和访问的安全,利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

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

技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。

1.2 区块链发展历程

互联网时代,技术发展、行业创新层出不穷。相比于大数据、云计算、物联网等新技术一经出现便在全球范围掀起热潮,区块链作为比特币这一虚拟货币的底层支撑技术,在比特币发展繁荣的过程中并未引起足够的重视与关注,社会各界对区块链的发现和认识过程经历了一段较长的时间。在此对区块链的诞生背景、发展过程以及当前现状做简单介绍。

1.2.1 数字货币时期

20 世纪后半期,伴随着电子技术的发展,“电子货币终将取代纸币”这一看法成为了一种趋势。以银行信用卡为代表的电子货币迅速流行,成为当今主流的货币形式。电子货币作为法定货币的电子化形式,继承了传统法定货币的弊端:交易成本高、不具有匿名性、不能全球通用等。于是有人开始设计新的电子货币方案,如 20 世纪 90 年代的电子钱币(DigiCash)、Beez、Flooz 及比特金(BitGold)等,但其影响极其有限。究其原因,此类电子货币依赖于一个中心服务节点,在缺乏国家信用支撑的情况下,此中心服务节点面临法律、道德、技术等方面的风险,容易导致其信用破产。

1.2.2 比特币时期

区块链起源于比特币。标志着上轮金融危机起点的雷曼兄弟公司(Lehman Brothers)倒闭后两周,2008 年 11 月 1 日,化名中本聪(Satoshi Nakamoto)的人或组织在一次私密的小组讨论中发表了名为《比特币:一种点对点的电子现金系统》的论文,文中首次提出了比特币的概念。中本聪在论文中提出了一套“基于公钥加解密验证而不是基于信用,使得任何达成一致的双方能够端对端进行支付,而不需要一个中间的金融机构”的电子支付系统,同时提出了“一种基于 P2P(Peer-to-Peer)网络解决双重支付问题的方法,这个网络给支付交易打上时间戳,除非可以提供之前所有

的工作量证明,否则不能被篡改。只要占多数的 CPU 能量不被同时控制,并联合起来对网络进行攻击,它们就可以比攻击者生成更长的链条。”从而此系统就是安全的。中本聪的论文基于一定的前提,从理论上解决了困扰去中心化电子支付系统已久的双重支付问题,并在后续发展中获得广泛赞誉。

两个月后理论步入实践,2009 年 1 月 3 日第一个序号为 0 的比特币创世区块诞生。几天后,2009 年 1 月 9 日出现序号为 1 的区块,并与序号为 0 的创世区块相连接形成了链,标志着区块链的诞生。2010 年 7 月,比特币交易所 Mt. Gox 作为世界上第一个比特币交易平台在日本成立,此后比特币的价格开始呈现出增长趋势。随后几年比特币价格逐年攀升,从最初的零点几美元一路涨到 1242 美元,截至 2013 年年底,根据 Blockchain. info 组织的统计,有近 14 万个网络地址参与比特币交易,交易量为每天 6 万次。

然而,随着比特币的发展、繁荣,其自身的问题开始逐渐出现,同时面临社会各方压力。2011 年 7 月,比特币交易中心 Bitomat 的托管运营商宣称记录着 17 000 个比特币(当时价格约 22 万美元)的 wallet. dat 文件失去访问权限;2012 年,网站托管供应商 Linode 的服务器超级管理密码泄露,价值近 23 万美元的 46 703 个比特币失窃;2013 年 10 月,地下交易网站“丝绸之路”被美国多个执法部门查缴。此类事件的频发,逐渐冷却了比特币用户对这一数字货币的信心与热情。

近年来,世界对比特币的态度起起落落,但作为比特币底层技术之一的区块链技术却日益受到重视。

1.2.3 区块链时期

随着人们对比特币质疑的增多及对其热炒的降温,其底层的区块链技术反而越来越引起人们的关注。在比特币形成过程中,区块(block)是一个一个的存储单元,记录了一定时间内各个区块节点全部的交流信息。各个区块之间通过随机散列(也称哈希(Hash)算法)实现连接,后一个区块包含前一个区块的哈希值(Hash Function),随着信息交流的扩大,一个区块与一个区块相继接续,形成的结果就叫区块链。关于区块链技术越来越多的应用价值开始被提出并研究,相关机构也开始关注区块链,对于区块链的