doi:10.3772/j.issn.2095-915x.2019.06.002

区块链模型、技术与典型应用探究

刘硕[1] 胡泽文[2] 李玉平[3]

1. 南京大学信息管理学院 南京 210023；
2. 南京信息工程大学管理工程学院 南京 210044；
3. 南京天枢知识产权有限公司 南京 210004

开放科学（资源服务）标识码（OSID）

摘要：区块链是目前国际新兴前沿技术，涉及技术较多且应用领域广泛，需要进行全面解读。本文首先比较分析了五种区块链技术及其之间的异同，以及传统技术与区块链技术之间的差异。然后对国内外代表性区块链企业、区块链技术平台及其典型应用进行详细分析和比较，以期为国内外相关研究人员及从业者提供一定的指导。通过比较分析，我们发现：（1）区块链技术主要由区块结构、去中心化且开源的协议机制、加密解密算法、P2P 分布式网络、公有链和联盟链组成。（2）与传统技术相比，区块链技术的优势在于通过技术实现的去中心化交易机制，数学加密、共识和信任算法，实现数据不可篡改功能。（3）目前的区块链应用平台数量众多，广泛应用于社会公共事业、跨境支付、保险理赔、产品交易保障、金融和证券交易、贷款交易和管理、供应链管理、公益慈善、医疗、物流、商品溯源等领域。（4）世界顶级公司，如：高盛、微软、阿里巴巴、腾讯、百度和 360 等已经全面介入区块链技术，并针对不同场景设计和应用了区块链平台和产品。

关键词：区块链；联盟链；私有链；技术；应用；比特币

中图分类号：G358 P315.69

Investigation on Models, Technologies of Blockchain and its Typical Applications

LIU Shuo[1] HU Zewen[2] LI Yuping[3]

基金项目：国家自然科学基金青年项目“海量低被引论文的科学价值评估与预测研究”（71603128），江苏省自然科学基金青年项目“海量科技文献价值的负面评估指标及自动化评估模型研究”（BK20160974）。

作者简介：刘硕（1997-），硕士研究生，研究方向：科学计量与科技评价；胡泽文（1985-），博士，副教授，主要研究方向：科学计量与科技评价、数据挖掘与文档分类，E-mail: huzewen915@163.com；李玉平（1983-），专利代理师，主要研究方向：专利计量与评价、专利信息分析与预测。

doi:10.3772/j.issn.2095-915x.2019.06.002

1. School of Information Management, Nanjing University, Nanjing 210023, China;
2. School of Management and Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China;
3. Nanjing Tianshu Intellectual Property Co., Ltd, Nanjing 210004, China

Abstract: Blockchain is currently an emerging international frontier technology, involving many technologies and a wide range of applications, requiring comprehensive analysis and review. This paper first briefly compared the differences and similarities among the five blockchain technologies，as well as between traditional technologies and blockchain technologies. Then, we made a detailed analysis and comparison of representative companies, technology platforms for blockchain, and their typical applications at home and abroad, in order to provide some guidance for relevant researchers and practitioners. Through comparative analysis, we find that: (1) Blockchain technology is mainly composed of block structures, decentralized and open source protocol mechanisms, encryption and decryption algorithm, P2P distributed networks, and public chains. (2) Comparing with traditional technologies, the advantages of blockchain technology lie in the decentralized transaction mechanism implemented through technology, mathematical encryption, consensus and trust algorithms, and data non-mutability. (3) The current number of blockchain application platforms is widely used in social utilities, cross-border payments, insurance claims, product transaction protection, financial and securities transactions, loan transactions and management, supply chain management, charity, medical, Logistics, product traceability and other fields. (4) The world's top companies, such as Goldman Sachs, Microsoft, Alibaba, Tencent, Baidu, and 360, have fully intervened in blockchain technology and designed and applied blockchain platforms and products for different scenarios.

Key words: Blockchain; alliance chain; private chain; technology; applications; bitcoin

引言

互联网应用速度最快的是微信、QQ、Skype 等即时通讯领域，达到瞬时无延迟通讯。现代先进的科学技术：语音、视频通话、E-mail、图片以及即时消息等，使用户可以进行直接瞬时的通讯，即使通讯双方相距甚远，他们彼此之间仍然可以保持信任。然而涉及物品和金钱的交易领域，人们不得不借助于信任的第三方平台。区块链技术利用数学和密码学，实现“去中心化”的分布式记账，建立起安全性更高，成本更低、速度更快的信任机制和交易机制。目前区块链已经成为国内外新兴前沿技术领域，涉及技术较多且应用领域广泛。全球特许金融分析师 (CFA, Chartered Financial Analyst）协会自 2019 年起首次在 I 和 II 级 CFA 考试中加入数字货币和区块链科目。2018 年 6 月，工信部公示全国区块链和分布式记账技术标准化技术委员会筹建方案；7 月，中国三大运营商：中国移动、中国电信和中国联通联合成立可信区块链电信应用组织，同时，苏宁也发布《区域链白皮书》详细解读了区块链在零售、物流、科技、金融、文创和公共服务等领域的应用场景，为未来区块链技术可以服务的众多产业指明了发展路线。2018 年 8 月路透社报道，世界银行首次使用区块链技术发行和运营债券，以简化融资和交易。

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，在实现快速交易和构建信任机制方面具有先天独厚的优势，其中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。在交易领域，最常见的是交易合同的签订。例如：苏宁、京东、阿里巴巴、美的集团和格力电器等大型企业在产品生产、制造、采购和零售等供应链环节会涉及数量众多的参与者，交易过程中需要签订非常多的交易合同和实施大量的资金转帐。如果采用传统的合同签订方式，首先需要大量的合同文本，提升纸张成本和间接产生环境污染。然后合同签订者分布在不同国家和区域，合同的邮递、签订会耗费大量的邮费、旅费和时间成本。稍有延迟，可能错失重大的交易合同。然而融合区块链的智能交易系统能够实现纸质合同的电子化，电子合同的分布式实时签订和存储，合同签订的不可篡改和不可伪造。此外，区块链技术能够革新传统的超级帐本结构，实现超级帐本的分布式记帐和存储，任何节点帐本的丢失不会影响整体财务的安全性。

此外，比特币是区块链技术的典型应用，区块链技术起源于比特币系统的构建。因此从比特币的价格趋势可以看出区块链的发展趋势。2009 年比特币诞生，2010 年仅为 0.0025 美元，自 2016 年首次币发行（Initial Coin Offering，ICO），比特币价格开始启动飞速上涨模式，2017 年底涨到最高 2 万美元，与原始价格相比，上涨了近千万倍。此后回调到 2018 年 7 月时的 7000 美元左右。也正是 2017 年比特币价值达到顶峰之时，区块链技术开始兴起，并发展成为当前最具前沿和革命性的热点技术。2018 年 07 月，三星宣布：多国专卖店接受加密货币付款，包括比特币、ETH、XRP、LTC、Dash、NEM 等。此外，小米也发布新品：米路通平台和小米 WiFi 链，用区块链产品“米粒”对用户进行奖励。

1 区块链概念模型

1.1 区块链概念解析

2008 年，区块链作为构建比特币数据结构与交易信息加密传输的基础技术，在学者 Satoshi Nakamoto[1] 的《比特币：一种点对点电子现金系统》一文中首次被提出，行业内目前还未形成公认的区块链概念。在投资百科（Investopedia）中，区块链被定义为比特币交易赖以支撑的分布式公共帐本。国内学者袁勇，王飞跃 [2] 综合不同的区块链概念，从狭义和广义两个角度对区块链进行了定义。从狭义来讲，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，区块链是一种新型的分布式框架和计算范例，数据通过块、链接的数据结构、共识算法来生成，并记录和存储，建立基于加密的数据信任机制以及使用智能合约操作数据。区块链最显著的特点是去中心化，区块链利用分布式的系统结构，进行数据的记录、传递、存储和检验，通过公有账簿，实质性解决可复制性的问题，从而建立信任机制。此外，区块链还具有开放性、自治性、信息安全可靠、匿名性等特点。清华大学互联网金融实验室和新浪科技联合发布的《2014—2016 全球比特币

doi:10.3772/j.issn.2095-915x.2019.06.002

发展研究报告》提到区块链是比特币的底层技术和基础架构[3]，即本质上是一个去中心化的数据库，同时作为比特币的底层技术。区块链是一串通过密码学方法相关联产生的数据块，每一个数据块包含了一次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块[4]。

1.2 区块链研究进展

国外学者和机构最早提出区块链问题，对其研究已有近 10 年的历史，涌现了一大批理论成果，并将区块链技术应用到了金融、通信、供应链管理、域名管理、版权确认、公证、医疗、投票和物联网等领域。Michael Nofer（2017）等[5]在《Blockchain》一文中将区块链视为“一种颠覆性技术”，并对其应用和未来趋势进行了分析。美国约翰霍普金斯大学的 Polina Mamoshina（2018）等[6]探讨了区块链在生物医学研究和医疗保健方面的应用。国内学者和机构对区块链的研究虽然起步较晚，但近几年来发展迅猛，相关企业和研究机构积极投入区块链技术研发和应用推广，出现了一批具有较高理论价值的成果。2018 年 8 月 11 日以“区块链”作为关键词或标题词字段在中国知网期刊数据库中进行精确检索，发现 2003-2018 年期间国内学者发表了区块链方面的研究论文 3348 篇，其中 2003-2015 年期间仅发表 19 篇，2016 年开始呈爆发式增长，发表了 553 篇，2017 年 1269 篇。西安电子科技大学的沈鑫，裴庆祺和刘雪峰[7]分析了区块链技术的应用、监管和安全问题。谢辉和王健[8]基于技术层面研究了区块链的设计与实现，比较了区块链系统和传统的中心化系统在安全架构方面的异同。朱建明和付永贵（2017）[9]从区块链特点、技术、各国发展概况、发展阶段和创业团队等方面介绍了区块链领域的发展现状及进展。

目前，区块链经历了三个阶段的发展：第一阶段区块链技术的酝酿期（2009-2012），经济形态主要是比特币及其产业生态。第二阶段区块链技术的萌芽期（2012-2015），区块链开始受到人们关注，融合区块链技术的新钱包支付和汇款公司开始出现，区块链技术不断创新，并逐渐与比特币系统分离。第三阶段是自 2016 年以来的发展期，区块链的应用价值被全世界广泛关注。2016 年 10 月，我国首个官方区块链文件《中国区块链技术和应用发展白皮书 (2016)》发布。同年 12 月，区块链首次“亮相”《“十三五”国家信息化规划》。2017 年 1 月，由中国人民银行助力的数字票据交易区块链平台成功通过测试。同年 5 月，中国电子技术标准化研究院与微众银行、万向、蚂蚁金服等企业联合，推出了我国第一个区块链标准《区块链参考架构》。区块链创业公司不断涌现，BAT 等大型企业也相继设立了区块链研究机构，诞生了一系列区块链应用产品[10]。2018 年 7 月，国际标准组织、国际电工委员会和第一联合技术委员会正式通过了由中国主导提交的关于成立物联网与区块链融合研究组的提案，进行两者融合的标准化研究。这标志着我国区块链技术在新一代信息技术融合创新发展上能够引领全球发展。

1.3 区块链应用模型

韩国的 Lee（2018）等[11]提出利用区块链

技术为数字身份管理服务引入新的身份识别标识（ID，identification, identity），构建了一个区块链数字身份识别模型 BIDaaS（blockchain based ID as a Service）。该模型涉及三个实体：通讯公司（BIDaaS 提供者）、公司移动用户和公司合作伙伴，通讯公司将经过数字签名的用户虚拟 ID 和公钥等信息融入 BIDaaS 模型中，当用户向公司合作伙伴要求所需的服务时，公司合作伙伴无需亲自向用户确认身份信息，而是直接凭借用户的虚拟 ID，访问通讯公司的 BIDaaS 平台，用通讯公司提供的私钥来确认用户信息 [11]。新加坡南洋理工大学的 Khaqqi（2017）等 [12] 提出了基于区块链的新型排放交易计划（ETS，Emission Trading Scheme）模型，用于解决 ETS 的管理和欺诈问题，同时利用声誉系统提高 ETS 效能。模型通过区块链技术（Blockchain Technology）构建新型排放交易的声誉子系统 (Reputation System)，通过声誉子系统实现基于声誉的新型排放交易机制 (Trading Mechnism)。

中国科学院自动化研究所的袁勇和王飞跃（2016）[2] 通过解构区块链的核心要素，提出了区块链系统的基础架构模型，如图 1 所示。作者将区块链基础架构模型从下往上分为六个层次：数据层 -- 网络层 -- 共识层 -- 激励层 -- 合约层 -- 应用层。蔡维德等 [13] 在《基于区块链的应用系统开发方法研究》一文中从区块链的技术和应用层面出发，对区块链进行了分类，并提出了账户区块链（account blockchain，简称 ABC）和交易区块链（trading blockchain，简称 TBC）的双链设计模型，模型中交易区块链 TBC 的每位参与者都拥有自己的子账户，所有的子帐户组合成分布式的区块链总帐户。

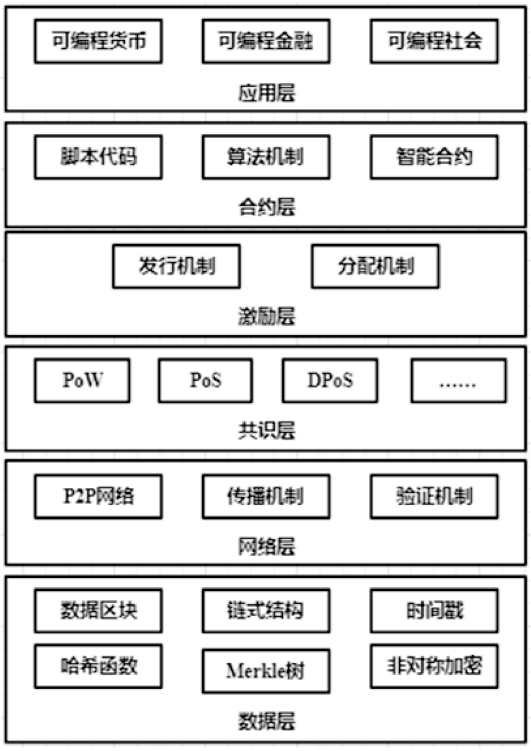


图 1 区块链基础架构模型

聂静（2017）[14] 设计构建了一款基于区块链技术的数字版权管理服务平台模型，模型涵盖六大层次，分别为：资源层、分析层、网络层、共识层、合约层和应用层。模型通过三条区块链：账户区块链、版权区块链和交易区块链将服务平台的各功能模块嵌入融合，实现基于不同区块链实现平台不同功能的区块链版权管理服务平台模型。平台模型中，账户区块链负责实现用户注册和钱包两个功能模块。版权区块链实现作品上传、版权登记、作品授权和内容审核四大功能模块。交易区块链实现渠道分销、付费欣赏、智能合约、数据统计和监控报警五大功能模块。郝世博和徐文哲（2018）[15] 从主体、客体、功能角度论述了区块链应用于科学数据共享的适用性，构建科学数据共享层

doi:10.3772/j.issn.2095-915x.2019.06.002

次化区块链架构模型。模型涵盖五大功能模块：机构内部的公有链、机构之间的联盟链、科研人员个体的公共链、数据共享区块结构和数据共享智能合约功能模块。然而作者并未将五大功能模块融为一体和互联互通。汪传雷和万一荻（2017）[16] 设计了一个基于区块链的供应链物流信息生态圈模型，模型设计了区块链与供应链物流信息资源管理在主体、交易机制和智能合约 3 个方面的耦合机制，其中区块链与信息资源管理主体之间的耦合机制涵盖：多主题协同、权利与业务对等、信息交换和保存等方面的耦合机制；区块链与供应链物流信息资源管理的交易机制耦合，主要针对供应链各主体间存在多重复杂交易，引入区块链系统的去中心化信任机制和分布式节点链式结构，在供应链的各交易环节实现真实记录和验证交易并减少或消除主体间因缺乏信任导致的机会成本；智能合约耦合方面，供应链通过一系列基于区块链的智能合约保证交易的自动执行，避免不可控因素恶意干扰合约的正常执行，同时具有成本效率优势。

2 区块链相关技术

区块数据结构、智能合约、分布式体系结构、加密解密、P2P 分布式网络、公有链和联盟链是区块链应用的核心技术。不同技术协同实现区块链交易应用的基本原理如图 2 所示。

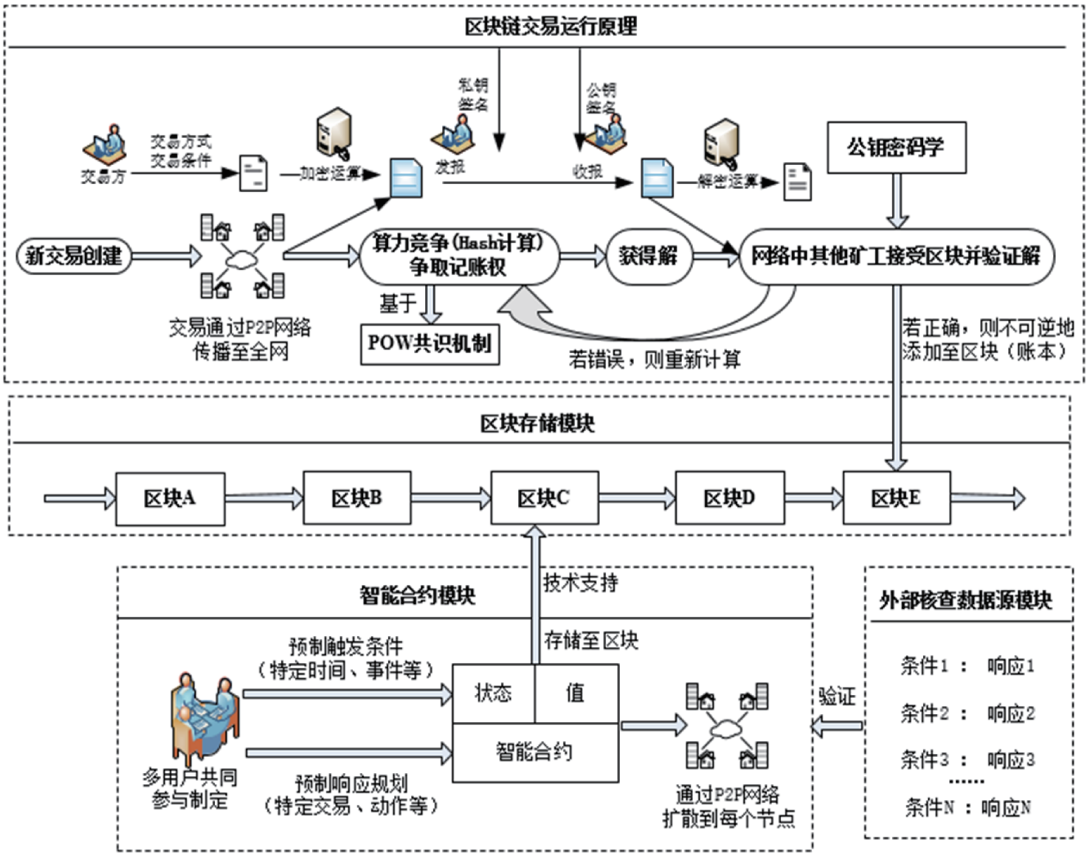


图 2 区块链交易应用的基本原理

从图 2 可以看出，区块链交易应用开始于新交易创建，即交易双方创建新的交易，并通过 P2P 网络传播至全网。网络中各节点基于工作量证明（Proof of Work，简称 POW）共识机制，通过算力竞争获得记账权，率先获得结果的节点向全网广播，网络中的其他矿工接受并验证该结果的正确性，若正确，则不可逆地添加至自己的区块（账本）；若错误，则重新进行计算。区块链系统中的信息分区块链状存储，每个区块包含一部分交易记录。智能合约为交易过程中合同签订和交易业务的自动完成提供技术和信用支撑。POW 共识机制通过引入分布式节点的算力竞争来保证数据一致性和共识的安全性。在区块链系统中，各参与方借助自己的计算机节点处理能力或算力互相竞争去共同解决一个求解复杂但验证容易的 SHA256 数学难题（即挖矿），最快解决该难题的节点将获得区块记账权和系统自动生成的比特币奖励。SHA256 就是哈希函数，又称散列算法，是一种从任何一种数据中创建更小单元的数字“指纹”方法。该函数将数据打乱混合，重新创建一个叫做散列值（或哈希值）的指纹。对于任意长度的消息，SHA256 都会产生一个 256bit 长的哈希值，称作消息摘要。

2.1 智能合约

智能合约是密码学家 Szabo Nick[17] 在 1994 年首次提出，认为智能合约是承诺或事务的数字化定义，以及支撑合约参与方自动执行这些承诺或事务的协议。智能合约定义了交易逻辑及访问状态数据的业务规则，由系统中的多用户共同参与制定，通过预制触发条件（特定时间和事件等），以及每个触发条件所引发的响应（特定交易和动作等），形成达成一致的智能合约，然后由 P2P 网络传播至全网，并存储在区块链中。外部核查数据源或应用（如以太坊中的去中心化应用）会定期对智能合约进行状态检查，验证满足已制定条件的事务并自动依照合约执行交易和访问状态数据等响应动作，完成后通知用户。外部应用与智能合约间的关系非常类似于传统数据库应用与存储过程间的关系，存储过程运行于数据库管理系统之中，访问关系数据库数据。而智能合约运行于区块链系统之中，访问区块和状态数据。Jesse 和 Deokyoon 等 [18] 学者将智能合约界定为利用区块链技术为多个合约参与方之间自动创建协议的实现方案。区块链的分布式处理和信任机制为智能合约实现提供了诚信环境，一旦合约条件触发，合约条款就会被区块链平台自动执行。

2.2 区块链数据结构

区块链数据结构由区块头部和区块体构成，在区块链中，数据通过电子记录的方式被保存下来。区块是用来存储这些电子记录的文件。某一时间段内的所有交易数据均由该时间段内创建的区块进行记录，下一时间段将产生下一个区块用于数据的记录，整个过程不断重复。区块链数据结构的块头主要用来与前面的区块进行链接，并保证区块链数据库的完整性。块体则用来存储该区块中的所有数据记录。区块结构具有两个重要属性：其一，在特定时间段内创建的区块会在此期间记录所有交易数据和信息，以确保系统数据库中的数据是完整的。其二，通常情况下，一旦某个区块完成记录被

doi:10.3772/j.issn.2095-915x.2019.06.002

放到区块链的最后，该区块中已经存在的数据记录将永远无法被篡改或删除，以确保系统数据库是严谨的。各个区块以链的方式进行组合，形成区块链，进而形成区块链数据库，被系统内的所有节点共享。时间戳由区块和链组成，交易数据在被记录的同时，也会被盖上时间戳，以确保永远不会被改变和删除。时间戳记录了区块中每一次活动的时间，可以有力地证明某件事发生的时间、某个想法的提出者、某个专利的所有者、某份合同的签订者等。因为时间戳和数据记录的存在，证明将会变得非常简单[19]。邵奇峰等学者（2018）[20]详细介绍了两种比特币区块链的哈希结构和区块链表，涵盖前块哈希（PrevBlockHash）、随机数（Nonce）交易 Merkle 根等。PrevBlockHash 存放前一区块的块哈希，所有区块按照生成顺序以 PrevBlockHash 为哈希指针链接在一起，就形成了一条区块链表。区块头包含交易 Merkle 根，所以通过块哈希可以验证区块头部和区块中的交易数据是否被篡改。同时作者也介绍了基于交易的区块链模型和基于帐户的区块链模型。

2.3 分布式体系结构

与目前已有的中心化系统不同，区块链系统属于分布式体系结构，系统中的每一个节点都将会记录并存储系统运行过程中涉及的所有数据。区块链系统的开源协议机制确保了系统中的数据是可信的，各节点在记录数据之前，系统中的其他节点会对数据进行检验，只有半数以上的节点认为数据可信，该数据才能通过检验并被记录。区块链根据其去中心化且开源的协议机制，建立起一个所有参与者共同参与数据生成和记录的分布式体系结构，利用分布式记录将记录责任分散开来，并确定每一笔交易记录的内容和时间。记录结束后，再利用区块链系统的分布式网络结构将记录的数据传输给系统中的其他节点。去中心化的分布式体系结构能够保证系统中的所有数据都能够实时更新并且被记录下来，从而使得信息安全可靠，除非系统中的所有节点同时被损坏或崩溃，该系统就可以一直安全稳定运行下去[19]。

2.4 加密解密

区块数据可信和使用问题是区块链应用的一个核心问题，解决该问题的关键是密码学中的加密解密算法。区块链借助密码学中的加密解密算法来构建共识机制，通过非对称加密数学算法提高区块数据交易的可信度和安全性。用于加密的密码被称为“公钥”，全网公开，任何人都可以利用公钥加密信息，从而保证了信息的真实性。用于解密的密码被称为“私钥”，私钥不公开，属于信息的所有者，加密过后的信息只有通过相应的私钥才能进行解密，从而保证了信息的安全性。在区块链中，所有的规则都是借助于数学加密解密算法进行表述的，在进行交易时，人们不需要确定交易的另一方是否可信任，也不需要借助第三方交易机构，彼此之间的信任来自于可靠的数学加密解密算法。安瑞和何德彪等（2017）[21]充分利用区块链技术的去中心化、开放、自治、匿名和不可篡改等特性，以及集密码学加密解密算法、安全防伪、存储量大和使用方便等特性于一身的 IC 卡芯片，设计和实现了一款基于区块链技术的防伪系统，实现防伪证书发行和防伪证书验

证两大功能。

2.5 可编程的脚本

区块链去中心化的特性使得系统无法直接设定完成所有价值交易所需要满足的条件，所有的协议都需要提前获得众多参与者的共识，因此会耗费系统大量的资源，延长完成时间。然而借助于可编程的脚本，系统可以自动获取参与者共识信息，并处理某些人们无法预料的交易模式，从而使得区块链技术更加具有实用性，并能够与时俱进。脚本就是一系列计算机指令的组合，每次进行价值交易时，脚本程序会自动记录价值接收方获取价值的方式（交易方式），以及价值交易需要满足的条件（交易条件）。通常情况下，价值接收方在使用交易机制获取到价值之前，需要向脚本提供相应的公钥和签名（用来证明价值接收方拥有与该公钥相对应的私钥）。脚本的可编程性使得价值交易活动更具灵活性，脚本可以灵活地改变交易的条件，也可以在交易时附加一些价值再转移的条件。基于加密解密算法脚本的区块链交易机制如图 3 所示。

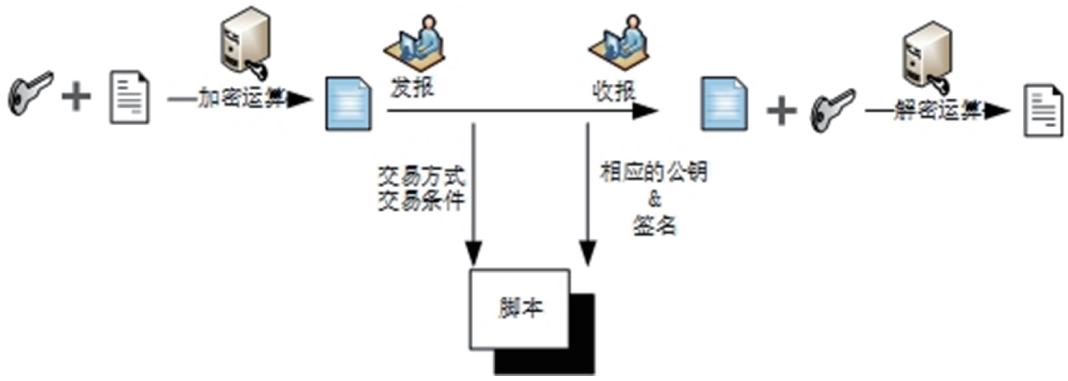


图 3 基于加密解密算法脚本的区块链交易机制

2.6 P2P分布式网络

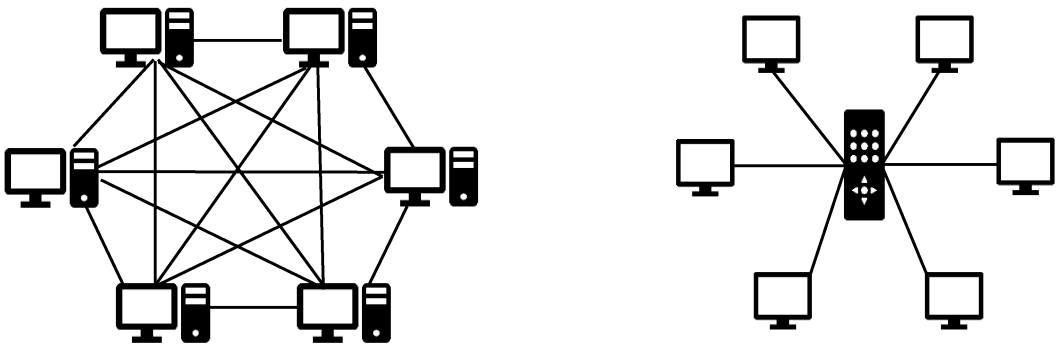
P2P 分布式网络是一种对等计算机网络。在 P2P 网络中，所有彼此相连的计算机都处于对等的地位。一台计算机既可以作为服务器，为网络中的其他计算机提供资源和服务，也可以作为工作站，网络中不存在中心化的服务器，突破了传统的客户端 / 服务器（Client/Server，C/S) 模式。P2P 分布式网络具有去中心化、可扩充（节点数扩大的同时，系统性能随之扩充）、鲁棒性、擅长隐私保护等特点。P2P 网络模式与传统的中心化网络模式对比，如图 4 所示。

2.7 公有链和联盟链

公有链是任何组织或个人都可以加入、交易和获取信息的公共区块链，公有链的参与门槛很低，且系统中所有交易信息透明公开，网络中的各节点在进行交易时无需向另一方提供个人信息，个人隐私不会被泄露。典型的公有链有比特币、量子链、以太坊等。而联盟链是部分去中心化的区块链应用，由若干企业或者机构组成联盟，共同管理区块链网络平台。联盟链不允许随意加入，加入的节点必须获得联盟中各成员的一致同意。

doi:10.3772/j.issn.2095-915x.2019.06.002

每个企业或机构负责和运行某个或某些节点，且共同记录系统中的交易信息，各企业或机构被认为是可信的。典型的联盟链有中国区块链研究联盟、金联盟，以及开源超级账本(Hyperledger) 区块链的 Fabric 联盟链等。苏宁区块链平台可支持联盟链和私链业务，支持苏宁黑名单、信用证、商品溯源、积分应用等区块链应用场景。苏宁区块链黑名单共享平台系统，就是在 Fabric 联盟链基础上实现了加密算法，主要包括添加、查询、删除黑名单及投诉四大功能。具体而言，金融机构将本机构产生的黑名单数据作为一个交易发布到区块链上，发布即可获得积分，用于查询其他机构发布的黑名单数据。设置投诉服务，当发现的黑名单数据造假时，查询机构可在系统中追诉数据提供方。



（a）P2P 网络模式　　（b）传统的中心化网络模式

图 4 P2P 网络模式与传统的中心化网络模式对比图

3 区块链技术系统与传统技术系统的比较

区块链技术的核心在于数据由系统各方共同记录、存储和维护，且数据一旦被写入，则无法篡改。区块链技术与传统交易技术之间存在较大差异，为此，本文从网络架构、数据记录方式、交易方式、信任方式、交易一致性、交易诚信、数据安全性、用户隐私 8 个方面对传统技术系统与区块链技术系统进行比较与分析，如表 1 所示[22]。

表 1 传统技术系统与区块链技术系统比较分析结果

系统分类	传统技术系统	区块链技术系统
网络架构	中心化，主从式的 B/S 网络	去中心化，P2P 分布式网络
数据记录方式	由中心节点进行记录	基于共识算法，所有节点共同参与
交易方式	中心节点监督、确认	所有节点共同监督、确认
信任方式	彼此信任来自于中心节点	彼此信任来自于可靠的数学算法
交易一致性	由中心节点账本保障	所有节点通过共识算法保障
交易诚信	存在欺诈和造假的可能	不存在欺诈和造假
数据安全性	数据可能被篡改、销毁	数据不可篡改、部分节点故障对数据安全没有影响
用户隐私	存在隐私被盗取泄露的可能	用户 ID 加密，隐私不会被泄露

从表 1 可以看出，区块链技术系统完全不同于传统技术系统，主要表现在以下几点：

（1）网络架构。传统的技术系统基于主从式的 B/S 网络，存在中心化的第三方平台；区块链系统中不存在中心化的第三方平台，网络结构是分布式的，交易数据由所有节点进行确认和记录，更加安全可靠。

（2）数据记录方式。传统技术系统由中心节点进行数据的记录和保存，中心节点具有绝对的权威；区块链技术系统基于共识算法确定记录权，所有节点共同参与数据的记录，记录权被分散和下放。

（3）交易方式。在传统的交易中，每笔交易都要由中心节点参与，并由中心节点进行监督，确认交易的有效性；在区块链技术系统中，交易通过点对点的方式进行，交易的有效性由所有节点集体监督，共同确认。

（4）信任方式。中心节点为传统技术系统中的所有节点进行信任背书，用户通过中心节点判断交易的另一方是否可信；区块链系统采用去中心化的信任机制，交易双方不需要向另一方公开自己的身份信息，也不需要了解对方的真实信息，彼此之间的信任和交易的有效性依赖于数学算法。

（5）交易一致性。传统的技术系统借助中心节点保证交易的一致性，每一笔交易都将由中心节点记账；区块链系统中的交易数据由所有节点共同记录和存储，基于分布式的网络结构确保交易信息一致。

（6）交易诚信。传统技术系统中，存在中心节点主动欺诈和造假的可能；区块链技术系统基于分布式存储和共识算法，不依赖于某个节点，不存在欺诈和造假的可能性，交易更加诚信化，透明化。

（7）数据安全性。在传统技术系统中，一旦中心节点和容灾备份被攻击毁坏，系统中的数据将面临着被泄露、篡改、删除的命运；区块链技术系统基于分布式存储、链式数据结构、时间戳和数字签名，除非系统中的所有节点同时被损坏或崩溃，该系统就可以一直运行下去。

（8）用户隐私。传统技术系统中的用户个人隐私信息由中心节点负责记录和保存，一旦中心节点出现故障，用户隐私将受到威胁；在区块链技术系统中，所有用户通过加密后的 ID（identification, identity）进行身份标识区分，交易时不再需要所有交易者提供身份隐私信息，同一个交易者也可以通过多个 ID 进行的多次交易来保障隐私信息不被泄露。

4 区块链应用

在区块链技术应用方面，软件公司甲骨文（Oracle）2018 年 7 月 16 日正式推出其区块链平台，运用分布式记账法，使用户能够通过区块链数据监控供应链，追踪全球运输系统，实现跨境交付。Satoshi Nakamoto 在他的文章《比特币：一种点对点电子现金系统》中设想使用密码学来建立一个脱离传统第三方平台的新型电子支付系统。2009 年 1 月 3 日，世界上首枚比特币问世，标志着基于分布式架构、去中心化的新货币体系的到来。2009 年 1 月 12 日，Satoshi Nakamoto 向密码学家 Halfinney 发送了 10 个比特币。2010 年 7 月，Jed McCaled 在日

doi:10.3772/j.issn.2095-915x.2019.06.002

本东京创立 Mt.Gox 比特币交易所，比特币被人类认可和使用。2017 年，区块链和相关行业发展迅速，越来越多的国家开始不断探索区块链技术及其应用。目前，区块链技术的应用主要涉及金融、物联网、供应链、公益和公共服务等领域。具体应用如图 5 所示。

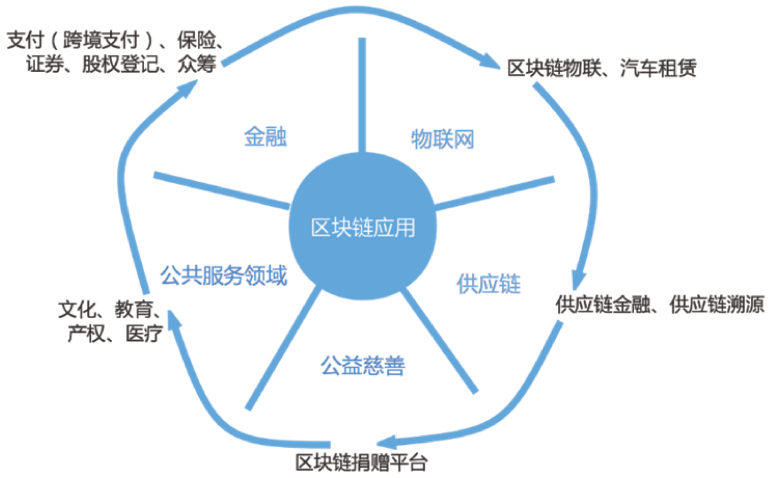


图 5 区块链应用现状

目前已有的区块链应用大致可以分为三类：数字货币、区块链技术应用平台以及区块链代表性企业，下面对这三类应用分别展开叙述并对比分析不同类型应用之间的差异。

4.1 数字货币

数字货币（Digital currency）是电子货币形式的替代货币。部分政府的中央银行表示要发行数字货币，但政府发行的数字货币，与企业和非货币发行机构发行的数字货币不同，一定要有基准货币和中央银行，以保证数字货币的权威。数字货币不同于虚拟世界中的虚拟货币，因为它能被用于真实的商品和服务交易，而不局限在网络游戏中。早期的数字货币（数字黄金货币）是一种以黄金重量命名的电子货币形式。现在的虚拟数字货币 -- 比特币、莱特币、Eco 和 PPCoin 都是依靠校验和密码技术来创建、发行和流通的电子货币。其特点是运用 P2P（peer-to-peer）对等网络技术来发行、管理和流通数字货币，理论上避免了官僚机构的审批，让每个企业和个体都有权发行虚拟数字货币。

（1）比特币（BitCoin）是一种去中心化的虚拟数字货币，它基于一套密码编码和数学算法而非货币发行机构产生，可以通过任意一台接入互联网的计算机实现在全球范围内的流通，任何人都可以挖掘、购买、出售或收取比特币。利用比特币进行交易时，P2P 网络中的其他节点负责交易的确认和交易信息的记录。其设计中蕴含的数学算法和密码学保证了比特币的安全机制和信任机制。由于比特币由数学算法产生，所以其数量非常有限，总数不超过 2100 万，是稀缺物品，很难成为大众意义上的数字货币。由于比特币的匿名性和稀缺性，成为网络勒索、洗钱、非法交易、逃避外汇管制等的工具。

（2）莱特币（Litecoin）基于比特币，也是一种虚拟的点对点货币。莱特币基于 Scrypt 加密算法，不受任何中央机构的限制或管理。相对于比特币，莱特币可以执行更快速更高效的交易处理和确认。预计将产生 8400 万个 Litecoin，是比特币数量的四倍。

（3）Eco 是 Uber 联合创始人 Garret Camp 发行的个人数字加密货币。Eco 仅使用经过验证的节点来提供网络支持和交易确认，匿名商户无法通过网络上的未知节点进行交易。Eco 将发行大量虚拟货币（初始阶段至少有 1 万亿），Eco 具备非常简单的网络和移动应用操作平台，可提高用户体验。Eco 将开发更多节能系统并减少生产和贸易过程中的能源消耗 [23]。

（4）莱茨狗是百度设计和实现的一款区块链养狗游戏项目，提供形态各异的虚拟宠物狗供领养。“莱茨狗”类似于英语“Let’s go”，百度根据不同的属性将莱茨狗分为若干个等级。每只狗都有自己独一无二的基因属性，这些属性是根据其体型、眼睛、嘴巴和身体颜色等因素确定的。目前，莱茨狗已实现繁殖功能，用户可以繁殖莱茨狗并将其出售给其他用户 [24]。

本文从发行时间、是否活跃、市值、加密算法、单个块处理时间和最大虚拟货币发行量 6 个方面对比分析了比特币、莱特币和 Eco 的异同，分析结果如表 2 所示。

表 2 三种虚拟数字货币的比较结果

虚拟数字货币	发行时间	是否活跃	2018.8.14 市值	加密算法	单个块处理时间	2018.8.14 发行量	最大发行量
比特币	2009 年	是	~ $1048 亿美元	SHA-256	10 分钟	1721 万	2100 万
莱特币	2011 年	是	~$30 亿美元	Scrypt	2.5 分钟	5784 万	8400 万
Eco	2018 年	是	~$9.9 万美元	Https	无	117 万	1 万亿

从表 2 可以看出，比特币是发行时间最早的虚拟数字货币，而 Eco 是 2018 年最新发行的虚拟数字货币。截止到 2018 年 8 月 14 日，比特币的市值最大，达到 1048 亿美元，而最新发行的 Eco 币市值最小，为 9.9 万美元。在 2018 年 8 月 14 日的虚拟数字货币发行量方面，Eco 币目前的发行数量最多，达到 117 万，但仍离 1 万亿的最大发行量遥不可及。比特币目前的发行数量最少，为 1721 万枚，离最大发行量 2100 万枚仅差 379 万枚。三种不同比特币采用的加密算法各不相同，比特币采用 SHA-256 加密算法，莱特币采用 Scrypt 加密算法，而 Eco 币采用 Https 加密算法。

4.2 区块链技术应用平台

区块链技术应用平台是国内外各区块链企业在研究区块链技术的基础上推出的区块链应用探索产品，涉及教育、房地产、医疗档案管理、公益、供应链、证券投资等多个领域。其特点是将区块链技术引入传统行业领域，借助区块链去中心化的特点和优势，改进传统业务的处理方式和信用机制。目前典型的区块链应用：

（1）以太坊（Ethereum）。以太坊（Ethereum）是一个基于智能合约（Smart Contract）的公共区块链平台。由于比特币存在扩展性不足的问题，程序员 Vitalik Buterin 在 2013 年首次提出了以太坊的概念，其核心是合约，可以提供几

doi:10.3772/j.issn.2095-915x.2019.06.002

乎所有的业务，且技术开源，协议简洁。以太坊在区块链的基础上向前迈进了一大步，实现了从分布式的数据库到分布式的计算机的转变。智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议，允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。智能合约概念于 1994 年由 Nick Szabo 首次提出。智能合约可以提供优于传统合约的安全方法，并减少与合约相关的其他交易成本。国内上市企业易见股份联合 IBM 中国研究院推出易见区块（http://www.easy-sight.com/）便是基于智能合约供应链管理系统，该系统基于区块链分布式和信用机制能够实现供应链各参与方合同协议的线上签订和资金自动转帐交易。

（2）Visa B2B Connect。Visa B2B Connect 是一个基于区块链的 B2B 支付平台，由国际银行卡组织 Visa 和区块链公司 Chain 联合推出，该平台使用链式核心技术记录私人区块链网络中的金融交易。Visa B2B Connect 平台为全球金融机构提供安全快捷的 B2B 支付服务，帮助他们处理实时支付，提高效率并降低成本，并通过 Visa B2B Connect 平台实现跨境支付交易。该平台自 2017 年起开始运作 [25]。

（3）LenderBot。LenderBot 是 2016 年由巴黎区块链应用企业 Stratumn，德勤和支付服务提供商 Lemonway 联合推出的一项微型保险平台，为资产交易提供保险服务。该平台允许用户通过 Facebook、Messenger 等社交媒体注册量身定制的小额保险产品，当用户在平台上进行物品交易时，LenderBot 能够在无需第三方参与的情况下提供工具来创建可信任的工作流程 -- 比特币区块链，对双方之间的交易进行保险。通过在流程中添加签名信息，用户可以从区块链中获得带时间戳和加密元素的链接，从而保证链接无法更改。由于比特币区块链的开放性，这个概念也提供了更好的透明度。通过在区块链中使用加密和时间戳数据来确保传输的信任性，同时也确保了交易的真实性和安全性，以及隐私和保险合同签名过程中每个步骤的可追溯性 [26]。

（4）Linq。Linq 平台是纳斯达克在 2016 年 1 月与区块链公司 Chain Chain 合作推出的一个私募股权交易平台，该平台使用了区块链技术来管理发行上市前公司的股份，致力于以全新的方式推动私募股权转让和销售。Linq 平台为私募股权发行人提供数字化所有权，同时缩短结算时间，降低资本成本并降低系统性风险。传统销售和材料采购所需的审批流程进一步简化，提高了交易和管理的效率。交易方的身份和交易量等信息实时记录在区块链中，有助于提高发行人的决策效率。开放，透明和可追踪的系统有利于证券发行人和监管机构的市场维护，并减少黑箱和内幕交易的发生 [27]。

（5）ADEPT。ADEPT（Autonomous Decentralized Peer-to-Peer Telemetry）物联网系统是由 IBM 和三星联合开发的区块链分布式物联网。该系统基于三个协议：区块链，BitTorrent（文件共享）和 TeleHash（P2P 消息系统），它允许各种物联网设备自动运行以提供最佳的交易安全性保护。理论上，该系统可以在家电出现故障时自动发送信号，并自动更新软件。设备本身也可以使用 ADEPT 与外设进行通信以提高能源效率。当数十亿设备自动在 ADEPT 系统中交换信息时，Blockchain 分布式账本将发挥

作用。通过在系统中嵌入区块链协议，ADEPT 系统作为设备之间桥梁的成本可以显著降低[28]。

（6）区块链租车项目。区块链租车项目由 Visa 与数字商务管理公司 DocuSign 于 2015 年 10 月合作推出的平台，通过区块链和智能合约进行汽车租赁交易。使用区块链技术来收集和存储租赁数据并促进租赁过程的数字化。该项目利用区块链为客户设立数字指纹，将其注册到链中，并使用分布式总账记录，实时更新租赁和保险项目内容，从而简化传统汽车租赁流程中繁琐的步骤[29]。

（7）Ujo Music。Ujo Music 平台是基于区块链构建的音乐版权管理平台模式，歌曲的创作者和消费者之间可以建立直接连接，在保护创作者版权的同时，也节省了中介费用和盗版现象[30]。

（8）BitProof 区块链认证。BitProof 是一家基于区块链技术进行文件认证的创业公司，与加州软件工程学校 Holberton School 合作，基于区块链技术向学生颁发学历证书，以验证学历系统的真实性。同时，通过区块链资格认证系统，当企业招聘人员进行学生背景调查时，在线区块链系统可以快速获得关于学生教育和完成证书的信息，从而降低学历欺诈风险[31]。

（9）文件安全区块链平台。平台由美国房地产区块链公司 Ubitquity 开发，用于确保房地产行业交易过程中文件和信息的安全和可追溯性。平台通过区块链技术在房地产交易过程中创建和记录当前和未来的所有文件和相关事件，公众可以访问平台上不可更改的记录。这使得房产所有权的转让更加便捷。从具体操作的角度来看，应用区块链专有权保护技术可以缩短产权搜索时间，实现所有权信息的交换，避免房地产交易过程中的欺诈行为，提高房地产交易运营效率[32]。

（10）Guardtime。Guardtime 是由数据安全初创公司 Guardtime 和爱沙尼亚电子卫生保健基金会联合发起的医疗记录管理项目。该项目使用区块链技术确保患者记录的安全，防止敏感数据被非法操纵、删除和错误更新。区块链技术可以保证数据的完整性，全面记录数据修改过程，实现对病历和档案的实时性保护[33]。

（11）GiveTrack。GiveTrack 是由非营利慈善组织 BitGive 开发团队开发的捐赠平台，致力于利用比特币和相关技术开展慈善和人道主义项目，以推动慈善事业的发展。2015 年，BitGive 宣布了慈善 2.0 计划，并使用区块链技术创建了一个开放透明的捐赠平台，旨在让捐赠者和公众能够充分利用区块链技术进行捐赠。GiveTrack 平台通过启用资金转账和追踪解决方案，为非营利性融资提供了极大的透明度。 此外，它将永久保存所有交易记录，包括资金来源和资金使用方面的信息，可以防止捐赠资金的非法使用[34]。

（12）供应链追溯服务。伦敦区块链公司 Provenance 为企业提供供应链追溯服务，通过记录零售链中的所有流程信息来捕获和追踪产品材料，追溯商品的来源和去向，提高整个供应链的可视性和真实性。Provenance 的区块链平台将所有信息集成到整个产品制造，运输和交易过程中，重建供应链中的信用系统，并促进系统的稳固发展[35]。

（13）共享云计划。该计划是 360 发布的基于区块链的安全共享云平台，平台将闲置的

doi:10.3772/j.issn.2095-915x.2019.06.002

带宽资源，计算资源和磁盘空间，利用 360 共享云平台供给有需要的人使用。用户可以通过贡献带宽流量和内存空间获得 360 云钻奖励 [36]。

（14）万云区块链云平台。该平台由中国万向控股有限公司于 2017 年推出的一站式区块链云平台，是国内第一个中立区块链应用平台。万云区块链云平台结合了区块链和云计算技术，深化区块链的底层技术服务，为相关企业和个人提供专业化更高、灵活性更好的区块链服务 [37]。

从推出时间、相关企业和应用领域 3 个方面对上述十四个区块链技术应用平台进行分析与比较。具体比较结果如表 3 所示。

表 3 区块链技术应用平台的比较结果

应用平台	推出时间	相关企业	应用领域	应用平台	推出时间	相关企业	应用领域
以太坊	2013 年	程序员 Vitalik Buterin（个人）	公共	BitProof	2015 年	BitProof	教育
Visa B2B Connect	2017 年	国际银行卡组织 Visa 与区块链公司 Chain	跨境支付	文件安全存储区块链平台	2016 年	Ubitquity	房地产
LenderBot	2016 年	Stratumn、德勤（Deloitte）与支付服务商 Lemonway	保险理赔；产品交易保障	Guardtime	2015 年	数据安全初创企业 Guardtime、爱沙尼亚电子卫生基金会	医疗档案管理
Linq	2016 年	纳斯达克、区块链企业 Chain	证券交易	GiveTrack	2015 年	BitGive	公益
ADEPT 物联网	2015 年	IBM、三星	物联网	Provenance	2013 年	Provenance	供应链
汽车租赁	2015 年	Visa 、数字交易管理公司 DocuSign	租车	共享云计划	2018 年	360	资源共享
Ujo Music	2015 年	Ujo Music	文化	万云区块链云平台	2017 年	中国万向控股有限公司	存证公示、版权服务、信息认证、投票、抽奖等

表 3 显示，不同区块链技术应用平台的创建者有企业、个人、机构和证券交易所，创建时间在 2013-2018 年期间，其中 2015 年创建的区块链技术应用平台最多，达到 6 家，涉及的应用领域非常广泛，涵盖：公共、跨境支付、保险理赔、产品交易保障、证券交易、物联网、租车、文化、教育、房地产、医疗档案管理、公益、供应链、资源共享、存证公示、版权服务、信息认证、投票和抽奖等。

4.3 区块链代表性企业

区块链技术与应用在北美、欧洲和亚洲等全球主要市场逐渐受到重视。与此同时，自 2015 年底，中国真正出现了区块链领域的创新创业，目前国内已经有近百家与区块链技术相关的公司，出现了许多代表性的企业。国内外代表性企业的类型，区块链业务的优势、特点、案例及方案的比较结果如表 4 所示 [22]。

表 4 国内外区块链代表企业的比较结果

	类型	代表企业	优势 / 特点	案例 / 方案
国外	初创公司或组织	R3 CEV	以搭建底层技术协议为主	公布源代码的 Corda 分布式账本
	金融机构	高盛	以解决金融机构现有应用场景需求、降低交易成本为主	银行间清算、外汇交易等
	大型科技公司	微软	将原有技术能力（如云服务）延伸至区块链领域	基于 Azure 云服务，发展莱切利（Bletchley）项目支持不同区块链联盟组建
	系统集成商 /IT 咨询公司	德勤	结合系统集成能力与区块链技术服务企业客户	基于以太坊协议的 Rubix 项目，例如：区块链智能身份识别与确认项目
国内	初创公司或组织	万向区块链实验室	搭建开源的技术研究生态及投资孵化生态	基于以太坊的基础设施
	Fintech	微众银行	搭建区块链底层服务	清算、票据
	大型科技公司	腾讯	将原有技术能力（如云服务）延伸至区块链领域	腾讯金融云 + 区块链解决方案。用于票据、资产登记及交易等场景

从表 4 可以看出，国内外区块链代表性企业涵盖企业创新创业不同阶段的不同类型企业：初创公司、大型科技和金融公司、系统集成商和 IT 咨询公司。企业发展区块链技术应用的优势各不相同。初创企业注重构建底层技术协议和搭建开源技术研究生态；大型科技和金融公司注重使用区块链技术变革原有的技术生态。目前国内外大型科技和金融公司的区块链技术发展和应用进展主要表现为：

（1）高盛（Goldman Sachs）在 2016 年发布了区块链报告 *Block chain: Putting Theory into Practice*，报告探索了包括旅游业、能源、房地产和金融在内的广泛市场具体应用情景，分析了区块链功能适用的现有业务问题以及区块链将如何做出改变。继 2015 年投资了比特币服务商 Circle 之后，高盛于 2016 年再次投资了纽约区块链创业公司 Digital Asset Holdings，高盛区块链致力于解决金融领域区块链应用问题，旨在降低金融业务运营成本 [38-39]。

（2）微软区块链基于 Azure 云计算平台，自 2014 年加入比特币市场以来，一直与众多的区块链初创公司合作，并于 2016 年推出了微软 BaaS 平台，该平台旨在为区块链开发人员提供方便易用的开发测试环境，可以支持 26 种不同类型的区块链测试实现。在进行产品开发的同时，微软积极地与 Bitpay、MultiChain 和 Storj 等区块链初创公司合作，组建区块链联盟 [40]。

（3）阿里巴巴是目前国内区块链发展势能第一的企业，在 2018 年 2 月发布的《2017 全球区块链企业专利排行榜》中，中国企业占据了前 100 名中的 49 个席位，美国以 33 个位居第二，国内阿里巴巴专利总量 49 占据榜首。2015 年，阿里旗下的蚂蚁金融集团成立了区块链兴趣小组，并于 2016 年开始尝试慈善项目。到目前为止，阿里依靠其在电子商务和新零售方面的优势，不断推进其在公共物品、产品可追溯性和租赁住宿等领域的区块链布局。2017 年 3 月，区块链技术入驻支付宝捐赠平台，所有捐赠的来源和去向可追溯；2018 年 2 月，淘宝物流引入区块链技术，跨境进口货物均标有

doi:10.3772/j.issn.2095-915x.2019.06.002

“身份证”，以供消费者验证[41]。

（4）腾讯区块链基于底层技术，依靠其社交优势，在奠定技术基础的同时探索价值场景落地。2017 年 4 月，腾讯发布旨在构建区块链生态体系的区块链方案白皮书和区块链行业解决方案。腾讯区块链基于可信赖的交易连接，借助可视化的数据管理方法，提供“高质量、高性能”的区块链产品及服务。其区块链技术涉及贷款清算/审核、数字资产、物联网、供应链、保险等诸多领域[22]。

（5）Qtum 量子链公司是第一个基于股权认证的智能合约平台，旨在探索区块链技术的创新，并因其安全性，可扩展性和商业可用性而获得认可。 Qtum 量子链公司与多家国内外机构紧密合作，在区块链技术方面积累了丰富的研发经验，量子链本身也获得全球认可。目前在 Quantum Chain 平台上构建了超过 50 个多域项目，全球范围内拥有近 300 万社区用户和近 250 位开发人员[42]。

（6）万向区块链实验室于 2015 年 9 月成立，是中国首家研究区块链技术的非盈利先锋机构。该实验室汇聚了来自世界各地的专家，致力于技术研发和商业应用、产业战略的探索，为企业提供建议，推动产业发展和政策制定，促进区块链技术服务于社会经济发展[43]。

（7）360 金融区块链研究中心是 360 公司于 2017 年 12 月 20 日成立的金融技术研究平台，标志着 360 金融在 Blockchain 掘金领域的重要一步。360 金融区块链研究中心致力于区块链核心技术研究，利用其已有的资源优势，实现产业集成，科技创新为一体的新型生态金融体系。致力于推动区块链金融技术的应用和创新，为未来新的金融体系提供一系列高效，低成本的解决方案[44]。

（8）百度建立的金融区块链实验室致力于提供企业级和面向用户的应用级区块链解决方案，利用百度自身的平台优势，深入区块链研究技术，进行前沿领域的区块链研究，并将技术应用于实际业务，促进区块链平台全球化标准的形成。其在 2018 年推出的区块链游戏项目莱茨狗是百度在区块链应用领域的一次大胆尝试[45-46]。

为了更深层次展示上述八个代表性企业之间在区块链产品发展方面的差异，本文从各企业主要区块链研究机构、研究内容、典型产品、特点、技术和应用领域 6 个方面对八个代表性企业之间的差异进行分析与比较。具体结果如表 5 所示。

表 5 所示的区块链代表性企业全部为国内外超大型科技、金融、汽车零部件和互联网等领域企业，探索使用区块链技术变革企业原有的技术生态和业务流程。这些代表性企业除了研究金融领域区块链应用之外，更注重研究涵盖各个不同领域的区块链生态。它们的主要区块链产品表现为金融区块链平台、量子链智能合约平台、物流区块链平台、医联体区块链项目、企业级区块链基础设施、行业解决方案和区块链云服务等。区块链应用开发的特点体现为开源、联盟、开放、创新、多元和跨界，以及高性能、高安全性、高速接入、高效运营、适用性、兼容性和模块化设计。采用的技术涵盖：共识算法、智能合约、分布式存储、云计算、价值传输协议、权益共识机制、分布式账本、非对称加密和授权技术、点对点传输、等等。此外，代表性企业区块链技术的应用领域也非常广泛，

涉及金融、公益慈善、医疗、物流、商品溯源、并行记账、智能投顾、航空延误理赔、知识产权保护、物联网、供应链、社交游戏和股权等各个不同领域。

表 5 代表性企业区块链发展差异的比较结果

企业	区块链研究机构	研究内容	典型产品	特点	技术	应用领域
高盛	高盛全球投资研究	金融区块链	高盛区块链平台	“区块链 + 金融 ” 新模式	共识算法、密码学、智能合约、分布式存储等	金融
微软	微软研究中心、微软亚洲研究院	区块链生态	Azure 云计算平台、BaaS 平台、Bletchley 项目	基于 Azure 云服务、开源、联盟	云计算、共识机制、加密算法等	金融、IT、贷款、证券、供应链等
阿里巴巴	蚂蚁金服技术实验室	区块链生态	支付宝捐赠平台、淘宝物流平台、“医联体 + 区块链” 项目	应用多元化、起步早、技术相对成熟	智能合约、共识机制、分布式架构等	公益慈善、医疗、物流、商品溯源、供应链等
腾讯	腾讯 FiT、腾讯研究院、腾讯公共战略委员会办公室、腾讯战略发展部	区块链生态	企业级区块链基础设施、行业解决方案、区块链云服务	高性能、高安全性、高速接入、高效运营	共识机制、SQL 和 API 的接口	并行记账、智能投顾、航空延误理赔、知识产权保护等
Qtum 量子链公司	量子链 Qtum 社区	量子链	量子链智能合约平台	适用性、向下兼容性设计、模块化	价值传输协议 (Value Transfer Protocol)、权益共识机制（PoS）	金融、物联网、供应链、社交游戏、慈善、数字资产、股权等
万向	万向区块链实验室、万向区块链商业创新咨询、万向新链加速器、万云	区块链生态	万云区块链云平台	开放、创新、多元、跨界	Cosmos、Stellar、Factom、Qtum、趣链	金融、版权认证与交易、智能医疗、游戏、智能锁、房屋租赁等
360	360 金融区块链研究中心	金融区块链	360 金融区块链平台	“区块链 + 金融 ” 新模式	分布式账本、智能合约、非对称加密和授权技术、共识机制	金融
百度	百度金融区块链实验室	金融区块链	“BaaS” 区块链开放平台、莱茨狗	“区块链 + 金融 ” 新模式	分布式数据存储、点对点传输、共识机制、加密算法	金融

4.4 区块链对情报工程领域的意义

（1）保障军事情报工作的隐秘性 [47]。在传递军事情报时，提供军事情报的“线人”的身份不便透露和公开，在对这些“线人”进行奖励或激励时，区块链的匿名属性即可在交易记录的过程中发挥作用，从而确保双方身份信息等关键信息的安全。

（2）完善武器装备的档案建立和管理各环节。武器装备从生产到投入使用，再到报废更新换代，这一系列周期内的传统信息记录方式一般为电子媒介或纸质记录备案，一方面存在信息泄露、丢失、与实际情况不符等安全隐患，另一方面在管理人员变动，需要进行工作转接时，也存在交接困难等缺陷。将区块链技术应用到武器装备管理的各环节，建立包括上级管理部门、信息记录备案方、武器使用方和装备生产维修厂家等在内的武器装备信息管理网络，各方均持有并保存完整的备案副本，不仅可以

doi:10.3772/j.issn.2095-915x.2019.06.002

解决传统管理方式存在的问题，还可以有效提高信息的真实性和安全性。

（3）保护著作权和产权。区块链的信息追溯特性可以用于著作权和产权所有人的身份认证，一旦出现盗版等侵权行为，可以提供可靠的数据证据链，有效打击假冒伪劣。

5 结论与建议

区块链作为一种去中心化的分布式账本，能够为所有涉及价值交易的领域构建信任机制。社区中的任何人都可以参与交易的验证、确认和记录。区块链是当前新兴前沿技术，涉及技术较多，涵盖：区块结构设计与互操作、分布式处理、加密解密算法、P2P 分布式网络、公有链和联盟链实现技术。同时区块链技术应用领域非常广泛，广泛应用于社会公共事业、跨境支付、保险理赔、产品交易保障、金融和证券交易、贷款交易和管理、供应链管理、公益慈善、医疗、物流、商品溯源等领域。目前国内外针对区块链的研究还有很大发展空间，区块链技术发展处于初期，研究不够深入，技术积累不足。虽然国内外已经出现大量区块链企业，然而这些企业在区块链技术应用方面仍然处于探索和初级试验阶段，无法进行成熟应用阶段；区块链应用产品相对单一，无法大面积拓展到不同行业领域的交易过程。政府及相关企业应积极探索、发展和应用区块链技术，积极融入区块链的全球化浪潮中，促进技术革新、经济和信任机制转型。

区块链技术的发展和应用，必将对社会信用机制产生重大影响，从而加速“数字化信用社会”的到来。在全球积极发展区块链技术的浪潮下，政府应考虑将区块链纳入国家发展战略，鼓励相关企业和组织进行区块链技术探索，并进行有效恰当的监管和整治。为有效促进我国区块链技术的发展，积极地参与全球化竞争，提出相关建议如下：

（1）提高区块链技术应用的安全性。区块链目前处于发展阶段，相关技术并不成熟，区块链业界最大的众筹项目 The DAO（Decentralized Autonomous Organization，去中心化的自治组织）、以太坊组织和 Bitfinex 交易所就曾发生过虚拟数字货币失窃事件，说明区块链技术仍然存在安全风险和漏洞。政府和相关企业应加大区块链安全机制研究力度，填补技术漏洞，确保区块链技术安全稳步发展。

（2）加强核心技术研究，鼓励创新。促进“企企联手”、“校校联手”、“企校联手”，鼓励相关专业性人才和组织强强联手进行区块链核心技术研发，借助相关政策鼓励创新，促进区块链产品多样化发展，构建涵盖：金融交易、医疗、教育、食品安全和财税等领域的区块链生态系统，提高我国区块链技术的核心竞争力。

（3）保持区块链技术发展环境优质化。区块链技术的发展必将对中心化的信用机制和社会机制产生一定的冲击和挑战，传统的金融中介平台都将受到不同程度的挑战，政府应加大中央调控，积极与相关部门交流协商，向区块链技术成熟的国家借鉴学习，出台相关政策支持区块链技术的发展，保持区块链技术发展环境优质化。

（4）促进区块链技术行业标准的形成。2018 年 6 月，工信部公示全国区块链和分布式

记账技术标准化技术委员会筹建方案。从公示时间可以看出，目前国内缺乏权威的区块链技术行业标准。因此需要关注区块链技术发展的重要环节，促进国际沟通与合作，制定并完善区块链技术行业标准，在推动区块链技术快速发展的同时，也要遏制发展过程中有问题的步骤和环节，推动区块链技术高质量发展。

（5）推动区块链应用试点。目前国内的区块链应用产品相对单一，相关技术仍有很大发展空间，应积极推动相关企业开展区块链技术及其应用研究，选取技术条件好和应用效果明显的地区或领域作为应用试点，鼓励有能力的企业或地方先发展起来，进而在全国范围内推广和实施。

（6）促进区块链国际化发展。积极引进国外先进的区块链技术，推动国际交流协作，借鉴优质的国际区块链应用模式，依据中国的基本国情，发展有中国特色的区块链技术，建设中国特色区块链体系。

参考文献

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. [2018-03-02]. https://bitcoin.org/bitcoin.pdf.

[2] 袁勇 , 王飞跃 . 区块链技术发展现状与展望 [J]. 自动化学报 , 2016, 42(4): 481-494.

[3] 新浪财经 . 2014-2016 全球比特币发展研究报告 [EB/OL]. [2018-01-19]. http://slide.tech.sina.com.cn/internet/slide_5_18966_70159.html

[4] 张健 . 区块链 : 定义未来金融与经济新格局 [J]. 中国商界 , 2016(9):75.

[5] Nofer M, Gomber P, Hinz O, et al. Blockchain. Business & Information Systems Engineering, 2017, 59(3):183-187.

[6] Mamoshina P, Ojomoko L, Yanovich Y, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare[J]. Oncotarget, 2018, 9(5):5665-5690.

[7] 沈鑫 , 裴庆祺 , 刘雪峰 . 区块链技术综述 [J]. 网络与信息安全学报 , 2016, 2(11):11-20.

[8] 谢辉 , 王健 . 区块链技术及其应用研究 [J]. 信息络安全 , 2016, (9):192-195.

[9] 朱建明 , 付永贵 . 区块链应用研究进展 [J]. 科技导报 , 2017, 35(13):70-76.

[10] 坤鹏论 . 阿里和腾讯的区块链布局 [EB/OL]. [2018-03-23]. http://www.techweb.com.cn/article/2018-01-15/2628924.shtml.

[11] Lee J H. BIDaaS: Blockchain Based ID As a Service[J]. IEEE Access, 2018, 6(99):2274-2278.

[12] Khaqqi K N, Sikorski J J, Hadinoto K, et al. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application[J]. Applied Energy, 2017, 209:8-19.

[13] 蔡维德 , 郁莲 , 王荣 , 等 . 基于区块链的应用系统开发方法研究 [J]. 软件学报 , 2017, 28(6):1474-1487.

[14] 聂静 . 基于区块链的数字出版版权保护 [J]. 出版发行研究 , 2017(9):33-36.

[15] 郝世博 , 徐文哲 , 唐正韵 . 科学数据共享区块链模型及实现机理研究 [J]. 情报理论与实践 . 2018, 41(11):57-62.

[16] 汪传雷 , 万一荻 , 秦琴 , 等 . 基于区块链的供应链物流信息生态圈模型 [J]. 情报理论与实践 , 2017, 40(7):115-121.

[17] Nick S. “Smart Contracts”[EB/OL]. [2018-03-05]. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[18] Jesse Y H, Deokyoon K, Sujin C, et al. Where Is Current Research on Blockchain Technology?—A Systematic Review[J]. PLoS One, 2016, 11(10): e0163477.

[19] 林小驰 , 胡叶倩雯 . 关于区块链技术的研究综述 [J]. 金融市场研究 , 2016, 45(2):97-109.

[20] 邵奇峰 , 金澈清 , 张召 , 等 . 区块链技术 : 架构及进展 [J]. 计算机学报 , 2018, 41(5):969-988.

[21] 安瑞 , 何德彪 , 张韵茹 , 等 . 基于区块链技术

doi:10.3772/j.issn.2095-915x.2019.06.002

的防伪系统的设计与实现 [J]. 密码学报 , 2017, 4(2):199-208.

[22] 腾讯财经. 腾讯区块链方案白皮书 [EB/OL]. [2018-03-05]. http://www.cebnet.com.cn/upload//Tencent_TrustSQL_White Paper.pdf.pdf.

[23] 腾讯财经 . Uber 创始人将发行 1 万亿枚数字加密货币 [EB/OL]. [2018-03-05]. https://finance.qq.com/a/20180304/005343.htm?pgv_ref=aio2015&ptlang=2052.

[24] 搜狐网 . 百度区块链“莱茨狗”繁殖功能即将上线 [EB/OL]. [2018-03-06]. http://www.sohu.com/a/223015465_163726?qq-pf-to=pcqq.c2c.

[25] Pymnts. Visa Announces New B2B Payments Using Blockchain[EB/OL]. [2018-03-06]. https://www.toutiao. com /i6345278948431102466/.

[26] LenderBot. Stratumn 与德勤合作推出基于区块链的保险产品 LenderBot[EB/OL].[2018-03-06].http://www.fxark.com/hangyebaodao/xy/detail?newid=7351.

[27] linq[EB/OL]. [2018-03-06].http://www.8btc.com/linq.

[28] IBM Adept 系统：使用区块链技术的物联网架构 [EB/OL]. [2018-03-06]. http://www.8btc.com/ibm-adept.

[29] Visa 联合 DocuSign 推出区块链租车项目，你看懂了 么 [EB/OL]. [2018-03-06].http://www.8btc.com/visa-docusign-car-lease.

[30] Ujo Music[EB/OL]. [2018-03-07]. https://blog.ujomusic.com/.

[31] Now Blockchain To Help In Authenticating Academic Certificates! [EB/OL]. [2018-03-07]. http://www.newsbtc.com/2015/10/21/now-blockchain-to-help-in-authenticating-Academic-certi icates/.

[32] 搜狐网 . Ubitquity 在比特币公共账本上进行房产产权转移 [EB/OL]. [2018-03-07]. https://www.sohu.com/a/105228746_286863.

[33] 爱沙尼亚宣布启动基于区块链的医疗健康档案安全项目 [EB/OL]. [2018-03-07]. http:/www.qqya.cc/qu/22783/.

[34] BitGive Foundation Launches GiveTrack Blockchain Fund -tracking Platform[EB/OL]. [2018-03-07]. https://www. newsbtc.com/2016/12/09/bitgive-foundation-launches-givetrack-blockchain-fund-tracking-platform/.

[35] 巴比特网 . Provenance[EB/OL].[2018-03-07]. http://www.8btc. com/?tag=Provenance.

[36] 太平洋电脑网 . 360 进军区块链：共享宽带能获得“云钻”奖励 [EB/OL]. [2018-03-07]. http://pcedu.pconline.com. cn/1066/10663407.html?qq-pf-to=pcqq.c2c.

[37] 万云网 . 万云区块链开放创新平台 [EB/OL]. [2018-03-07]. https://www.wancloud.io/#/.

[38] 巴比特网 . Block chain: Putting Theory into Practice[EB/OL]. [2018-03-23]. book.8btc.com/gaosheng_blockchain_report.

[39] 巴比特网 . 高盛、IBM 追投，区块链公司 DAH 融资 6000 万美元 [EB/OL]. [2018-03-23]. http://www.8btc.com/ibm-goldman-sachs.

[40] 中文业界资讯 . 微软区块链服务（BaaS）正式开放基于 Azure 云平台 [EB/OL]. [2018-03-23]. https://www.cnbeta.com/articles/tech/526519.htm.

[41] 新浪财经 . 突围 BAT 区块链创业者机会在场景化 [EB/OL]. [2018-03-23]. https://finance.sina.cn/2018-03-23/detail-ifyspcwh9715401.d.html?from=singlemessage.

[42] 巴比特网 . 走进 Qtum 量子链——联合创始人帅初最新采访 [EB/OL]. [2018-03-07]. http://www.8btc.com/qtum-btcmanager.

[43] 万向集团 . 万向区块链实验室 [EB/OL]. [2018-03-07]. http://www.blockchainlabs.org/index_cn.html.

[44] 360 社区 . 360 金融成立区块链研究中心 [EB/OL]. [2018-03-07]. http://bbs.360.cn/thread-15292780-1-1.html.

[45] 中金在线 . 百度推出区块链宠物莱茨狗实验室提供应用级区块链解决方案 [EB/OL]. [2018-03-07]. http://news.cnfol.com/chanyejingji/20180204/25994687.shtml.

[46] 亿欧网 . 继网易之后，百度携“莱茨狗”进军区块链，两家巨头意欲何为 ?[EB/OL]. [2018-03-07]. https://www.iyiou.com/p/66617.

[47] 廉蔺 , 朱启超 , 赵炤 . 区块链技术及其潜在的军事价值 [J]. 国防科技 , 2016, 37(2): 30-34