区块链发展研究报告 2020

2020 年第 5 期

清华大学人工智能研究院
北京智源人工智能研究院
清华 - 中国工程院知识智能联合研究中心

2020 年 7 月

目录

图目录

表目录

摘要

区块链是密码学、分布式系统、博弈论的集大成者。目前，区块链技术正处在加速演进成熟的过程中，其应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域。近两年来，全球主要国家都在加快布局区块链技术发展。在此背景下，我国更将区块链作为核心技术自主创新的重要突破口。

清华大学人工智能研究院曾于 2018 年发布了《区块链基础理论与研究概况》报告。本报告在 2018 版报告的基础上，针对近两年区块链技术研究、应用发展、人才研究等方面进展进行了更为深入的调查研究，其主要内容包括：

一、区块链基本概念梳理和国内外区块链发展现状分析。简要概括了区块链技术的产生背景和基本概念，分别探讨区块链 1.0 数字货币阶段、区块链 2.0 智能合约阶段和区块链 3.0 多行业应用阶段的技术架构，总结出区块链技术 6 大特征，并梳理了区块链的国内外最新政策和行业发展现状。

二、区块链基础理论和技术研究现状分析。通过 AMiner 系统提供的大数据信息，分别对密码学、分布式系统（共识协议）和博弈论等领域的研究现状进行全面梳理。

三、区块链领域人才现状分析。通过 AMiner 系统提供的大数据信息，整理区块链领域的国内外专家学者、研究机构、代表论文、研究热点及热点变化趋势、中外研究情况对比，对区块链领域人才现状进行全面梳理。

四、区块链典型应用场景及典型应用分析。主要分析了区块链在以比特币为代表的数字货币中的应用，以及区块链在金融服务、智能制造、物联网与供应链管理、文化娱乐、民生公益、政府管理 6 大方面的应用场景，并对区块链应用价值进行展望。

最后，分析归纳了区块链未来发展面临的技术和监管等方面挑战，挖掘生成了区块链技术发展趋势。

报告说明

编写方法

本报告在上一版《区块链基础理论与研究概况》报告基础上进行更新，主要更新了区块链关键技术领域的国内外进展、技术趋势、研究学者以及应用场景等。

一是收集国内外区块链最新研究成果和总结报告。本研究收集了主要国家政府和国际政府间组织发布的区块链报告和白皮书，如联合国《数字货币和区块链技术在构建社会团结金融中如何扮演角色》（How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?）、中国人民银行《金融分布式账本技术安全规范》（JR/T 0184—2020）、工信部《中国区块链技术和应用发展白皮书（2016）》和《2018 年中国区块链产业白皮书》、KPMG 区块链研究报告《共识—价值互联的不变协议》、iiMedia Research《2017-2018 中国区块链热点专题研究报告》和《2019-2020 中国区块链发展现状、应用场景与未来趋势分析》等，从政府、学术研究以及行业发展等角度全面把握区块链技术的发展动向。

二是利用 AMiner 平台整理区块链基础技术国内外研究状况。重点分析了密码学、分布式系统、博弈论领域当前世界学者分布、代表学者、学者关系、研究成果、研究趋势和中外研究概况对比，以丰富的图文数据展示区块链基础理论在全球范围内的发展状况和未来的研究潜力。

通过 AMiner 系统对近 10 年（2010-2020 年）发表在 SJR（Scimago Journal & Country Rank）一区的信息技术领域学术会议及期刊（具体名单详见附录）论文进行挖掘，提取区块链领域论文中所有学者信息，并按照相关性进行排序，进行学者分布与多维画像等方面的分析，介绍了部分该领域国内外知名度较高的活跃学者。

领域关键词由区块链顾问组给出，具体包括区块链（Blockchain）、密码学（Cryptography）、量子计算（Quantum Computing）、分布式账本（Distributed Ledgers）、博弈论（Game Theory）、计算经济学（Computational Economics）、策略制定（Strategy Formulation）、比特币（Bitcoin）、共识层（Consensus Layer）、共识机制（Consensus Mechanism）、共识协议（Consensus Protocol）、去中心化（Decentralized OR Decentralizing）、加密货币（Cryptocurrency）、

点对点技术（P2P OR Peer-to-Peer Network）、以太坊（Ethereum）和智能合约（Smart Contract）等。

此外，基于 AMiner 系统的“Topic 必读论文”功能（详见网址 https://www.aminer.cn/search/pub?q=Blockchain），通过本领域热心专业读者推荐，选取代表性的论文进行解读。

基于以上“区块链”领域关键词组，从 AMiner 数据库中查找出 2010 至 2020 年区块链国内相关专利申请数据、国家自然科学基金支持的区块链项目（包含未结题的项目）数据并进行了相应展示分析。

三是分析区块链应用的典型案例。通过对比特币、以太坊和传统金融机构的区块链应用案例进行分析，了解区块链采用的底层基础设施、应用架构和应用价值，展现区块链与现实场景结合状况与现存问题，为区块链理论与实践的进一步发展提出展望。

术语和缩略语

本报告涉及的术语如表 1 所示。

表 1　术语

术语	定义/解释
区块链	区块链是在分布式账本中排序及验证交易的方式，是数据存储、点对点传输、共识机制、加密算法等计算机技术的集成应用。
密码学	研究编制密码和破译密码的技术科学。
分布式账本	一个可以在多个站点，不同地理位置或者多个机构组成的网络中记录的资产数据库。其中，资产可以是货币以及法律定义的、实体的或是电子的资产。
共识机制	共识机制是一种通过节点之间相互收发消息，或者结合其他的一些方法例如密码学算法，达到在分布式系统的节点之间一致目的的分布式算法。
博弈论	博弈论是数学的分支，也是运筹学的重要组成部分，研究公式化了的激励结构间的相互作用，是研究具有斗争或竞争性质现象的数学理论和方法。
智能合约	一种用计算机语言取代法律语言记录条款的计算机程序。
数字货币	货币的数字化，通过数据交易并发挥交易媒介、记账单位及价值存储

术语	定义/解释
	的功能。

本报告涉及的缩略语如表 2 所示。

表 2　缩略语

缩略语	原始术语
PoW	工作量证明（Proof of Work）
PoS	股权证明（Proof of Stake）
DPoS	股权授权证明（Delegate Proof of Stake）
PBFT	实用拜占庭容错（Practical Byzantine Fault Tolerance）
P2P	点对点（Peer to Peer）
DAPP	分布式应用（Decentralized Application）
RSA	RSA 加密算法（RSA Algorithm）
ECC	椭圆加密算法（Elliptic Curve Cryptography）
KYC	客户识别（Know Your Customer）
AML	反洗钱（Anti Money Laundering）

1　概述篇

1.1 产生背景

区块链的出现最初是为了通过数字的方式来记录账本，从而达到替代现金货币的目的；后来逐渐成为通过计算机联网运行来达到有效利用社会资源、解决商业民生政务等问题。

货币产生和发展的历史很长。废弃金本位制之后，当今货币体系容易造成货币滥发并面临金融危机的风险。2008 年，由美国次贷危机所引发的金融危机席卷全球，暴露了当前金融体系在全球化背景下的严重失衡问题。于是，有人试图摒弃现有货币体系和规则，完全模拟黄金，运用计算机系统技术等，形成一套新的货币运行机制。

2008 年 11 月，有人以中本聪的名义发表了一篇文章提出了比特币的概念及模式，描述了一种新的货币体系；2009 年，中本聪为该模式建立了一个开放源代码项目，正式宣告了比特币的诞生。

比特币面世之后，一直稳定运行，不仅产生了新的产业生态，也通过解决价值传输等问题，完成了对传统产业的改造和升级，给整个社会带来了巨大的影响。凭借去中心化的理念和信任建立机制，基于密码学的加密体系以及基于时间序列的链式叠加模式逐渐被抽离出来，成为一种面向未来的新型互联网协议，推动着“信息互联网”向“价值互联网”转型，使全球信息的价值传递成为可能。

1.2 区块链概念

区块链本质上是一个去中心化的分布式账本数据库，目的是解决交易信任问题。广义来看，区块链技术是利用块链式数据结构验证与存储数据、利用分布式节点共识算法生成和更新数据、利用密码学方式保证数据传输和访问的安全、利用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。狭义来看，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的不可篡改和不可伪造的分布式账本。

区块链通常涉及到以下基本概念：

交易（Transaction）：指导致区块链分布式账本状态改变的一次操作，如添

加一条记录或者是一笔在两个账户之间的转账操作。它代表了一次数字现金的转移过程。

区块（Block）：用于记录一段时间内发生的交易和状态结果。区块通常用区块头的哈希值和区块高度来进行标识。**区块头**一般包括前一个区块的哈希值（父哈希）、时间戳以及其他信息。区块头的哈希值是通过 SHA256 算法对区块头进行二次哈希计算而得到的数字。区块哈希值可以唯一标识一个区块。**区块高度**是指在区块链中的位置。第一个头部区块被称为创世区块（genesis block），高度为 0，其他区块依次类推。

链（Chain）：由一个个区块按照发生顺序串联而成，是整个状态变化的日志记录。

区块链技术的最大优势与努力方向是“去中心化”，通过运用密码学、共识机制、博弈论等技术与方法，在网络节点无需相互信任的分布式系统中实现基于去中心化信用的点对点交易。因此，区块链成为以比特币为代表的数字货币体系的核心底层技术。

根据系统是否具有准入机制，区块链系统可以分为无许可的区块链和有许可的区块链，前者被称为公有链（Public Blockchain），后者则被称为许可链，如表 3 所示。许可链又可进一步分为联盟链（Consortium Blockchain）和私有链（Private Blockchain）。准入机制的有无往往会影响区块链系统所面临的环境假设并导致系统采用不同的共识机制[1]。

表 3　区块链的类型及特性

类型		特性
公有链		世界上任何个体或团体都能发送交易，且交易能获得该区块链的有效确认 任何人均可参与其共识过程。 最早出现、目前应用最广泛的区块链。 现阶段每秒 3—20 次数据写入。
许可链	联盟链	某个群体内部指定多个记账节点，每个区块的生成由所有预选节

[1] 刘艺华，陈康，区块链共识机制新进展[J]，计算机应用研究，2020 年 03 期

		点共同决定。 预选节点参与共识过程，其他接入节点可以参与交易，但不过问记账过程，可满足监管 AML（Anti Money Laundering,反洗钱）/KYC（Know Your Customer,客户识别）。 现阶段每秒 1000 次以上数据写入。
	私有链	仅使用区块链记账技术进行记账，某一组织或个人独享写入权限 改善可审计性，不解决信任问题。

1.3 区块链发展阶段

2008 年，化名为“中本聪”（Satoshi Nakamoto）的学者或组织发表论文《比特币：一种点对点电子现金系统》，这一事件被认为是区块链技术的起源。随着比特币等数字货币的日益普及，区块链技术的发展引起了政府部门、金融机构、初创企业和研究机构的广泛关注。区块链的研究成果与应用成果呈现几何级数增长的态势，与大数据、物联网、智能制造等场景紧密结合，依托现有技术进行独创性组合创新。

根据比特币大会所发布的《布雷顿森林体系 2015 白皮书》，区块链发展经历了从 1.0 到 3.0 的三个阶段：**区块链 1.0**，即以可编程数字加密货币体系为主要特征的区块链模式，主要体现在比特币应用上；**区块链 2.0**，即依托智能合约、以可编程金融系统为主要特征的区块链模式，区块链技术被运用在金融或经济市场，延伸到股票、债券、期货、贷款、按揭、产权、智能资产等合约上；**区块链 3.0**，即广泛创新应用阶段，主要是广泛应用于某些全球性的公共服务上，能够满足更加复杂的商业逻辑。有一些研究[2]基于此阶段的自治理特征称这个阶段为 DAO（区块链自洽组织）、DAC（区块链自洽公司）。本报告认为 DAO 或 DAC 仍是区块链的应用，即通过一系列公开公正的规则，可以在无人干预和管理的情况下自主运行的组织形式。当前，区块链发展已经进入区块链 3.0 模式。

另外，**区块链模式是平行发展而非质变式演进的**，区块链 1.0 模式与 2.0 模式目前同时存在于人类社会，且以数字加密货币为应用代表的 1.0 模式仍在探索之中。区块链 2.0 是区块链技术在金融业务上的延伸，其应用涵盖金融机构和金

[2] R Beck, C Müller — Bloch & J L King, “Governance in the Blockchain Economy: A Framework and Research Agenda”, [J]Journal of the Association for Information Systems, 2018 (19) , pp. 1 - 41;

融工具等。区块链 3.0 包括行业中的新兴应用，拓展了包括银行和金融科技在内的广泛应用。**区块链的不同发展阶段呈现出相互影响、相互补充的互动态势。**

1.3.1 区块链 1.0：数字货币

区块链是利用密码学方法关联产生的数据块，用于验证信息有效性或防伪，并生成下一个区块。在区块链 1.0 阶段，以比特币为代表的数字货币和支付行为是最典型的应用。继 2008 年一个自称为中本聪的人提出比特币设想后，2009 年比特币正式上线运行。随着比特币在世界范围内的普及，人们开始意识到作为比特币底层技术的区块链具有去中心化的优良性质。区块链采用纯数学方法而不是中心机构建立信任关系，使得互不信任或弱信任的参与者之间能够维系不可篡改的账本记录。

区块链 1.0 技术架构如图 1 所示。具体而言，区块链 1.0 使用了如下的相关技术：

- **分布式账本(Distributed Ledger)**：分布式账本是在网络成员之间共享、复制和同步的数据库，记录网络参与者之间的交易，部分国家的银行将分布式账本作为一项节约成本的措施和降低操作风险的方法。
- **块链式数据（Chained-Block Data Structure）**：区块链采用带有时间戳的链式区块结构存储数据，从而为数据增加了时间维度，具有极强的可验证性和可追溯性。
- **梅克尔树（Merkle Trees）**：梅克尔树是区块链的重要数据结构，能够快速归纳和校验区块数据的存在性和完整性。
- **工作量证明（Proof of Work, PoW）**：通过引入分布式节点的算力竞争保证数据一致性和共识的安全性。

图 1　区块链 1.0 技术架构[3]

1.3.2 区块链 2.0：智能合约

区块链 2.0 进入可编程金融阶段。在这一阶段，区块链系统渗入经济、金融与资本市场，形成股票、债券、期货、贷款、抵押、产权、智能财产等的智能合约。除了构建货币体系之外，区块链在泛金融领域也有众多应用案例。例如，智能合约的核心是利用程序算法替代人执行合同，这些合约包含三个基本要素：要约、承诺、价值交换，可以实现资产、过程、系统的自动化组合与相互协调。

区块链 2.0 技术架构如图 2 所示，具体使用了如下的技术：

- **智能合约**（Smart Contract）：1994 年，Nick Szabo[4]首次提出智能合约概念，即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，能够在没有第三方的情况下进行可信交易。智能合约是已编码的、可自动运行的业务逻辑，通常有自己的代币和专用开发语言。
- **虚拟机**（Virtual Machine）：指通过软件模拟的运行在一个完全隔离环境中的完整计算机系统，在区块链技术中，虚拟机用于执行智能合约编译后的代码。
- **去中心化应用**（Decentralized Application,简称 DApp）：去中心化应用是运行在分布式网络上、参与者的信息被安全保护（也可能是匿名的）、通过网络节点进行去中心化操作的应用。包含用户界面的应用，包括但

[3]工信部，《中国区块链技术和应用发展白皮书（2016）》[S]，http://www.cbdforum.cn/bcweb/index/article/rsr-6.html

[4] Szabo N. Smart contracts[J]. Unpublished manuscript, 1994.

不限于各种加密货币，如以太坊（Ethereum）的去中心化区块链及其原生数字货币以太币（Ether）。

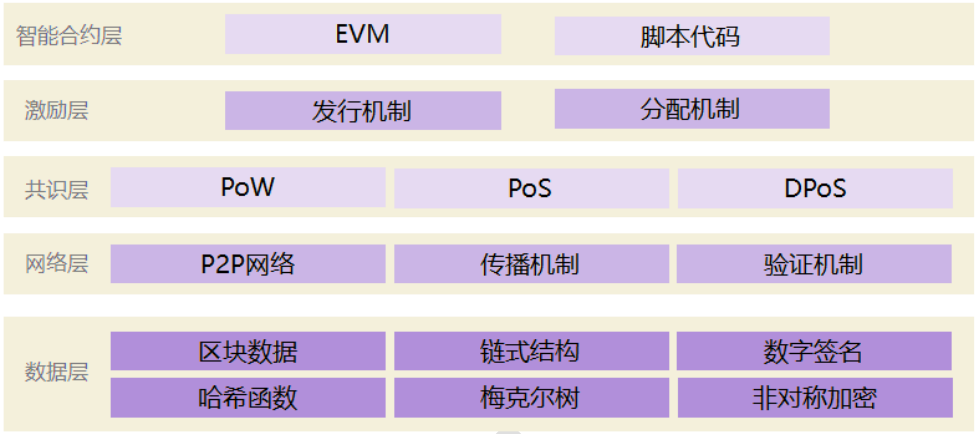


图 2　区块链 2.0 技术架构[5]

1.3.3 区块链 3.0：多行业应用

继区块链 1.0、区块链 2.0 后，目前已开启了区块链 3.0 时代，即可编程社会系统时代。区块链 3.0，代表的是解决了关键性技术难题的全领域生态级别的底层系统出现以及区块链技术应用到各个垂直行业中去的时代。这个时代的底层协议能够在保证去中心化、去信任中介的同时，保证了商用级别的高性能。

区块链 3.0 的根本特征之一是区块链与大数据、人工智能技术融合，通过新的区块链技术，实现新的存储模式的创新。区块链 3.0 与区块链 1.0 和 2.0 最重要的一个区别在于区块链技术的使用方式与领域。在 3.0 时代，区块链技术应用已超出金融领域，扩展到人类生活的各个方面，为各种行业提供去中心化解决方案，包括在司法、医疗、物流等领域，利用区块链技术来解决信任问题、实现信息的共享，将数据进行分布式的存储和连接，实现真正的大数据化[6]，提高整个系统的运转效率。

区块链 3.0 主要应用在社会治理领域，包括了身份认证、公证、仲裁、审计、域名、物流、医疗、邮件、签证、投票等领域，应用范围扩大到了整个社会，区块链技术有可能成为“万物互联”的一种最底层的协议[7]。

[5] 工信部，《中国区块链技术和应用发展白皮书（2016）》[S]，http://www.cbdforum.cn/bcweb/index/article/rsr-6.html
[6] 海外科技风云《什么区块链 3.0 技术？区块链 3.0 技术给未来带来了什么变革？》[N] https://baijiahao.baidu.com/s?id=1640688251621987558&wfr=spider&for=pc
[7] 董宁，朱轩彤．区块链技术演进及产业应用展望[J]．信息安全研究，2017，3(3):200-210.

区块链 3.0 技术架构如图 3 所示，相关技术又有了新的发展：

- **超级账本（HyperLedger）：**超级账本是 Linux 基金会于 2015 年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各种用户案例，并简化业务流程。由于点对点网络的特性，分布式账本技术是完全共享、透明和去中心化的。通过创建分布式账本的公开标准，实现虚拟和数字形式的价值交换。
- **分片技术（Sharding）：**分片是一种基于数据库分成若干片段的传统概念扩容技术，它将数据库分割成多个分片并将这些分片放置在不同的服务器上，在底层公有链的系统内，网络上的交易将被分成不同的分片，其由网络上的不同节点组成。因此，只需要处理一小部分输入的交易，并且通过与网络上的其他节点并行处理就能完成大量的验证工作。

图 3　区块链 3.0 技术架构

1.4 区块链特征

区块链共有五大特征：去中心化、开放性、自治性、信息不可篡改和匿名性。具体介绍如下。

- **去中心化：**区块链是由众多节点共同组成的一个端到端的网络，不存在中心化的设备和管理机构。区块链数据的验证、记账、存储、维护和传输都不是基于中心机构，而是利用数学算法实现。去中心化使网络中的各节点之间能够自由连接，进行数据、资产、信息等的交换。
- **开放性：**区块链中的所有数据信息是公开的，每一笔交易都会通过广播

的方式，让所有节点可见。区块链具有源代码开源性，即网络中设定的共识机制、规则都可以通过一致的、开源的源代码进行验证。任何人都可以加入（公开链），或者通过受控方式加入（联盟链）。

- **自治性**：任何人都可以参与到区块链网络，每个节点都能获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争计算来共同维护整个区块链。区块链技术采用基于协商一致的规范和协议，使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，任何人为的干预不起作用。
- **信息不可篡改**：不可篡改性是指单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制超过 51%的节点同时修改。区块链使用了密码学技术中的哈希函数、非对称加密机制保证区块链上的信息不被篡改。由于每一个区块都是与前续区块通过密码学证明的方式链接在一起的，当区块链达到一定的长度后，要修改某个历史区块中的交易内容就必须将该区块之前的所有区块的交易记录及密码学证明进行重构，有效实现了防篡改。
- **匿名性**：由于节点之间的交换遵循固定的算法，其数据交互是无需信任的，区块链中的程序规则会自行判断活动是否有效，因此，交易对手无须通过公开身份的方式让对方自己产生信任。

1.5 国内外发展现状

凭借其独有的信任建立机制，区块链正在改变诸多行业的应用场景和运行规则，是未来发展数字经济、构建新型信任体系不可或缺的技术之一。

1.5.1 相关政策现状

近年来，随着区块链逐步应用于金融、供应链、工业制造、公益等领域，各国政府及监管机构对区块链技术及其研发应用的态度逐渐从观望转向鼓励，并且越来越积极地进行更多尝试，相关政策动态如图 4 所示。对于以比特币为代表的数字货币政策虽然仍然褒贬不一，但是少数国家已开始接纳，例如德国、日本等。

2016 年 1 月 19 日，英国政府发布《分布式账本技术：超越区块链》白皮书，

积极探索区块链未来在减少金融诈骗、降低交易成本的潜力；2016 年 6 月，新加坡金融管理局推出“沙盒计划”（Sandbox），在可控范围内允许金融科技公司的发展；2017 年 4 月 1 日，日本正式实施《支付服务法案》，承认比特币的合法地位；美国各州政府也采取措施学习与探索区块链技术，并尝试通过区块链提高政府工作的透明度和效率；2018 年 6 月，日本推出了沙盒制度，以加快推出新的商业模式和创新技术，如区块链、人工智能和物联网；2018 年 12 月，欧洲议会呼吁采取措施促进贸易和商业区块链的采用；2019 年 1 月，韩国政府将区块链技术纳入其“研究与开发税收减免中增加了 16 个领域”之一，以促进其创新；2019 年 7 月，美国参议院商业、科学和运输委员会批准了《区块链促进法案》；2020 年以来，新加坡出台新法案允许全球加密公司在新加坡当地扩展业务；日本金融监管机构宣布启动其全球区块链治理倡议网络，旨在促进“区块链社区的可持续发展”。

来源：根据公开资料整理

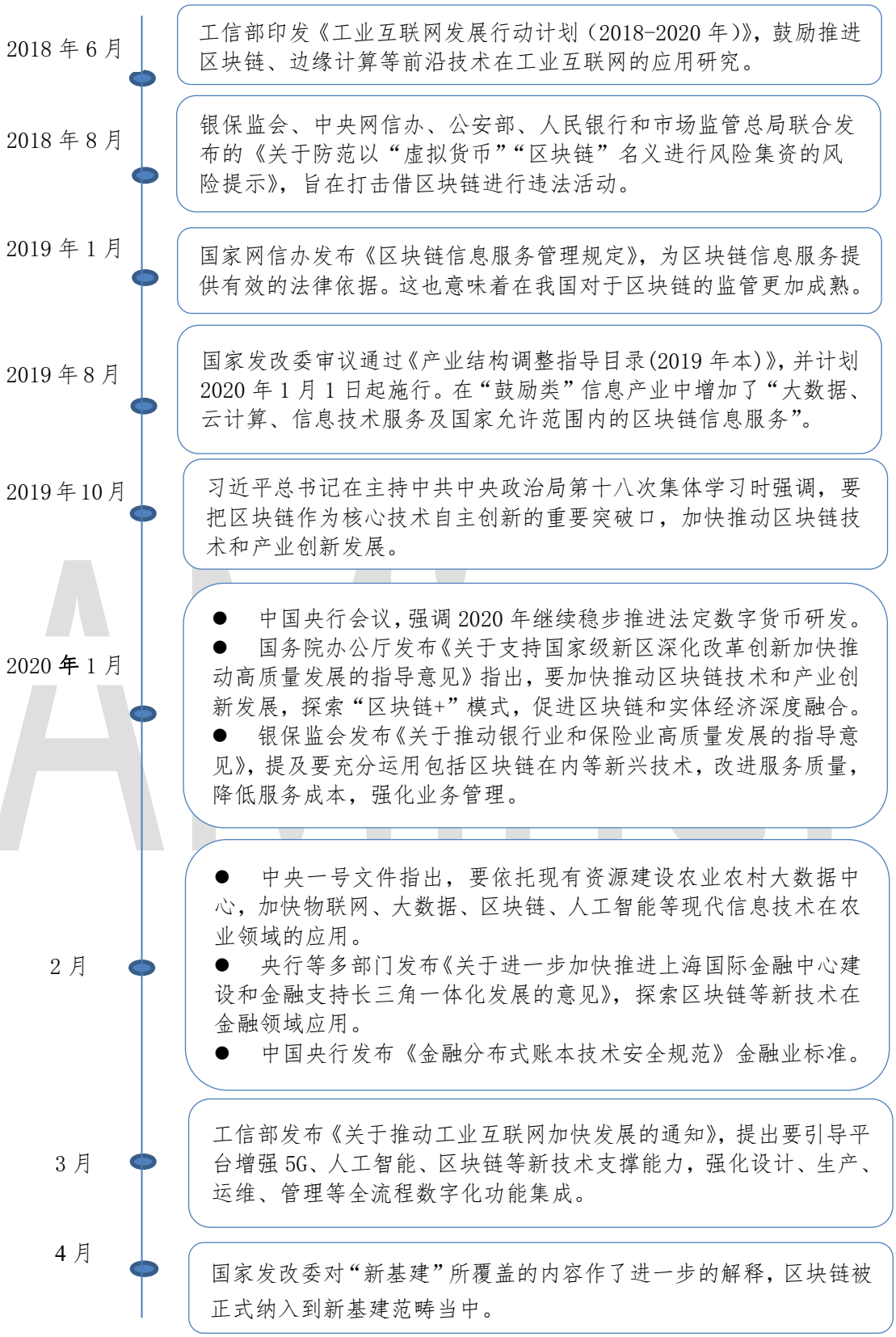
图 4　近年来国外主要国家的区块链相关政策动态

我国从 2013 年开始陆续出台虚拟货币监管政策，国内大众也逐渐对区块链的技术逻辑和底层价值开始了解。自 2016 年 10 月工业和信息化部发布《中国区块链技术和应用发展白皮书（2016）》及 2016 年 12 月区块链首次被作为战略性前沿技术写入国务院发布的《国务院关于印发“十三五”国家信息化规划的通知》以来，各地政府纷纷出台有关区块链的政策指导意见及通知文件。中国互联网金融协会也成立区块链研究工作组，深入研究区块链技术在金融领域的应用及影响。2017 年 5 月，中国电子技术标准化研究院联合数十家单位发布《中国区块链技术和产业发展论坛标准 CBD-Forum-001-2017》，为区块链的落地应用设定标准。

近两年来，中国区块链相关的最新政策动态如图 5 所示。从政策走向来看，我国政府对区块链发展的鼓励和促进发展态度更加明朗化。中国政府对区块链技术给予高度关注，已经于 2019 年将区块链技术上升为国家战略，并将其作为核心技术自主创新重要突破口。

2018 年，为了避免区块链被人利用、带来不利的社会影响，我国开展了打击借区块链之名进行违法行为的活动。随后几年，中国政府和监管部门积极支持区块链技术发展和应用落地。2019 年 1 月，国家互联网信息办公室发布《区块链信息服务管理规定》，为区块链信息服务提供有效的法律依据；同年 10 月 24 日，习近平在中共中央政治局第十八次集体学习时指出，要把区块链作为核心技术自主创新重要突破口，将区块链技术上升为国家战略。

2020 年以来，国务院办公厅发布了《关于支持国家级新区深化改革创新加快推动高质量发展的指导意见》，指出要加快推动区块链技术和产业创新发展，探索“区块链+”模式，促进区块链和实体经济深度融合。相关监管部门相继推进法定数字货币研发、农业区块链核心技术突破、基于区块链的全球航运服务网络平台研究应用，以及推进区块链在金融、在线教育等方面的应用。



来源：根据公开资料整理

图 5　2018-2020 年中国区块链发展相关政策动态

1.5.2 行业发展及市场规模

点对点传输、共识机制、加密算法、博弈论等基础技术及理论的发展与完善，为区块链技术取得进展奠定了坚实基础。国内外学者与科研机构对区块链领域的研究成果不断涌现，进一步助力区块链技术的完善与进化。日本经济贸易产业省《区块链技术及相关服务的调查报告（2015）》（Survey on Blockchain Technologies and Related Services FY2015 Report）、英国政府《分布式账本技术：超越区块链》（Distributed Ledger Technology: Beyond Blockchain）、中国工业和信息化部《中国区块链技术和应用发展白皮书（2016）》和《2018 年中国区块链产业白皮书》、工信部下属中国信通院《区块链白皮书》（2019）、CB Insights《区块链报告 2020》以及赛迪区块链研究院《2019-2020 年中国区块链年度发展报告》，均对区块链及技术发展最新动向进行跟踪总结。

随着区块链技术的发展，其在各行业的应用潜力逐渐得到释放。联合国、国际货币基金组织，以及美国、英国、日本等国家都对区块链的发展给予高度关注。

数据显示[8]，2019 年，全球区块链产业规模呈现稳定增长，达到 24.5 亿美元，产业年度增速为 30.6%。从国家来看，美国仍处于全球区块链产业的领导地位，规模为 7.3 亿美元，占全球区块链产业 29.9%；中国在全球区块链产业中占比为 12.1%，位居第二。我国区块链产业受国家政策的积极影响，2019 年的产业规模达 20.8 亿元（人民币），同比增长 179.5%。其中，广东省区块链产业规模达到 1.7 亿元，占中国区块链产业规模的 8.1%，位居国内第一。其次是浙江省、占比 7.3%，产业规模达 1.5 亿元，位居第二。北京市、江苏省、上海市分别位列第三至第五。

国内外先后成立各种类型的**区块链产业联盟**，协调推进区块链技术和应用发展。R3 区块链联盟于 2015 年 9 月成立，致力于为银行提供探索区块链技术的渠道和区块链概念产品。同年，Linux 基金会成立超级账本（Hyperledger），推进区块链数字技术和交易验证开源项目。中国先后成立中关村区块链产业联盟、中国分布式总账基础协议联盟（China Ledger）、金融区块链合作联盟（金链盟）

[8] 赛迪顾问数字经济产业研究中心，《2019-2020 年中国区块链产业发展研究年度报告》[R]，2020 年 2 月，http://www.mtx.cn/#/report?id=683815

和区块链微金融产业联盟（微链盟），积极探索推动区块链的应用。

区块链企业数量近年来增长放缓，行业发展逐渐回归理性。

有数据显示[9]，截至 2019 年 8 月全球区块链企业数量有 2450 家，其中美国区块链企业数量最多，占 21.8%；其次是中国，占 20.4%。从新增企业数量来看，2017 年全球区块链新增企业数量达到高峰，超过 600 家；2018 年全球新增区块链企业数量为 400 余家；2019 年以来全球区块链新增企业数量锐减，截至 8 月新增企业数量不足 50 家。

另一项数据显示[10]]，中国区块链行业在 2016 年之前，经营区块链相关业务的公司不足 1000 家，且数量增长缓慢；但从 2016 年开始，区块链公司数量也开始爆发式增长，连续两年增幅均超 250%，成为创业热门领域和资本热捧的目标。之后几年，区块链企业数量增长放缓。

从区块链企业的经营主体来看，国内外互联网、IT、金融等领域企业涉足区块链行业较早，着手研发或推出从基础设施到应用案例的一系列解决方案。**全球主流金融机构布局区块链**，2015 年 10 月，美国纳斯达克推出基于区块链技术的证券交易平台 Linq，进行金融证券市场去中心化的尝试。高盛、摩根大通、瑞银集团等银行业巨头分别各自成立各自的区块链实验室、发布区块链研究报告或申请区块链专利，并参与投资区块链初创公司。

国内从 2016 年开始，一些传统金融机构和金融科技企业就先后涉足区块链金融场景应用。目前，蚂蚁金服、腾讯、阿里巴巴、浪潮、京东和百度等重点企业在区块链专利、底层 BaaS 平台和行业解决方案均取得了一定成绩，主要布局在底层平台、行业应用以及区块链硬件三个方向[11]。

此外，**区块链初创公司及各类投资机构**也纷纷涉足区块链领域，为区块链技术落地提供资金支持。初创公司 Ripple Labs 致力于推动 Ripple 成为世界范围内各大银行通用的标准交易协议，使货币转账能像发电子邮件那样成本低廉、方便快捷；R3CEV 推出的 BaaS（Blockchain as a Service）服务，已与美国银行、

[9] 联合国向全球推荐支付宝区块链应用！中国区块链技术布局现状及发展趋势分析[J]，2020 年 3 月 24 日，艾媒网，https://www.iimedia.cn/c1020/70276.html

[10] 腾讯研究院.《2019 腾讯区块链白皮书》[R]，2020 年 10 月，https://tisi.org/11408

[11] 赛迪顾问数字经济产业研究中心，《2019-2020 年中国区块链产业发展研究年度报告》[R]，2020 年 2 月，http://www.mtx.cn/#/report?id=683815

花旗银行、招商银行等全球 40 余家大型银行机构签署区块链合作项目，致力于制定银行业的区块链行业标准与协议。

2　技术理论篇

区块链技术本身并不是一种全新的技术，而是集成了密码学、分布式系统、博弈论等多种技术的新型组合。本篇主要介绍了区块链所集成的密码学、分布式系统与共识机制、博弈论等技术和理论，同时，还介绍了以区块链为底层技术环境的智能合约技术，以及实现区块链互联互通、提升可扩展性的跨链技术。为了帮助读者更多了解区块链技术，本篇还拓展介绍了区块链领域必读论文和专利申请情况。

2.1 密码学

区块链系统中使用了大量的密码学知识，同时，区块链在不同场景的应用也促进了密码学的发展。早期密码学将通俗易懂的明文转换成为普通听众无法理解的密文，并设计特殊规则让合法听众将密文还原为明文。早期简单密码的设计体现在实现方式上，即通过替换、换位方式进行密码变化，如古罗马 Caeser 密码、法国 Vigenere 密码。

伴随着信息通信即计算机技术的飞跃式进步，密码学在实现效率和实现方式上均实现了前所未有的系统发展。1949 年，Shannon 发表“保密系统的通信理论”[12]，奠定密码学数学基础。1973 年，IBM 开发 Feistel 分组密码结构[13]，其物理上的对称性和反复性极大降低了对硬件实施中编码量和线路传输的要求，奠定了数据加密标准（Data Encryption Standard, DES）的结构基础。1976 年，Diffie 和 Hellman 提出“密码学新方向”[14]，打破 DES 加密安全性对密钥保密的依赖，开辟公钥密码理论，为密钥协商、数字签名技术提供新解法。

《中华人民共和国密码法》（简称《密码法》）于 2019 年十三届全国人大常委会第十四次会议表决通过，并于 2020 年 1 月 1 日正式施行。《密码法》明确规定，密码分为核心密码、普通密码和商用密码。国家对密码实行分类管理。其中，核心密码、普通密码属于国家秘密，用于保护国家秘密信息，都由密码管理部门依法实行严格统一管理。商用密码用于保护不属于国家秘密的信息，其广泛应用于国民经济和社会生产生活的方方面面，影响着老百姓的日常生活。

[12] Shannon C E. Communication theory of secrecy systems[J]. Bell Labs Technical Journal, 1949, 28(4): 656-715.
[13] Meyer C H. Design considerations for cryptography[C]//Proceedings of the June 4-8, 1973, national computer conference and exposition. ACM, 1973: 603-606.
[14] Diffie W, Hellman M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6): 644-654.

当前，中国国家密码局认定的国产商用密码算法已经形成一套完整体系：既有 SM1、SSF33、SM4、SM7、祖冲之密码算法等对称密码算法，又有 SM2、SM9 非对称密码算法，同时还有 SM3 杂凑密码算法[15]。其中，SM1 为对称加密算法，不公开，主要用于电子政务等加密；SM2 为非对称加密算法，公开，主要用于数字签名、密钥交换等加密；SM3 为哈希算法，SM4 是在国内广泛使用的 WAPI 无线网络标准中使用的加密算法。这几种国密算法满足多种密码应用的安全需求，为建设行业网络安全环境提供技术基础。

目前，密码学广泛应用于网络信息加解密、身份认证、数字签名，以及关于完整性、安全电子交易（Security Electronic Transaction,简称 SET）等的安全通信标准和网络协议安全性标准中[16]。

区块链的安全主要依赖于密码学技术。在基于区块链的交易中，确保交易数据安全和客户隐私是区块链能够进一步发展的必要条件[17]。密码学为区块链数据不可伪造、不可篡改、可公开验证和隐私保护提供了基础保障。密码学在区块链中的具体应用主要体现在防止交易数据被篡改，对网络节点进行数字身份认证，通过多重签名实现多人共同管理某个账户的比特币交易，以及使用同态加密技术提高用户隐私安全性等方面。

2.1.1 公钥密码体制

公共密钥密码体制于 1976 年提出，其原理是加密密钥和解密密钥分离。密码体制的基本模型如图 6 所示。

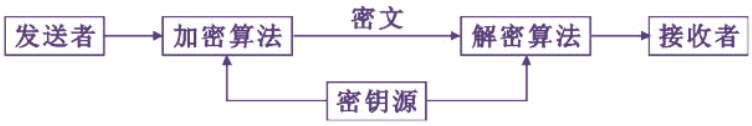


图 6　密码体制的基本模型

公钥加密流程如图 7 所示。用户可以将自己设计的加密密钥和算法公诸于众，而只保密解密密钥。任何人利用这个加密密钥和算法向该用户发送的加密信息，该用户均可以将之还原。消息发送者从密钥源得到密钥，通过加密算法对消

[15] 柳彩云,陈雪鸿,杨帅锋.国产密码算法与工业互联网平台的结合势在必行[J].中国信息安全,2019(04):86-89.
[16] 郑东，赵庆兰，张应辉.密码学综述[J].西安邮电大学学报，2013，18(06):1-10.
[17] 吴涛，王化群. (2017). 区块链中的密码学技术[J].南京邮电大学学报自然科学版，2017 年 12 月，Vol.37 No.6.

息进行加密得到密文；接收者收到密文后，利用从密钥源得到的密钥，通过解密算法对密文进行解密，得到原始消息。公共密钥密码的优点是不需要经安全渠道传递密钥，大大简化了密钥管理。

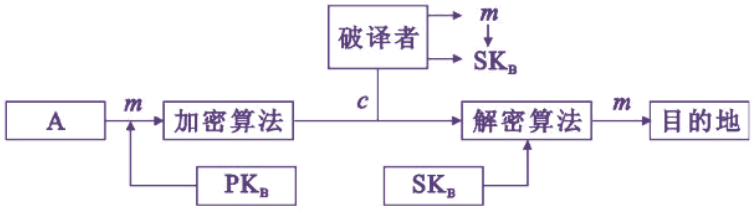


图 7　公钥加密流程

公钥密码体制的建立，对密码学具有革命性的意义。公钥密码体制分为对称密码体制和非对称密码体制。

在对称密码体制中，解密算法是加密算法的逆算法。也就是说，加解密过程使用的密钥具有唯一性，解密方必须事先知道加密密钥。这使得对称加密体制具有算法公开、加密速度快、加密效率高的优势。对称密码体制的加密流程如图 8 所示。另外，随着加密用户增加，密钥数量呈几何级数增长，密钥管理成本高，对称密码体制在分布式网络的应用受到阻碍。目前，广泛应用的对称密码体制有 DES、3DES、国际数据加密算法（International Data Encryption Algorithm, 简称 IDEA）、高级数据加密标准（Advanced Encryption Standard, 简称 AES）和国内的 SM1、SM4 等。

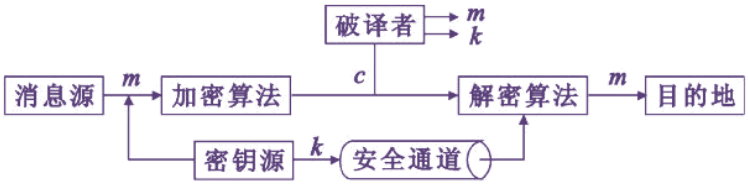


图 8　对称密码体制加密流程

在非对称密码体制中，公钥和私钥的配对使用是明文加解密的关键。公钥用于加密明文，私钥用于解密密文。若发信方（加密者）想发送只有收信方（解密者）才允许解读的信息，发信方必须首先知道收信方公钥，并利用此公钥加密；该份密文用且仅能用收信方的私钥解密。由此可见，非对称密码体制拥有两个密钥，且由公钥推出私钥在计算上是极为困难的，这也极大提高了数据加密安全性。目前，广泛应用的非对称密码体制有 RSA、椭圆曲线密码（Elliptic Curve Cryptography, ECC）等。

对称加密和非对称加密的加解密算法类型及其特征、优缺点及代表算法，如

表 4 所示。

表 4　加解密算法类型

算法类型	特点	优势	缺陷	代表算法
对称加密	加解密的密钥相同	计算效率高，加密强度高	需要提前共享密钥，易泄密	DES、3DES、AES、IDEA
非对称加密	加解密的密钥不相关	无需提前共享密钥	计算效率低，仍存在中间人攻击的可能性	RSA、Elgamal、椭圆曲线系列算法

数字签名应用了公钥密码体制，公钥加密系统的加入，保证了数字签名的不可伪造性和不可抵赖性。数字签名跟手写签名的作用实质上是一样的，用来证明某个消息或者文件是本人发出/认同的。我国在 2005 年就已经施行《电子签名法》，确立了电子签名（包括但不限于数字签名）的法律效力。《电子签名法》后于 2019 年 4 月 23 日第十三届全国人民代表大会常务委员会第十次会议进行了修正。

常见的签名算法有 RSA，DSA，ECDSA，其中 RSA 是实现数字签名最简单的公钥加密算法。RSA 既可以用公钥加密然后私钥解密，也可以用私钥加密然后公钥解密。因为 RSA 中的每一个公钥都有唯一的私钥与之对应，任一公钥只能解开对应私钥加密的内容。

如果某用户生成了一对 RSA 密钥，可以把公钥向全世界公布出去。之后该用户只要在发送的消息，比如“abcd”，后面加上用私钥加密过的密文，其他人拿公钥解密，看解密得到的内容是不是“abcd”就可以知道这个“abcd”是不是该用户发的。其他人没有对应的私钥，没法生成公钥可以解密的密文，所以是不可伪造的。又因为公钥对应的私钥只有一个，所以只要能成功解密，那么发消息的一定是该用户，而不会是其他人，所以是不可抵赖的。

数字签名的用途很多，最常见的用处就是用来认证一个网站的身份，比如百度主页的数字签名证书，如图 9 所示。

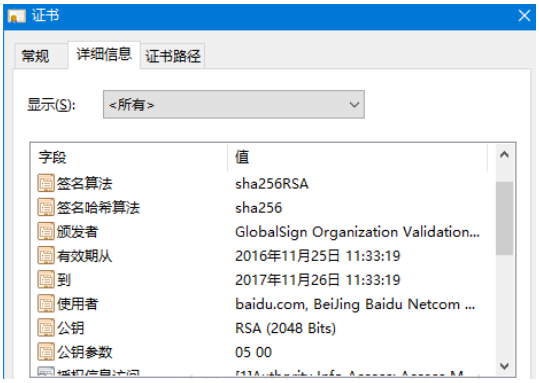


图 9　百度数字签名证书页面

除此之外，代码签名也是其重要的用途。如果 Windows 上的可执行程序来源于正规公司，那么通常它会有代码签名，用于确保其来源可靠且未被篡改。

2.1.2 哈希函数

哈希函数（Hash Function），也称散列函数，是一种在有限合理的时间内，将任意长度消息压缩为固定长度的消息摘要的函数。哈希函数是用于实现数据完整性和实体认证的算法。哈希函数的表示形式为：

$$h = H(m)$$

其中，h为固定长度的哈希值，m为任意长度消息，H为哈希函数。

MD5（Message Digest Algorithm 5）是 1991 年由 Rivest 开发出的在计算机领域广泛使用的散列函数[18]，提供将大容量信息在用数字签名软件签署私钥前被压缩成一定长度二进制数据。美国联邦信息处理公开标准文件（FIPS 180-2）定义了四种安全的哈希算法：SHA-1，SHA-256，SHA-384，SHA-512[19]，每种算法都是某种单项哈希函数的迭代过程。这些哈希函数可以处理任意长度的消息输入，形成“消息摘要”（Message Digest）。在我国，由密码学学者王小云和国内其他专家设计的哈希函数算法标准 SM3 于 2010 年 12 月 17 日发布，已被广泛应用于数字签名及验证、消息验证码生成及验证、随机数生成，为超过 6 亿智能电网用户和上亿银行卡提供保护。

[18] Rivest R. The MD5 message-digest algorithm[J]. 1992.
[19] FIPS N. 180-2: Secure hash standard (SHS)[J]. US Department of Commerce, National Institute of Standards and Technology (NIST), 2012.

表 5　典型散列算法特点

加密算法	安全性	运算速度	输出大小（位）
MD5	低	快	128
SHA1	低	中	160
SHA256	高	比 SHA1 略低	256
SM3	高	比 SHA1 略低	256

具体而言，如表 5 所示的四种算法均包含两个处理阶段：预处理（Preprocessing）和哈希计算（Hash Computation）。预处理进行消息填充、分割已填充消息、设置哈希计算初始化值等工作，而哈希计算则利用预处理消息迭代生成一系列连续哈希值，即消息摘要（Message Digest）。

哈希函数具有如下特性：

- **正向快速**：给定明文和 Hash 算法，在有限时间和有限资源内能计算出 Hash 值；
- **逆向困难**：给定了若干 Hash 值，在有限时间内很难（基本不可能）推出明文；
- **输入敏感**：一旦原始输入信息做出一点修改，产生的 Hash 值应该有很大不同；
- **冲突避免**：很难找到两段内容不同的明文，使得它们的 Hash 值一致（发生冲突）。

区块链系统各节点通过一定的共识机制选取具有打包交易权限的区块节点，该节点需要将新区块的前一个区块的哈希值、当前时间戳、一段时间内发生的有效交易及其梅克尔树根植等内容打包成一个区块，向全网广播。对原数据的任何改动，都将生成不同的消息摘要，这就使得该算法充分保证原数据的完整性。正是由于上述重要特性，哈希算法被广泛应用于生成和验证数字签名、消息认证码、随机数产生、错误校正与检测等领域。

2.1.3 密码学研究热点

密码学作为区块链重要理论基础，具有一个完备而复杂的知识体系，涵盖了

庞大的知识图谱，这些学科的发展支撑了现代密码学研究的爆发式增长。数论、线性代数、信息论、近世代数为密码学的发展奠定了基础。

从密码学的近期研究趋势来看，如图 10 所示，Elliptic Curve（椭圆曲线）、Hash Function（哈希函数）、Public Key（公钥）、Data Security（数据安全）、Key Distribution（密钥分配）、Encryption（加密）、Access Control（访问控制）、Data Privacy（数据隐私）、Network Security（网络安全）、Digital Signature（数字签名）是近期学者关注的焦点。在传统热点之下也有许多具有潜力的研究方向逐渐浮出水面，受到各国学者越来越多地关注。其中，Hash Function（哈希函数）和 Elliptic Curve（椭圆曲线）加密受到学者们高度关注。曾经发展势头强劲的话题 public key（公钥）的热度却出现大幅下滑。

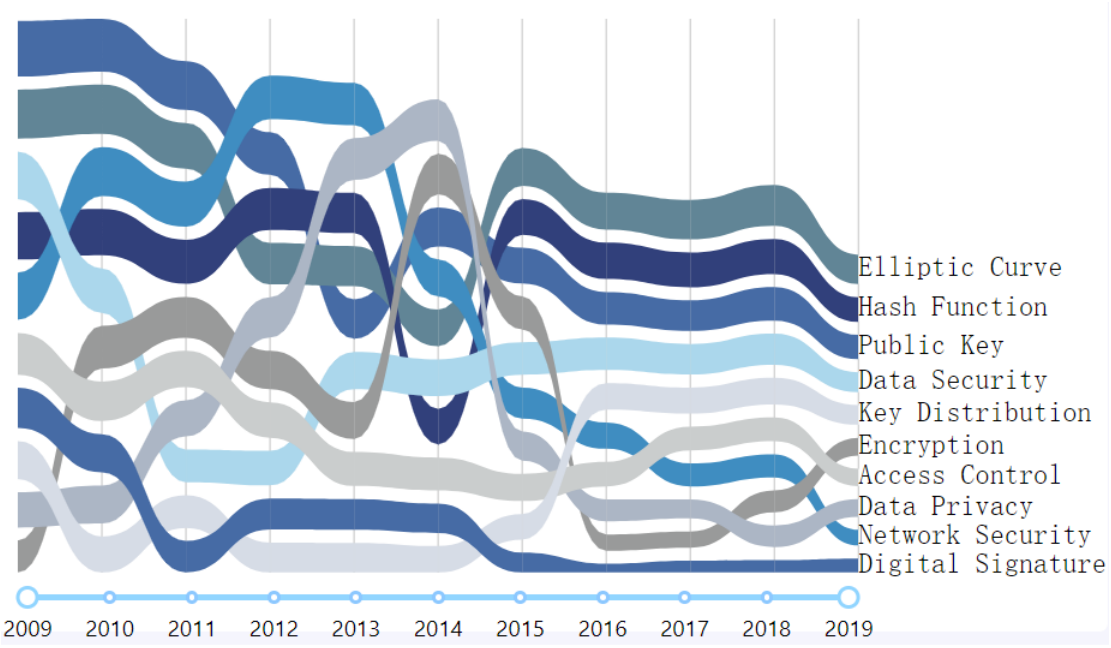


图 10　密码学研究技术热点

2.2 分布式系统与共识协议

分布式系统（distributed system）是建立在网络之上的软件系统。分布式系统的出现是为了利用更多机器完成单个计算机无法完成的数据计算、存储任务。

分布式系统具有三大优点：一是充分利用各个分布节点的资源；二是多节点协同工作可以提升工作效率；三是安全性高，可以避免由于单个节点失效而使整个系统崩溃的风险。

分布式系统是区块链的基础思想，主要体现在分布式记账和分布式存储两方面。分布式记账，是指每个参与系统的记账节点都可以记账，且记录可以追溯

查询，但不可篡改。但分布式并不是说任何系统的所有节点都会有记账权，根据不同的共识机制，能参与记账的节点类型是有所不同的[20]。例如，在 POW 共识机制下，每个节点都可能取得比特币的记账权，在完成工作量证明后，第一时间让全网认可，即确定了记账的有效性。在 DPOS 共识机制下，只能那些被选举出来的超级节点才有记账权；在 RPCA（Ripple Protocol Consensus Algorithm，瑞波共识机制）下，只有那些信任节点才有记账的权力。

区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。数据节点可以是不同的物理机器，也可以是云端不同的实例[21]。

共识协议或共识平台是分布式账本技术的核心。分布式账本能在点对点（Peer to Peer,简称 P2P）网络中的不同节点之间相互复制，且各项交易均由私钥签署。区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。如何在分布式系统中高效地达成共识，是分布式计算领域的重要研究问题。决策权越分散，系统达成共识的效率越低，但系统稳定性和满意度则越高；与此相对，决策权越集中，系统更易达成共识，但同时更容易出现独裁。

区块链的分布式存储的独特性体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据；二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，数据节点可以是不同的物理机器，也可以是云端不同的实例。区块链解决的核心问题之一，就是通过决策权高度分散的“去中心化”系统提升稳定性和满意度，使各节点针对区块数据的有效性达成共识。

2.2.1 共识机制的功能

共识机制的主要功能是维持区块链上账本的相同这一基本问题。区块链系统中，每一个网络节点都将各自独立维护一份区块链账本。为了避免不同的区块链

[20] 分布式系统与区块链[N]，链圈社区，2018 年 11 月 6 日，https://www.jianshu.com/p/ed75c125bb29
[21] 区块链技术的核心[Online]，swift_kotlin，2018 年 1 月 7 日，https://www.jianshu.com/p/df19e23ce349

账本出现数据混乱的问题，必须要设计公平的挑选机制，每次只挑选一个网络节点负责写入数据。当被挑选的网络节点写入数据后，其他网络节点必须能够准确及时地进行数据同步。为了避免网络中出现伪造、篡改新增数据的情况，必须设计可靠的验证机制，使所有网络节点能够快速验证接收到的数据是由被挑选的网络节点写入的数据[22]。

2.2.2 共识机制的分类

共识协议要解决的核心问题是在网络中有节点作恶时如何能够达成共识。要解决这个困难，首先需要了解“拜占庭将军问题”。1982 年，Leslie Lamport、Robert Shostak 和 Marshall Pease 发表论文《拜占庭将军问题》[23]，提出一项思维实验：假设一组将军分别统领拜占庭军队的一部分，共同围困一座城市。这些将军只能通过信使将自己的策略相互传递。但是，这组将军中有一人或多人可能已经叛变，并试图传递错误信息以破坏作战计划。该实验的问题就在于，这支军队最多允许存在多少名叛变的将军，使得作战仍然可以顺利完成？数字货币运行机制可类比于拜占庭将军问题场景。在分布式账本中，各参与者节点可近似看作将军。此问题即转化为，分布式系统可容许多少作恶节点，使得交易仍可正常进行，且不损害整体系统的可靠性？Lamport 本人已经给出了达到拜占庭容错的架构[24]，但算法复杂，难以投入应用。此后，Miguel Castro 和 Barbara Liskov 于 1999 年提出实用拜占庭容错算法（PBFT）[25]，此系统能够提供高性能的运算，可以每秒处理成千的请求。比特币系统则利用去中心化的点对点加密协议运行区块链，实现了无需信任单个节点即可达成共识和建立互信。

除了拜占庭问题外，Sybil 攻击也是共识机制解决的重要问题之一。**Sybil 攻击**，又称女巫攻击，是指社交网络中的少数节点通过控制多个虚假身份来影响网络中的正常节点。Sybil 攻击原理如图 11 所示。具体来说，这些少数节点可能会对一个点对点网络呈现多个身份，且以不同节点的功能进行活动。因此，这些节点可能在网络上获得不成比例的控制权，随后做出恶意行为，如影响投票结

[22] CCF 区块链专业委员会，《区块链关键技术研究进展》[C]，2019 年 7 月.
[23] Lamport L, Shostak R, Pease M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, 4(3): 382-401.
[24] Pease M, Shostak R, Lamport L. Reaching agreement in the presence of faults[J]. Journal of the ACM (JACM), 1980, 27(2): 228-234.
[25] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//OSDI. 1999, 99: 173-186.

果、降低点对点网络节点查找效率、破坏网络文件共享安全、消耗节点链接资源等。Sybil 攻击最早由学者 Douceur 在点对点网络环境中提出[26]，他指出这种攻击方式将破坏分布式存储系统中的冗余机制。此后，一些学者如 Karlof[27]和 Newsome[28]发现 Sybil 攻击对传感器网络的路由机制同样存在威胁。Sybil 攻击能够对网络产生多大程度的影响，取决于攻击节点能够以多低成本产生虚假身份。Sybil 攻击只能控制单个节点，对全网的影响相对较小；但是，在 Sybil 攻击的基础上产生的 Eclipse 攻击和 DDoS 攻击，则会使部分节点脱离点对点网络，甚至占用大量受害节点资源，对全网造成致命打击。

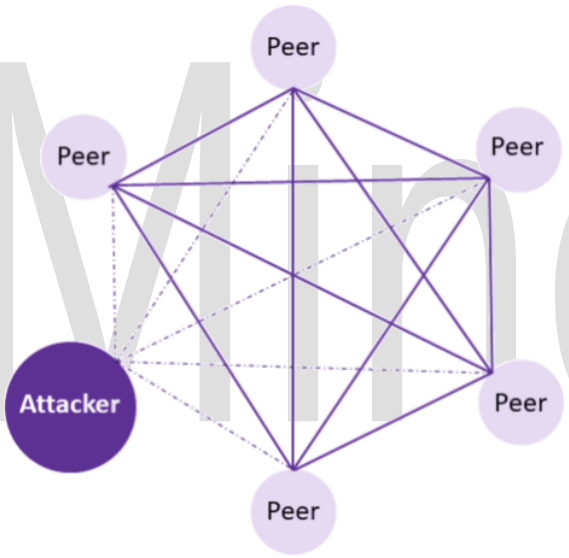


图 11　基于点对点网络的 Sybil Attack 原理

Sybil 攻击产生影响的方式主要为破坏信任、控制资源和低成本地加入网络。因此，防御 Sybil 攻击，也可以从信任认证、资源测试、提高节点加入网络代价三方面入手。工作量证明（Proof of Work,简称 PoW）是抵御 Sybil 攻击的有效方式。PoW 机制能够实现区块链的一致性，由于网络中每个节点完成工作量的证明由其拥有的计算资源决定，因此攻击节点不能通过创建多个虚假身份提高自身完成工作量证明的概率，也就有效抵御了 Sybil 攻击。

在分布式账本之中，共识机制使大部分（或全部）网络成员就某条数据或拟

[26] Douceur J R. The sybil attack[C]//International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002: 251-260.
[27] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures[J]. Ad hoc networks, 2003, 1(2-3): 293-315.
[28] Newsome J, Shi E, Song D, et al. The sybil attack in sensor networks: analysis & defenses[C]//Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004: 259-268.

定交易达成一致，并就此对账本进行更新的机制。换言之，共识机制是在参与节点之间管理一系列连贯实施操作的规则。

共识算法允许关联机器连接起来进行工作，并在某些成员失效的情况下，工作仍能正常进行。这种容错能力是区块链与分布式账本的另一主要优势，并有内置冗余余量以作备用。

用以建立共识的算法是多种多样的，并建立基于性能、可扩展性、一致性、数据容量、治理、安全性和失效冗余等方面的要求。目前，广泛应用的共识机制包括 PoW、PoS、DPoS 和 PBFT 等，如表 6 所示。

表 6　共识机制及技术水平

共识机制	技术水平	应用场景
PoW	依赖机器进行数学运算获取记账权，资源消耗相比其他共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性较高。	公有链
PoS	主要思想是节点记账权的获得难度与节点持有的权益成反比。相对于 PoW，一定程度上减少了数学运算带来的资源消耗，性能也得到相应提升但依然基于哈希运算竞争获取记账权的方式，可监管性弱，容错性较高。	公有链
DPoS	与 PoS 主要区别在于节点选举若干代理人，由代理人验证和记账，其合规监管、性能、资源消耗和容错性与 PoS 相似。	公有链
PBFT	采用许可投票、少数服从多数来选举领导者进行记账，但该共识机制允许拜占庭容错，允许强监管节点参与，具备权限分级能力，性能更高，耗能更低。该算法每轮记账都会由全网节点共同选举领导者，允许 33%的节点作恶，容错性为 33%。	许可链
VRF	弥补了 DPoS 下相对中心化的选举所带来的弊端，同时保留了 DPoS 具备较高的效率和性能的优点，很好地兼顾了去中心化和性能。VRF 机制本身并不足以保证足够多的诚实节点进入委员会，所以往往需要 PoW 或者 PoS 等机制的配合以防范女巫攻击（恶意节点虚构出多个身份参与网络以增加自己比重）。	公有链
Sharding	将数据库分割成多个分片并放置在不同的服务器上，即将网络中的工作分摊给所有参与的节点。缺点是系统复杂度高。	公有链/许可链

Raft	相对清晰易懂，易于实现并且能够提供优异的性能，被工业界广泛采用。其核心流程可分为 Leader 选举和日志同步。	私有链
Tendermint	区块成为了共识的基本单位。借助区块链的链式特点，共识流程得以被充分简化，算法复杂度也得以被进一步降低。	公有链/许可链
HotStuff	相对于 Tendermint，提高了系统的性能，简化了共识流程。同时，可以支持更大的网络规模。	公有链/许可链

根据应用条件，共识机制可以分为：没有节点作恶和有节点作恶两类，如表 7 所示。

表 7　共识机制分类

应用条件	共识机制
没有节点作恶	Paxos、Raft、ZooKeeper、ViewTimestamp Replication
有节点作恶	PBFT、PoW、PoS、DPoS、Algorand、Sleepycat、SnowWhite

根据区块链系统如何选取记账节点，共识机制又可以分为选举类、证明类、随机类、联盟类和混合类五种类型[29]：

- 选举类共识是指矿工节点在每一轮共识过程中通过“投票选举”方式选出当前轮次的记账节点，首先获得半数以上选票的矿工节点将会获得记账权。如 PBFT、Paxos 和 Raft 等。
- 证明类共识被称为“Proof of X”类共识，即矿工节点在每一轮共识过程中必须证明自己具有某种特定的能力，证明方式通常是竞争性地完成某项难以解决但易于验证的任务，在竞争中胜出的矿工节点将获得记账权。例如 PoW 和 PoS 共识算法等。
- 随机类共识是指矿工节点根据某种随机方式直接确定每一轮的记账节点，例如 Algorand 和 PoET 共识算法等。
- 委任类共识是指矿工节点基于某种特定方式首先选举出一组代表节点，而后由代表节点以轮流或者选举的方式依次取得记账权。例如 DPoS 等。
- 混合类共识是指矿工节点采取多种共识算法的混合体来选择记账节点，

[29] CCF 区块链专业委员会，《区块链关键技术研究进展》[C]，2019 年 7 月.

例如 PoW+PoS 混合共识、DPoS+BFT 共识等。通过结合多种共识算法，能够取长补短，解决单一共识机制存在的能源消耗与安全风险问题。

2.2.3 共识机制的评价

不同的共识机制会对区块链系统整体性能产生不同影响。因此，评价共识机制技术水平，通常从安全性、扩展性、性能效率和资源消耗四个方面入手，如表 8 所示。

表 8　共识机制评价维度

评价维度	含义
安全性	即是否可以更好地防止二次支付、自私挖矿等攻击，是否有良好的容错能力。自私挖矿通过采用适当的策略发布自己产生的区块，获得更高的相对收益，是一种威胁比特币系统安全性和公平性的理论攻击方法。
扩展性	即是否支持网络节点扩展。扩展性是区块链设计要考虑的关键因素之一。根据对象不同，扩展性又分为系统成员数量的增加和待确认交易数量的增加两部分。扩展性主要考虑当系统成员数量、待确认交易数量增加时，随之带来的系统负载和网络通信量的变化，通常以网络吞吐量来衡量。
性能效率	即从交易达成共识被记录在区块链中至被最终确认的时间延迟，也可以理解为系统每秒可处理确认的交易数量。区块链技术通过共识机制达成一致，因此其性能效率问题一直是研究的关注点。
资源消耗	即在达成共识的过程中，系统所要耗费的计算资源大小，包括 CPU、内存等。以比特币系统为例，基于工作量证明机制的共识需要消耗大量计算资源进行挖矿，提供信任证明完成共识。

2.2.4 分布式系统研究热点

从分布式系统的近期研究趋势来看，如图 12 所示，Multi-Agent System（多代理系统）、Spatial Distribution（空间分布）、Probability Distribution（概率分布）、System Performance（系统性能）、Distributed Control（分散式控制）、Distributed System（分布式系统）、Reliability（可靠性）、Distributed Generation（分布式发电）、Distributed Computing（分布式计算）、Distributed Processing（分布式处理）是近期学者关注的焦点。其中，Distributed System（分布式系统）和 Distributed Computing（分布式计算）的研究热度近年来有所下降。Multi-Agent System（多代理系统）研究热度不断升温。

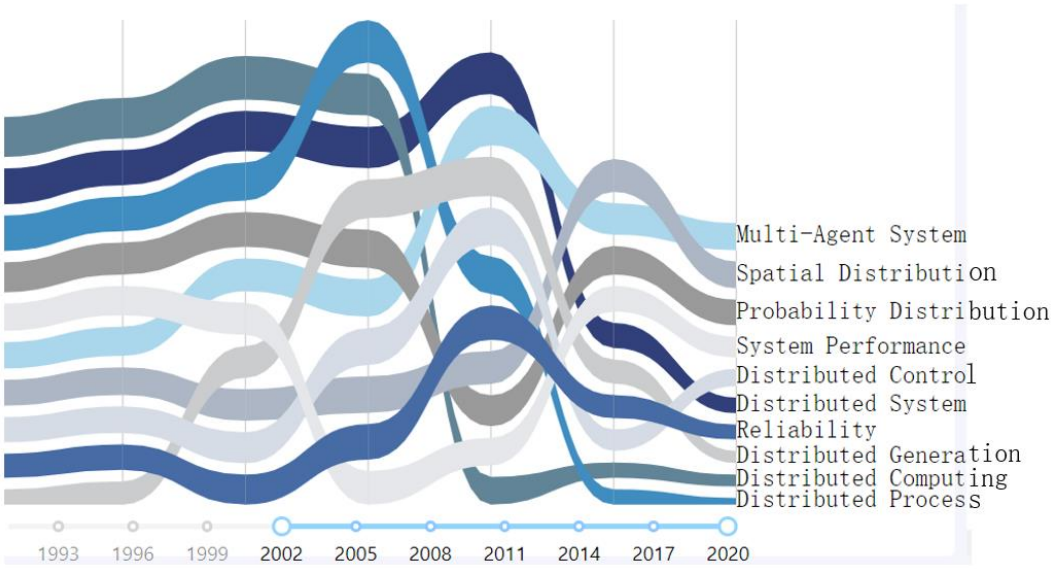


图 12　分布式系统领域研究热点

2.3 博弈论

博弈论，也称为“对策论”“赛局理论”，是研究决策主体行为发生直接相互作用的时候的决策以及这种决策的均衡问题，具有斗争或竞争性现象的数学理论和方法。最初，博弈被视为与“赌博”相关，而后成为数学的分支学科，博弈论被用于分析经济现象，随后又被理解为策略互动、思维方式和研究工具。博弈论考虑游戏中的个体的预测行为和实际行为，并研究它们的优化策略。

近代对于博弈论的研究，开始于冯·诺伊曼（Von Neumann）。1928 年，冯·诺依曼证明了博弈论的基本原理，从而宣告了博弈论的正式诞生。1944 年，冯·诺依曼和摩根斯坦共著的划时代巨著《博弈论与经济行为》将二人博弈推广到 n 人博弈结构并将博弈论系统地应用于经济领域，从而奠定了这一学科的基础和理论体系。1950 至 1951 年，纳什利用不动点定理证明了均衡点的存在，为博弈论的一般化奠定了坚实的基础，其开创性论文《n 人博弈的均衡点》（1950）[30]，《非合作博弈》（1951）[31]，给出了纳什均衡（Nash Equilibrium）的概念和均衡存在定理。所谓纳什均衡，指的是在策略组合上，任何参与人单独改变策略都不会得到好处；也就是说，如果在一个策略组合上，当所有其他人都不改变策略时，没有人会改变自己的策略，则该策略组合就是一个纳什均衡。纳什均衡的重要性

[30] Nash J F. Equilibrium points in n-person games[J]. Proceedings of the national academy of sciences, 1950, 36(1): 48-49.
[31] Nash J. Non-cooperative games[J]. Annals of mathematics, 1951: 286-295.

体现在两方面：其一，纳什均衡是其他所有均衡概念的基础，博弈逻辑的核心就是寻求纳什均衡；其二，纳什均衡描述了参与者为了达到自身利益的最大化，必须采用合作来达到一直稳定最大收益函数，每个参与人的策略是对其他参与人策略的最优反应。纳什均衡策略比冯·诺依曼的标准更加一般化，开启了非合作博弈的里程碑。

法国博弈论专家克里斯汀·蒙特（Christian Montet）和丹尼尔·塞拉（Daniel Serra）在 2011 年出版的《博弈论与经济学》专著中这样定义:“博弈”这个词应理解为明智的、理性的个人或群体间冲突与合作的情形[32]；1994 年诺贝尔经济学奖获得者豪尔绍尼（John C. Harsanyi）在获奖词中给出这样的解释：“博弈论是关于策略相互作用的理论，就是说，它是关于社会形势中理性行为的理论，其中每个局中人对自己行为的选择必须以他对其他局中人将如何反应的判断为基础”。2005 年诺贝尔经济学奖获得者罗伯特·奥曼（Robert J. Aumann）将“博弈”定义为策略性的互动决策[33]。

在 Niyato 和 Ekram Hossain 共同发表的论文《认知无线电网络中频谱共享的竞争性定价：动态博弈、纳什均衡的不足和共谋》[34]中，解决了认知无线电网络中的频谱定价问题。在这个网络中，多个主要服务提供商相互竞争，为次要用户提供频谱访问机会。在服务质量（QoS）约束下，各主要服务提供商均以利润最大化为目标，采用均衡定价策略。他们利用贝特朗博弈模型，分析了频谱可替代性、信道质量等系统参数对纳什均衡的影响，并提出了一种分布式算法来求解这个动态博弈。他们研究了动态博弈算法收敛于纳什均衡的稳定性，并表示在初级服务提供者的总利润没有最大化的情况下，纳什均衡是低效的，提出可以得到总利润最高的最优解决方案是将主要服务之间相互勾结，从而获得比纳什均衡更高的利润。但是，他们补充道，由于一个或多个主要服务提供者可能偏离最优解决方案，因此可以对偏离的主要服务提供者应用惩罚机制，并制定了一级服务提供者之间的重复博弈，说明如果所有一级服务提供者都知道这种惩罚机制，就可以维持共谋，适当衡量自己未来可获得的利润。

[32] Montet C, Serra D. Game theory and economics[M]. New York: Palgrave macmillan, 2003.
[33] Aumann R J. Game theory[J]. The New Palgrave Dictionary of Economics, 2017: 1-40.
[34] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of Nash equilibrium, and collusion," [J] IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 192-202, January 2008.

今天，博弈论已发展成一门较完善的学科。博弈论提供了一种计算各种可能决策所产生效益的数学方法，该理论为在各种竞赛性场合做出最佳决定建立了一套具体的数学公式。正如经济学家赫伯特·金迪斯（Herbert Gintis）所说，博弈论是我们“研究世界的一种工具”。但它不仅仅是一种工具，“它不仅研究人们如何合作，而且研究人们如何竞争”。同时，“博弈论还研究行为方式的产生、转变、散播和稳定”。

从博弈论的角度看，去中心化的、具有分布式共识、交易权利均等的区块链系统其实是一个达到纳什均衡的共识系统。博弈论可以用来分析区块链中的共识节点的策略以及它们之间的相互作用[35]。比特币引入了节点竞争记账权的方式，即俗称的“挖矿”，竞争获胜者获得区块记账权并且获得区块奖励。节点之间可以学习和预测彼此的挖掘行为，从而在均衡分析的基础上获得最优的反应策略。此外，博弈论可以用来开发激励机制，阻止节点执行不当行为或发起攻击。而比特币 51%攻击之所以没有发生，并不是这些矿池掌控人的道德高尚，而是这些矿池经过计算，发现挖矿收益高于攻击收益，所以才选择维系比特币系统而非破坏它。这其实也是博弈论在起作用。

从博弈论的近期研究趋势来看，如图 13 所示，Nash Equilibrium（纳什均衡），Evolutionary Game Theory（进化博弈论），Pricing（定价），Economics（经济学），Resource Allocation（资源分配），Resource Management（资源管理），Supply Chain（供应链），Optimization（优化），Cognitive Radio（认知无线电），Decision Theory（决策理论）是近期学者关注的焦点。博弈论的研究热点方向更多是其在经济、通信等领域的具体应用。

[35] Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y. C., & Kim, D. I. (2019). A survey on applications of game theory in blockchain. [J] arXiv preprint arXiv:1902.10865.

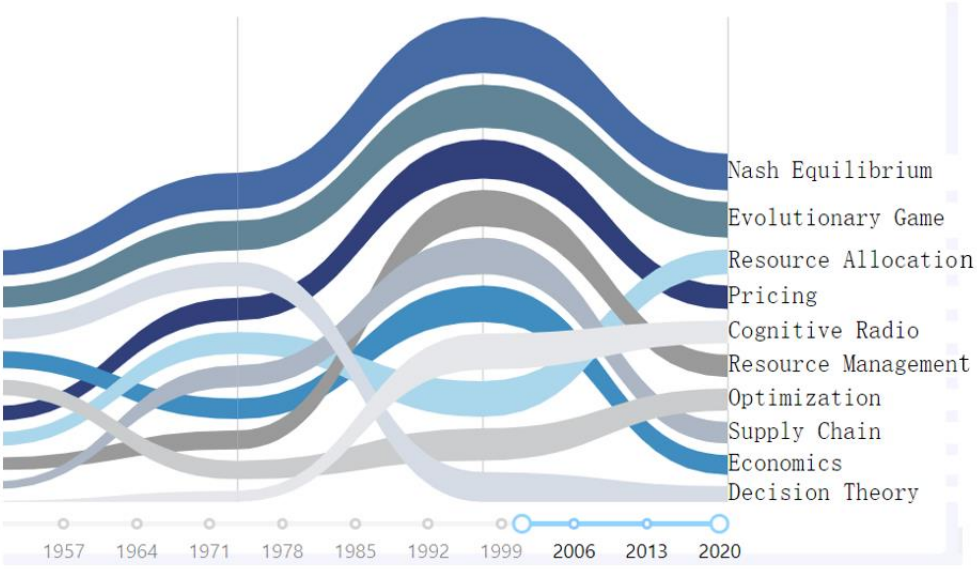


图 13　博弈论研究热点

2.4 智能合约

智能合约（Smart Contract）的概念可以追溯到 1994 年，是由美国跨领域学者尼克·萨博（Nick Szabo）提出并定义为“一个智能合约是一套以数字形式定义的承诺（Promises），包括合约参与方可以在上面执行这些承诺的协议[36]。”由于缺少可信的执行环境，智能合约当时并没有被应用到实际产业中。

比特币诞生后，其底层技术区块链可以为智能合约提供可信的执行环境。以太坊作为世界上首个内置了图灵完备编程语言并正式引入智能合约概念的公有区块链,是目前最为流行的智能合约开发平台[37]。于是，智能合约随着区块链技术的深入发展而受到广泛关注和研究。不同平台上智能合约的运行机制不同,以太坊和超级账本是目前应用最广泛的两种智能合约开发平台。

智能合约是一种由事件驱动的、具有状态的代码合约和算法合同,智能合约利用协议和用户接口完成合约过程的所有步骤,允许用户在区块链上实现个性化的代码逻辑。智能合约程序是一个可以自动执行的计算机程序，同时它自己也是一个系统参与者，可以接收发送信息以及储存价值。

[36] Szabo N. Smart contracts[Online], avaliable: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, November 5, 2018

[37] 欧阳丽炜, 王帅, 袁勇, 倪晓春, 王飞跃. 智能合约:架构及进展[J]. 自动化学报, 2019, 45(3): 445-457. doi: 10.16383/j.aas.c180586，http://html.rhhz.net/ZDHXBZWB/html/2019-3-445.htm

智能合约一般具有值和状态两个属性，代码中用 If-Then 和 What-If 语句预置了合约条款的相应触发场景和响应规则，智能合约经多方共同协定、各自签署后随用户发起的交易提交，经 P2P 网络传播、矿工验证后存储在区块链特定区块中，用户得到返回的合约地址及合约接口等信息后即可通过发起交易来调用合约。矿工受系统预设的激励机制激励，将贡献自身算力来验证交易，矿工收到合约创建或调用交易后在本地沙箱执行环境（如以太坊虚拟机）中创建合约或执行合约代码，合约代码根据可信外部数据源和世界状态的检查信息自动判断当前所处场景是否满足合约触发条件以严格执行响应规则并更新世界状态。交易验证有效后被打包进新的数据区块，新区块经共识算法认证后链接到区块链主链，所有更新生效[38]。

基于区块链的智能合约技术具有去中心化、自治化、可观察、可验证、可信息共享等特点，可以有效构建可编程金融和可编程社会[39]。智能合约是基于可信的不可篡改的数据，可以自动执行一些预先定义好的规则和条款。

智能合约研究主要包括合约编码、合约性能、合约安全性以及合约隐私问题。针对智能合约存在的隐私、安全、性能以及统一标准等问题，随着区块链技术的研究进展和突破，国内越来越多的学者也在关注着智能合约的优化研究。但总体来看，有关智能合约的研究还处于起步阶段，特别是智能合约的优化方面，还没有形成有效的方法[40]。

智能合约是个较细分的研究领域。从智能合约领域的近期研究趋势来看，如图 14 所示，Contract Design（合约设计）、Contract Net Protocol（合同网络协议）、Performance Measurement（绩效评估）、Contract Theory（契约论）、Contract Performance（合同履行）、Contract Security（合约安全）是近期学者关注的几个研究焦点。

[38] 欧阳丽炜, 王帅, 袁勇, 倪晓春, 王飞跃. 智能合约:架构及进展[J]. 自动化学报, 2019, 45(3): 445-457. doi: 10.16383/j.aas.c180586，http://html.rhhz.net/ZDHXBZWB/html/2019-3-445.htm

[39] 贺海武，延安，陈泽华.基于区块链的智能合约技术与应用综述[J]，《计算机研究与发展》.2018 年 11 期

[40] 斯雪明、孙毅、祝烈煌、朱建明等.（2019），区块链关键技术研究进展，CCF 区块链专业委员会[C]，https://www.ccvalue.cn/article/203469.html

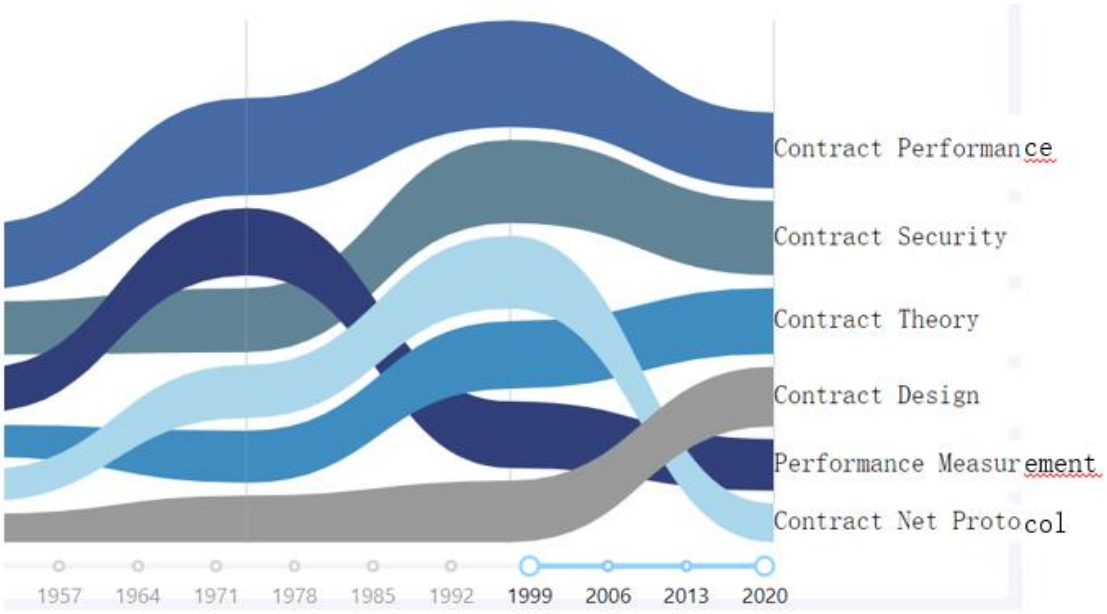


图 14　智能合约领域研究热点趋势

2.5 跨链技术

随着不同特点、不同应用场景的区块链快速发展，以及公有链、私有链、联盟链大量共存，现存各区块链之间的数据通信、价值转移面临着因相互独立而导致价值孤岛现象的挑战。基于此需求，跨链技术逐渐发展起来。跨链技术是区块链实现互联互通、提升可扩展性的重要技术手段。它既是区块链向外拓展和连接的桥梁，也是实现价值网络的关键。

代表性的区块链跨链技术如下。

1.Ripple

Ripple 公司主导设计发起了互联账目协议 Interledger Protocol(简称 ILP)实现跨链交易转账。通过 Ripple 协议实现跨境转账,将大大降低所需的手续费,统计 Ripple 网络事实清算将大大提高交易处理效率。它将实现不同账本之间的连接从而创造账本之间的协作。Interledger 协议适用于所有记账系统、能够包容所有记账系统的差异性，ILP 推出的目标就是打造全球统一支付标准，创建统一的网络金融传输的协议。

Ripple 提供了三种解决方案：协助银行处理全球支付的 xCurrent、为支付服务商提供流动性的 xRapid 以、协助普通公司接入瑞波网进行支付的 xVia。2014 年开始，Fidor 银行、Cross River 银行、CBW 银行等金融机构接入 Ripple 协议。现在 Ripple 生态已较为成熟了，越来越多的金融机构与 Ripple 保持合作

关系，但是由于 Ripple 主要解决跨境转账的问题，而且 ILP 需要公证人，Ripple 在跨链通信上没有更多的进展。

2.侧链技术

狭义的侧链技术指以锚定某种原链（主要是比特币区块链）为基础的新型区块链。广义的侧链技术是指为了解决现有区块链可拓展性问题、延伸性问题以及互操作性问题的跨链基础设施。

较知名的比特币侧链是 ConsenSys 的 BTC Relay、Rootstock、RSK 和 BlockStream 推出的元素链（Elements）与 Liquid，非比特币的侧链如 Lisk、Polkadot 和 Asch 等。

3.闪电网络（Lightning network）和雷电网络（Raiden Network）

闪电网络和雷电网络都是为了解决转账速度慢和网络拥堵的问题而采取的一种链下支付技术，都是状态通道的应用。其中，闪电网络针对比特币，而雷电网络是针对以太坊。

闪电网络是一个通过智能合约实现即时、高容量支付的分布式网络。其目的是实现安全的链下交易，哈希锁定技术使得它可以进行原子级的跨链交换，需要进行跨链交换的两条区块链上均支持闪电网络。

雷电网络是以太坊上的链下扩容方案。其目的是利用链下状态网络对以太坊的交易能力进行扩展。雷电网络的支付通道由智能合约控制而非多签名地址、雷电网络使用智能合约可以实现更多复杂的交换条件。

2.6 区块链领域必读论文

基于 AMiner 系统的“Topic 必读论文”功能，通过本领域热心专业读者推荐，本部分选取其中代表性的八篇论文进行解读。如欲查看区块链领域更多的必读论文，请查看网站：https://www.aminer.cn/search/pub?q=Blockchain。

1. ***Bitcoin: A Peer-to-Peer Electronic Cash System*《比特币：一个点对点的电子现金系统》**：中本聪（Satoshi Nakomoto）在 2008 年发表的这篇论文开创了区块链的时代。该论文将哈希链、公钥加密、使用工作量证明进行去中心化的共识、最长链机制、挖矿激励等几个核心要素有机结合，赋予区块链巨大的能量。这篇论文是所有区块链从业者的入门必读。

地址：

https://www.aminer.cn/pub/53e9a603b7602d9702f30a45

2. *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains*《Hyperledger Fabric：基于私有区块链（也叫许可区块链）的去中心化操作系统》：这是一篇 2018 年发表的同行评审文章，它介绍了私有区块链 Hyperledger Fabric 的架构。与比特币和以太坊这些公有区块链不同，私有区块链是封闭的，只有得到许可的用户才能参与其中。这篇文章论证了将交易的执行过程与交易的验证过程分离，以及不等交易完成验证就执行交易的好处。Hyperledger Fabric 的共识机制可以支持定制化、模块化的设计。

地址：

https://www.aminer.cn/pub/5a9cb66717c44a376ffb8636

3. *The latest gossip on BFT consensus*《关于拜占庭容错共识算法的最新进展》：这是一篇 2018 年发表的论文，文章中提出了简化的拜占庭容错（Byzantine Fault Tolernant，简称 BFT）共识协议。这个改进的协议需要多回合的执行，每一个回合都会有一个专门的提议者。协议为便于理解和实现做出了优化，在提议者不表现出恶意行为且通信不受影响的理想情况下，它只需执行三个回合就能达成共识。同时，文章中提供了协议正确性的形式化证明。

地址：

https://www.aminer.cn/pub/5b67b4b417c44aac1c867825

4. *The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance*《Swirlds 哈希图共识算法》：哈希图是一个 2016 年提出的基于有向无环图（Directed Acyclic Graph，简称 DAG）的协议，该共识协议使用了一个基于 gossip 的算法，可以提供可证明的拜占庭容错共识。在理想没有故障的情况下，该协议可以做到无需领导，异步且快速地建立共识。与其他协议相比，它可以以最少的通信量达到整体的排序。使用到有向无环图的协议还包括 IOTA 和 Spectre。

地址：

https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

5. *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*《Ouroboros：一个可证明安全的权益证明区块链协议》：这篇 2017 年发表的论

文介绍并从数学的角度分析了对应于区块生成的按回合运行的同步协议 Ouroboros，该协议以分批次的方式运行。Ouroboros 专为被誉为区块链 3.0 的 Cardano 区块链开发。在每个回合的开始阶段，权益相关者组成的委员会使用安全多方计算来为该时段选择一个区块生产者的随机序列，并选取下一回合的委员会。每个用户被选择成为区块生产者的概率取决于他所投入的权益。

地址：

https://www.aminer.cn/pub/5c8bccb64895d9cbc6ad5567

6. *Algorand: Scaling Byzantine Agreements for Cryptocurrencies* **《Algorand：加密货币高可拓展性拜占庭容错共识协议》**：该文发表于 2018 年，提供了一种改进的拜占庭容错协议机制，即使用可验证随机函数（Verifiable Random Function,简称 VRF)以隐秘且非交互的方式来选择一部分用户参与共识。这个协议参考了权益证明机制的思想，按照每个参与者投入的货币价值给予其相应的权重。该协议的亮点在于可扩展性，它可以支持很高的交易吞吐量并避免了工作量证明区块链在计算上付出的昂贵代价。

地址：

https://www.aminer.cn/pub/599c77ec601a182cd258a68b

7. *Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies* **《Avalanche：一种亚稳态的新共识协议》**：这篇由匿名组织“火箭团队”撰写的论文于 2018 年发表。它提出了一种无需领导的，基于 gossip 协议，使用有向无环图的概率共识协议。与其他区块链协议相比，Avalanche 协议表现出更好的通信复杂度，因而具有更强的可扩展性。同时，论文中还论证了协议的安全性和存活能力。然而，在 Avalanche 协议的设计中考虑到了女巫攻击，但没有考虑到区块链的激励机制。不过好在，基于有向无环图的区块链协议 Perlin 在 Avalanche 共识的基础上解决了这些问题。

地址：

https://ipfs.io/ipfs/QmUy4jh5mGNZvLkjies1RWM4YuvJh5o2FYopNPVYwrRVGV

8. *Tortoise and Hares Consensus: the Meshcash Framework for Incentive-Compatible, Scalable Cryptocurrencies* **《乌龟和野兔共识**

（Tortoise and Hares Consensus）：针对激励兼容，可扩展性的加密货币 Meshcash 框架》：这篇 2017 年发表的论文结合了基于工作量证明的公有区块链拜占庭容错共识协议（慢速的乌龟）与可能会出错但运行快速的共识协议（快速的野兔）。该协议在降低平均共识建立时间的同时，即使在最坏的安全状况下，它也能保证最终结果的一致性和不变性。它是一种区块的有向无环图协议。

地址：

https://www.aminer.cn/pub/599c77ea601a182cd2589e48

2.7 区块链话题模型（Topic Model）

本节针对 AMiner 平台上收录的 100 篇必读论文（https://www.aminer.cn/search/pub?q=Blockchain），采用经典的隐含狄利克雷分配（Latent Dirichlet Allocation，简称 LDA）模型来分析这些区块链相关论文的研究话题模型。

LDA 模型假定文本中的每个词由一些混合的话题产生的，每个话题都有一定的权重，即$p(w) = \sum_z p(w|z)p(z)$，其中$p(z)$又是一个 Dirichlet 分布产生。LDA 的贝叶斯网络结构如图 15 所示，图中 K 为话题个数，M 论文总数，N 是某个论文中单词总数，α和β分别是每个话题下词的多项式分布和每个论文下话题的多项分布的 Dirichlet 先验参数。LDA 模型中有一组隐含变量z，参数求解采用吉布斯采样，构建 Markov 链，逼近目标概率分布。获取参数后可以计算论文的主题关键词，$p(w|d) = \sum_z p(w|z)p(z|d)$。

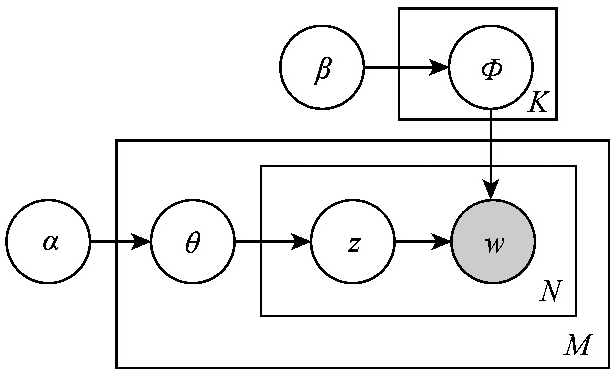


图 15　LDA 结构图[41]

利用 LDA 模型算法，本报告设置话题数 K=5，通过对论文的标题和摘要进行

[41] Wikipedia，https://en.wikipedia.org/wiki/Latent_Dirichlet_allocation

分析，获取了这些区块链研究论文的话题模型，结果如表 9 所示。

表 9　区块链话题模型

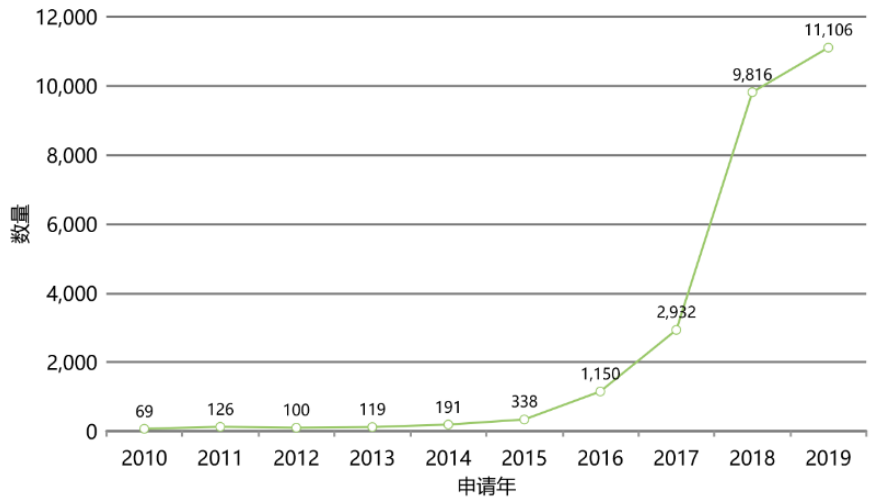
话题模型	相关论文	作者
Bitcoin	Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.	Radziwill Nicole
	Blockchain Inefficiency in the Bitcoin Peers Network	Pappalardo Giuseppe, Matteo di Tiziana, Caldarelli Guido and Aste Tomaso
	Bitcoin Blockchain Dynamics: the Selfish_Mine Strategy in the Presence of Propagation Delay	Gobel Johannes, Keeler Paul, Krzesinski E A and Taylor G Peter
Consensus Protocol	Proteus - A Scalable BFT Consensus Protocol for Blockchains	Jalalzai M. Mohammad, Busch Costas and III G. Richard Golden
	Blockchain Consensus Protocols in the Wild	Cachin Christian and Vukolic Marko
	A Secure Sharding Protocol for Open Blockchains	Luu Loi, Narayanan Viswesh, Zheng Chaodong, Baweja Kunal, Gilbert Seth and Saxena Prateek.
Smart Contract	Evaluation of Logic_Based Smart Contracts for Blockchain Systems	Idelberger Florian, Governatori Guido, Riveret Régis and Sartor Giovanni
	Blockchains and Smart Contracts for the Internet of Things.	Christidis Konstantinos and Devetsikiotis Michael
	Hawk: The Blockchain Model of Cryptography and Privacy_Preserving Smart Contracts	Kosba E. Ahmed, Miller Andrew, Shi Elaine, Wen Zikai and Papamanthou Charalampos
Architecture	A Hybrid Blockchain Architecture for	Desai Bimal Harsh,

话题模型	相关论文	作者
	Privacy_Enabled and Accountable Auctions	Kantarcioglu Murat and Kagal Lalana
	A Taxonomy of Blockchain_Based Systems for Architecture Design	Xu Xiwei, Weber Ingo, Staples Mark, Zhu Liming, Bosch Jan, Bass Len, Pautasso Cesare and Rimba Paul
	Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT	Novo Oscar
Privacy	Blockchain's roles in strengthening cybersecurity and protecting privacy	Kshetri Nir
	Decentralizing Privacy: Using Blockchain to Protect Personal Data	Zyskind Guy, Nathan Oz and Pentland Alex
	A Lightweight Blockchain_Based Privacy Protection for Smart Surveillance at the Edge	Fitwi Alem, Chen Yu and Zhu Sencun

2.8 区块链国内专利申请情况

根据“区块链”领域关键词，从专利数据库中查找出 2010 至 2019 年期间“标题和摘要”中包含领域关键词的国内相关专利申请情况。领域关键词包括：去中心化（Decentralized or Decentralizing）、共识层（Consensus Layer）、共识机制（Consensus Mechanism）、共识协议（Consensus Protocol）、数字加密货币（Digital Cryptocurrency）、分布式对等网络（Distributed Peer-to-Peer Network）、以太坊（Ethereum）、能力证明（Proof of Capacity）、股权证明（Proof of Stake）、工作证明（Proof of Work）、自私采矿（Selfish Mining）、智能合约（Smart Contract）、比特币（Bitcoin）、区块链（Blockchain）、拜占庭式（Byzantine）。

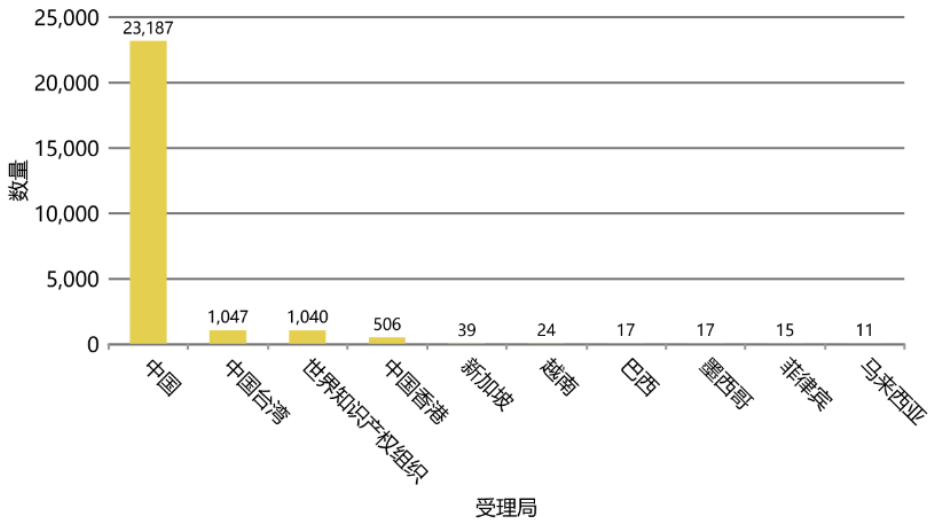
过去十年期间，区块链专利申请量共计 25947 条。其中，2019 年相关专利申请量最高，达 11106 条。整体来看，区块链相关专利申请趋势呈现稳步上升态势，且自 2017 年起上升增幅明显，如图 16 所示。



来源：智慧芽

图 16　2010 至 2019 年期间区块链相关专利申请量

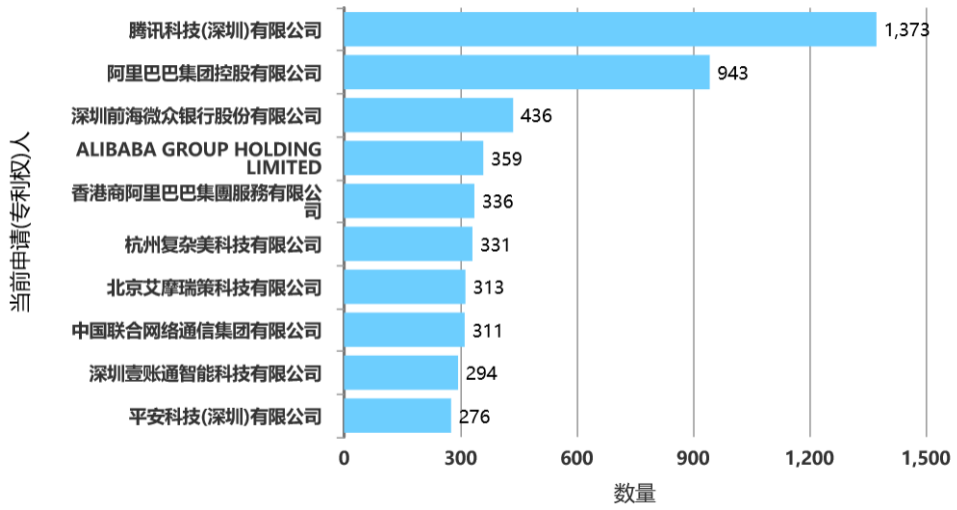
从专利受理局排名来看，如图 17 所示，区块链专利在中国地区申请受理量最多，达 23187 件。这反映出中国对区块链技术和产业创新发展的高度关注。



来源：智慧芽

图 17　2010 至 2019 年期间区块链专利受理局排名

从专利申请排名看，国内区块链相关专利申请量最多的机构是腾讯科技，申请量为 1373；其次，是阿里巴巴集团和深圳前海微众银行，专利申请量分别为 943 和 436，位于第二和第三位，如图 18 所示。



来源：智慧芽

图 18　2010 至 2019 年期间国内区块链相关专利申请排名前十机构

3　人才篇

本篇通过 AMiner 大数据平台对近 10 年发表在 SJR（Scimago Journal & Country Rank）一区的信息技术领域学术会议及期刊[42]论文进行挖掘，提取区块链领域论文中所有学者信息，并按照相关性进行排序，进行学者分布与画像等情况分析，介绍了部分该领域国内外知名度较高的活跃学者。领域关键词由区块链顾问组给出，具体包括区块链（Blockchain）、密码学（Cryptography）、量子计算（Quantum Computing）、分布式账本（Distributed Ledgers）、博弈论（Game Theory）、计算经济学（Computational Economics）、策略制定（Strategy Formulation）、比特币（Bitcoin）、共识层（Consensus Layer）、共识机制（Consensus Mechanism）、共识协议（Consensus Protocol）、去中心化（Decentralized OR Decentralizing）、加密货币（Cryptocurrency）、点对点技术（P2P OR Peer-to-Peer Network）、以太坊（Ethereum）和智能合约（Smart Contract）等。

3.1 区块链领域人才分布

- 全球学者概况

根据 AMiner 平台数据统计分析全球人才分布情况，有利于分析各地域的人才竞争关系。根据论文中作者的工作地区等信息，统计分析了世界范围内“区块链”领域顶尖人才的分布情况，如图 19 所示。

图 19　区块链领域顶尖人才全球分布

[42] SJR 官网（https://www.scimagojr.com/）公布的一区会议期刊上公开发表的论文，一区期刊/会议目录见附录。

区块链技术在 2008 年由一位自称中本聪（真实身份未知）的人发表的“Bitcoin: A Peer-to-Peer Electronic Cash System”中首次提出[43]，并在短短十年内迅速发展。当前，在全球范围内，北美洲和欧洲是先进区块链领域学者分布最集中的地区，其次是东亚地区，大洋洲有较少顶尖人才分布，非洲、南美洲极度匮乏。其中北美洲主要集中在美国的东西海岸；欧洲主要分布于德国、荷兰、意大利、法国等国家；亚洲主要分布于的中国、日本和新加坡等地区。

目前，全球各国政府部门都在密切关注区块链技术，主要国家也在加紧区块链的布局。区块链技术的发展离不开科研人员的通力合作，我们根据 AMiner 大数据平台分析了不同国家“区块链”领域的学者数量、发表论文数量和论文的平均引用量（如表 10 所示）。从区块链领域的学者数量和论文数量方面来看，美国的学者数量和论文数量位居全球第一，遥遥领先于排位第二的中国。从平均引用量方面来看，英国和美国论文的平均引用量位于第一梯队，远高于其他八个国家。因为论文引用量是衡量一个国家科研文献被其他国家或机构的认可度的标志（或数据等），所以在引用量方面中国还有很大的进步空间。

表 10　区块链领域学者数量排名前十的国家

序号	国家	学者数量	论文数量	平均引用量
1	美国	698	8320	31.30
2	中国	475	5145	11.31
3	日本	150	1329	7.78
4	德国	95	1404	13.38
5	加拿大	90	1310	14.48
6	意大利	90	1060	18.62
7	澳大利亚	80	843	18.22
8	英国	78	1306	36.29
9	希腊	66	460	16.37

[43] Nakamoto S. Bitcoin: A Peer-to-peer Electronic Cash System[R]. Manubot, 2019.

序号	国家	学者数量	论文数量	平均引用量
10	印度	63	709	15.17

- 中国学者概况

我国学者在区块链领域的分布如图 20 所示。从图中，我们可以发现，中国的区块链领域学者主要分布于京津地区，其次是长三角地区。相比之下，内陆地区人才匮乏，这与该区域的经济落后、收入低、工作生活条件差不无关系。同时，通过观察中国周边国家的学者数量情况，特别是与日韩、东南亚等亚洲国家相比，中国在区块链领域学者数量较多。

图 20　区块链领域顶尖人才中国分布

借助 AMiner 数据平台，中国与其他国家在区块链领域的合作情况可以通过以下方式获得。通过统计论文中作者的单位信息，将作者映射到各个国家中，进而统计出中国与各国之间合作论文的数量，并按照合作论文发表数量从高到低进行了排序，如表 11 所示。

表 11　区块链领域中国与各国合作论文情况

序号	合作国家	论文数	平均引用数	总引用数
1	中国-美国	550	27.59	15174
2	中国-澳大利亚	104	15.21	1582
3	中国-加拿大	97	13.75	1333
4	中国-新加坡	93	24.71	2298
5	中国-英国	82	14.19	1163
6	中国-日本	82	8.24	675
7	中国-法国	33	6.90	228
8	中国-德国	23	20.84	479
9	中国-意大利	17	33.20	564
10	中国-韩国	15	20.14	302

从表 11 数据可以看出，中美合作的论文数、引用数遥遥领先，表明中美间在区块链领域合作之密切；从地域角度看，中国与欧洲的合作非常广泛，前 10 名合作关系里中欧合作共占 4 席；从合作论文质量上看，中国与意大利合作的论文数虽然不是最多，但是平均引用数位列首位，反映出中意两国领域合作论文达到了较高的水平。

3.2 区块链代表学者

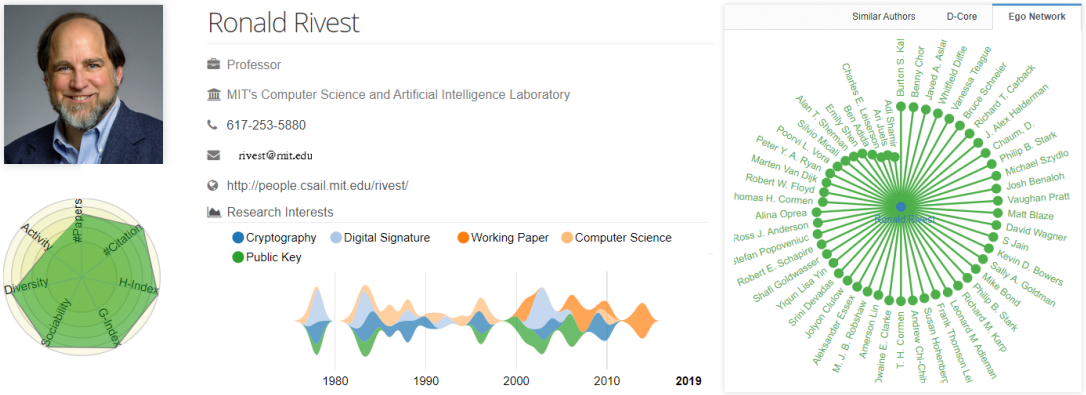
综合 h-index 以及领域知名度与活跃度，我们收集整理了国内外“区块链”领域高水平学者，如 Ronald L. Rivest 和 Schahram Dustdar 等。本部分将对这些学者按领域进行简要介绍，排名不分先后。此外，限于报告篇幅，不能逐一罗列所有学者，请登录网址 https://www.aminer.cn/获取更多学者资料。

3.2.1 密码学

- Ronald L. Rivest

h-index: 106 | #Paper: 422 | #Citation: 139424

麻省理工学院教授、图灵奖得主



Ronald L. Rivest，1977 年从斯坦福大学获得计算机博士学位，现任麻省理工学院电子工程和计算机科学系安德鲁与厄纳·维特尔比（Andrew and Erna Viterbi）教授、美国国家密码学会的负责人。

Ronald L. Rivest 研究兴趣集中在密码学、数字信号、计算机科学、公钥体系等。Ronald L. Rivest 曾担任欧洲密码和密码会议的组织机构国际密码研究协会（International Association for Cryptologic Research）的理事，以及金融密码协会（Financial Cryptologic Association）的理事。他是 MIT 计算机科学和人工智能实验室的成员，并领导着其中的信息安全和隐私中心。主要从事密码安全、计算机安全算法的研究。他和 Adi Shamir 和 Len. Adleman 一起发明了 RSA 公钥算法，这个算法在信息安全中获得巨大的突破，这一成果也使他和 Shamir 以及 Adleman 一起获得 2002 年 ACM 图灵奖。

主要科研成就

RSA 因其创始人 Ronald L. Rivest,Adi Shamir 和 Len. Adleman 而得名。RSA 的难度与大整素数因子分解难度等价。RSA 算法研制的最初理念与目标是努力使互联网安全可靠，旨在解决 DES 算法密钥的利用公开信道传输分发的难题。而实际结果不但很好地解决了这个难题，还可利用 RSA 来完成对电文的数字签名以抗对电文的否认与抵赖，同时还可以利用数字签名较容易地发现攻击者对电文的非法篡改，以保护数据信息的完整性。

相关论文精选

1. *Introduction to Algorithms*

作者：Cormen T H, Leiserson C E, Rivest R L, Stein C.

专著：Introduction to algorithms, (2001)

论文链接：https://www.aminer.cn/pub/53e9a94cb7602d97032a30e6/introduction-to-algorithms-nd-ed

2. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*

作者：Rivest R L, Shamir A, Adleman L.

期刊/会议：Communications of the ACM - Special 25th Anniversary Issue, no. 2 (1978): 120-126

论文链接：https://www.aminer.cn/pub/53e9baecb7602d970471e0d0/a-method-for-obtaining-digital-signatures-and-public-key-cryptosystems

3. *The MD5 Message-Digest Algorithm*

作者：Rivest R, Dusse S.

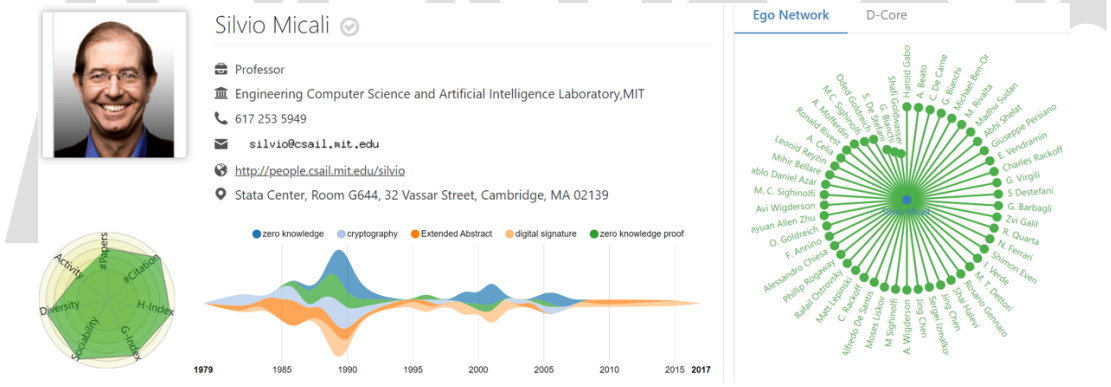
期刊/会议：CRYPTO, pp.303-311, (1990)

论文链接：https://www.aminer.cn/pub/53e9bde2b7602d9704a916c3/rfc-the-md-message-digest-algorithm

● Silvio Micali

h-index: 85 / #Paper: 345 / #Citation: 40778

麻省理工学院教授、图灵奖得主



Silvio Micali 本科毕业于罗马大学数学系，获得加州大学伯克利分校计算机博士学位。自 1983 年就在麻省理工学院电子工程和计算机系担任教授，头衔为福特工程教授（Ford Professor of Engineering）。他的研究兴趣包括密码学、零知识证明、伪随机生成、安全协议和机械设计。曾在 1993 年获哥德尔奖，又于 2012 年获得图灵奖，并入选为美国国家科学院和美国国家工程院成员。2017 年，Micali 创建了 Algorand 区块链，它是一个可以为分散型经济构建产品和服务的平台。

主要科研成就

Micali 和他的共同获奖者 Goldwasser 使密码学成为一门精确的科学。他们创造的数学结构，包括正式的隐私观念、对手、伪随机数、交互式证明、零知识

证明和许多其他基本概念都是非常微妙的定义，他们在严格的最高标准的基础上设置密码，并开辟了在计算机科学领域的全新研究。他们的第一篇论文《概率加密》（Probabilistic Encryption），是计算机科学史上最具影响力的论文之一。文中提出并回答的第一个问题“什么是秘密？”在该领域从未被正式对待，而他们用高标准将“秘密”定义为“一个对手不应该能够获得哪怕一部分关于一个秘密的信息。”在文中，他们定义了概率加密、语义安全以及计算不可分辨性，即在高效算法看来相同的对象实际上是相同的。使用这些概念，他们能够从正式意义上解释 Diffie 和 Hellman 提出的计算密码学。Micali 和 Goldwasser 将所有这些结合起来，给出了一个公钥加密方案，该方案在他们的标准下是安全的。这样的正式定义和证明在之前的开创性论文中是缺失的，因此，他们这篇论文促进了密码学的发展，并对互联网商业应用的发展影响重大。

相关论文精选

1. *Probabilistic Encryption*

作者：Shafi Goldwasser, Silvio Micali

期刊/会议：Journal of Computer and System Science, no. 2 (1984): 270-299

论文链接：https://www.aminer.cn/pub/53e997aeb7602d9701f880a1/probabilistic-encryption

2. *A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attakcs*

作者：Shafi Goldwasser, Silvio Micali, Ronald L. Rivest

期刊/会议：SIAM Journal on Computing, no. 2 (1988): 281-308

论文链接：https://www.aminer.cn/pub/53e9bae6b7602d9704716f59/a-digital-signature-scheme-secure-against-adaptive-chosen-message-attacks

3. *How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority*

作者：Oded Goldreich, Silvio Micali, Avi Wigderson

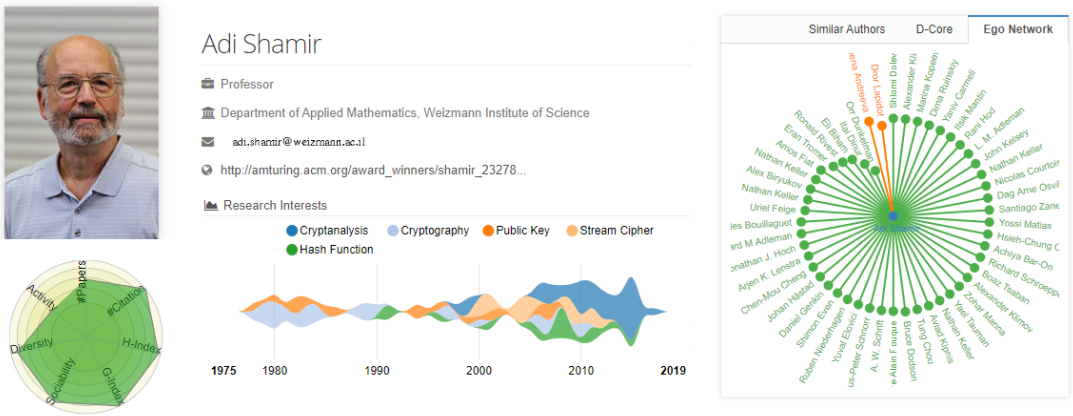
期刊/会议：STOC, pp.218-229, (1987)

论文链接：https://www.aminer.cn/pub/53e9b59ab7602d97040ddeb1/how-to-play-any-mental-game

- Adi Shamir

h-index: 93 | #Paper: 334 | #Citation: 96831

巴黎高等师范学校教授、图灵奖得主



Adi Shamir 分别于 1975 年和 1977 年获得以色列魏茨曼科学研究所的硕士和博士学位，其博士论文题目为《不动点的递归程序和它们之间的 Agard 微分关系》。曾于 1977 至 1980 年担任美国麻省理工学院研究员和助理教授，2002 年获得图灵奖，并从 2006 年起受邀担任巴黎高等师范学院教授。其研究兴趣包括密码学理论、分组密码、侧通道攻击、穷举搜索等。

主要科研成就

Adi Shamir 是国际公认的密码学家。他的主要科研成就包括 RSA 公开密钥加密编码和解码消息算法、零知识证明方案、Shamir 秘密共享方案、Merkle-Hellman 密码系统的破解、视觉密码以及 TWIRL 和 TWINKLE 因子分解设备，他还同 Eli Biham 一起提出了差分密码分析法，就是一种用来破解分组密码的方法。

相关论文精选

1. ***A Method for Obtaining Digital Signatures and Public-Key Cryptosystems***

作者：Rivest R L, Shamir A, Adleman L.

期刊/会议：Communications of the ACM - Special 25th Anniversary Issue, pp. 120-126, 1978.

论文链接：https://www.aminer.cn/pub/53e9baecb7602d970471e0d0/a-method-for-obtaining-digital-signatures-and-public-key-cryptosystems

2. ***How to share a secret***

作者：Adi Shamir

期刊/会议：Commun. ACM, no. 11 (1979): 612-613

论文链接：https://www.aminer.cn/pub/53e9a91ab7602d970326da29/how-to-share-a-secret

3. *How to prove yourself: practical solutions to identification and signature problems*

作者：Amos Fiat, Adi Shamir, Santiago Zanella Beguelin

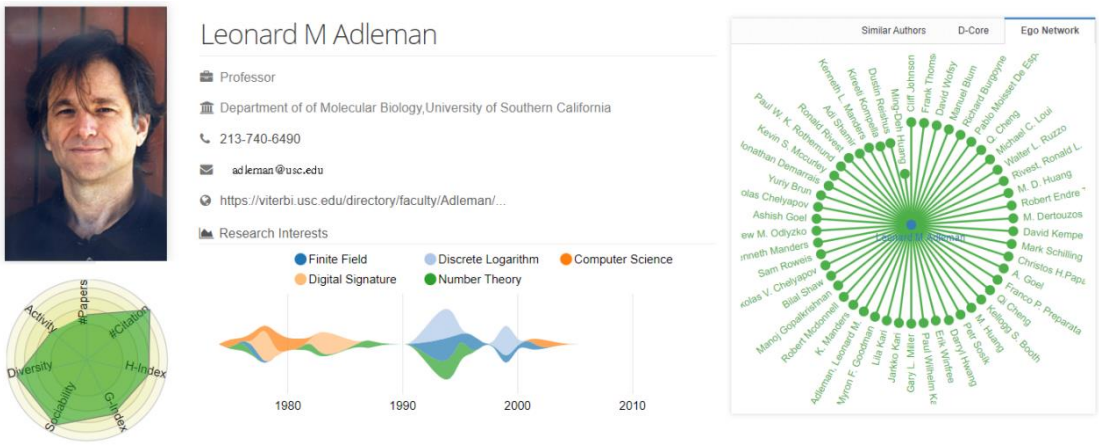
期刊/会议：International Cryptology Conference, pp.186-194, (1986)

论文链接：https://www.aminer.cn/pub/53e99cdfb7602d9702591fb2/how-to-prove-yourself-practical-solutions-to-identification-and-signature-problems

- Leonard M. Adleman

h-index: 39 / #Paper: 94 / #Citation: 40524

美国南加州大学教授、图灵奖得主



Leonard M. Adleman 于 1976 年获得美国加利福尼亚大学伯克利分校计算机博士学位，现任美国理论计算机科学家和南加州大学计算机科学家、图灵奖得主。曾于 1976 年至 1980 年就职于 MIT。1977 年，他因与 Ronald L. Rivest 和 Adi Shamir 一起发明了 RSA 加密算法和 DNA 运算而知名，并因在公钥密码学 RSA 加密算法取得的杰出贡献而获得图灵奖。RSA 被广泛使用在计算机安全应用上，包括 https。

主要科研成就

1994 年，他在论文《分子计算应用于解决组合问题》中，使用 DNA 作为一个计算系统解决了一个七节点的哈密顿图问题，一个类似旅行推销员问题的 NP 完全问题。该论文是第一个“利用 DNA 来计算”的成功实例。DNA 计算现已被证明为有潜力的计算方式，可以解决大型组合搜索问题。2002 年，他和他的研究小组成功地利用 DNA 计算解决了 20 个变量的 SAT 问题。

相关论文精选

1. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*

作者：Rivest R L, Shamir A, Adleman L.

期刊/会议：Communications of the ACM - Special 25th Anniversary Issue, pp. 120-126, 1978.

论文链接：https://www.aminer.cn/pub/53e9baecb7602d970471e0d0/a-method-for-obtaining-digital-signatures-and-public-key-cryptosystems

2. *On Data Banks and Privacy Homomorphisms*

作者：Rivest R L, Adleman L, Dertouzos M

期刊/会议：Foundations of secure computation, 1978

论文链接：https://www.aminer.cn/pub/53e9b2b8b7602d9703d659e9/on-data-banks-and-privacy-homomorphisms

3. *Molecular Computation of Solutions to Combinatorial Problems*

作者：Adleman L

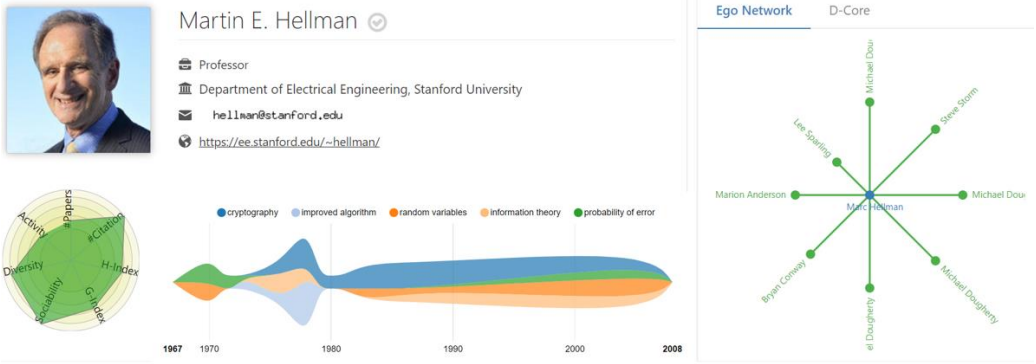
期刊/会议：Science (New York, N.Y.), no. 5187 (1994): 1021-1024

论文链接：https://www.aminer.cn/pub/53e9b115b7602d9703b93ff7/molecular-computation-of-solutions-to-combinatorial-problems

● Martin Edward Hellman

h-index: 34 / #Paper: 98 / #Citation: 28429

斯坦福大学教授、图灵奖得主



Hellman 于 1969 年在斯坦福大学获得电子工程博士学位，在麻省理工学院担任两年助理教授后，Hellman 回到斯坦福大学教课直至 1996 年荣誉退休。Hellman 主要研究课题包括密码学、信息学理论、随机变数等，他对科技发展的伦理学和国际安全也十分感兴趣。他被选进美国国家工程院、美国发明家名人堂，

获得了“斯坦福工程英雄”等诸多荣誉，并与 Whit Diffie 一起获得 2015 年图灵奖。另外，Hellman 曾是七、八十年代的“第一次密码战”中的重要参与者，最终使得密码学研究学者们可以不受政府干预的发表论文。

主要科研成就

Martin E. Hellman 最为人知的是他与 Diffie 和 Merkle 共同创造的公钥密码学，这是一项可以保障互联网交易安全的技术。他与 W Diffie 于 1976 年发表的论文《密码学的新方向》介绍了世界公钥和电子签名技术，是目前互联网最常用的技术之一，被誉为现代密码学的奠基石。两人提出了公共密钥密码体制，其原理是加密密钥和解密密钥分离。这样，一个具体用户就可以将自己设计的加密密钥和算法公之于众，而只保密解密密钥。任何人利用这个加密密钥和算法向该用户发送的加密信息，该用户均可以将之还原。公共密钥密码的优点是不需要经安全渠道传递密钥，这大大简化了密钥管理。

相关论文精选

1. *New Directions in Cryptography*

作者：W Diffie, M Hellman

期刊/会议：Information Theory, IEEE Transactions , Volume 22, Issue 6, 1976, Pages 644-654.

论文链接:https://www.aminer.cn/pub/53e99a74b7602d97022e646b/new-directions-in-cryptography

2. *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.)*

作者：Stephen C. Pohlig, Martin E. Hellman

期刊/会议：IEEE Transactions on Information Theory, no. 1 (1978): 106-110

论文链接：https://www.aminer.cn/pub/53e9b496b7602d9703fa007c/an-improved-algorithm-for-computing-logarithms-over-gf-p-and-its-cryptographic

3. *Hiding information and signatures in trapdoor knapsacks*

作者：Merkle, R., Hellman, M.E.

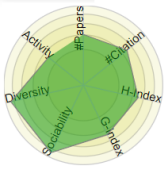
期刊/会议：Information Theory, IEEE Transactions , no. 5 (1978): 525-530

论文链接：https://www.aminer.cn/pub/53e9a5a1b7602d9702eca818/hiding-information-and-signatures-in-trapdoor-knapsacks

● 来学嘉

h-index: 26 / #Paper: 167 / #Citation: 6275

上海交通大学教授

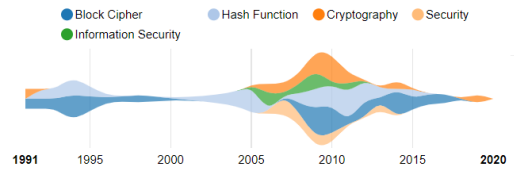


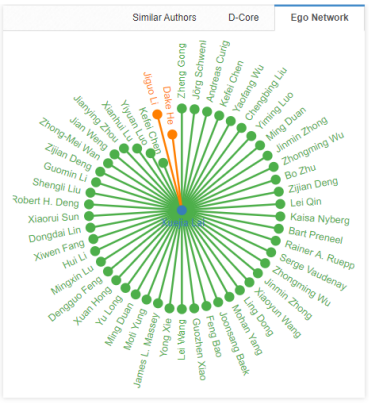
Xuejia Lai (来学嘉)

Professor

Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China

Research Interests





来学嘉于 1992 年获得苏黎世瑞士联邦理工学院博士学位，现任上海交通大学计算机科学与工程系教授、中国科学技术大学研究生院名誉教授、西南交通大学顾问教授、中国密码学学会常务理事。曾于 1994 年就职于 R3 安全工程公司，自 2001 年起担任瑞士 S.W.I.S.集团高级顾问和技术总监，参与欧洲银行使用的欧洲芯片的算法设计，参与制定 3ISO 安全标准。研究兴趣为分组密码设计与分析、哈希函数、DNA 计算和 DNA 密码、白盒加密、云中的终端安全、一次性密码系统。

主要科研成就

来学嘉与 James L. Massey 在 1990 年提出了一种建议标准算法 PES（Proposed Encryption Standard），在 1992 年改进强化了抗差分分析的能力，将该算法改称为 IDEA（International Data Encryption Algorithm）。在所提出的密码中，明文和密文为 64 位大小的数据块，密钥为 128 位长。该密码基于“不同代数群混合运算”的设计思想，用硬件和软件都很容易实现且比 DES 在实现上快得多。IDEA 自问世以来，已经在多种商业产品中被使用。

相关论文精选

1. *A proposal for a new block encryption standard*

作者：Xuejia Lai, James L. Massey

期刊/会议：EUROCRYPT, pp.389-404, (1991)

论文链接：https://www.aminer.cn/pub/53e9ba69b7602d97046877a9/a-proposal-for-a-new-block-encryption-standard

2. *Markov Ciphers and Differentail Cryptanalysis*

作者：Xuejia Lai, James L Massey, Sean D Murphy

期刊/会议：Theory and Application of Cryptographic Techniques, pp.17-38, (1991)

论文链接：https://www.aminer.cn/pub/53e9af26b7602d970396391d/markov-ciphers-and-differentail-cryptanalysis

3. *Cryptanalysis of the hash functions MD4 and RIPEMD*

作者：Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, Xiuyuan Yu

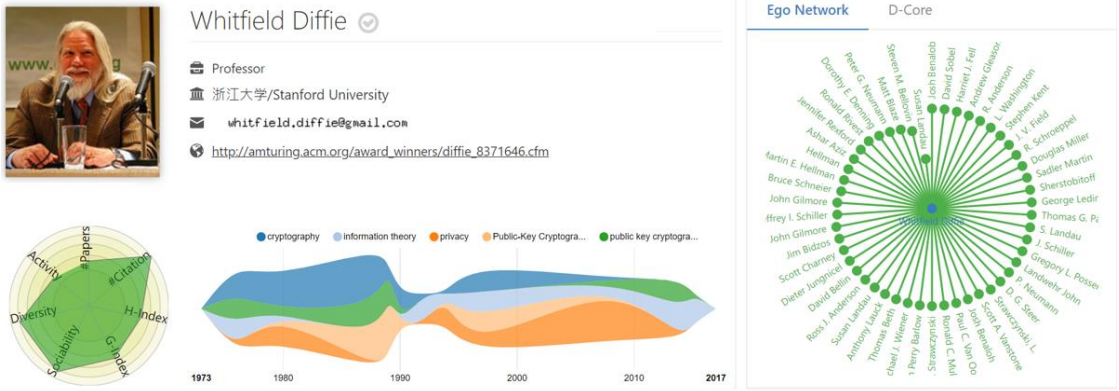
期刊/会议：EUROCRYPT, pp.1-18, (2005)

论文链接：https://www.aminer.cn/pub/5c7858d04895d9cbc6930e45/cryptanalysis-of-the-hash-functions-md-and-ripemd

● Bailey Whitfield Diffie

h-index: 20 / #Paper: 86 / #Citation: 23509

斯坦福大学教授、图灵奖得主



Bailey Whitfield Diffie 于 1965 年毕业于麻省理工学院数学系，于 1992 年获得瑞士联邦理工学院名誉博士。现任斯坦福大学教授。Diffie 曾在斯坦福人工智能实验室（SAIL）、IBM 的 Thomas J. Watson 研究中心、Sun 微系统实验室担任过研究程序员。曾于 1978 到 1991 年期间在北方电讯(Northern Telecom)担任安全系统经理。他还曾作为访问教授在伦敦大学和浙江大学教授过课程。他是“公钥加密”概念的发明人，被誉为“现代密码学之父”，2015 年获得图灵奖。他的研究兴趣包括密码学、网络安全与隐私、计算机犯罪等。

主要科研成就

Diffie 是世界著名的密码技术与安全技术专家。他与 Martin Hellman 于

1976 年发表的论文《密码学的新方向》介绍了一种十分新颖的方式来解决密码学中密钥分配这一根本问题。这项技术被称为 Diffie-Hellman 密钥交换，而这篇文章也推动了新的加密算法的发展，即非对称式密钥学（asymmetric cryptography）。

相关论文精选

1. *New Directions in cryptography*

作者：W Diffie, M Hellman

期刊/会议：Information Theory, IEEE Transactions, no. 6 (1976): 644-654

论文链接：https://www.aminer.cn/pub/53e99a74b7602d97022e646b/new-directions-in-cryptography

2. *Authentication and authenticated key exchanges*

作者：W Diffie, PC Van Oorschot, MJ Wiener

期刊/会议：Des. Codes Cryptography, no. 2 (1992): 107-125

论文链接：https://www.aminer.cn/pub/53e9ab1ab7602d97034a354f/authentication-and-authenticated-key-exchanges

3. *Multiuser cryptographic techniques*

作者：Whitfield Diffie, Martin E. Hellman

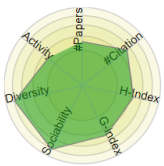
期刊/会议：AFIPS Spring Conference, pp.109-112, (1976)

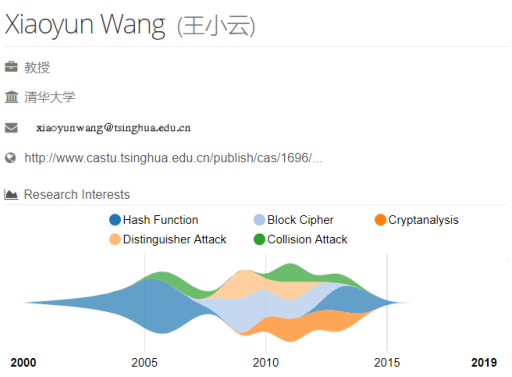
论文链接：https://www.aminer.cn/pub/53e99842b7602d970206d2ec/multiuser-cryptographic-techniques

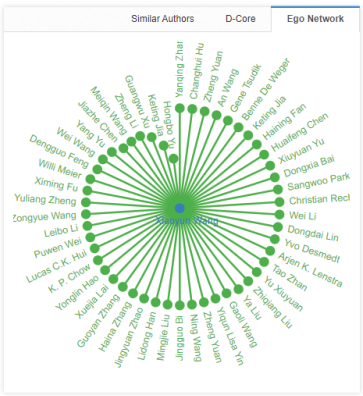
- 王小云

h-index: 23 | #Paper: 103 | #Citation: 6401

清华大学教授、中科院院士







王小云于 1993 年获得山东大学数学系博士学位。现为中科院院士、清华大学高等研究院杨振宁讲座教授、清华大学密码理论与技术研究中心主任、山东大学密码技术与信息安全教育部重点实验室主任、山东大学数学学院教授。

王小云主要从事密码理论与密码数学问题研究。在密码分析领域，给出了包括 MD5，SHA-1 在内的系列国际通用 Hash 函数算法的碰撞攻击理论，提出了 MAC 算法 ALPHA-MAC、MD5-MAC 与 PELICAN 的子密钥恢复攻击以及 HMAC-MD5 的区分攻击思想。在密码设计领域，主持设计了 Hash 函数算法 SM3。有 4 篇论文获最佳论文，包括 2005 年度国际密码年会、欧密会与美密会的最佳论文。MD5 破解的论文获得 2008 年汤姆森路透卓越研究奖（中国）。2019 年，王小云教授获得未来科学大奖数学与计算机科学奖，成为该领域第一位女性获奖人。

主要科研成就

美国标准及数据（NIST）颁布的基于哈希函数的 MD5 和 SHA-1 多年来被公认为是最先进、最安全的算法。按照常规方法，破解 MD5 和 SHA-1 是不可能或几乎行不通的，这也在一定程度上确保了电子签名的安全。2004 年 8 月 17 日，王小云在美国加州圣巴巴拉召开的国际密码学会议（Crypto'2004）上首次宣布她和她的研究小组对 MD5、HAVAL-128、MD4 和 RIPEMD 四种密码算法的破译结果，对曾经被认为是“不可破解”的世界通行密码标准 MD5 宣告攻破。2005 年 2 月的 RSA 年会，SHA-1 也由王小云宣告破解。在她的算法下，普通计算机只需几分钟就能够找到 MD5 的“碰撞信息对”，这意味着现行的基于哈希函数的密码系统及应用都面临被攻击的风险。

相关论文精选

1.*Finding Collisions in the Full SHA-1*

作者：Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu

期刊/会议：Lecture Notes in Computer Science(2006): 17-36.

论文链接：https://www.aminer.cn/pub/53e9b66cb7602d97041d4336/finding-collisions-in-the-full-sha

2.*How to Break MD5 and Other Hash Functions*

作者：Xiaoyun Wang, Hongbo Yu

期刊/会议：EUROCRYPT, pp.19-35, (2005)

论文链接：https://www.aminer.cn/pub/53e9a3c7b7602d9702cd5d50/how-to-break-md-

and-other-hash-functions

3. *Cryptanalysis of the Hash Functions MD4 and RIPEMD*

作者：Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, Xiuyuan Yu

期刊/会议：EUROCRYPT，pp.1-18, (2005)

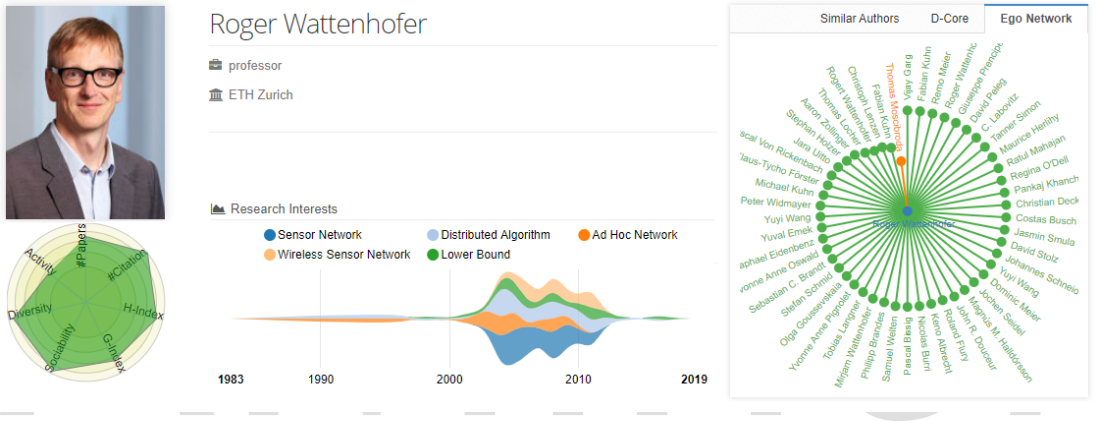
论文链接：https://www.aminer.cn/pub/5c7858d04895d9cbc6930e45/cryptanalysis-of-the-hash-functions-md-and-ripemd

3.2.2 分布式系统和理论

- Roger Wattenhofer

h-index: 86 / #Paper: 479 / #Citation: 28147

苏黎世联邦理工学院教授



Roger Wattenhofer 于 1999 年获得苏黎世联邦理工学院博士学位。现任瑞士苏黎世联邦理工学院信息技术与电气工程系的全职教授，曾供职于雷德蒙德的微软研究院、罗德岛州普罗维登斯的布朗大学和澳大利亚悉尼的麦觉理大学。

研究兴趣是计算机科学、信息技术的算法和系统，例如分布式系统、定位系统、无线网络、移动系统、社交网络、深层神经网络。论文发表在：分布式计算数据库（PODC，SPAA，DISC）、网络和系统（SIGCOMM，MobiCom，SenSys，OSDI）以及算法理论(STOC，FOCS，SODA，ICALP)。从获奖方面来说，Roger Wattenhofer 因在分布式近似中的突出贡献而荣获分布式计算创新奖。另外，由他编著的《区块链科学：分布式分类账技术》广受业内关注，已被翻译成中文、韩文和越南文等多国语言。

主要科研成就

2014 年，Wattenhofer 和 Christian Decker 共同发现了 Mt. Gox 被恶意攻

击后丢失的近 850,000 比特币是可以被避免的。另外，在 Wattenhofer 与三位同事的论文《多跳无线自组网中节电运行的分布式拓扑控制》中，他们提出了一个简单的分布式算法，其中每个节点对其传输功率进行局部决策，这些局部决策共同保证了全局连接。具体来说，基于方向信息，一个节点增加其传输能力，直到在每个方向找到一个邻居节点。由此产生的网络拓扑通过降低传输功率增加网络寿命，通过低节点度减少流量干扰。此外，他们证明多跳网络中的路由在功耗方面是有效的。他们给出了一个近似方案，其中每条路径的功耗可以通过仔细选择参数来任意接近最优。仿真结果显示了显著的性能改进。

相关论文精选

1. *Distributed topology control for power efficient operation in multihop wireless ad hoc networks*

作者：Roger Wattenhofer,Li Li,Paramvir Bahl,Yi-Min Wang

期刊/会议：INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. P..., (2001): 1388-1397vol.3

论文链接：https://www.aminer.cn/pub/558ab99ce4b0b32fcb387dbe/distributed-topology-control-for-power-efficient-operation-in-multihop-wireless-ad-hoc

2. *Farsite: federated, available, and reliable storage for an incompletely trusted environment*

作者：Atul Adya, William J. Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, John R. Douceur, Jon Howell, Jacob R. Lorch, Marvin Theimer, Roger P. Wattenhofer

期刊/会议：OSDI, no. SI (2002): 1-14

论文链接：https://www.aminer.cn/pub/53e9b281b7602d9703d289c3/farsite-federated-available-and-reliable-storage-for-an-incompletely-trusted-environment

3. *Achieving high utilization with software-driven WAN*

作者：Chi-Yao Hong, Srikanth Kandula, Ratul Mahajan, Ming Zhang, Vijay Gill, Mohan Nanduri, Roger Wattenhofer

期刊/会议：SIGCOMM, no. 4 (2013): 15-26

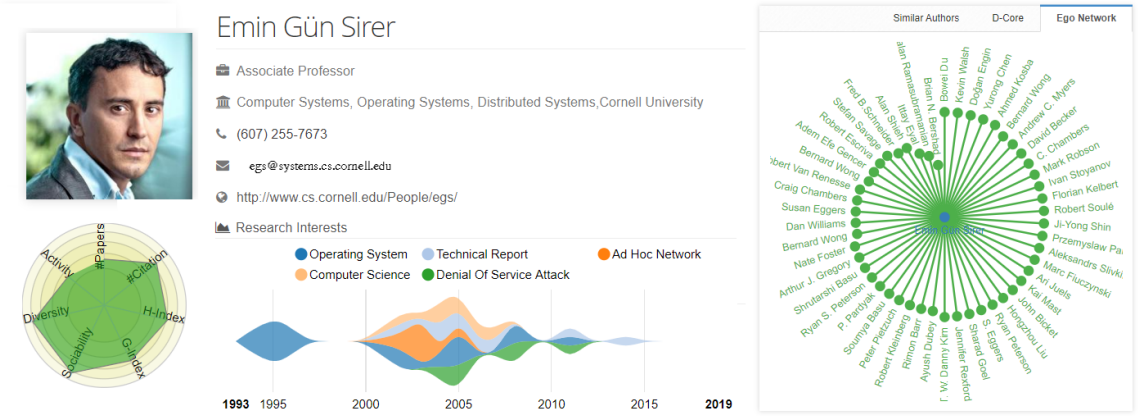
论文链接:https://www.aminer.cn/pub/53e9b4d4b7602d9703ff2f93/achieving-high-

utilization-with-software-driven-wan

- Emin Gün Sirer

h-index: 46 / #Paper: 105 / #Citation: 13021

康奈尔大学副教授



Emin Gün Sirer 在普林斯顿大学本科毕业后，2000 年获得华盛顿大学计算机和工程博士学位，其博士论文题目为《安全、高效和可管理的虚拟机器》。他的主要研究方向是操作系统、联网和分布系统，近期的项目包括一个新的安全操作系统和用于高性能云计算应用程序的系统基础设施。在成为康纳尔大学教授之前，Sirer 曾在 AT&T 贝尔实验室、系统研究中心（Systems Research Center）和日本电气（Nippon Electric Corporation）工作过。2018 年，Sirer 同 Kevin Sekniqi 和 Ted Yin 共同创立了 Ava Labs，旨在创建一个可上线高度去中心化的软件、金融原语和可共同操作的区块链的平台，并发行加密货币。

主要科研成就

Sirer 曾获得美国国家科学基金会职业奖，他早在 2003 年，Bitcoin 问世六年前创造了基于 P2P 和工作量证明的电子货币 Karma。Karma 是对等系统的虚拟货币。它的主要优点是不受任何单一实体的控制。它的执行以及控制其供应和价值的手段是完全分散的。Karma 的设计目的是阻止在许多点对点系统中遇到的搭便车问题，通过一个安全的交换机制来确保节点不能伪造 Karma，一个反通货膨胀/通货紧缩的机制来调节 Karma 的供应和价格，一个奖励机制使系统对参与者具有激励兼容性，以及一个用于跟踪转移 Karma 的完全对等方案来保护系统免受对手的破坏。

相关论文精选

1. *Extensibility Safety and Performance in the SPIN Operating System*

作者：Brian N. Bershad, Stefan Savage, Przemyslaw Pardyak, Emin Gün Sirer, Marc E. Fiuczynski, David Becker, Craig Chambers, Susan J. Eggers

期刊/会议：ACM SIGOPS Operating Systems Review, no. 5 (1995): 267-283

论文链接：https://www.aminer.cn/pub/53e9bd92b7602d9704a3a6e4/extensibility-safety-and-performance-in-the-spin-operating-system

2. *Majority is not Enough: Bitcoin Mining is Vulnerable*

作者：Ittay Eyal, Emin Gün Sirer

期刊/会议：Communications of the ACM, no. 7 (2018): 95-102

论文链接：https://www.aminer.cn/pub/53e9a775b7602d97030b101a/majority-is-not-enough-bitcoin-mining-is-vulnerable

3. *Meridian: a Lightweight Network Location Service without Virtual Coordinates*

作者：Bernard Wong, Aleksandrs Slivkins, Emin Gün Sirer

期刊/会议：SIGCOMM, no. 4 (2005): 85-96

论文链接：https://www.aminer.cn/pub/53e99ca1b7602d9702553650/meridian-a-lightweight-network-location-service-without-virtual-coordinates

- Leslie B. Lamport

h-index: 52 | #Paper: 126 | #Citation: 30522

微软计算机科学家、图灵奖得主

Leslie Lamport 于 1972 年获得布兰迪斯大学数学博士学位，现任微软公司计算机科学家。曾在麻省计算机协会、斯坦福国际研究中心、美国 DEC 公司和康柏电脑就职，后于 2001 年加入微软公司。Lamport 的博士毕业论文题目为《用

奇异数据分析柯西问题》(The analytic Cauchy Problem with Singular Data)，其主要研究方向为并发程序、拜占庭协议、分布式系统等。2013 年获图灵奖。

主要科研成就

在正式理论尚未成型时，他的研究揭示了并发程序的基础问题，并掌握了许多基本概念，诸如因果关系和逻辑时间、原子和规则共享寄存器、顺序一致性、状态机复制、拜占庭协议和等待自由等。他研究的算法已经成为容错分布式系统的标准运作工程。Lamport 还进行了大量关于并发系统的规范和验证工作，并为开发应用这些方法的自动化工具做出了贡献。此外，他提出的互斥方案和面包店算法成为了计算机学的教材内容，而他所开发的 LaTex 排字系统成为了计算机科学和许多其他领域中技术发布的实际标准。

相关论文精选

1. *Time, Clocks, and the Ordering of Events in a Distributed System*

作者：Leslie Lamport

期刊/会议：Commun. ACM, no. 7 (1977): 558-565

论文链接：https://www.aminer.cn/pub/53e9a3c0b7602d9702ccdfc9/time-clocks-and-the-ordering-of-events-in-a-distributed-system

2. *The Byzantine Generals Problem*

作者：Leslie Lamport

期刊/会议：ACM Transactions on Programming Languages and Systems (TOPLAS), no. 3 (1982): 382-401

论文链接：https://www.aminer.cn/pub/56d902e1dabfae2eeee33d4f/the-byzantine-generals-problem

3. *Distributed snapshots: determining global states of distributed systems*

作者：K. Mani Chandy, Leslie Lamport

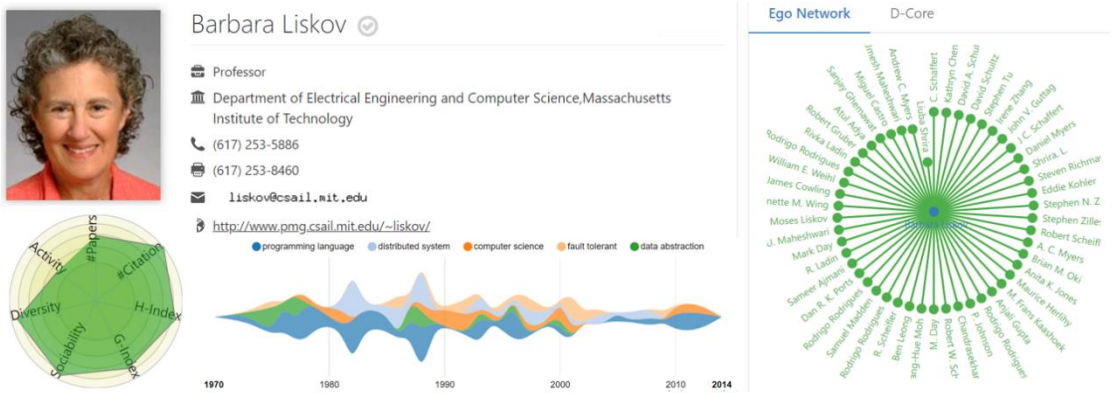
期刊/会议：ACM Transactions on Computer Systems, no. 1 (1985): 63-75

论文链接：https://www.aminer.cn/pub/53e9bb1cb7602d9704755e58/distributed-snapshots-determining-global-states-of-distributed-systems

- Barbara Liskov

h-index: 79 / #Paper: 335 / #Citation: 27844

麻省理工学院教授、图灵奖得主



Barbara Liskov 于 1968 年获得斯坦福大学计算机博士学位。现任麻省理工学院电子工程与计算机科学系教授。

Liskov 的主要研究方向为编程方法论、编程语言和系统以及分布式计算。主要研究项目包括支持数据抽象的第一语言 CLU 的设计与实现；第一种支持分布式程序实现的高级语言 Argus 的设计和实现；以及 Thor 面向对象数据库系统，这一系统提供了对大范围分布式环境中持久、高可用对象的事务访问。目前 Liskov 的研究兴趣还包括拜占庭容错存储系统、点对点计算以及支持在大型分布式系统中自动部署软件升级。

Liskov 是美国国家工程学院的成员，美国艺术与科学学院和计算机机械协会的成员。1996 年，她获得了美国女性工程师协会的成就奖，并于 2004 年获得了 IEEE 冯诺伊曼奖章。在 2008 年 ACM SIGPLAN 编程语言设计与实现大会上，获得了编程语言成就奖。2009 年，获得了 ACM 颁发的图灵奖。

主要科研成就

Barbara Liskov 为编程语言和系统设计的实践和理论基础做出了重要贡献，特别是在数据抽象、容错和分布式计算方面。她通过创建和实现编程语言、操作系统和创新的系统设计引领了计算领域的重要发展，这些设计促进了数据抽象、模块化、容错、持久性和分布式计算系统的发展。

Venus 操作系统是一个原则性操作系统设计的早期示例。CLU 编程语言基于抽象数据类型形成的模块，结合早期和后期绑定机制，是最早也是最完整的编程语言之一。ARGUS 将许多 CLU 思想扩展到分布式编程，合并了嵌套事务的最初版本，以保持可预测的一致性。

相关论文精选

1. *Practical Byzantine Fault-tolerance*

作者：Miguel Castro, Barbara Liskov

期刊/会议：OSDI, pp.173-186, (2000)

论文链接： https://www.aminer.cn/pub/53e99b26b7602d97023c212f/practical-byzantine-fault-tolerance

2. *Practical Byzantine Fault Tolerance and Proactive Recovery*

作者：Miguel Castro, Barbara Liskov

期刊/会议：ACM Trans. Comput. Syst., no. 4 (2002): 398-461

论文链接： https://www.aminer.cn/pub/53e9a774b7602d97030ac38b/practical-byzantine-fault-tolerance-and-proactive-recovery

3. *A Behavioral Notion of Subtyping*

作者：Barbara H. Liskov, Jeannette M. Wing

期刊/会议：ACM Trans. Program. Lang. Syst., no. 6 (1994): 1811-1841

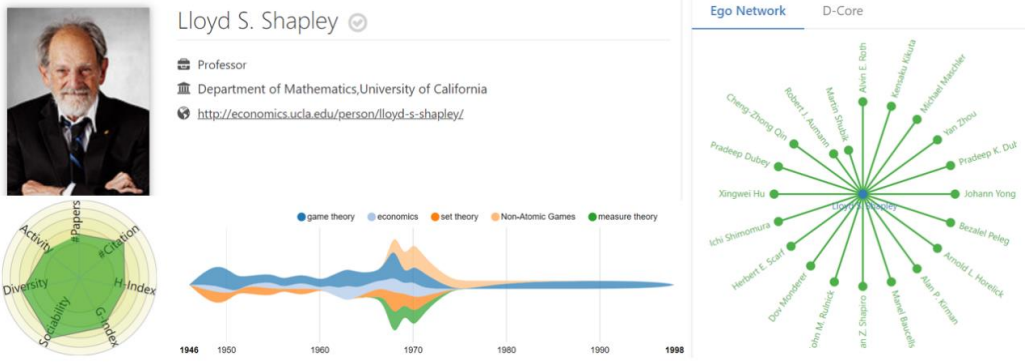
论文链接：https://www.aminer.cn/pub/53e9ab0db7602d970349050b/a-behavioral-notion-of-subtyping

3.2.3 博弈论

- Lloyd S. Shapley

h-index: 58 / #Paper: 98 / #Citation: 44832

加利福尼亚大学教授、诺贝尔经济学得主



Lloyd Shapley 毕业于普林斯顿大学与哈佛大学，是美国杰出的数学家和经济学家。曾任美国加州大学洛杉矶分校数学和经济学名誉教授，对数理经济学，特别是博弈论理论做出过杰出贡献。他的研究领域包括随机博弈、战略市场博弈、分配博弈、合作与非合作市场模型、投票博弈与权力指数、潜在博弈、成本分配

与组织理论等。2012 年获得诺贝尔经济学奖。

主要科研成就

Lloyd Shapley 被广泛认为是博弈论的创始人之一。他的主要贡献有：沙普利价值、随机对策理论、Bondareva-Shapley 规则、Shapley－Shubik 权力指数、Gale－Shapley 运算法则、潜在博弈论概念、Aumann－Shapley 定价理论、Harsanyi－Shapley 解决理论、Shapley－Folkman 定理。

相关论文精选

1. *Potential Games*

作者：Dov Monderer, Lloyd S. Shapley

期刊/会议：Games and Economic Behavior, no. 1 (1996): 124-143

论文链接：https://www.aminer.cn/pub/53e997aeb7602d9701f88c41/potential-games

2. *On Balanced sets and Cores*

作者：Lloyd S. Shapley

期刊/会议：Naval Research Logistics Quarterly, no. 4 (1967): 453-460

论文链接：https://www.aminer.cn/pub/53e9adf6b7602d9703802fcc/on-balanced-sets-and-cores

3. *On market games*

作者：Lloyd S Shapley, Martin Shubik

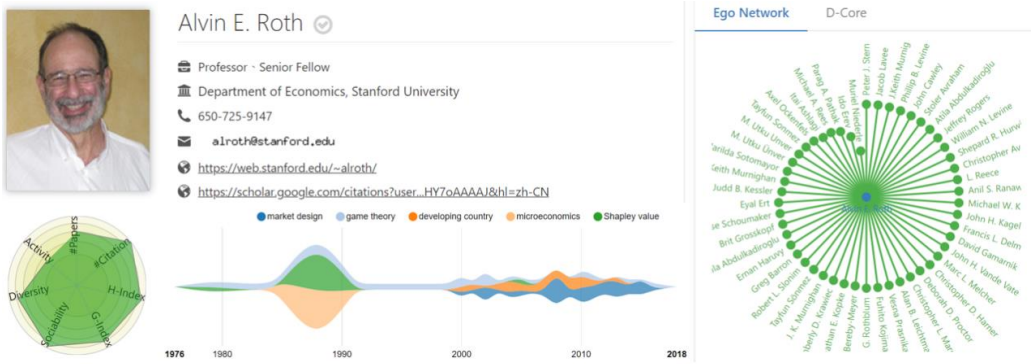
期刊/会议：Journal of Economic Theory, no. 1 (1969): 9-25

论文链接：https://www.aminer.cn/pub/53e9983db7602d9702064490/on-market-games

● Alvin E. Roth

h-index: 99 | #Paper: 363 | #Citation: 49548

斯坦福大学教授、诺贝尔经济学奖得主



Alvin E. Roth 于 1971 年获得哥伦比亚大学学士学位，其后获得斯坦福大学硕士和博士学位。他是美国经济学家，现为斯坦福大学教授、国家经济研究局（NBER）研究员和斯坦福经济政策研究所（SIEPR）高级研究员。曾任哈佛大学商学院经济学与工商管理乔治·冈德教授，曾在伊利诺斯大学和匹兹堡大学任教。

Roth 是美国杰出年轻教授奖斯隆奖的获得者，古根海姆基金会成员，美国艺术和科学院院士，2012 年获得诺贝尔经济学奖。研究兴趣包括博弈论、市场设计与实验经济学等。主要著作包括谈判的博弈论模型（1985）、《实验经济学：六个观点》（1987，2008 年翻译为中文版）、《实验经济学手册》（1995）、《鲍勃·威尔逊传统中的经济学》（2001）等。

主要科研成就

如何以最好的方式将不同的参与者聚集在一起是一个关键的经济问题。Lloyd Shapley 从理论上研究了不同的匹配方法，Alvin Roth 从 20 世纪 80 年代开始，利用 Shapley 的理论结果来解释市场在实践中的作用。通过实证研究和实验室实验，Roth 证明了稳定性是成功匹配方法的关键。Roth 还开发了医生与医院、学生与学校、器官捐赠者与病人的匹配系统。

相关论文精选

1.*Two-sided matching*

作者：Alvin E Roth, Marilda Sotomayor

专著：Handbook of Game Theory With Economic Applications, (1992)

论文链接：https://www.aminer.cn/pub/56d92419dabfae2eeeb0224c/two-sided-matching

2.*Predicting How People Play Games: Reinforcement Learning in Experimental Games with Unique, Mixed Strategy Equilibria*

作者：Ido Erev, Alvin E Roth

期刊/会议：The American Economic Review, (1998)

论文链接:https://www.aminer.cn/pub/56d90a0adabfae2eee10952b/predicting-how-people-play-games-reinforcement-learning-in-experimental-games-with-unique

3.*Learning in extensive-form games: Experimental data and simple dynamic models in the intermediate term*

作者：Alvin E. Roth, Ido Erev

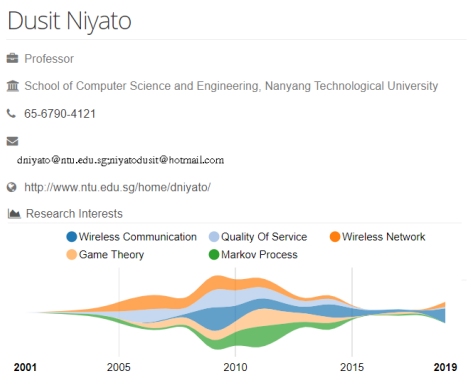
期刊/会议：Games and Economic Behavior, no. 1 (1995): 164-212

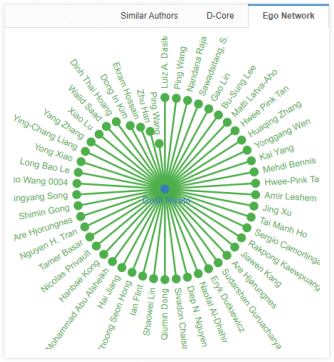
论文链接：https://www.aminer.cn/pub/53e9a7eab7602d9703127ddc/learning-in-extensive-form-games-experimental-data-and-simple-dynamic-models-in

- Dusit Niyato

h-index: 82 / #Paper: 581 / #Citation: 30610

新加南洋理工大学教授





Dusit Niyato 于 2018 年获得加拿大曼尼托巴大学博士学位。现任新加坡南洋理工大学计算机科学与工程学院教授。研究方向是无线通信、物联网和传感器网络的能量收集。目前已在无线与移动通信领域发表了超过 360 篇学术论文，并拥有 4 项美国与德国专利。著有包括《无线与通信网络中的博弈论：理论、建模与应用》等 4 部专著（由剑桥大学出版社出版）。他获得了 IEEE 通信学会亚太地区最佳青年研究者奖项，以及 2011 年 IEEE 通信学会 Fred W. Ellersick 奖。

主要科研成就

Niyato 在和 Ekram Hossain 共同发表的论文《认知无线电网络中频谱共享的竞争性定价：动态博弈、纳什均衡的不足和共谋》中，解决了认知无线电网络中的频谱定价问题。该论文利用贝特朗博弈模型，分析了频谱可替代性、信道质量等系统参数对纳什均衡的影响，并提出了一种分布式算法来求解这个动态博弈。

相关论文精选

1. *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*

作者：Zhu Han, Dusit Niyato, Walid Saad, Tamer Baar, Are Hjrungnes

期刊/会议：Game Theory in Wireless and Communication Networks: Theory, Models, and Applications, (2012)

论文链接：https://www.aminer.cn/pub/53e9b9dab7602d97045d35c7/game-theory-in-wireless-and-communication-networks-theory-models-and-applications

2. *Dynamics of Network Selection in Heterogeneous Wireless Networks: An Evolutionary Game Approach*

作者：Dusit Niyato, Ekram Hossain

期刊/会议：IEEE T. Vehicular Technology, no. 4 (2009): 2008-2017

论文链接：https://www.aminer.cn/pub/53e9aa24b7602d9703394fa5/dynamics-of-network-selection-in-heterogeneous-wireless-networks-an-evolutionary-game-approach

3. *Dynamics of Multiple-Seller and Multiple-Buyer Spectrum Trading in Cognitive Radio Networks: A Game-Theoretic Modeling Approach*

作者：Dusit Niyato, Ekram Hossain, Zhu Han

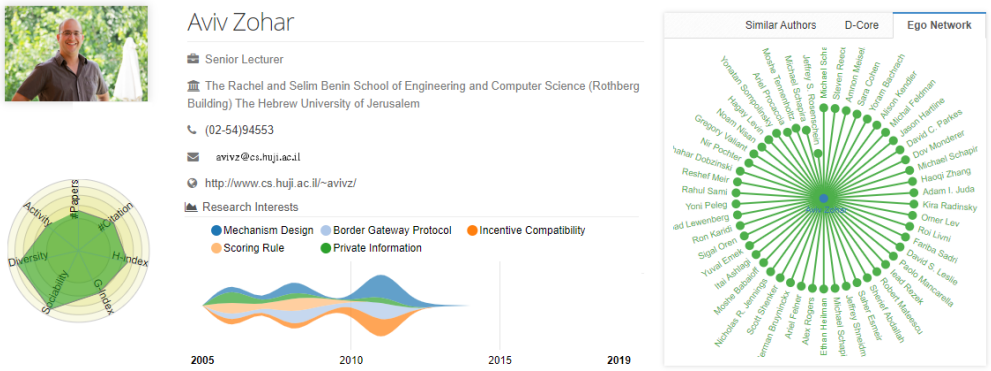
期刊/会议：IEEE Trans. Mob. Comput., no. 8 (2009): 1009-1022

论文链接：https://www.aminer.cn/pub/53e9afe9b7602d9703a3f797/dynamics-of-multiple-seller-and-multiple-buyer-spectrum-trading-in-cognitive-radio

- Aviv Zohar

h-index: 25 / #Paper: 69 / #Citation: 3786

以色列希伯来大学副教授



Aviv Zohar 获得希伯来大学计算机博士学位。现任希伯来大学工程与计算机科学学院的副教授、QED-it 首席科学家。他还是零知识标准化努力的指导委员会的成员和共同组织者，曾担任第五届比特币研讨会的共同主席。研究兴趣包括计算系统和协议的经济学、加密货币、多代理系统、博弈论、机制设计和网络。2013 年 12 月，他在与 Yonatan Sompolinsky 共同发表的论文中，提出了 GHOST

协议，还介绍了使用 GHOST 协议的 BlockDAG 结构。这个结构从本质上将比特币区块链架构变成了树结构，并且提高了比特币的安全性和交易时间。

主要科研成就

成就主要包括四方面。一是 SPECTRE 协议，该协议是一个快速、可扩展、安全的加密货币。二是劫持比特币：路由攻击加密货币，展示了比特币的攻击在网络路由层面。三是最优自利挖掘，关于比特币(缺乏)对战略挖掘攻击的适应能力的工作。四是 Eclipse 对比特币 P2P 网络的攻击，展示了攻击者如何利用 Eclipse 攻击破坏比特币的 P2P 网络，并提出了一些改进措施来缓解这一问题。

相关论文精选

1. *Secure High-Rate Transaction Processing in Bitcoin*

作者：Sompolinsky Y, Lewenberg Y, Zohar A

期刊/论文：Financial Cryptography, pp.507-527, (2015)

论文链接：https://www.aminer.cn/pub/573696d76e3b12023e5d7aa8/secure-high-rate-transaction-processing-in-bitcoin

2. *Optimal Selfish Mining Strategies in Bitcoin*

作者：Ayelet Sapirshtein, Yonatan Sompolinsky, Aviv Zohar

期刊/论文：Financial Cryptography, (2016)

论文链接：https://www.aminer.cn/pub/5736960c6e3b12023e51fe70/optimal-selfish-mining-strategies-in-bitcoin

3. *Hijacking bitcoin: Routing attacks on cryptocurrencies*

作者：Apostolaki M, Zohar A, Vanbever L.

期刊/论文：IEEE Symposium on Security and Privacy, pp.375-392, (2017)

论文链接：https://www.amner.cn/pub/599c7dd3601a182cd2857832/hijacking-bitcoin-routing-attacks-on-cryptocurrencies

4　应用篇

近年来，多个国家在大力促进区块链技术发展的同时，也在加速相关监管机制的设立和优化。在诸多政策的推动下，区块链技术的应用从最初的加密数字货币向多个领域延伸，如贸易金融、供应链、社会公共服务、选举、司法存证、税务、物流、医疗健康、农业、能源等。以下将对几个主要应用场景进行简要介绍。

4.1 数字货币

4.1.1 数字货币概述

数字货币源自电子支付，由电子货币、虚拟货币演化而来，并逐渐与电子货币和虚拟货币分离。目前，金融发展的趋势是“去中心化”和金融脱媒。“去中心化”是互联网发展中信息传递效率提高而形成的扁平化社会关系形态，区块链技术创新使“去中心化”的数字货币发行机制得以实现。**数字货币是最早、也是迄今为止最成功的区块链应用场景。其中，**比特币、以太坊、瑞波币、比特币现金和莱特币是数字货币及其交易平台的典型代表。近年来，基于区块链技术的数字货币受到了各国央行的重视。

数字货币的设计理念实现了由三方模式到两方模式的突破。三方模式是传统货币体系的典型，借方和贷方通过银行这一中介方连接，借贷双方各自通过银行进行资金结算完成债权债务的转移。数字货币则是两方模式，完全通过 p2p 实现的电子现金系统。数字货币在区块链技术创新的支持下具有基于账户和不基于账户两种。

早期的数字货币系统安全性得不到保障，需要解决货币伪造和双重支付两个问题。2008 年 Nakamoto 提出了比特币的概念，**比特币的核心支撑技术就是区块链，区块链技术为比特币系统解决了数字加密货币领域的一大难题：双重支付问题。**双重支付问题，即利用数字货币的特性两次或多次使用“同一笔钱”进行支付。双重支付问题能够解决与比特币防伪技术紧密相关。比特币通过三方面努力解决双重支付问题[44]。第一，比特币所有交易全网公开，每个账号中的比特币数量不是由一个数据表示的，而是根据历史交易得出的，并且，历史交易是经过全网公认的，这样保证了交易信息不被造假；第二，利用时间戳给交易赋予先后顺序，比特币系统中的每一笔交易都是根据上一笔交易生成的，时间顺序避免了双重支付的发生；第三，投入计算资源对交易进行确认，引入 PoW 投入算力打包交

[44] 李靖.比特币的发展研究综述[J].当代经济，2015(31):134-137.

易，使得篡改或伪造信息在数学上无法或几乎不可能实现。在这种分布式节点验证和工作量证明的保障下，比特币在信息传输的过程中完成了价值转移，有效避免双重支付问题。

从本质上来说，数字货币的发展并未脱离信用货币的范畴。作为一种信用货币，数字货币没有实际价值，存在着容易超发的问题，因此数字货币发行的锚定物就相对重要。基于区块链技术，数字货币以信息技术容量为限，采用技术锚定解决数字货币发行量问题。依据数字货币的设计规则，用户通过“挖矿（Mining）”来获得数字货币，数字货币的价值则由“挖矿”消耗的计算处理能量转化而来，这样就实现了数字货币的发行量与网络技术处理能力挂钩。挖矿就是指产生新区块并计算随机数的过程。

去中心化的数字货币依然存在以下问题：一是市场垄断问题，目前货币市场状况尚不符合私有货币理论自由竞争的前提；二是风险监管问题，货币体系需要及时地监管和调控来防范风险；三是数字货币如何公平有效的发行；四是技术革命对数字货币币值的影响。因此，去中心化的风险及监管问题还需要进一步研究探讨。

4.1.2 数字货币分类

根据发行主体，数字货币分为国家数字货币、社群数字货币、企业数字货币。由于数字货币目前发展还不成熟，所以很多国家对其态度非常慎重。近几年来，越来越多的企业涌入区块链行业并积极探索发行自己的代币。

根据数字货币的技术和激励机制等，数字货币又可以分为交易数字货币、实用数字货币和平台数字货币。交易数字货币是为了进行交易，以取消银行的中心化控制，例如比特币；实用加密货币是为特定目的而设计的加密货币，例如 Siacoin；平台数字货币允许创建智能合约，可以快速开发其他解密后的应用程序/加密货币，例如以太坊和 NEO。

■ 纯数字货币

比特币（Bitcoin，简称 BTC）

比特币是一种运用 SHA-256 算法、链式加密结构、点对点（P2P）形式的数字货币，它利用 P2P 网络中众多节点构成的分布式数据库来确认并记录所有的交

易行为。P2P 传输使其具有去中心化的特点，每个节点中都保存着一份区块链账本数据，理论上，矿工可以从任意区块开始向下挖掘新的区块，同时，P2P 去中心化特征和算法可以确保无法通过大量制造比特币来人为控制币值。比特币采用工作量证明和最长链机制两种共识来决定货币分配并保证区块链是有效的[45]。

比特币是自带安全属性的数字货币，被称之为“密码学货币”，该币采用非对称曲线加密算法和哈希算法两种。“非对称密码”是当代密码学最核心的突破，保证了比特币加密和解密采用两种密码，也就是“公钥-私钥”密码不同，私钥可推出公钥，而反之则不能。哈希算法的引入解决了双重花费的问题，避免了僵尸节点对不合格交易的随意确认。

比特币依靠特定算法并通过大量计算产生，但去中心化特征和算法本身使得比特币数量被永久限制在 2100 万个。因此比特币具有极强的稀缺性，也就蕴藏着巨大的升值空间

比特币的技术特点也存在一些缺陷：交易时间长，每笔交易需要六次区块链确认才能不可逆，不能满足小额交易需要；比特币的匿名性导致丢失和被盗都难以找回。

比特币现金（Bitcoin Cash,简称 BCH）

2017 年 7 月 21 日，比特币分叉方案 BIP91 已经获得全网算力支持，但是挖矿巨头比特币大陆旗下的矿池 ViaBTC 准备了一套硬分叉的体系，基于比特币的原链推出“比特币现金”。2017 年 8 月 1 日 20 时 20 分，比特币现金开始挖矿。关于比特币现金是比特币的新分支还是另外一种“山寨币”，业内论调不一。

比特币现金作为比特币的硬分叉币种，遵循比特币创始人提出的通过链上扩容实现全球普及的路线图，区块大小最高支持提升到 8M，删除了隔离验证（SegWit）。相比比特币，比特币现金每个区块可以容纳更多的交易，在一定程度上降低了交易拥堵性。

BCH 采用新的签名哈希类型，提供了重放攻击保护、改善硬件钱包安全性，也解决了二次哈希问题。BCH 还采用新的难度调整算法（DAA），响应式的 POW 难度调整允许矿工按其意愿从旧的比特币链迁移至新链，同时提供保护以抑制算力过度波动。

[45] 贾丽平.比特币的理论、实践与影响[J].国际金融研究，2013(12):14-25

比特币现金并非是首个硬分叉币种，以太坊经典也属于硬分叉货币。在数字货币领域，开发者意见分歧可能导致区块链分裂，而比特币现金和以太坊经典的成功催生出更多的分叉货币。2017 年 11 月 SegWit2x 分叉计划取消后诞生了比特币黄金、比特币钻石、闪电比特币、超级比特币。2018 年 4 月 XMR 修改核心共识算法分裂出 XMR 及 XMC 两条区块链。

门罗币（Monero,简称 XMR）

门罗币是基于 CryptoNote 协议的加密数字货币，着重于隐私、去中心化和可扩展性。CryptoNote 协议可以通过数字环签名提供更好的匿名性，并在区块链模糊化方面有显著的算法差异。

环签名（One-time Ring Signature）技术将签名者的公钥和另外一个公钥集合进行混合，然后再对消息进行签名，这样对于签名验证者来说，无法区分哪个公钥对应的是真正的签名者，实现了不可追踪性，从而为用户的交易信息提供了很好的隐私性。

门罗币采用了隐蔽地址（Stealth Addresses），每次发起一次交易都会先用接收者的公钥随机计算出一个临时中间地址，网络上的其它用户包括矿工都无法确认地址归属，从而保证了不可链接性。不过，这种做法导致公私钥长度变为原来的两倍，再加上环签名技术，签名的产生和验证过程复杂度都明显增加。

瑞波币（XRP）

瑞波币(XRP)是 OpenCoin 公司在 2012 年接管 Ripple 项目之后，为了解决当前跨国清算缓慢，费用高等弊端而发行的建立在 Ripple 结算协议系统内的虚拟数字货币。2004 年一个叫做 Ryan Fugger 的工程师就推出了第一版 Ripple。瑞波币（XRP）可以在整个 Ripple 网络中流通，总数量为 1000 亿，并且随着交易的增多而逐渐减少。

通过 Ripple 支付网络可以任意转账一种货币，包括美元、欧元、日元或者比特币。瑞波币是 Ripple 系统中唯一的通用货币，其不同于 Ripple 系统中的其他货币，其他货币比如 CNY、USD 是不能跨网关提现的。

同比特币一样，Ripple 也是一种可共享的公共数据库，同时它也是全球性的收支总账，这个总账本分布在所有网络节点中并时刻保持同步。瑞波币提出一种共识算法，使一组节点能够基于特殊节点列表表达共识。允许 Ripple 网络中

的所有计算机在几秒钟内自动接受对总账信息的更新，而无需经由中央数据交换中心。这意味着 Ripple 的交易确认时间仅为 3 至 5 秒，而比特币则需要 40 分钟。因此，瑞波币能让小型企业在几秒钟内就能收到客户的汇款，这种迅速到款的特性对管理企业的每日现金流有很大帮助。全球三大转账服务公司 UAE Exchange、MoneyGram 和 Western Union 都已经和 Ripple 建立合作探索基于 Ripple 区块链技术的支付项目。

莱特币（Litecoin,简称 LTC）

莱特币是一种脱胎于比特币，但又与比特币差异化运营的虚拟数字货币。莱特币在技术上与比特币具有相同的实现原理，但也做出一些改进。莱特币在工作量证明算法中使用了由 Colin Percival 首次提出的 Scrypt 加密算法，相比比特币更容易挖掘，交易速度也提高，从而达到每 2.5 分钟就可以出来一个区块，满足了小额即时支付的需求;同时为 Scrypt 算法开发出 FPGA(可编程逻辑门阵列）和 ASIC（专用集成电路），相比比特币的 sha256 更为昂贵；莱特币总产量为 8400 万个，是比特币网络发行货币量的四倍之多。较大的供应将确保它总是比比特币相对便宜。

莱特币与比特币的技术相似性使其具有后者的弱点，包括交易可锻性、区块扩容问题等，为此，莱特币已经在 2017 年成功应用隔离见证技术（SegWit），像 Lightning Network、MAST、机密交易、Schnorr 签名等这些技术一样最初的对象都是比特币。

Libra 加密货币

2019 年 6 月 18 日，Facebook 发布 Libra 白皮书，正式推出虚拟加密货币。最初由美元、英镑、欧元和日元这 4 种法币计价的一篮子低波动性资产作为抵押物。除了 Facebook 之外，VISA、Mastercard、Paypal、Uber 等大机构都参与其中。2020 年 4 月 16 日，Libra v2.0 版本白皮书发布。Libra 白皮书 2.0 的主要变化在于新增锚定单一法币的单币种稳定币方案，并调整原先的多币种稳定币 LibraCoin（LBR）为这些单币种稳定币的固定权重组合。Libra 采取积极拥抱监管的态度，放弃长期向公有链过渡的计划、导入分层监管和准备金机制，但又同时保持超主权货币设计理念、区块链技术框架，以及普惠金融的宗旨不变。

Libra 是一种零知识证明协议，可实现极快的证明者时间以及简洁的证明大

小和验证时间。它不仅在渐近性上具有良好的复杂性，而且其实际运行时间也完全在启用实际应用程序的范围内[46]。

Libra 推出之后，引发了世界范围的强烈反响，多数国家对其谨慎甚至反对态度，如表 12 所示。2019 年 7 月，美国众议院金融服务委员会举行有关 Facebook 虚拟货币的听证会；10 月，PayPal 宣布放弃参与 Libra 以法国为首的欧盟五国联手抵制 Libra 进入欧洲市场，并要求 Facebook 放弃该项目。

表 12　主要国家对 Libra 的态度

国家	态度	监管态度
中国	谨慎	已经认识到 Libra 是对传统货币形式的潜在威胁，可能会将数字货币的发行委托给商业实体，中国央行已开始开发自己的数字货币以应对。
美国	反对	众议院金融服务委员会要求 Facebook 及其合作伙伴停止开发 Libra stablecoin 和 Calibra 钱包。
法国	反对	强烈反对稳定币成为传统货币替代品的想法。
德国	谨慎	监管机构应该密切关注
英国	中立	需要仔细检查
俄罗斯	反对	将不会在俄罗斯合法接受，因为它可能对该国的金融体系构成威胁。
日本	谨慎	已设立一个联络会议，负责调查 Facebook 稳定币对货币政策和金融稳定的影响。
韩国	怀疑	该项目没有受到监管，可能会变成洗钱通道
新加坡	中立	监管机构需要准确了解科技巨头的系统将如何运作。

■ 支持智能合约的货币

以太坊（Ethereum, 简称 ETH）

以太坊是一个开源的具有智能合约功能的公共区块链平台，于 2015 年由程序员 Vitalik Buterin 发表上线。以太坊是区块链 2.0 的典型代表，由其专用货

[46] Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation[R], by Tiancheng Xie, Jiaheng Zhang, Yupeng Zhang, Charalampos Papamanthou, and Dawn Song on February 12, 2020 at 10:00 AM,

币以太币提供去中心化的虚拟机（Ethereum Virtual Machine，简称 EVM）来处理点对点合约。以太坊虚拟机是以太坊的核心，可以执行任意算法复杂度的代码，它使用了 256 比特长度的机器码，是一种基于堆栈的虚拟机，用于执行以太坊智能合约。

以太坊使用混合型的共识协议，前期使用 PoW 挖矿算法，后续将逐步切换为 PoS 机制。PoS 基于矿工拥有的数字货币数量和持有时间进行分配，相比 PoW 能源成本更低，网络更高效，PoS 网络的安全由用户在网络上持有 Token 来保证，而不是用户提供算力来保证 PoW 网络的安全。PoS 机制下，拥有更多财富的个人比拥有较少财富的个人获得创建区块和交易费用的机会更大，这意味着将加大财富差距。

以太坊采用区块链的原理，允许在区块链上创建智能合约，这是其最大的特点。智能合约是一种应用，能够存储数据、封装代码、执行计算任务。目前以太坊支持 Solidity、Serpent 和 LLL 三种语言编写的智能合约，可以根据的习惯选择不同的高级语言，其中，Solidity 最为流行。

以太坊发行总量不设上限。2018 年曾经因为以太坊创始人 Vitalik Buterin 提出的为以太坊设置总量上限提案，网上掀起过一场有关“应不应该给以太坊总量设上限”的激烈讨论。Vitalik Buterin 提议将以太坊上限设置为 1.2 亿个。目前，以太坊尽管没有总量限制，但越往后，其产量提升越难。

据 stateofthedapps 网站 2018 年 3 月的统计，目前在全球已有 1252 个以太坊应用诞生，随着时间的推移将会有越来越多的项目在以太坊平台上构建。Ethereum 上的应用程序都需要锁定 ETH 作为抵押品才能正常工作。不过，以太坊每秒只能处理 20 个交易，而所有应用都只能共用一条主链，从而导致网络拥堵效率低，扩展性也不足。以太坊 2.0 预计将在 2020 年第二季度末推出，它是当前以太坊主网的 PoS 版本，计划通过引入了分片技术来提高网络吞吐量。

以太经典（Ethereum Classic,简称 ETC）

以太坊经典来自以太坊的一次硬分叉，ETC 坚持去中心化、不可逆转、不受第三方审查干扰的原则。ETC 从 2017 年 12 月起每 500 万个区块链减产 20%，最终总量固定在 2.1 亿至 2.3 亿之间。

ETC 采用 POW 共识算法，任何动态组网接入的节点都有利可图，ETH 则将改

用 POS 共识算法。ETC 已经将 EVM（以太坊虚拟机）替换为速度更快的 SputnikVM，以适合开发物联网应用。以太坊经典目标是成为去中心化的物联网基础设施。另外，ETC 采用的侧链技术具有交易免费的特点，普通个人设备也可享受这种服务。

达世币（Dash）

达世币原名暗黑币，于 2014 年推出，是一款支持即时交易、以保护用户隐私为目的的数字货币，总量约 2200 万。相比其他数字货币减半，该币每年的供应按照 7%的速度减产。

达世币采用广泛使用的链接运算“X11 哈希算法”，减少专门为数字货币挖矿涉及的 ASIC 使用的概率。达世币采用独创的“服务量证明”机制，引入 two-tier 激励模型，也就是主节点网络技术，而非单层激励模型，使得添加更多类型服务成为可能；该币所应用的 Darksend（匿名发送）技术除了具有 CoinJoin（提供匿名技术的软件）核心理念，还具有去中心化、使用链接实现强匿名、相同面值和被动先进的混币技术。

零币（Zcash，简称 ZEC）

零币是基于比特币 0.11.1 版本代码基础上进行修改的分支，保留了比特币原有的模式，总量 2100 万个。与比特币的区别在于，零币使用了先进密码学技术自动隐藏了交易信息，只有持有私钥的人才有权限查看交易信息。

零币首个实施零币协议的数字货币。零币协议使用零知识证明来实现完全的金融隐私。零知识证明是一种密码学方法，其中一方可以向另外一方证明某个给定的声明是正确的，除了该声明确实是正确的意外，无需传达其他的信息。零币协议允许很多匿名设置，使其在金融隐私方面相比其他协议更有效。

零币采用的工作量证明机制引入了卢森堡两位博士提出的 equihash 理论，削弱了专业矿机的显卡设备优势，强化内存带宽为 PoW 的瓶颈，为大众挖矿打下基础。

■ 央行 DC/EP

DC/EP 是央行发行的数字货币的英文简称，其中，DC 是指数字货币（Digital Currency），EP 则是指电子支付（Electronic Payment）。DC/EP 属于央行负债，具有国家信用，与法定货币等值。

DC/EP 借鉴应用了区块链部分组成技术，例如，利用智能合约实现资金的定

向流通，利用非对称加密认证身份。其中，比特币区块链中的非对称加密与“传统”的数字身份认证类似，或将被用于 DC/EP 的大量场景，例如，由用户钱包的安全模块生成公、私钥对，两者一一对应，公钥可公开，私钥不公开，私钥可用于对消息签名，公钥可用于验证私钥签名后的信息，以此确认私钥所有者的身份。全球央行一直在关注货币数字化演进状况。早在 1996 年，10 国集团(G10)的中央银行专门在国际清算银行(Bank for Int'l Settlements，简称 BIS)开会讨论电子货币对支付体系和货币政策的潜在影响以及央行的应对策略，并委托 BIS 密切关注电子货币在全球的应用情况。自此以后，BIS 定期发布对于电子货币发展情况的调研报告。近年来，主要经济体央行加快了应对策略的研究和评估进程。中国人民银行一直高度关注数字货币发展，并积极开展相关研究工作。相关研究发现[47]，基于分布式账本的共识记账和国密 SM2 运算是影响央行数字货币转移性能的关键操作。

从使用场景上看，DC/EP 不计付利息，可用于小额、零售、高频的业务场景，相比于纸币没有任何差别。DC/EP 不需要绑定任何银行账户。即便在没有网络的情况下，其双离线技术可保证两个装有 DC/EP 数字钱包的手机碰一碰，就能实现转账或支付功能。

需要注意，央行数字货币和比特币、以太坊、Libra 等有着本质区别。央行数字货币是法定的数字货币，是由国家来发行的，是法币的数字化。比特币等是非法定的数字货币，在法律允许的框架内，发行主体不受限制。比特币是去中心化的，而央行数字货币则是中心化的管理模式。

4.1.3 数字货币优点和风险

数字货币有着其他货币无可比拟的优点。首先，数字货币可以有效降低银行经营成本，无论是发行还是交易都有着低成本高效率的特点。从发行环节来看，数字货币不会产生实体货币发行所需要的成本费用，从交易环节来看，数字货币不需要建立和维护个人账户，而是完全使用电子记账的方式，并且数字货币的交易账簿也不需要货币清算，节省了交易成本。其次，数字货币推动了共享金融的发展，数字货币的交易基本不需要金融中介机构的介入，同时与物联网等现代科技紧密结合。此外，数字货币可以有效解决互联网金融监管面临的信息不对等等

[47] 姚前.中央银行数字货币原型系统实验研究[J].软件学报,2018,29(09):2716-2732.

问题，简化数据处理流程，更进一步推动了互联网金融的发展。除此之外，数字货币的核心技术区块链更是在金融、物流等领域得到了广泛地应用。

数字货币也存在着风险。以比特币为例，自诞生以来，其价格经常剧烈波动，这也是多数国家对于比特币的政策仍持保守态度的原因之一。选择具有稳健价值的锚定物，是货币获得稳定价值的关键。作为私人发行的数字货币，比特币的价值来源为个人投机，价值不稳，公信力不强，可接受范围有限，容易产生较大负外部性。一方面，从比特币产生机制上看，在去中心化的比特币系统中，任何人都可下载运行比特币软件并参与比特币生产，只要创建一个区块，便可拥有该区块中包含的比特币，但是，由于比特币总量固定，相当于不可再生资源，因此，参与“挖矿”的人数越多，算法越复杂，“挖矿”的成本也越高，开发新比特币的难度就越大。另一方面，从比特币的交易模式来看，比特币的发行和交易集中于“私人小圈子”，交易流程灵活化、个性化，却缺乏强大机制保证其不会违约。由于比特币是虚拟商品，不产生实际经济价值，一旦违约，持有者将没有任何担保或索赔权。由比特币的价格走势可见，随着比特币存量不断减少，剩余比特币价值迅速上升，具有很大的投机性质。因此，比特币在自身稳定价值和稳定投资者信心的机制建设上仍然不够完善。

虽然比特币拥有国际通用、流通的价值特性，并且拉动了一系列新兴产业的发展，如比特币交易所、第三方支付平台、比特币投资行业、“挖矿”行业，但这些新兴产业基本处于监管的“灰色地带”，没有统一的交易机制进行约束，因此，坐地起价、违约现象时有发生，难以追踪打击，也容易诱发投机行为、金融欺诈和道德风险。目前，**世界上多数国家对其并不友好，仅有少数国家将比特币纳入监管体系。**除了德国于 2013 年 8 月宣布承认比特币的合法地位并纳入国家监管体系，是世界上首个承认比特币合法地位的国家；日本于 2016 年 5 月批准了数字货币监管法案，后又正式立法承认比特币是一种支付方式，多数国家并没有承认比特币的合法地位。

在中国，早在 2013 年 12 月 5 日，中国人民银行联合五部委发布《中国人民银行工业部和信息化部 中国银行业监督管理委员会 中国证券监督管理委员会 中国保险监督管理委员会关于防范比特币风险的通知》，明晰了比特币的属性是“特定的虚拟商品”，禁止各金融机构和支付机构开展比特币相关业务，加强比

特币网站管理，防范比特币潜在洗钱风险，并加强对社会公众货币知识的教育及投资风险提示。2017 年 9 月 30 日，比特币中国关闭所有交易功能，标志着比特币交易在国内已被全面禁止。2018 年 1 月，央行下发《关于开展为非法虚拟货币交易提供支付服务自查整改工作的通知》，严禁辖内各法人支付机构为虚拟货币交易提供服务，并采取有效措施防止支付通道用于虚拟货币交易。2018 年 8 月，中国银行保险监督管理委员会、中共中央网络安全和信息化委员会办公室、公安部、人民银行和市场监管总局联合发布《关于防范以“虚拟货币”“区块链”名义进行风险集资的风险提示》。2020 年 1 月中国人民银行工作会议强调 2020 年继续稳步推进法定数字货币研发；2 月中国人民银行正式发布《金融分布式账本技术安全规范》（JR/T 0184—2020）金融行业标准。该标准规定了金融分布式账本技术的安全体系，包括基础硬件、基础软件、密码算法、节点通信、账本数据、共识协议、智能合约、身份管理、隐私保护、监管支撑、运维要求和治理机制等方面，适用于在金融领域从事分布式账本系统建设或服务运营的机构。

4.2 区块链其他应用场景

区块链系统具有分布式高冗余储存、时序数据且不可篡改和伪造、去中心化信用、自动执行的智能合约、安全和隐私保护等显著特点，因此，区块链不仅可以应用于数字加密货币领域，同时还广泛应用于金融服务、智能制造、供应链管理、文化娱乐、社会公益和政府管理等多个领域，如图 21 所示。在今年的新冠疫情防控中，区块链也发挥了重要作用，如公益捐赠追溯、疫情信息监测和预警等，具有极大的应用探索空间和发展潜力。区块链技术应用呈现出传统大公司重点布局整个生态链及基础平台、初创企业注重某个行业的具体应用的特征。

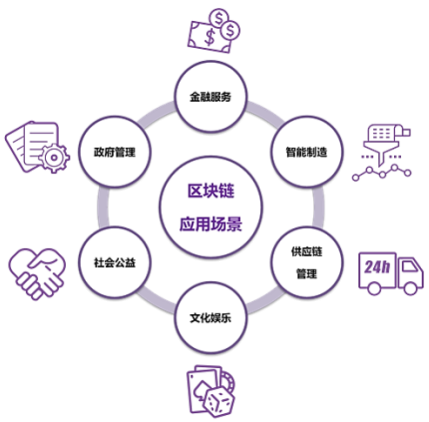


图 21　区块链主要应用场景

4.2.1 金融服务

区块链的核心创新点在于去中心化信用，能够不依靠中心机构信用背书建立金融市场，成为“金融脱媒”的重要实践，也对传统金融机构、金融服务模式产生极大冲击。**区块链在金融领域的应用，体现在证券与银行业务、资产管理、贸易融资、保险业务、反洗钱业务和票据交易等方面。**

在证券银行业务方面，区块链可编程的特性能够提高证券交易与金融服务的效率，节约交易成本，并简化交易流程。同时，区块链和比特币即时到账的特点可使银行实现比 SWIFT 代码体系更快捷、经济和安全的跨境转账以及银行间结算与支付。相比之下，传统金融服务在跨境支付领域存在多个痛点。比如，需要经过开户行、央行、境外银行、代理行、清算行等机构，每个机构都有自己的账务系统，这些复杂的过程不仅加大了交易成本也占据了用户更多的时间，因此造成交易的速度慢、效率低。自 2015 年以来，全球主流金融机构纷纷开始布局区块链，以高盛、摩根大通、瑞银集团为代表的银行业巨头分别成立各自的区块链实验室、发布区块链研究报告或申请区块链专利，并参与投资区块链初创公司。除此之外，上海证券交易所、纳斯达克、纽约证券交易所、芝加哥商品交易所等多国证券交易所也对区块链技术进行深入探索，包括证券交易与发行中的主数据管理、证券等资产的发行服务、资产交易、交易确认、复杂资产记录和匹配、净额清算、担保品管理、结算等。

在资产管理方面，区块链的时间戳技术和不可篡改的特性为防假防伪、知识产权保护、资产授权和控制提供便利，对无形资产管理和有形资产管理方式都进行了革新。传统的资产管理从规划、部署、运营到运输、跟踪、处置等全过程很复杂，涉及供应商、物流公司和客户等多个利益相关方的数据系统。一旦有环节出现问题，很难让所有系统对资产的实际状态达成共识。解决这些问题需要很高的成本，而且会造成延迟。利用区块链技术，能够捕获资产所发生的所有交易和状态变化，并且提供每种资产的核心信息的单一事实来源，允许交易在一个计算机网络上进行电子验证，无需中心账本。这样，无论资产在供应链中进行转移的过程中发生了什么，所有利益相关者和系统都能了解它的状态。

在贸易融资方面，区块链凭借数字加密、点对点技术、分布式共识与智能合约，能够实现信息的快速、透明交换，克服了人工搜集数据、核对信息、贸易接

洽的高成本和潜在风险。一个完整区块链贸易融资平台，能够在线全流程管理并实时掌控贷前调查、贷中审核、贷后管理各个方面，让贸易融资流程简化。代表着在国际贸易中的应用与低交易成本时代来临。

例如，福费廷业务是指银行等金融机构无追索权地从出口商或其他金融机构那里买断由于出口商品或劳务而产生的应收账款。在传统的福费廷交易中，由于缺少一个可以多方协作的公开可信平台，银行常常面临着缺乏公开报价市场、多主体双边交易标准不统一等问题。而引入区块链技术之后，能够使这些问题迎刃而解。目前福费廷在区块链技术上的应用已经有不少成功案例。例如，国内的中国银行、中信银行、民生银行联合开发并于 2018 年 9 月推出了基于“分布式架构、业务环节全上链、系统衔接全自动”的“区块链福费廷交易平台”。该平台采用联盟链的形式，依据银行间交易业务场景，自主研发区块链应用层功能，独创 Business Point 管理端，有效便利衔接银行多层级组织管理架构。

在保险业务方面，区块链将对传统保险模式带来变革性的影响，目前的应用较多处于技术验证阶段。保险业目前存在海量信息整合和共享难、信息不对称、数据泄露等问题。区块链技术利用其特性可以帮助保险业实现行业内、行业间以及用户间大量分散节点的信息分享和连接。例如，区块链的可追溯特性，可以让保险服务流程更透明；保险公司所有的理赔记录都能够在全网公开并被集体验证，防止“双重索赔”现象发生，防范骗保行为，规范保险秩序。此外，区块链的安全性，可以解决数据传播中的隐私保护及商业信息安全问题；而区块链的共识机制，则从源头上进一步保障了交易的可信度。

在反洗钱业务方面，由于数字货币式存储在计算机中的电磁符号，不存在物理形态的仿冒或改变，能够从源头上组织假币问题泛滥。同时，数字货币认证登记系统能够鼓励商业银行、工商企业和居民个人共同识别打击数字货币造假和洗钱问题。反洗钱工作需要大量的信息情报、尽职调查和巨大的监管成本。从目前各金融机构反洗钱机制来看，仍然存在着客户身份识别效率低、反洗钱工作信息化程度低、反洗钱监管成本高以及金融机构间相关数据不同步不共享等问题。引入区块链可以实现跨国家和跨部门数据按需即时共享和实时监管。

此外，将区块链技术引入到金融机构内部进行日常身份登记验证、金融交易及检测审计环节中，可以实现监管规则的数字化、自动化、智能化，有助于进一

步完善金融机构反洗钱事前预防、事中监控及事后处置流程，提升金融机构和监管部门的反洗钱水平。

基于区块链的数字票据可以替代现有电子票据的构建方式，实现价值的点对点传递。传统电子票据因为人为介入较多，存在很多违规操作的发生风险。相比而言，拥有去信任、时间戳、非对称加密、智能合约等特征的区块链，可以解决目前票据市场存在的真实性、及时性、违规操作等问题，弥补了电子票据的不足。目前已有很多区块链发票应用场景落地。例如，2018 年，腾讯在深圳某餐厅亮相区块链电子发票；蚂蚁金服在杭州、台州、金华三地医院开出 60 万张区块链电子票据。

4.2.2 智能制造

智能制造是在制造过程中采用诸如分析、推理、聚类、分类、回归等智能活动辅助或直接决策，通过人与智能机器的合作共事，去扩大、延伸和部分地取代人类专家在制造过程中的脑力劳动[48]。《中国制造 2025》提出“创新驱动、质量为先、绿色发展、结构优化、人才为本”的基本方针，在新一轮科技革命和产业变革与我国加快转变经济发展方式形成历史性交汇的背景下，提升制造业效率和竞争优势成为建设智能制造格局的重心。

智能制造区别于传统制造的关键在于知识的产生及应用。传统制造业存在生产链长、生产要素多等不足。区块链技术的广泛应用不仅可以弥补传统制造业的不足，降低生产成本、提升利润率，而且可以帮助制造业建立安全完整的数据库、产品信息追溯链，加快制造业的转型升级。区块链技术可以让供应链系统以及从原材料到制造、测试和成品的生产链变得更加透明、实时和可见，以便制造商能够快速检测并解决突发问题，减少设备停机时间。区块链技术能够利用大数据分析为制造企业提供更为高效、安全的运营机制，让制造企业第一时间掌握库存、产能、订单和市场供求信息，提升企业上下游互联互通水平。除了实时信息交换，区块链技术可以利用智能合约，实现订单的发布、采购，更快响应生产需求，加速业务流程并获得更高的运营效率。

[48] 百度百科，https://baike.baidu.com/item/智能制造/4753603?fr=aladdin

4.2.3 物联网与供应链管理

区块链基于共享账本、智能合约、机器共识、权限隐私等技术优势，在工业互联网的各领域中广泛渗透和融合创新，能够降低中心化架构高额运维成本，保护用户的数据和隐私，还可以打破物联网现存的多个信息孤岛桎梏，提升工业制造各环节生产要素的优化配置能力，加强生态多主体之间的协作共享，而且能够以低成本建立起互信的“机器共识”和“算法透明”，促进信息的横向流动和网间合作，加速重构现有的业务逻辑和商业模式。区块链+物联网融合正成为数据共享、协同创新、柔性监管的新模式和新范式。

区块链与物联网的结合掀起了供应链管理领域的深刻变革。传统供应链管理面临由于信息不对称导致的效率低下、协调困难等问题，在流程追踪和统筹安排方面困难重重。区块链“去中心化”特性能够使交易网络信息公开化、透明化，保证信息流的完整与流畅，可以在很大程度上减少交易各方之间的信息不对称、提高供应链周转效率，还可以确保参与各方能及时发现供应链系统运行过程中存在的问题，找到应对问题的方法。同时，区块链数据不可篡改、时间戳和交易可追溯的特征能很好地运用于解决供应链体系内各参与主体之间的纠纷，实现有效举证与追责，并且还能够有效遏制供应链管理中假冒伪劣产品问题，形成完整的供应链闭环。区块链与供应链融合，能够提高供应链之端到端的数据透明度，降低成本和风险，同时有效解决信息孤岛现象，打通采购、生产、物流、销售、监管等一系列环节。

目前，区块链+供应链的落地方式非常依赖于物联网技术，通过物联网技术将实现线下数据以 RFID 射频识别、二维码、商品条码、近场通信等方式连接到线上，主要落地领域涵盖覆盖食品生鲜、医疗药品、珠宝奢侈品方面。2018 年以来，基于区块链的供应链项目在应用落地方面呈现多头并进的形式。例如，在电子商务领域，东已经将区块链与物流结合，用于加强食品安全；菜鸟与天猫国际共同宣布启用区块链跟踪、上传、查证跨境进口商品物流全链路信息。在零售业领域，沃尔玛从进货、管理、配送，及供应链的各个环节全面拥抱区块链变革，并宣布从 2019 年 9 月开始，沃尔玛超市以及山姆会员店的新鲜绿叶蔬菜供应商要使用 IBM 开发的数字分类账技术，以实现产品的实时、端到端的可追溯性；苏宁于 2018 年 7 月《苏宁区块链白皮书》，宣布计划用区块链助力智慧零售健康发

展，称将会大规模应用区块链技术，尤其是在与信誉、契约相关的产品溯源上。

4.2.4 文化娱乐及传媒

文化娱乐及传媒业涵盖数字音乐、数字图书、数字视频、数字游戏等，存在着大量的可复制的数字资产，容易出现篡改、盗版及交易纠纷等问题。利用区块链的不可篡改和公开透明等技术特性，可以实现针对这些数字资产的版权证明，同时还能大幅提高相关流转的安全性和隐私性。

在音乐领域，区块链技术将在实现粉丝经济最大化、解决数字音乐版权管理难题、帮助音乐人实现完全创收等方面颠覆现有音乐产业格局。区块链可以使音乐行业的整个生产和传播过程中的收费和用途都变得透明、真实，并能有效确保音乐人直接从其作品的销售中获益。利用区块链平台，音乐人可以跨过出版商和发行商，自行发布和推广作品，不需要担心侵权问题，还能更好地管理自己的作品。除此之外，也可以利用区块链进行文化消费端的众筹服务，使消费者能够参与到 IP 创作、生产、传播和消费的过程中，而不需要依靠第三方众筹平台。

全球最大音乐流媒体平台 Spotify 于 2017 年收购了区块链初创公司 Mediachain。该公司可以通过提供开放源代码对等数据库和协议的方式，让创作者将自己的身份与其作品关联起来，进而能够确保所有歌曲都能追踪到创作者和版权所有人信息，并由 Spotify 使用合理的途径支付版权费用，同时也能缓解流媒体平台与版权所有人之间的矛盾。此外，在全球范围内拥有超过 20 万音乐人客户的数字版权管理及货币化初创公司 Vydia 于 2018 年完成了 700 万美元的 A 轮融资；MIT 的 Media Lab 已经与伯克利音乐学院合作的音乐区块链应用项目，能做到去中心化分发内容。这项由三大版权公司、英特尔、Spotify 和 Netflix 参与的大项目成为区块链技术能否在全球音乐产业里大规模推广使用的重要转折。2019 年 9 月，华纳音乐集团投资了区块链游戏公司 Dapper Labs 1120 万美元，共同合作开发新的公共区块链平台 Flow，以创建新的数字资产。

在游戏行业，区块链技术的应用在区块链游戏、游戏基础研发、基于区块链的道具交易平台、特色内容的版权保护、支付环节、分布式算法硬件发售等方面。根据 DappRadar 的统计数据，目前全球范围内至少已经出现了 100 多款区块链游戏。这些游戏中主要分为宠物养成类、地产类、经营类、购买类和博彩类等。区块链不仅可以保障玩家在虚拟世界的合法财产，还可以避免虚拟资产交易中的欺

诈现象。

在内容分发领域，区块链技术围绕媒体信源认证、公民新闻审核、数字版权保护、付费内容订阅、传播效果统计、用户隐私保护、数字资产管理等一系列应用，为媒体深度融合提供了全新的视角和解决方案。

在文化旅游领域，区块链可以解决旅游业由于信任不足所产生的一系列问题。利用区块链技术分布式存储、去中心化、数据不可篡改等特性，一方面可以使旅游产品的消费变得有迹可循，降低消费者买到假冒伪劣和不安全产品的概率，另一方面可实现不同区域间的信息共享，降低在线旅游平台巨头垄断导致的运营成本上升问题，缩短产业链并严防出行用户隐私信息泄露；将平台信息透明化，增加服务者消费者之间的信任，解决点评造假等问题。目前较多的论调是区块链将为旅游业带来颠覆性的革新。

4.2.5 民生公益

2019 年 10 月，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习，习近平总书记在主持学习时强调指出：要探索“区块链+”在民生领域的运用，积极推动区块链技术在教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用，为人民群众提供更加智能、更加便捷、更加优质的公共服务。

社会公益与区块链的结合，集中体现在区块链不可篡改性和高透明度的特征上。公益事业信息的不公开、不透明成为社会公益难以发展和存在争议的重要原因。公益援助中还会存在一些援助捐赠遗失问题，可能牵扯到官僚主义、转移成本和腐败等多种因素。为了解决公益捐赠遗失或真实到达的问题，世界各地的慈善机构纷纷转向区块链技术。区块链公益既能有效减少成本，使援助流程更高效，又能利用区块链技术的透明性提高援助资金的可追溯性和可信性。区块链上存储的数据利用了分布式技术和共识算法，以共信力助力公信力，天然适用于公益场景。公益项目的相关信息，如资金流向、捐助对象、募捐明细等，都能够加入区块链节点，受到全网的验证与监督。区块链与公益结合，让区块链真正成为“信任的机器”，让社会公益的运作“在阳光下进行”。

例如，在约旦难民援助过程中，联合国通过其技术合作伙伴使用区块链技术进行资金援助和支持，难民可以通过一个基于以太坊的支付平台获得财政援助。

在中国，区块链技术也被用于精准扶贫、助残，运用区块链平台记录贫困、残障人员的身份信息，特别是在贵州省，已有多个市区开始相关项目的上线和运用。案例包括腾讯“公益寻人链”、支付宝听障儿童公益基金、“心链”等项目。

在医疗领域，电子健康病例是区块链最重要的应用，此外，还有 DNA 钱包、药物防伪、比特币支付、蛋白质折叠等许多区块链应用。医疗数据安全和患者隐私保障仍是医疗行业的核心问题。区块链作为“分布式账本”，具有透明共享、时间戳、不可篡改等特点，可以为医疗数据的安全流通保驾护航。区块链可以实现医疗信息全过程的记录，包括患者的就医记录和医疗用品整个供应链过程。保证了医疗信息的真实性和完整性。在电子健康档案（EHR）方面，个体完整的健康历史记录对精准治疗和疾病预防有很重要的价值，区块链可以做到将这些数据实时存储和共享。此外，区块链可采用多私匙加密，查看用户链上数据需要用户私匙授权，这样可以保证用户敏感数据的合法流通使用，而不会泄露给不法分子、被恶意利用，一旦出现问题是可以溯源追责的。

目前，多个国家正在与商业机构合作建立基于区块链的医疗信息体系。例如，美国疾病控制与预防中心（Centers for Disease Control and Prevention，简称 CDC）与 IBM 签署合作协议，联合利用区块链技术存储和交换医疗数据，以便更好的共享电子医疗记录、临床试验以及从可穿戴设备收集的健康数据。国内也有个别地区开展了区块链与医疗结合的项目，如佛山市禅城区启动了全省首个“区块链+疫苗”项目建设，旨在实现疫苗流通过全过程的可视化监管，并简化疫苗预约接种流程。

药品监管的核心难点在于生产环节记录造假、流通环节信息封闭。基于区块链技术的药品监管体系将大大改进目前药品安全现状，呈现一个更公开、更透明、可溯源的药品监管态势。区块链上的每份药品都具备唯一的商品信息，可以公开识别其真实性。企业可以通过区块链了解原材料的生产和运输情况，政府也可以通过区块链跟踪药品，了解药品加工、出厂、质检、交易及使用的各个环节，消费者也能知道产品各个信息。区块链+药品监管将最大程度保证消费者的基本权益不受侵犯、提高食品药品监管体系的工作能力、重拾消费者的信任。

区块链技术还可实现传染病的精准管控和智能追踪。利用区块链的分片机制，依托区、市、省和国家各级的疾控中心，建立区块链自动化数据同步网络，建立突

发传染病数据采集和实施预警自治能力，同时,通过国家级防疫链不断更新和补充其他省份的数据,形成实时自动化的数据交换机制,成立具备一定区域自治能力的防疫网络。

在教育领域，区块链应用主要体现在学位认证和学习证明的信任、学生档案管理、学术资源共享等方面，涉及到教育机构、课程形式和知识库等。

传统教育机构试验利用区块链技术对其资格证书进行验证，可以降低成本，消除欺诈并简化跨机构间的学分认证。例如，位于美国旧金山的 Holburton 学校是一所软件教育学校，提供作为大学课程的另一选择的项目教育。该学校已经在使用区块链来存储和发布的证书，能够防止认证造假。麻省理工学院试点使用比特币区块链进行学位认证，并开放源代码。

区块链为教育机构或组织提供了低成本的共享资源。在国家层面，国家区块链数据库可以解决本国内部系统中的各级证书的验证和共享。在全球层面，基于区块链技术的学历资质数据库也在尝试中。例如，索尼全球教育的基于区块链的平台可以用于评估成绩，目标是为全球的学校和大学使用该服务，以便个人可以与雇主等第三方共享数据。此外，运用区块链技术保存学生档案，可以保证安全性和保密性，并且区块链有其独特的去中心化优势，被记录在档的文件能够立即根据需要被调用。

区块链可能促进产生一个点对点的知识生态系统。很多初创企业和项目正在使用区块链技术来支持点对点知识交换。这些模型将知识直接与需要知识的人联系起来，将“机构化的中介”实现去中介化，可以大幅度降低教育成本。

此外，**将区块链技术应用在房地产和土地登记、交易方面，可以提高透明度，增强可追溯性，保证房产交易安全性。**目前，印度、俄罗斯、乌克兰、迪拜等国家都已表示将尽快利用区块链技术，对土地登记或房地产交易的流程进行改造转移。其中，乌克兰政府欲建立区块链房地产平台，使外国投资者可在此平台低价安全地购买优质房产。迪拜土地局则表示在未来 2-3 年内将所有房地产记录在区块链上，并创建基于区块链技术的庞大数据库。

区块链在交通运输领域的应用也颇有前景。从物流到高速公路收费，从交通大数据分析到基础设施建造工程的招投标和质量溯源，区块链技术将信息化发展推向了新的水平。2020 年 2 月，中国交通运输部印发《关于大力推进海运业高

质量发展的指导意见》，提出要推进基于区块链的全球航运服务网络平台研究应用。泰国邮政和国家铁路局也将采用区块链技术改善国内物流服务，实现邮政服务和铁路运输的现代化建设。

4.2.6 政府管理

目前国内多地开始尝试将政府业务“上链”，如南京、天津、佛山、青岛等地区政府，启动了基于区块链技术的平台，打造更加方便快捷且安全可靠的政务服务。有研究显示[49]，2018 年公布的政府招标采购项目中，有 18 项与区块链相关，2019 年公布的政府招标采购项目中与区块链相关的则达到了 31 项，其中区块链+政务的项目达到 12 个。可以看出，政务应用在 2019 年政府采购区块链项目类别中占比最大，占所有政府采购区块链项目的 39%，占区块链应用类项目的 54.5%。这些**区块链政务应用涉及到数字身份、电子存证、电子票据、产权登记、工商注册、数据共享、涉公监管、行政审批等诸多场景。**

在身份认证方面，传统的身份认证系统常受数据库信息安全问题、认证速度较慢、流程复杂不科学等问题。而**区块链技术则可以大幅提高身份数据的真实性、效率和认证范围。**联合国与世界身份网络组织（World Identity Network，简称 WIN）在人道主义区块链峰会上宣布合作声明，旨在利用区块链技术进行身份认证试点项目，将数字身份储存在区块链上，能提高抓住罪犯、找回儿童的几率，并可以保护隐私追溯和预防人口贩卖活动。同时，美国伊利诺伊州也发起出生证明区块链试点项目，旨在运用区块链技术将新生儿的出生证明数字化，为公民带来更多样的身份信息验证及保护方式。

区块链技术在政府管理领域的应用还体现在选举投票与智能监管。运用区块链不可篡改的特性和分布式共识验证技术，能够高效率、低成本地完成政治选举，避免人为操作和清点票数造成的失误，同时提高了投票选举过程的透明度，保证了数据存储的安全。

区块链技术可以在政府管理上起到督促廉政的效果。比如，中国的雄安新区在建设过程中，上线了区块链管理平台，尝试利用区块链技术解决传统工程项目中存在的资金挪用、合同违约、施工质量低、拖欠工资等问题。通过对工程招投

[49] 国家信息中心智慧城市发展研究中心联合火币区块链应用研究院《区块链助力中国智慧政务发展驶入快车道》[R]，2020 年 4 月 20 日，http://www.eeo.com.cn/2020/0420/381652.shtml

标等每一项决策进行全过程信息留档，保存了可随时调取查看的证据，出现问题即依法问责。爱沙尼亚政府在 2007 年受到网络攻击后，就开始发展基于区块链的“无密码签名设施”（Keyless Signature Infrastructure，简称 KSI）管理政府和公民信息。爱沙尼亚的每个公民都可以在该系统上独立检查政府记录的完整性，有效监督政府行为。而政府内部的特权人员却无法清除系统上的电子日志，从而避免了公职人员的犯罪行为。这极大地增强了该国信息系统的安全性。

将区块链技术用于选举中，将会极大提高选举过程的安全性和透明性，被看作是公平选举的未来。目前已有多个地区的政府正筹划或已开始采用区块链技术清点统计选票，巴西、丹麦、韩国和瑞士等国也在探索区块链选举。例如，美国犹他州使用区块链技术，选出参加美国总统选举的共和党候选人；犹他州投票人可以直接坐在家里或任何地方的电脑前参与网络投票；海外服役的美国西弗吉尼亚州军可以在手机上为家乡的选举投票。这些投票情况被加密技术和区块链结合的注册信息所记录。

电子数据存证是潜在区块链技术重要应用落地领域。区块链技术具有防止篡改、事中留痕、事后审计、安全防护等特点，有利于提升电子证据的可信度和真实性。**区块链与电子数据存证的结合，可以降低电子数据存证成本，方便电子数据的证据认定。**截至 2019 年 6 月底，全国已有吉林、山东、天津、河南、四川省等 12 个省（直辖市）的高院、中基层法院和杭州互联网法院已上线区块链电子证据平台。2020 年 1 月 7 日，司法部印发《公共法律服务网络平台、实体平台、热线平台融合发展实施方案》，提出探索推进“区块链+公共法律服务”，开展自助式法律服务机器人的试点应用，提升公共法律服务智能化水平，缓解农村地区、欠发达地区法律服务资源不足的问题。另外，英国和荷兰的司法机关也正在利用区块链技术构建数字化法律体系，以解决当前大量人工、手动处理程序下的低效率、高成本等问题。

5　趋势篇

5.1 区块链发展面临的障碍和挑战

5.1.1 技术问题

区块链集成了私钥加密算法、P2P 网络、工作量证明 PoW 等多种技术。这些组成技术存在一些长期以来难以解决的技术障碍或弊端，可能会对区块链造成综合性的技术问题。

从密码学来看，加密算法的安全通常定义为在当前技术水平下，加密信息在相当长的一段时间内（例如 100 年以上）无法被解密。但是，随着新的数学算法的出现以及计算能力的提高（例如量子计算机），以往安全的加密信息可能在较短时间内被解密。

从 P2P 网络的稳定性来看，当前大量节点的参与维持了网络的健壮性。一个重要原因是比特币自身的价格处于高位，且电费便宜，成本可以覆盖收益。但是，如果有一天因为成本、政治或其他因素，大量节点开始退出网络，则要防范由此可能带来的区块链网络的不稳定性。

从工作量证明机制来看，系统在仅拥有少数节点的时候，使用工作量证明机制存在一定的风险。因为，供给者此时很容易超过全网算力的 50%，进而轻松实现 51%攻击，导致整个系统的瘫痪和失效。

尚未成熟的区块链技术，也面临着平台安全、应用安全的严峻形势。2011 年 6 月，Allinvain 被盗走了 25000 个比特币，成为比特币历史上第一个因为黑客攻击而遭受重大损失的玩家。2012 年 9 月，比特币平台 Bitfloor 被一个黑客成功攻破，损失 24000 个比特币，Bitfloor 平台也于 2013 年 4 月被迫关闭。2016 年 6 月，基于区块链技术的全球最大众筹项目 The Dao 被黑客攻击，导致价值 6000 万美元的 360 多万以太币被劫持，引起业内震动和高度关注。

在反洗钱业务方面，虽然数字货币能够为反洗钱业务提供技术支撑，但是也需要警惕数字货币本身具有的局限性。例如，由于现行假币识别与处理方法不是适用于数字货币，一旦数字货币出现仿冒行为，将难以被追踪核查。此外，洗钱行为逐渐多样化、复杂化，且日益显现国际化犯罪特征，需要政府及金融监管机构警惕游离于正规数字货币交易场所之外的数字货币洗钱可能性，建立国际间合作监管机制，更新完善反洗钱准则。

5.1.2 高耗能问题

区块链技术的应用在节约中心化成本并逐步提高金融安全性的同时，需要考虑是否过度使用了电子耗能成本。在比特币交易中，比特币单笔交易能耗成本是 VISA 的 74 万倍，其能耗包括二氧化碳、电力消耗、电子垃圾等成本；此外，区块链的“时间成本”也极高。仍以比特币支付为例，一般需要 10 分钟才能完成 1 次支付确认，以及至少需要 1 小时的时间确认保证支付交易的不可逆转。相比之下，银行网银支付或支付宝等第三方支付，通常都是秒级完成。可见，区块链的规模与效率成反比，与能耗成正比，这是它未来发展面临的巨大挑战[50]。从整体性来考虑，使用区块链技术要权衡成本收益选取最优化的方案。

5.1.3 安全挑战

区块链技术面临极大的安全挑战，2018 年 5 月 24 日 EDU 智能合约爆出漏洞，通过这个漏洞，攻击者不需要私钥就可以转走指定账户的所有 EDU，并且由于合约没有 Pause 设计，无法止损。这类事件使得区块链的面临的安全挑战越来越引起关注。复旦大学教授斯雪明将区块链面临的安全挑战分为算法漏洞、协议漏洞、实现漏洞、使用漏洞和系统漏洞五个方面。并针对这五个漏洞提出了常识性的解决方案，在算法安全性方面，针对量子攻击要进行后量子密码算法研究，同时采用经验验证的密码算法；在协议安全方面，采用能够阶段性离线的共识机制、避免目标确定的共识机制、设计防 ASIC 等共识运算优势明显的共识算法、加强关键节点的网络安全强度；在实现安全性方面，要对智能合约安全性验证同时要对区块链以及使用的模块做标准化处理；使用安全性方面，可以采用冷钱包、多因素验证钱包、物理随机数生成、私钥单一性使用等措施；在系统安全性上，要利用传统网络防御增强网络安全性，同时采用新型区块链架构。

5.1.4 监管风险

区块链技术因其去中心化、难篡改、自激励等特性，为当前的法律监管带来了挑战：一是去中心化的分布式共享账本带来了监管主体分散的问题；二是自动执行的智能合约带来了其法律有效性的问题；三是区块链难以篡改的特性带来的数据隐私和内容监管问题；四是激励机制与数字资产特性带来的金融监管问题[51]。

[50] 赵晓.“区块链数字货币”的不可承受之重[J].中外管理,2019(12):10-11.
[51] 中国信息通信研究院《区块链白皮书（2019）》[R]，2019 年 10 月.

我国对区块链的监管力度逐渐增大，监管体系也在不断完善中。目前，我国区块链监管主要集中在金融领域，也拓展到供应链、食品药品等区块链应用领域的监管，同时，各地方政府也在积极探索推动本地区块链行业监管制度。

2016 年 2 月，中国人民银行行长周小川在谈到数字货币相关问题时曾提及，区块链技术是一项可选的技术，并提到人民银行部署了重要力量研究探讨区块链应用技术。他认为，目前区块链存在占用资源过多的问题，不管是计算资源还是存储资源，还应对不了现在的交易规模。2016 年 9 月 9 日，中国人民银行副行长范一飞在 2015 年度银行科技发展奖评审领导小组会议中提出，各机构应主动探索系统架构转型，积极研究建立灵活、可延展性强、安全可控的分布式系统架构。由此可见，区块链技术的监管不仅应该包括区块链的平台监管，还应该涵盖区块链的应用监管、区块链“生态圈”的监管。

区块链的平台监管的对象是诸如比特币、以太坊等系统。这一层网络需要对区块链所有的可用范围进行考虑，而不仅仅是金融方面的监管。区块链的应用监管涉及智能合约等技术和新型的创新驱动融资方式 ICO（Initial Coin Offering，首次币发行融资），但是，ICO 融资手段暴露出了诸如不合规、虚假等问题，所以，对于加快 ICO 市场监管法规落实的需求日益显现。至于整个区块链“生态圈”的监管，我国区块链标准体系起步较晚，仍处于积极试探建设阶段。尚未有通用的评价标准和体系，能对区块链的技术性能和效率、可扩展性、安全性等问题详细规范。需要重点关注建设一套系统的分类标准，从而规范化、标准化区块链“生态圈”的管理。

2017 年 9 月，中国人民银行等七部委联合发布的《关于防范代币发行融资风险的公告》中明确指出，ICO 行为涉嫌非法集资、非法发行证券以及非法发售代币票券等违法犯罪活动，在中国境内叫停所有代币发行融资活动，清理整顿 ICO 平台并组织清退 ICO 代币。

2018 年 1 月，中国互联网金融协会在其官网发布《关于防范变相 ICO 活动的风险提示》，呼吁广大消费者和投资者应认清相关模式的本质，增强风险防范意识，理性投资，不要盲目跟风炒作。2018 年 7 月，央行会同相关部门搜查出国内 88 家数字货币交易平台和 85 家 ICO 交易平台，并基本实现无风险退出。

2019 年 1 月，国家互联网信息办公室发布《区块链信息服务管理规定》，也

意味着在我国对于区块链的监管更加成熟。之后几年，尽管国家陆续出台许多加快推动区块链技术和产业创新发展的支持政策，但是区块链监管没有明确的主管部门。区块链未来发展所面临的监管趋势将不断地调整和加强。

从全球来看，主要国家虽然加快布局区块链技术的研究和发展，但由于行业仍未形成统一的技术标准体系，区块链在应用和推广方面仍受到很多限制。大部分国家对于区块链的态度比较谨慎，对区块链领域制定的监管法规大多基于项目情况，尽量接入现有的监管体系；部分国家则采用禁止区块链资产发行或交易的措施，对区块链的态度较为保守。

5.2 技术趋势与升级

领域技术分析系统（http://trend.aminer.cn）可以基于 AMiner 近 3 亿篇论文的数据进行深入挖掘，对技术趋势、国际趋势及机构趋势等方面进行分析。本次研究以 AMiner 大数据平台上的区块链相关期刊会议论文作为研究基础，对区块链领域的热点趋势进行分析。

5.2.1 技术趋势

随着网络技术的发展，信息资源也呈现出爆炸性增长。我们根据“区块链”领域关键词，从 AMiner 数据库中查找出历年论文，其中包含论文所在领域的分支术语和年份，统计含有这些术语论文数量，给出论文数量排名前十的技术术语，再统计这些术语的起止年份，划分时间窗格，生成大数据智能的发展趋势图，如图 22 所示。

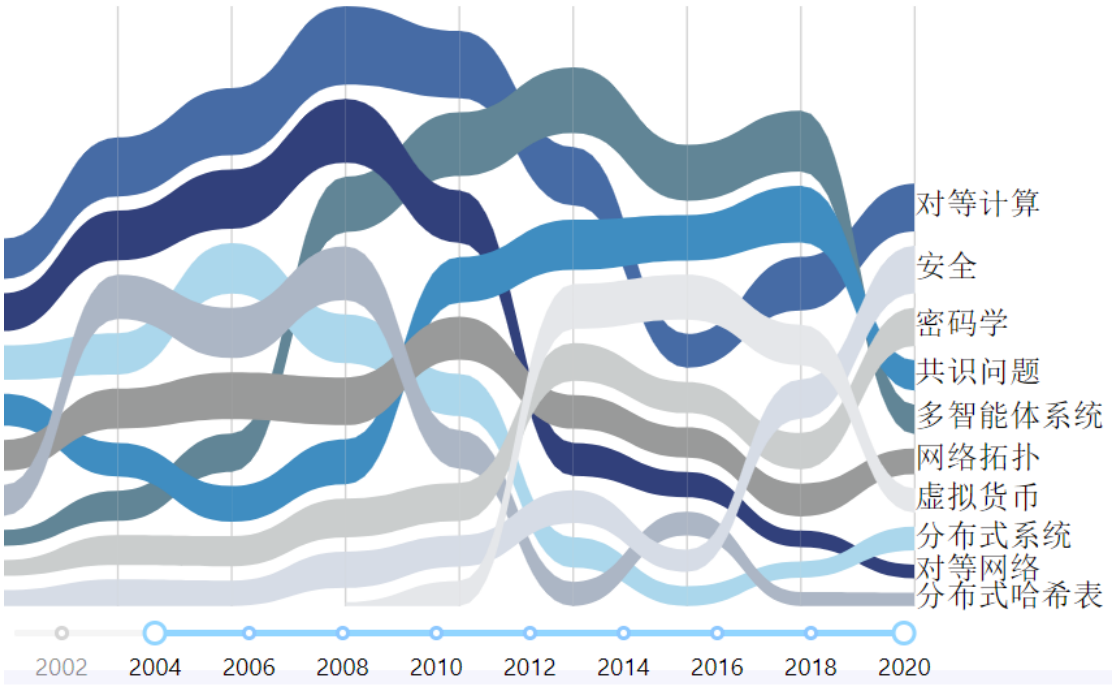


图 22　区块链的热点技术趋势图

上图中的每个颜色表示一个领域分支术语，其宽度表示该术语在当年的热度，与当年该分支领域的论文数量呈正相关；各分支在每一年份中按照其热度进行排序，越热的在越上方。对目前热度靠前的 10 个分支领域进行历史热度展示，从趋势图中可以看出，“共识问题”的研究热度持续增加，一直处于“区块链”热点趋势的前列。“对等计算”、“安全”、“分布式系统”和“密码学”也是“区块链”领域的重要分支领域。

5.2.2 国际趋势

根据 AMiner 平台分析不同国家在“区块链”领域的趋势（如图 23 所示），图中每条色带表示一个国家，其宽度表示该国家在当年的研究热度，与当年该国论文数量呈正相关，每一年份中按照其热度由高到低进行排序。通过国家趋势分析可以发现当前“区块链”领域研究热度 Top10 的国家分别是：中国、美国、加拿大、英国、意大利、德国、澳大利亚、印度、法国和日本。

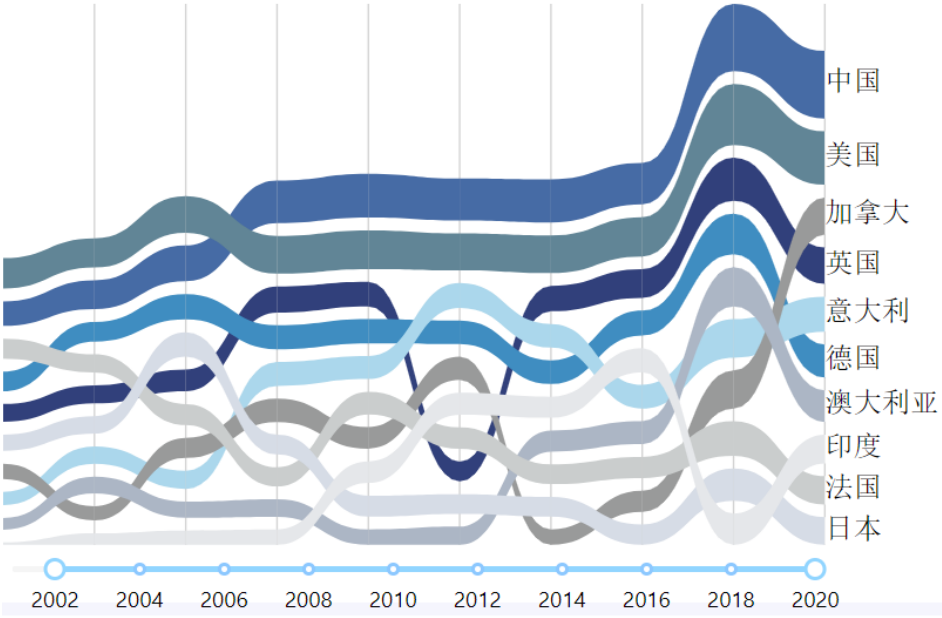


图 23　区块链技术国家发展趋势

根据国家趋势分析我们可以发现，“区块链”领域当前研究热度最高的国家是中国，从全局热度来看，美国在早期有着领先优势，但是在 2019 年以后，中国超过美国，成为各国之首。另外，其他“区块链”领域研究热度较高的国家还有加拿大、英国和意大利等西方国家。

5.3 产业趋势与升级

随着被正式划入新基建“国家队”，区块链正在迎来产业发展的新机遇。有研究认为[52]，与产业互联网一样，“与合作伙伴‘共创’也是产业区块链发展的最佳路径。虽然有多个应用场景落地，但是区块链技术目前仍处于未成熟阶段，还存在大量技术、安全以及监管方面的问题有待解决。区块链技术若要进一步深入实际场景，必须克服其在技术上、人才上、开发成本上和法律上的障碍，形成区块链研究与应用标准化体系，为学术研究和行业实践带来新的创新红利。2019 年下半年以来，党中央发布了一系列政策，培育区块链等数字经济发展新动能。毋容置疑，区块链技术将是我国自主创新核心技术的重要突破口，是推动社会治理体系和治理能力现代化的重要动力。

[52] 汤道生、徐思彦、孟岩、曹建峰.《产业区块链》[N]，腾讯，2020，https://www.sohu.com/a/390535186_150915

参考文献

[1] Aumann R J. Game theory[J]. The New Palgrave Dictionary of Economics, 2017: 1-40.

[2] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//OSDI. 1999, 99: 173-186.

[3] CCF 区块链专业委员会，《区块链关键技术研究进展》[C]，2019 年 7 月.

[4] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of Nash equilibrium, and collusion," [J] IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 192-202, January 2008.

[5] Diffie W, Hellman M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6): 644-654.

[6] Distributed Ledger Technology: beyond block chain. [R] The UK Government Chief Scientific Adviser. 2016.

[7] Douceur J R. The sybil attack[C]//International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002: 251-260.

[8] FIPS N. 180-2: Secure hash standard (SHS)[J]. US Department of Commerce, National Institute of Standards and Technology (NIST), 2012.

[9] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures[J]. Ad hoc networks, 2003, 1(2-3): 293-315.

[10]Lamport L, Shostak R, Pease M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, 4(3): 382-401.

[11]Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation[R], by Tiancheng Xie, Jiaheng Zhang, Yupeng Zhang, Charalampos Papamanthou, and Dawn Song on February 12, 2020 at 10:00 AM , https://hackingdistributed.com/2020/02/12/libra/

[12]Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y. C., & Kim, D. I. (2019). A survey on applications of game theory in blockchain. [J]

arXiv preprint arXiv:1902.10865.

[13]Meyer C H. Design considerations for cryptography[C]//Proceedings of the June 4-8, 1973, national computer conference and exposition. ACM, 1973: 603-606.

[14]Montet C, Serra D. Game theory and economics[M]. New York: Palgrave macmillan, 2003.Aumann R J. Game theory[J]. The New Palgrave Dictionary of Economics, 2017: 1-40.

[15]Montet C, Serra D. Game theory and economics[M]. New York: Palgrave macmillan, 2003.

[16]Nakamoto S. Bitcoin: A Peer-to-peer Electronic Cash System[R]. Manubot, 2019.

[17]Nash J F. Equilibrium points in n-person games[J]. Proceedings of the national academy of sciences, 1950, 36(1): 48-49.

[18]Nash J. Non-cooperative games[J]. Annals of mathematics, 1951: 286-295.

[19]National Institute of Standards and Technology (NIST). Secure Hash Standard (SHS). Digital Signature Standard (DSS). FIPS PUB 180-2 Standard, [S] 2002.

[20]Newsome J, Shi E, Song D, et al. The sybil attack in sensor networks: analysis & defenses[C]//Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004: 259-268.

[21]Pease M, Shostak R, Lamport L. Reaching agreement in the presence of faults[J]. Journal of the ACM (JACM), 1980, 27(2): 228-234.

[22]R Beck, C Müller — Bloch & J L King, “Governance in the Blockchain Economy: A Framework and Research Agenda”, [J]Journal of the Association for Information Systems, 2018 (19) , pp. 1 - 41;

[23]Rivest R L, Shamir A, Adleman L M. Cryptographic communications system and method: U.S. Patent 4,405,829[P]. 1983-9-20.

[24]Rivest R. The MD5 message-digest algorithm[J]. 1992.

[25]Shannon C E. Communication theory of secrecy systems[J]. Bell Labs Technical Journal, 1949, 28(4): 656-715.

[26]Szabo N. Smart contracts[J]. Unpublished manuscript, 1994.

[27]Szabo N. Smart contracts[Online], avaliable:

http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, November 5, 2018.

[28]Zhu Liehuang, Gao Feng, Shen Meng, Li Yandong, Zheng Baokun, Mao Hongliang, Wu Zhen. Survey on Privacy Preserving Techniques for Blockchain Technology[J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186.

[29]董宁, 朱轩彤. 区块链技术演进及产业应用展望[J]. 信息安全研究, 2017, 3(3):200-210.

[30]分布式系统与区块链[N]，链圈社区，2018 年 11 月 6 日，https://www.jianshu.com/p/ed75c125bb29

[31]工信部，《中国区块链技术和应用发展白皮书（2016）》[S]，http://www.cbdforum.cn/bcweb/index/article/rsr-6.html

[32]国家信息中心智慧城市发展研究中心联合火币区块链应用研究院《区块链助力中国智慧政务发展驶入快车道》[R]，2020 年 4 月 20 日，http://www.eeo.com.cn/2020/0420/381652.shtml

[33]海外科技风云《什么区块链 3.0 技术？区块链 3.0 技术给未来带来了什么变革？》[N] https://baijiahao.baidu.com/s?id=1640688251621987558&wfr=spider&for=pc

[34]贺海武，延安，陈泽华.基于区块链的智能合约技术与应用综述[J],《计算机研究与发展》.2018 年 11 期

[35]贾丽平.比特币的理论、实践与影响[J].国际金融研究，2013(12):14-25.

[36]李靖.比特币的发展研究综述[J].当代经济，2015(31):134-137.

[37]联合国向全球推荐支付宝区块链应用！中国区块链技术布局现状及发展趋势分析[J]，2020 年 3 月 24 日，艾媒网，https://www.iimedia.cn/c1020/70276.html

[38]刘艺华，陈康，区块链共识机制新进展[J]，计算机应用研究，2020 年 03 期

[39]柳彩云,陈雪鸿,杨帅锋.国产密码算法与工业互联网平台的结合势在必行[J].中国信息安全,2019(04):86-89.

[40]欧阳丽炜, 王帅, 袁勇, 倪晓春, 王飞跃. 智能合约:架构及进展[J]. 自动化学报, 2019, 45(3): 445-457. doi: 10.16383/j.aas.c180586, http://html.rhhz.net/ZDHXBZWB/html/2019-3-445.htm

[41]区块链技术的核心[Online]，swift_kotlin，2018 年 1 月 7 日，

https://www.jianshu.com/p/df19e23ce349

[42]赛迪顾问数字经济产业研究中心，《2019-2020 年中国区块链产业发展研究年度报告》[R]，2020 年 2 月，http://www.mtx.cn/#/report?id=683815

[43]斯雪明、孙毅、祝烈煌、朱建明等.（2019），区块链关键技术研究进展，CCF 区块链专业委员会[C]，https://www.ccvalue.cn/article/203469.html

[44]汤道生、徐思彦、孟岩、曹建峰.《产业区块链》[N]，腾讯，2020，https://www.sohu.com/a/390535186_150915

[45]腾讯研究院.《2019 腾讯区块链白皮书》[R]，2020 年 10 月，https://tisi.org/11408

[46]吴涛，王化群. (2017). 区块链中的密码学技术[J].南京邮电大学学报自然科学版，2017 年 12 月，Vol.37 No.6

[47]姚前.中央银行数字货币原型系统实验研究[J].软件学报,2018,29(09):2716-2732.

[48]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(04):481-494.

[49]赵晓.“区块链数字货币”的不可承受之重[J].中外管理,2019(12):10-11.

[50]郑东，赵庆兰，张应辉.密码学综述[J].西安邮电大学学报，2013，18(06):1-10.

[51]中国信息通信研究院《区块链白皮书（2019）》[R]，2019 年 10 月，http://www.caict.ac.cn/kxyj/qwfb/bps/201911/P020191108365460712077.pdf

[52]朱雷钧.哈希函数加密算法的高速实现[D].上海交通大学，2008.

附录 1 区块链期刊

序号	刊名	国家	出版商
1	ACM Transactions on Computer Systems	美国	Association for Computing Machinery (ACM)
2	ACM Transactions on Information Systems	美国	Association for Computing Machinery (ACM)
3	ACS Applied Materials & Interfaces	美国	American Chemical Society
4	ACS Nano	美国	American Chemical Society
5	Acta Astronautica	英国	Elsevier Ltd.
6	Advanced Energy Materials	德国	Wiley-VCH Verlag
7	Advanced Functional Materials	英国	John Wiley & Sons Ltd.
8	Advanced Materials	美国	Wiley-Blackwell
9	Advanced Science	德国	Wiley-VCH Verlag
10	Applied Energy	英国	Elsevier Ltd.
11	Applied Physics B: Lasers and Optics	德国	Springer Verlag
12	Applied Physics Letters	美国	American Institute of Physics
13	Applied Soft Computing Journal	荷兰	Elsevier BV
14	Automatica	英国	Elsevier Ltd.
15	Big Data Research	美国	Elsevier Inc.
16	Biochimica et Biophysica Acta - Biomembranes	荷兰	Elsevier BV
17	Bioinformatics	英国	Oxford University Press
18	Biosensors and Bioelectronics	英国	Elsevier Ltd.
19	Carbon	英国	Elsevier Ltd.
20	Chaos	美国	American Institute of Physics
21	Chinese Journal of Aeronautics	中国	Press of Acta Aeronautica et Astronautica Sinica
22	Communications in Applied Mathematics and Computational Science	美国	Mathematical Sciences Publishers
23	Computers and Operations Research	英国	Elsevier Ltd.
24	Critical Reviews in Biotechnology	英国	Taylor & Francis
25	Energy	英国	Elsevier Ltd.
26	Energy Conversion and Management	英国	Elsevier Ltd.
27	Engineering Applications of Artificial Intelligence	英国	Elsevier Ltd.
28	Expert Systems with Applications	英国	Elsevier Ltd.

序号	刊名	国家	出版商
29	Future Generation Computer Systems	荷兰	Elsevier BV
30	GPS Solutions	德国	Springer Verlag
31	IEEE Antennas and Wireless Propagation Letters	美国	Institute of Electrical and Electronics Engineers
32	IEEE Communications Letters	美国	Institute of Electrical and Electronics Engineers
33	IEEE Computational Intelligence Magazine	美国	Institute of Electrical and Electronics Engineers
34	IEEE Electron Device Letters	美国	Institute of Electrical and Electronics Engineers
35	IEEE Geoscience and Remote Sensing Letters	美国	Institute of Electrical and Electronics Engineers
36	IEEE Internet of Things Journal	美国	Institute of Electrical and Electronics Engineers Inc.
37	IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing	美国	Institute of Electrical and Electronics Engineers
38	IEEE Journal on Selected Areas in Communications	美国	Institute of Electrical and Electronics Engineers
39	IEEE Journal on Selected Topics in Quantum Electronics	美国	Institute of Electrical and Electronics Engineers
40	IEEE Microwave and Wireless Components Letters	美国	Institute of Electrical and Electronics Engineers
41	IEEE Network	美国	Institute of Electrical and Electronics Engineers
42	IEEE Photonics Journal	美国	Institute of Electrical and Electronics Engineers
43	IEEE Photonics Technology Letters	美国	Institute of Electrical and Electronics Engineers
44	IEEE Sensors Journal	美国	Institute of Electrical and Electronics Engineers
45	IEEE Transactions on Aerospace and Electronic Systems	美国	Institute of Electrical and Electronics Engineers
46	IEEE Transactions on Antennas and Propagation	美国	Institute of Electrical and Electronics Engineers
47	IEEE Transactions on Automatic Control	美国	Institute of Electrical and Electronics Engineers
48	IEEE Transactions on Automation Science and Engineering	美国	Institute of Electrical and Electronics Engineers
49	IEEE Transactions on Biomedical Engineering	美国	Institute of Electrical and Electronics Engineers
50	IEEE Transactions on Circuits and Systems for Video Technology	美国	Institute of Electrical and Electronics Engineers
51	IEEE Transactions on Communications	美国	Institute of Electrical and Electronics Engineers
52	IEEE Transactions on Computers	美国	Institute of Electrical

序号	刊名	国家	出版商
			and Electronics Engineers
53	IEEE Transactions on Control Systems Technology	美国	Institute of Electrical and Electronics Engineers
54	IEEE Transactions on Cybernetics	美国	IEEE Advancing Technology for Humanity
55	IEEE Transactions on Dependable and Secure Computing	美国	IEEE Computer Society
56	IEEE Transactions on Electron Devices	美国	Institute of Electrical and Electronics Engineers
57	IEEE Transactions on Evolutionary Computation	美国	Institute of Electrical and Electronics Engineers
58	IEEE Transactions on Fuzzy Systems	美国	Institute of Electrical and Electronics Engineers
59	IEEE Transactions on Geoscience and Remote Sensing	美国	Institute of Electrical and Electronics Engineers
60	IEEE Transactions on Image Processing	美国	Institute of Electrical and Electronics Engineers
61	IEEE Transactions on Industrial Electronics	美国	Institute of Electrical and Electronics Engineers
62	IEEE Transactions on Industrial Informatics	美国	Institute of Electrical and Electronics Engineers
63	IEEE Transactions on Industry Applications	美国	Institute of Electrical and Electronics Engineers
64	IEEE Transactions on Information Forensics and Security	美国	Institute of Electrical and Electronics Engineers
65	IEEE Transactions on Instrumentation and Measurement	美国	Institute of Electrical and Electronics Engineers
66	IEEE Transactions on Intelligent Transportation Systems	美国	Institute of Electrical and Electronics Engineers
67	IEEE Transactions on Knowledge and Data Engineering	美国	Institute of Electrical and Electronics Engineers
68	IEEE Transactions on Medical Imaging	美国	Institute of Electrical and Electronics Engineers
69	IEEE Transactions on Microwave Theory and Techniques	美国	Institute of Electrical and Electronics Engineers
70	IEEE Transactions on Mobile Computing	美国	Institute of Electrical and Electronics Engineers
71	IEEE Transactions on Multimedia	美国	Institute of Electrical and Electronics Engineers
72	IEEE Transactions on Network and Service Management	美国	Institute of Electrical and Electronics Engineers
73	IEEE Transactions on Neural Networks and Learning Systems	美国	IEEE Computational Intelligence Society
74	IEEE Transactions on Parallel and Distributed Systems	美国	Institute of Electrical and Electronics Engineers
75	IEEE Transactions on Pattern Analysis and Machine Intelligence	美国	Institute of Electrical and Electronics Engineers

序号	刊名	国家	出版商
76	IEEE Transactions on Power Electronics	美国	Institute of Electrical and Electronics Engineers
77	IEEE Transactions on Signal Processing	美国	Institute of Electrical and Electronics Engineers
78	IEEE Transactions on Software Engineering	美国	Institute of Electrical and Electronics Engineers
79	IEEE Transactions on Systems, Man, and Cybernetics: Systems	美国	IEEE Advancing Technology for Humanity
80	IEEE Transactions on Vehicular Technology	美国	Institute of Electrical and Electronics Engineers
81	IEEE Transactions on Wireless Communications	美国	Institute of Electrical and Electronics Engineers
82	IEEE Wireless Communications	美国	Institute of Electrical and Electronics Engineers
83	IEEE Wireless Communications Letters	美国	IEEE Communications Society
84	IEEE/ACM Transactions on Audio Speech and Language Processing	美国	IEEE Advancing Technology for Humanity
85	IEEE/ASME Transactions on Mechatronics	美国	Institute of Electrical and Electronics Engineers
86	IET Radar, Sonar and Navigation	英国	Institution of Engineering and Technology
87	Information Fusion	荷兰	Elsevier BV
88	Information Sciences	荷兰	Elsevier BV
89	International Journal of Computer Vision	荷兰	Kluwer Academic Publishers
90	International Journal of Machine Learning and Cybernetics	美国	Springer Science + Business Media
91	Journal of Artificial Intelligence Research	美国	Morgan Kaufmann Publishers, Inc.
92	Journal of Field Robotics	英国	John Wiley & Sons Ltd.
93	Journal of Intelligent and Fuzzy Systems	荷兰	IOS Press
94	Journal of Intelligent and Robotic Systems: Theory and Applications	荷兰	Kluwer Academic Publishers
95	Journal of Materials Chemistry A	英国	Royal Society of Chemistry
96	Journal of Microelectromechanical Systems	美国	Institute of Electrical and Electronics Engineers
97	Journal of Physics D: Applied Physics	英国	Institute of Physics Publishing
98	Journal of Process Control	英国	Butterworth Scientific Ltd.
99	Journal of Sound and Vibration	美国	Elsevier Inc.
100	Journal of the American Chemical Society	美国	American Chemical Society

序号	刊名	国家	出版商
101	Lab on a Chip - Miniaturisation for Chemistry and Biology	英国	Royal Society of Chemistry
102	Laser and Photonics Reviews	德国	Wiley - VCH Verlag GmbH & CO. KGaA
103	Light: Science and Applications	英国	Nature Publishing Group
104	Materials Science and Engineering: R: Reports	荷兰	Elsevier BV
105	Measurement: Journal of the International Measurement Confederation	荷兰	Elsevier BV
106	Medical Image Analysis	荷兰	Elsevier BV
107	Nano Energy	荷兰	Elsevier BV
108	Nano Letters	美国	American Chemical Society
109	Nano Research	中国	Tsinghua University Press
110	Nano Today	荷兰	Elsevier BV
111	Nanoscale	英国	Royal Society of Chemistry
112	Nature	英国	Nature Publishing Group
113	Nature Communications	英国	Nature Publishing Group
114	Nature Energy	美国	Springer Nature
115	Nature Materials	英国	Nature Publishing Group
116	Nature Methods	英国	Nature Publishing Group
117	Nature Nanotechnology	英国	Nature Publishing Group
118	Nature Photonics	英国	Nature Pub. Group
119	Nature Physics	英国	Nature Publishing Group
120	Nature Reviews Materials	英国	Nature Publishing Group
121	Nuclear Instruments and Methods in Physics Research, Section A: Accelerators, Spectrometers, Detectors and Associated Equipment	荷兰	Elsevier BV
122	Nucleic Acids Research	英国	Oxford University Press
123	Optics Express	美国	Optical Society of America
124	Optics Letters	美国	Optical Society of America
125	Organic Electronics: physics, materials, applications	荷兰	Elsevier BV
126	Pattern Recognition	英国	Elsevier Ltd.
127	Physical Review A	美国	American Physical Society
128	Physical Review C	美国	American Physical Society

序号	刊名	国家	出版商
129	Physical Review D	美国	American Physical Society
130	Physical Review Letters	美国	American Physical Society
131	Physical review. E	美国	American Physical Society
132	Physics of Plasmas	美国	American Institute of Physics
133	Physics Reports	荷兰	Elsevier BV
134	PLoS ONE	美国	Public Library of Science
135	Proceedings of the IEEE	美国	Institute of Electrical and Electronics Engineers
136	Proceedings of the National Academy of Sciences of the United States of America	美国	National Academy of Sciences
137	Protein Engineering, Design and Selection	英国	Oxford University Press
138	Robotics and Autonomous Systems	荷兰	Elsevier BV
139	Science	美国	American Association for the Advancement of Science
140	Science Advances	美国	American Association for the Advancement of Science
141	Science Bulletin	荷兰	Elsevier BV
142	Science China Information Sciences	中国	Zhongguo Kexue Zazhishe/Science in China Press
143	Science China Technological Sciences	德国	Springer Verlag
144	Scientific Reports	英国	Nature Publishing Group
145	Sensors and Actuators, A: Chemical	荷兰	Elsevier BV
146	Sensors and Actuators, B: Chemical	荷兰	Elsevier BV
147	SIAM Journal of Scientific Computing	美国	Society for Industrial and Applied Mathematics
148	SIAM Journal on Computing	美国	Society for Industrial and Applied Mathematics
149	Signal Processing	荷兰	Elsevier BV
150	Small	德国	Wiley - V C H Verlag GmbbH & Co.
151	Soft Robotics	美国	Mary Ann Liebert Inc.
152	Swarm and Evolutionary Computation	荷兰	Elsevier BV
153	The Analyst	英国	Royal Society of Chemistry
154	Theranostics	加拿大	Ivyspring International Publisher

附录 2 近 10 年区块链相关的国家自然科学基金 NSFC 项目

根据“区块链”领域关键词，从 AMiner 数据库中查找出 2010 至 2020 年国家自然科学基金支持的区块链项目(包含未结题的项目)。具体情况如下表所示。

领域关键词包括：去中心化（Decentralized or Decentralizing)、共识层（Consensus Layer)、共识机制（Consensus Mechanism)、共识协议（Consensus Protocol)、数字加密货币（Digital Cryptocurrency)、分布式对等网络（Distributed Peer-to-Peer Network)、以太坊（Ethereum)、能力证明（Proof of Capacity)、股权证明（Proof of Stake)、工作证明（Proof of Work)、自私采矿（Selfish Mining)、智能合约（Smart Contract)、比特币（Bitcoin)、区块链（Blockchain)、拜占庭式（Byzantine)。

项目类别	依托单位	项目个数	汇总
创新研究群体项目	清华大学	1	1
地区科学基金项目	内蒙古大学	3	14
	江西理工大学	2	
	广西大学	1	
	广西师范学院	1	
	昆明理工大学	1	
	南昌大学	1	
	内蒙古农业大学	1	
	宁夏大学	1	
	西北民族大学	1	
	宜春学院	1	
	云南财经大学	1	
国际(地区)合作与交流项目	上海交通大学	1	2
	中国农业大学	1	
国家杰出青年科学基金	东南大学	1	1
联合基金项目	北京理工大学	1	2
	南京航空航天大学	1	
面上项目	东南大学	6	128
	清华大学	5	
	浙江大学	5	
	武汉大学	4	
	中南大学	4	
	北京航空航天大学	3	
	电子科技大学	3	
	广东工业大学	3	

项目类别	依托单位	项目个数	汇总
	哈尔滨工业大学	3	
	南京邮电大学	3	
	山东大学	3	
	上海交通大学	3	
	同济大学	3	
	西北工业大学	3	
	燕山大学	3	
	中国科学技术大学	3	
	东北大学	2	
	华东师范大学	2	
	华中科技大学	2	
	南京理工大学	2	
	西安电子科技大学	2	
	烟台大学	2	
	浙江工业大学	2	
	中国人民解放军国防科学技术大学	2	
	中山大学	2	
	重庆大学	2	
	安徽理工大学	1	
	安徽师范大学	1	
	北京大学	1	
	北京工业大学	1	
	北京化工大学	1	
	北京理工大学	1	
	北京市农林科学院	1	
	大连海事大学	1	
	大连理工大学	1	
	广西大学	1	
	哈尔滨工程大学	1	
	河南财经政法大学	1	
	河南科技大学	1	
	湖北工业大学	1	
	湖南城市学院	1	
	华北电力大学	1	
	华北电力大学（保定）	1	
	华东理工大学	1	
	暨南大学	1	
	南京大学	1	
	南京审计大学	1	
	南京师范大学	1	
	南开大学	1	

项目类别	依托单位	项目个数	汇总
	齐齐哈尔大学	1	
	三峡大学	1	
	厦门大学	1	
	沈阳理工大学	1	
	沈阳师范大学	1	
	四川大学	1	
	天津大学	1	
	温州商学院	1	
	西安交通大学	1	
	西安理工大学	1	
	西安邮电大学	1	
	西南交通大学	1	
	西南科技大学	1	
	香港城市大学深圳研究院	1	
	长安大学	1	
	浙江财经大学	1	
	浙江师范大学	1	
	中国地震局地质研究所	1	
	中国地质大学（武汉）	1	
	中国科学院计算技术研究所	1	
	中国科学院昆明动物研究所	1	
	中国科学院生态环境研究中心	1	
	中国科学院数学与系统科学研究院	1	
	中国林业科学研究院	1	
	中国人民大学	1	
	中国人民解放军第二炮兵工程大学	1	
	中国中医科学院中医临床基础医学研究所	1	
	珠海澳科大科技研究院	1	
青年科学基金项目	东北大学	8	117
	山东大学	4	
	哈尔滨工业大学	3	
	清华大学	3	
	中国科学院自动化研究所	3	
	北京理工大学	2	
	复旦大学	2	
	广东工业大学	2	
	杭州电子科技大学	2	
	合肥工业大学	2	
	河南理工大学	2	
	南京大学	2	

项目类别	依托单位	项目个数	汇总
	南京信息工程大学	2	
	三峡大学	2	
	山东财经大学	2	
	上海电力学院	2	
	西安建筑科技大学	2	
	西南大学	2	
	西南交通大学	2	
	中国科学院合肥物质科学研究院	2	
	中南财经政法大学	2	
	中央财经大学	2	
	北方工业大学	1	
	北京科技大学	1	
	北京控制工程研究所	1	
	北京信息科技大学	1	
	北京邮电大学	1	
	渤海大学	1	
	东莞理工学院	1	
	东南大学	1	
	哈尔滨工程大学	1	
	河北工业大学	1	
	河南城建学院	1	
	湖南城市学院	1	
	湖南大学	1	
	湖南科技大学	1	
	华北电力大学	1	
	华东理工大学	1	
	华中科技大学	1	
	吉林大学	1	
	江南大学	1	
	江苏师范大学	1	
	江西师范大学	1	
	兰州大学	1	
	聊城大学	1	
	鲁东大学	1	
	南京财经大学	1	
	南京理工大学	1	
	青岛大学	1	
	曲阜师范大学	1	
	山东科技大学	1	
	上海大学	1	
	上海海事大学	1	

项目类别	依托单位	项目个数	汇总
	上海理工大学	1	
	深圳大学	1	
	沈阳化工大学	1	
	天津大学	1	
	武汉大学	1	
	西安交通大学	1	
	西安理工大学	1	
	西安石油大学	1	
	西北工业大学	1	
	西交利物浦大学	1	
	西南财经大学	1	
	香港中文大学深圳研究院	1	
	燕山大学	1	
	长安大学	1	
	长江水利委员会长江科学院	1	
	浙江财经大学	1	
	浙江大学	1	
	浙江工业大学	1	
	郑州大学	1	
	中国地质大学（武汉）	1	
	中国电力科学研究院	1	
	中国科学技术大学	1	
	中国科学院生态环境研究中心	1	
	中国科学院声学研究所	1	
	中国人民解放军国防科学技术大学	1	
	中国人民解放军军械工程学院	1	
	中国人民解放军信息工程大学	1	
	中国社会科学院金融研究所	1	
	中南大学	1	
	中山大学	1	
	重庆邮电大学	1	
应急管理项目	福建师范大学	1	1
优秀青年科学基金项目	燕山大学	1	1
重大项目	北京航空航天大学	1	1
重大研究计划	中国地质大学（武汉）	1	2
	中国科学技术大学	1	
重点项目	暨南大学	1	3
	上海交通大学	1	
	中国科学技术大学	1	
专项基金项目	江苏大学	1	1
总计		274	274

版权声明

AMiner 研究报告版权为 AMiner 团队独家所有，拥有唯一著作权。AMiner 咨询产品是 AMiner 团队的研究与统计成果，其性质是供用户内部参考的资料。

AMiner 研究报告提供给订阅用户使用，仅限于用户内部使用。未获得 AMiner 团队授权，任何人和单位不得以任何方式在任何媒体上（包括互联网）公开发布、复制，且不得以任何方式将研究报告的内容提供给其他单位或个人使用。如引用、刊发，需注明出处为“AMiner.org”，且不得对本报告进行有悖原意的删节与修改。

AMiner 研究报告是基于 AMiner 团队及其研究员认可的研究资料，所有资料源自 AMiner 后台程序对大数据的自动分析得到，本研究报告仅作为参考，AMiner 团队不保证所分析得到的准确性和完整性，也不承担任何投资者因使用本产品与服务而产生的任何责任。

顾问　陈康　李涓子　唐杰

编辑　张淼　刘佳　高洁　叶静芸

数据　赵慧军

扫描二维码
下载报告全文

报告编号 AITR-20-05