区块链蓝皮书

BLUE BOOK OF BLOCKCHAIN

中国区块链发展报告（2017）

主编/李伟

执行主编/朱烨东

ANNUAL REPORT ON DEVELOPMENT OF CHINA'S BLOCKCHAIN (2017)

2017版

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

区块链蓝皮书
BLUE BOOK OF
BLOCKCHAIN

中国区块链发展报告（2017）

ANNUAL REPORT ON DEVELOPMENT OF CHINA'S BLOCKCHAIN
(2017)

主　　编／李　伟
执行主编／朱烨东

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

图书在版编目(CIP)数据

中国区块链发展报告. 2017 / 李伟主编. --北京：社会科学文献出版社，2017.9
（区块链蓝皮书）
ISBN 978-7-5201-1289-5

Ⅰ.①中… Ⅱ.①李… Ⅲ.①电子商务-支付方式-研究报告-中国-2017 Ⅳ.①F724.6

中国版本图书馆 CIP 数据核字（2017）第 202296 号

区块链蓝皮书
中国区块链发展报告（2017）

主　　编 / 李　伟
执行主编 / 朱烨东

出 版 人 / 谢寿光
项目统筹 / 恽　薇　高　雁
责任编辑 / 高　雁　梁　雁

出　　版 / 社会科学文献出版社·经济与管理分社（010）59367226
地址：北京市北三环中路甲 29 号院华龙大厦　邮编：100029
网址：www.ssap.com.cn
发　　行 / 市场营销中心（010）59367081　59367018
印　　装 / 北京季蜂印刷有限公司

规　　格 / 开 本：787mm × 1092mm　1/16
印 张：12.25　字 数：183 千字
版　　次 / 2017 年 9 月第 1 版　2017 年 9 月第 1 次印刷
书　　号 / ISBN 978-7-5201-1289-5
定　　价 / 89.00 元

皮书序列号 / PSN B-2017-649-1/1

本书如有印装质量问题，请与读者服务中心（010-59367028）联系

《中国区块链发展报告（2017）》
编　委　会

北京市投资促进局

北京市海淀区人民政府

中关村科技园区管理委员会

清华大学五道口金融学院

南开大学金融学院

上海高级金融学院

银行业信贷资产登记流转中心有限公司

主要编撰者简介

李　伟　电子科技大学工学学士，北京大学光华管理学院 EMBA。现任中国人民银行科技司司长。1995 年加入中国人民银行，先后担任中国人民银行清算总中心技术管理部总经理、副主任，中国人民银行石家庄支行副行长，跨境银行间支付清算（上海）有限责任公司（CIPS）执行董事等职务。长期从事支付清算研究与系统建设工作，参与编写制定中国现代化支付系统（CNAPS）业务需求和技术方案并主持小额支付系统工程实施。

朱烨东　经济学博士。北京中科金财科技股份有限公司董事长，北京区块链技术应用协会会长；中国软件和信息服务业十大领军人物，中国上市公司十大创业领袖人物；清华五道口全球创业领袖导师、长江商学院 MBA 导师。主编《中国互联网金融发展报告》《中国区块链发展报告》《中国资产证券化发展报告》等。

摘　要

近年来，区块链技术成为金融科技领域广泛探讨的热门话题，得到国内外监管机构、金融机构、科技公司、咨询公司等的关注，越来越多的参与机构、技术人员、市场资金投入区块链技术的研究与应用当中。

本报告首先从宏观层面对国际和国内区块链发展的现状、面临的问题、对经济社会生活的冲击与影响和未来的发展等做了深入的研究，提出了相应的政策建议。

其次从理论和实际应用两个维度出发，分析了政策监管、技术、场景应用、市场等区块链各个领域的发展状况，重点研究了数字货币、技术标准、各项应用、ICO 融资等社会普遍关注的热点问题，同时提出了相应的解决方案和对策建议。

关键词：区块链　场景　技术标准

目　录

Ⅰ　总报告

Ⅱ　技术篇

Ⅲ 应用篇

Ⅳ 市场篇

Ⅴ 附录

皮书数据库阅读使用指南

总 报 告

General Report

B.1
区块链总体运行分析*

李 伟

摘 要：近年来，区块链技术发展方兴未艾，在推动金融科技（FinTech）创新方面发挥了一定作用，逐步受到国内外广泛关注。作为一种分布式账本技术，区块链利用点对点网络、密码学技术、共识机制等将集中式记账模式转化为多节点参与的分布式记账模式。本文从区块链技术国内外发展现状出发，剖析了区块链技术架构、交易流程与运行机理，探索了其适用的金融业务场景，提出了有针对性的应用风险防范建议。最后对区块链技术在降低公共服务成本、提升社会运行效率等方面的发展前景进行了展望。

关键词：区块链 金融科技 分布式账本 金融风险

* 本文仅代表个人观点，不代表任何机构观点，特此说明。

一　国内外发展情况

（一）基本情况

区块链技术起源于2008年由化名为中本聪（Satoshi Nakamoto）的学者在密码学邮件组发表的一篇论文《比特币：一种点对点电子现金系统》，目前尚未形成行业公认的区块链定义。狭义的区块链，是指一种按照时间序列将数据区块以线性链表方式组合而成的特定数据结构，并借助密码技术确保交易信息数据的不可篡改和不可伪造。作为一种典型的分布式账本技术（Decentralized Ledger Technology，DLT），区块链技术能够安全存储简单的、有先后关系的、在系统内可验证的数据。广义的区块链，则是利用加密链式区块结构来存储与验证数据、利用分布式共识算法来新增和更新数据、利用运行在区块链上的代码（即智能合约）来保证业务逻辑自动强制执行的一种全新的多中心化基础架构与分布式计算范式。

近年来，区块链技术成为金融科技领域广泛探讨的话题，得到国内外监管机构、金融机构、科技公司、咨询公司等的关注，越来越多的参与机构、技术人员、市场资金投入区块链技术研究、开发、设计、测试与推广中，意在利用区块链技术优化现有金融业务模式和服务方式，并尝试构建新的金融服务基础设施（见表1）。目前，区块链技术仍处于技术分析、理论研究向技术应用、实践探索发展的阶段，部分基于区块链技术的平台搭建、系统开发和应用测试等工作正在有序推进。

表1　国内外机构部分区块链研究项目情况

地区	机构类型	机构名称	研究项目	应用领域或研究方向	目前进展
国外	跨国联盟	R3 CEV 联盟	Corda	支付结算、贸易融资等	测试阶段
	跨国联盟	Linux 基金会等	HyperLedger	数字货币、支付结算等	开发阶段

续表

地区	机构类型	机构名称	研究项目	应用领域或研究方向	目前进展
国外	监管部门	荷兰央行	DNBCoin	数字货币	开发阶段
	监管部门	英国央行	RSCoin	数字货币	测试阶段
	监管部门	爱沙尼亚政府	未公布	身份验证	开发阶段
	金融机构	澳大利亚联邦银行、德国 Fidor 银行等	Ripple	转账支付	测试阶段
	金融机构	纳斯达克证券交易所	Linq	证券交易	市场应用
	金融机构	巴克莱银行	Circle	数字货币、支付结算等	测试阶段
	金融机构	西班牙对外银行	Coinbase	数字货币、支付结算等	开发阶段
	金融机构	花旗银行	花旗币	数字货币、支付结算	测试阶段
	金融机构	Visa 公司、纳斯达克、花旗风投、Fiserv 公司、第一资本金融公司等	Chain	技术服务	测试阶段
	金融机构	新韩银行	Streami	结算清算	开发阶段
	金融机构	美国银行	未公布	贸易融资	开发阶段
	金融机构	瑞士银行	未公布	支付结算	研究阶段
	金融机构	俄罗斯 Sberbank	未公布	移动通信、金融交易等	开发阶段
	科技公司	印度 Infosys	EdgeVerve	支付结算、金融交易等	开发阶段
	科技公司	BitPagos	未公布	支付结算	测试阶段
	科技公司	飞利浦医疗集团	未公布	医疗保健	研究阶段
	咨询公司	安永公司	未公布	保险业	研究阶段
	咨询公司	德勤公司	Rubix	审计、登记、确权、咨询等	市场应用
	投资公司	美国 Draper & Associates, Blockchain Capital, Di-Ann Eisnor	Stampery	数据认证	开发阶段
	投资公司	美国 Arbor Ventures, RRE Ventures, First Round Capital	Abra	支付汇款	测试阶段
	投资公司	英国 Coinsilium, Kuala Innovations	SatoshiPay	支付汇款	开发阶段
	—	—	Bitcoin	数字货币	市场应用

续表

地区	机构类型	机构名称	研究项目	应用领域或研究方向	目前进展
国内	交易所	上海票据交易所	基于区块链技术的票据交易平台	票据业务	测试阶段
	金融机构	中国工商银行	未公布	资产汇划和账户管理	研究阶段
	金融机构	中国平安	未公布	资产交易和征信	研究阶段
	金融机构	中国邮储银行	未公布	资产托管	市场应用
	金融机构	招商银行	未公布	现金管理	市场应用
	金融机构	浙商银行	未公布	移动数字汇票	市场应用
	金融机构	阳光保险	区块链+航空意外险卡单	保险理赔	测试阶段
	科技公司	蚂蚁金服	未公布	慈善捐助	市场应用
	学术机构	北京航空航天大学、北京大学	北航链	银行交易	开发阶段
	科技公司	上海小蚁科技有限公司	小蚁	股权众筹	测试阶段
	科技公司	布比公司	数贝荷包、格格积分等	股权登记、供应链金融等	测试阶段
	科技公司	万向区块链实验室	万云区块链云平台	技术开发平台	市场应用
	科技公司	北京阿尔山金融科技公司	未公布	金融服务	研究阶段
	联盟组织	区块链应用研究中心（北京、杭州）	未公布	国内应用落地与发展研究	研究阶段
	联盟组织	中关村区块链产业联盟	未公布	知识产权保护、产业化应用研究等	研究阶段
	联盟组织	中国区块链研究联盟	未公布	技术与理论研究	研究阶段
	联盟组织	中国分布式总账基础协议联盟	未公布	分布式总账系统及其衍生技术	研究阶段
	联盟组织	银行间区块链技术研究组	未公布	银行间市场区块链技术、监管及法律框架等	研究阶段
	联盟组织	金融区块链合作联盟	未公布	技术及应用场景研究	研究阶段
	联盟组织	中国互联网金融协会	未公布	金融领域应用的技术难点、业务场景、风险管理、行业标准等	研究阶段

从国际来看，具有代表性的机构有英国央行、R3 CEV 联盟、Linux 基金会、花旗银行、澳大利亚联邦银行、纳斯达克证券交易所、德勤公司等，典型项目有 Corda、HyperLedger、RSCoin、花旗币、Ripple、Linq、Rubix 等，涉及数字货币、支付结算、贸易融资、证券交易、资产登记等领域。从国内来看，具有代表性的机构有万向控股有限公司、上海小蚁科技有限公司、北京阿尔山金融科技公司、中国分布式总账基础协议联盟、中国互联网金融协会、金融区块链合作联盟等，典型项目有万云区块链云平台、北航链、基于区块链技术的票据交易平台等，涉及技术服务、转账交易、保险理赔、股权众筹等领域。

（二）发展趋势

1. 区块链1.0

区块链 1.0 以 2008 年比特币的发明为开始标志，采用区块链技术构建了一种新型去中心化的数字支付系统，主要实现的功能是在区块链上实现货币的发行、转移、兑付和支付。区块链 1.0 是以数字加密货币为典型应用的区块链初级发展阶段，主要的应用包括比特币、莱特币、Dogecoin、Ripple 等。比特币作为区块链 1.0 的第一个应用，实现了点对点支付的功能；莱特币设计的初衷是作为比特币的补充，若比特币主要用于大宗购买，则莱特币用于日常消费；Dogecoin 设定了较大的发行量，因此币值较低，适用于慈善捐赠和打赏。区块链 1.0 是区块链发展的基础，提供了区块链基础平台和基本应用开发模式，但功能较为单一，可扩展性不足，只能承载支付等简单应用。

区块链 1.0 阶段的应用体现出一些基本特点。一是应用类型同质。区块链 1.0 阶段的绝大多数应用是对比特币的模仿，其主要功能集中在支付上，除比特币外的其他数字货币一般被称作“山寨币”或“竞争币”（Altcoin），意在某个垂直领域替代比特币的价值存储功能。在此阶段中，一些具有更多功能的所谓“二代币”（比特股、以太坊）展开对智能合约的应用，标志着区块链技术逐步向 2.0 阶段演进。二是核心技术相近。绝大多数“竞争币”采用了和比特币相似的技术框架，只是在具体密码算法和共识机制上进行了改进，甚至只修改了代码的具体参数设置。总体来说，区块链 1.0 的技术创

新有限。三是参与对象边缘化。比特币和“竞争币”的开发者、运营者和使用者均不来自主流经济社会，并诞生了“矿工”（计算能力提供者，并获得奖励）、“交易所”（进行数字货币撮合交易，并提供期货和杠杆服务）、“炒币者”（对数字货币价格进行炒作）等处在边缘地带的灰色职业链条。主流金融机构没有参与到区块链1.0的建设当中。

2. 区块链2.0

区块链2.0在2012年前后萌芽，是以智能合约为典型应用的区块链高速发展阶段，也是当前区块链研究的主要方向。通过把计算机代码记载在区块链上，实现了数字化合约的可信存储和执行，进而实现多业务系统的协同工作，并将区块链的功能扩展到其他金融领域。典型应用如下：比特股提供了建立数字资产去中心化交易所的解决方案；以太坊是供开发人员建立和发布分布式应用的平台，包括投票、域名、金融交易所、众筹、公司管理等应用；HyperLedger试图通过创建分布式账本的公开标准，实现数字形式的价值交换，并在制造业、银行业、保险业、物联网等行业取得应用。

区块链2.0体现出一些基本特点。一是应用平台化。区块链2.0阶段诞生了一批平台型的应用，无论是比特股、以太坊还是HyperLedger，都不是单一的应用，而是能支撑多应用的区块链技术基础架构或开发平台。二是业务代码化。区块链2.0阶段，不同业务参与主体构建分布式账本，使用计算机代码创建业务规则，该业务规则被记载在区块链网络上，保障规则透明且不可篡改，并通过外部机制执行代码，实现业务流程的自动化。三是多行业参与。区块链2.0阶段，金融机构、IT公司、咨询公司均参与到了区块链研究和验证过程中，代表性的有包含国际四十多家大型金融财团的区块链联盟R3 CEV、IBM推动建立的包括多家IT公司和咨询公司的开源技术项目HyperLedger等。主流行业开始尝试主动运用区块链技术优化业务流程。

3. 区块链3.0

区块链3.0是以去中心化组织为核心的区块链远景，试图在大规模协作领域帮助个人或组织协同工作，大约在2015年出现探索性应用。区块链技术的去信任特点，能够从根本上让组织形态减少摩擦并且提高效率，主要应

用包括去中心化域名系统、在线图片版权保护等。目前最有影响力的案例是DAO（Distributed Autonomous Organization），一个基于以太坊智能合约的公开的风险投资基金，任何人都可以使用以太币购买DAO带有表决权的股份，并对创业项目进行投票，DAO根据规则进行项目投资决策。DAO于2015年启动，用一年时间筹集了1.6亿美元，成为世界上最大的众筹项目，但目前因为底层代码存在漏洞已暂时中止。

从DAO的案例可以看出区块链3.0阶段具有以下基本特点。一是应用模式不明确。目前有关区块链3.0的应用，无论是去中心化域名系统还是去中心化公司，大多处在概念形成和验证阶段，没有成形的、经受过检验的解决方案。二是技术能力不成熟。从DAO的失败可以看出，使用区块链实现去中心化公司的业务复杂度高，技术难度大，现阶段尚不具备去中心化公司系统的设计和评估能力，暂不能开发高可靠、高可用的去中心化公司系统。

二　区块链技术实现

（一）技术架构

区块链技术利用点对点网络、密码学技术、共识机制等将集中式记账模式转化为各节点参与的分布式记账模式。其核心优势是不再需要一个传统的中心化机构，仅通过加密算法、共识机制、时间戳等技术手段，在分布式系统中实现了不依赖某个信用中心的点对点交易、协调与协作，从而为中心化机构普遍存在的数据安全、协同效率、风险控制等问题提供解决方案。区块链技术作为数字货币可选择的实现技术之一，在信用机制、系统架构、存储模式等方面具有一定的技术优势，但在网络安全、业务处理性能、交易一致性等方面存在一定不足。

区块链技术架构如图1所示，可分为物理层、数据层、网络层、共识层、应用层5个部分，其架构在数据层、网络层和共识层方面与传统技术架构具有明显差异，下面做重点分析。

图 1　区块链技术架构

1. 数据层

数据层利用密码学技术为区块链技术应用提供交易信息的分布式存储、完整性校验、可追溯性保障等数据服务，定义了区块、区块链等数据结构。

区块数据结构如图 2 所示，区块头利用 Merkle 根和时间戳保障区块信息的完整性和可追溯性；区块体存储区块生成时间内通过验证的所有交易单，并记录每个交易单的交易明细；交易单包括每笔交易的发起节点地址、交易金额、收款节点地址、交易时间、发起节点的数字签名等，并通过数字签名确保每个交易单的有效性和不可抵赖性。

区块链数据结构如图 3 所示，多个区块按照时间顺序以线性链表的形式链接起来形成区块链。每个区块的区块头存储前一区块头的哈希值，篡改某个区块的数据信息须修改其后所有区块的数据信息，能够有效保护整个区块链的数据完整性。

2. 网络层

网络层基于点对点网络结构和网络消息协议，为区块链技术应用提供基