DOI 10.15302/J-SSCAE-2018.02.005

区块链技术发展及应用：现状与挑战

孙毅[1,2]，范灵俊[1]，洪学海[1]

（1. 中国科学院计算技术研究所，北京 100190；2. 中国科学院大学，北京 101407）

摘要：本文介绍了区块链技术发展和行业应用的现状，对区块链未来大规模应用会面临的技术挑战进行了剖析，综述了区块链体系结构、共识算法、隐私保护、智能合约、跨链通信等关键问题的研究现状，从技术、人才和监管三个方面对我国进一步发展区块链技术及应用的政策提出了建议。

关键词：高通量区块链；共识算法；智能合约；跨链通信

中图分类号：TP319　　**文献标识码：**A

Technology Development and Application of Blockchain: Current Status and Challenges

Sun Yi[1,2], Fan Lingjun[1], Hong Xuehai[1]

(1. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China; 2. University of Chinese Academy of Sciences, Beijing 101407, China)

Abstract: Blockchain, as the backbone of the future "Internet of Value" model, is considered to have the potential to significantly alter the current state of the economy and society. This paper explains the state-of-the-art development in blockchain technologies (e.g. blockchain architecture, consensus algorithm, privacy preserving, smart contract, and chain interoperability) and its applications, especially considering the technological challenges encountered when blockchain is widely applied in different domains. Furthermore, respectively from the perspective of technology, talent and supervision, we propose suggestions that could facilitate the further development of blockchain in China.

Keywords: high-throughput blockchain; consensus protocol; smart contract; cross-chain communication

一、前言

区块链是一种把区块以链的方式组合在一起的数据结构，每一个区块通过散列的方式与上一个区块相连，实现了可追溯；同时，用密码学保证了数据的不可篡改和不可伪造。每一个区块的生成，都是参与者对整个系统交易记录的事件顺序和当前状态建立的共识。每一个参与者都可以参与数据的记录、存储，都可以拥有整个区块链数据的备份，从而在没有中央控制节点的情况下，使用分布式集体运作的方法，构建了一个分布式对等网络。因此，区块链技术具有去中心化、分布式、去信任、数据不可篡改、可追溯等诸多优点。

区块链技术起源于化名为“中本聪（Satoshi

收稿日期：2018-03-22；**修回日期：**2018-03-30

通讯作者：孙毅，中国科学院计算技术研究所，研究员，博士研究生导师，区块链方向学术带头人，研究方向为区块链、互联网服务；E-mail: sunyi@ict.ac.cn

资助项目：中国工程院咨询项目“‘互联网 +’行动计划的发展战略研究”(2016-ZD-03)；国家自然科学基金项目 (61772502，61672499)

本刊网址：www.enginsci.cn

Nakamoto）”的学者在 2008 年发表的奠基性论文《比特币：一种点对点电子现金系统》。作为比特币的底层实现技术，区块链是一种分布式账本技术（DLT），由于其具有分布式、去信任、不可篡改等优点，该技术被认为是构建未来“信任互联网”“价值互联网”的支撑性技术，已成为全球创新领域最受关注的话题，受到投资界、学术界、工业界及政府部门的热烈追捧。虽然各国政府对比特币和各种虚拟币的态度各不相同，但对区块链技术大多持积极的态度。

近年来，联合国、国际货币基金组织等机构以及多个发达国家先后发布了有关区块链的系列报告，探索区块链技术及其应用。当前，区块链技术的应用领域已经超越了金融领域，并逐步在供应链、征信、身份认证、公益慈善、物联网等领域展开实践。创业公司如雨后春笋般涌现，乌镇智库 2017 年发布的《区块链产业发展白皮书》指出，自 2012 年以来，全球区块链企业数量以超过 65.2% 的复合增长率快速增长。一种乐观的预测认为，到 2025 年之前，全球 GDP 总量的 10% 将利用区块链技术储存。据数字市场漫记（DMR）估计，到 2024 年，区块链产业规模有望达到 200 亿美元。

二、国内外行业应用现状

作为互联网技术的发源地，美国在区块链技术和应用上投入巨大。2017 年，美国至少有 8 个州提出和研究了提升区块链技术应用的法案。2018 年 2 月，美国众议院连续两次召开区块链听证会，探讨区块链技术的新应用。美国国务院强调通过区块链技术提高透明度，可以解决腐败、欺诈或挪用公共采购资金的问题。美国财政部正在进行试点计划，以确定区块链技术是否可以用于供应链管理，还采取了措施来改善针对基于区块链加密货币的“反洗钱 / 打击恐怖主义融资（AML/CFT）”的相关法律，并与金融机构形成公私合作关系（PPPs）以共享信息。佛蒙特州的南柏林顿市将试用区块链技术，记录房产交易。加利福尼亚州立法者已经提交了一项法案，如果能够顺利通过，那么该州的电子记录法律将会认可区块链签名和智能合约。纽约州电力公司 TransActive Grid 提出了基于区块链的 P2P 分布式微电网络的新能源概念，通过区块链建立微电网网络，提高清洁能源利用率，在区块链上记录剩余的电量并通过智能合约卖给邻居用户。

2016 年 1 月，英国政府发布了一份名为《分布式账本技术：超越区块链》的报告。报告指出，区块链技术在改变公共和私人服务领域都有着巨大的潜力。除了创建一个基于区块链的公共平台为全民和社会提供服务，英国政府还计划开发一个能够在政府和公共机构之间使用的应用系统。日本政府则大力支持区块链和数字货币行业，建立了首个区块链行业组织——日本区块链协会（JBA）与区块链合作联盟。俄罗斯正在大力推动区块链基础设施建设，俄罗斯最大的银行 Sberbank 与政府合作，用区块链转移和保存文件，成为区块链真实的应用案例。加拿大有一个庞大的区块链创业社区，汇集了包括以太坊创始人 Vitalik Buterin 在内的一大批区块链顶级人才。加拿大证券管理委员会（CSA）日前主动地推出了新的“Fintech 沙箱（SandBox）”计划，以促进加拿大区块链行业的发展。

区块链技术发源于开源社区，并在社区中发展壮大，此后逐渐受到金融机构、IT 巨头等机构的关注。例如，以比特币、以太坊为代表的开源项目主要以公有链为主，打造了区块链公共平台；Linux 基金会于 2015 年发起的超级账本项目（Hyperledger）则偏重于研究联盟链技术。同时，IBM、微软 Azure、AWS 等互联网国际巨头企业正在极力打造支持区块链应用的基础设施，区块链即服务（Blockchain as a Serveice，BaaS）。

2016 年以来，我国政府也通过多种形式关注和支持区块链技术和产业的发展。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）》[1]，同年 12 月区块链首次被作为战略性前沿技术、颠覆性技术写入国务院“十三五”国家信息化规划，明确提出需加强区块链等新技术的创新、试验和应用，以实现抢占新一代信息技术主导权。中国人民银行在 2017 年成立了数字货币研究所，研究数字货币发行和支撑该技术的商业运作框架。中国人民银行的基于区块链的数字票据交易平台于 2017 年初进入试运行阶段并测试成功。此外，腾讯计算机系统有限公司、阿里巴巴网络技术有限公司等国内知名互联网公司也积极布局区块链产业，全国另有超过 100 家区块链创业公司，主要瞄准区块链基础设施技术研发及其在征信、供应链、资产管理、物联网等

行业的应用。2008—2017 年，我国区块链技术领域专利申请数量全球第一，共递交 550 份专利申请；美国专利申请数量全球第二，共递交 284 份专利申请。

三、区块链面临的技术挑战

比特币是区块链技术的第一个成功应用。截至目前，比特币区块链系统已经运行了 8 年多，除了有限的几次分叉，没有出现重大安全事故，充分显示了其强大的稳定性和安全性。区块链技术目前的应用大多仍集中在金融领域，例如，数字货币、跨境支付、证券交易、财产注册与认证等。然而，其未来要在金融领域做大规模推广应用还需要攻克很多问题，如性能问题、可监管性问题等。

在供应链领域，通过区块链，供应链各方可以获得一个透明可靠的统一信息平台，实时查看状态，追溯物品的生产和运送整个过程，从而提高供应链管理效率、降低物流成本。当发生纠纷时，追查和举证也变得更加容易。然而，供应链管理往往涉及到诸多实体，包括物流、资金流、信息流等，这些实体之间存在大量复杂的协作和沟通，应用区块链进行链上链下的有效协同，也存在诸多技术难题需要攻关。

在制造业领域，工业 4.0 应用，可以使用区块链来记录生产过程的每一步，对于生产过程中的不同参与者，采用不同的权限来访问区块链，以更加可靠和安全的方式，为参与者提取相关信息并确认生产过程中的步骤。但是不同的终端和传感器要参与区块链网络，进行协同和验证，当前的物联网终端和传感器计算能力及存储很难支撑，而区块链网络协同的实时性也亟待提高和优化。

在能源领域，基于区块链的微电网络，也存在可扩展性问题和验证交易的能源消耗问题等。此外，由于区块链自身的存储能力有限，应用于社交、电子商务等领域时，还要考虑大量数据的存储问题、交易效率问题等。

当前区块链行业正高速发展，区块链技术也得到了越来越多的应用。然而，在基础研究领域，国内外相关研究工作仍处于初步阶段，区块链体系结构、共识算法、隐私保护、智能合约、跨链交易等方面的技术挑战越来越制约着区块链技术及行业的发展。尽快寻找有效方案，实现关键技术突破，增强完善区块链领域的理论基础与关键技术是当前区块链发展浪潮中的关键点与“杀手锏”。

（一）区块链体系结构研究

区块链体系结构是区块链系统运行的基础，但随着用户数量、系统规模的不断增加，其吞吐量低、交易确认时间长、共识节点接入速度慢、存储资源浪费等问题愈发突出，严重影响用户使用与行业拓展。近几年，工业界和学术界从区块链结构设计等方面开展了一些初步的研究工作。

并行化架构：区块链分片技术（Sharding）采用并行化思想，将用户划分到不同的网络分片内，并行处理不相交的交易集合，进而提升整体性能，但处理涉及不同分片的交易时，需要经过复杂的跨分片通信，开销很大。Plasma 则通过利用侧链层次树划分整个网络，用“分治”来扩大交易规模。

链上、链下协同架构：闪电网络（Lightning Network）以类比特币区块链为基础，提出将交易过程尽可能放在链下，进行链下快速交易，而链上交易仅用于担保与结算。本质上，闪电网络并没有提升链上交易性能，并且链下交易环节未存储到区块链中，会影响交易的可追溯性。雷电网络（Raiden Network）作为“以太坊版本”的闪电网络，可与 Sharding、Plasma 结合，进一步提升交易处理能力。

并行化、链上链下协同等新型架构为解决区块链的性能和资源占用问题提供了新的研究方向，但是这些研究工作目前还处于相对早期的阶段，很多具体的问题如并行化架构的合理分片、跨片通信、链上链下协同的去中心化、可追溯等问题还缺少高效的算法和机制。

（二）区块链共识算法研究

区块链共识算法保证了区块链系统中各节点可以维护相同的交易内容和顺序，是区块链系统的核心机制。目前应用比较广泛的、常见的共识算法包括工作量证明算法（PoW）、权益证明算法（PoS）、股份授权证明算法（DPoS）以及拜占庭容错算法（PBFT）[2]，这些算法各有优势但也都存在自身的问题（见表 1）。

近年来，为了适应实际应用的需求，一些新型共识算法被提出。Algorand 通过密码抽签机制随机选取一组验证者使用优化的拜占庭协议进行共识来

表 1　几种常见的共识算法对比

共识算法	安全性	网络规模	资源消耗	交易确认时间	交易吞吐量	分叉	去中心化
PoW	高	大	大	长	小	易	较高
PoS	较高	大	一般	一般	小	易	较高
DPoS	一般	大	小	短	一般	不易	低
PBFT	一般	小	小	短	一般	不易	一般

提高共识效率 [3]；Bitcoin-NG 通过工作量证明选取的领导者发布交易微块，一定程度上改善了比特币区块链 PoW 共识的性能 [4]；Casper 通过锁定保证金的验证人下注共识以提升 PoS 算法实现的安全性以及去中心化程度。

然而，无论是 PoW、PBFT 这些经典共识算法还是 Algorand、Bitcoin-NG 这些新型算法都面临“三难困境”问题，即区块链系统最多只能同时优化去中心化、高性能以及安全性三种目标中的两个，寻求“三难困境”的最优解将是未来的主要研究方向和技术挑战。

（三）区块链隐私保护研究

区块链隐私保护是为了解决公开的交易信息带来的账户隐私泄漏问题。目前主要通过直接或间接隐藏用户关键信息来实现，典型的隐私保护技术包括：混币技术（CoinJoin）、隐秘地址（Stealth Address）、环签名技术（Ring Signature）[5] 以及 zk-SNARKs 零知识证明算法 [6]。

混币技术、隐秘地址以及环签名技术只是间接隐藏交易涉及的关键信息，在可靠性方面存在不足；zk-SNARKs 零知识证明算法虽然属于直接隐藏信息，但是其具有“可信赖的公共参数”以及效率低下的问题。同时，量子计算的不断发展对隐私保护研究提出了新的要求，而这些典型的隐私保护技术都不具备抗量子攻击能力。新提出的 zk-STARKs 零知识证明算法完全依赖散列和信息理论，解决了 zk-SNARK“可信赖的设置”问题并具备抗量子攻击的能力，但是该研究处于早期阶段，技术还不成熟且存在证据过大等缺点。因此，设计既能保证高效安全，还能保证交易关键信息隐藏与交易有效性验证的技术方案依然是未来区块链研究面临的主要技术挑战。

（四）区块链智能合约研究

Nick Szabo 于 1996 年首次提出了智能合约的概念：一个智能合约是一套以数字形式定义的约定，包括合约参与方可以在上面执行这些约定的协议。区块链为智能合约提供了一个去中心化、不可篡改、公开透明的运行环境，使得智能合约无需信任第三方即可根据预设合约协议自动执行。目前针对智能合约的研究主要围绕智能合约虚拟机、智能合约升级、链下数据可信喂养等方面展开。

智能合约虚拟机可以分为两大类：自主可控的虚拟机，如以太坊虚拟机（EVM）；使用现有成熟的编译运行环境的虚拟机，如 Java 虚拟机（JVM）。使用现有成熟编译运行环境的虚拟机运行效率较高，但不可控因素较多，而 EVM 等自主可控的虚拟机当前的运行效率还存在较大问题。目前的研究工作主要有 Solidity 编译器的优化、适合智能合约的 Web 程序集（WASM）执行环境研发等，上述工作均处于早期研究阶段。

智能合约是现实世界契约的计算机化交易协议，在智能合约的开发过程中，开发者无法将所有情况考虑在内，当链上的智能合约没有按照预期运行时，就需要升级智能合约，并且对智能合约的行为作出解释。Corda 提出将合约法律文本与代码结合存储于链上，当合约代码发生未预期的行为时以法律文本为准，但仍缺乏代码可升级的灵活性，因此一套可升级且可解释的智能合约完整方案是智能合约大规模应用的关键所在。

智能合约存在于区块链空间，与链下真实世界活动相关联是其大规模应用的前提。Oraclize 将智能合约与 Web API 通过加密证明链接起来，使得智能合约无需额外的信任，即可获得现实世界的真实活动数据；IC3 提出可信数据喂养系统 Town Crier（TC），通过英特尔最新可信硬件 SGX 向智能合约提供认证可信以及机密性数据。然而，现有的可信数据喂养解决方案灵活性较差，如 Oraclize 需要将整个 https 请求响应返回并且依赖于链下的中心化服务器，TC 无法支持代码的更新，需要研究新型灵活、可信的数据喂养方案以满足智能合约对链外数据的喂养需求。

（五）区块链跨链通信研究

随着区块链技术被广泛应用于加密数字货币、资产追踪、身份管理等领域，产生了很多分立的区块链系统，而这些独立的区块链需要相互交易进而实现价值最大化，就需要研究跨链通信技术。解决跨链交易中有效性、可扩展性、原子性等问题是当前区块链跨链通信技术的研究重点。

目前区块链跨链通信技术研究代表性方案包括成对通信、Interledger、Cosmos、Polkadot 等。成对通信通过获取对方区块链的区块头与特定交易的简化付款验证（SPV）证明，可在没有外部参与的情况下验证跨链交易的有效性；Interledger 通过构建连接器，找到一条到接受者的资金转移路径，资金在连接器之间转移，从而实现跨链；Cosmos 利用 Hub 与 Zone，当源 Zone 与目的 Zone 进行跨链交易时，Hub 对 Zone 形成的包进行跨链转发；而 Polkadot 的愿景是实现异构区块链之间的跨链，同时事务可以在不同的区块链上并行执行，从而增加系统的吞吐量。

上述跨链通信方案大多面向跨链某一具体场景且性能较低，如成对通信仅限于交易存在性验证，Interledger 以及 Cosmos 仅用于跨链转账这个单一功能；虽然 Polkadot 支持的跨链类型更为丰富，但是其仍处于非常早期的方案设计阶段。随着跨链交易的需求不断增加，实现安全、高效且通用性好的跨链技术方案迫在眉睫。

四、高通量区块链

性能问题是制约区块链技术未来大规模应用的重要瓶颈之一。当前应用广泛的公有链（如比特币、以太坊）和联盟链（如超级账本）都无法支持高频交易的场景，在吞吐量方面与高频交易（如支付、大规模物联网）的实际需求存在几个数量级的差距。为了弥补这种差距，中国科学院计算技术研究所开展了高通量区块链技术的研究。

不同于已有的很多性能优化的工作主要集中在协议和算法层面 [2~4]，中国科学院计算技术研究所高通量区块链技术的研究聚焦于底层架构层面的技术突破，包括区块链基础架构以及承载区块链系统的硬件架构。首先，在区块链基础架构上，通过构建交易图谱，将原始区块链切分为很多切片，并行处理不同分片的交易记录，片内共识使用流水化技术优化共识效率，并通过随机轮换记账节点集合机制，在提升效率的同时保障安全性。对于跨切片的交易，设计了 InterChain 跨分片通信架构（见图 1），通过分片网关和互联链节点的协同实现交易的跨分片通信。其次，在硬件架构上，针对现有通用计算架构效率不足，而专用芯片仅针对特定算法应用范围有限的问题，提出支持自定义算法的专用芯片架构（见图 2），通过抽象各类共识、验证签名算法的计算内核，设计基于松耦合计算内核的芯片架构，并利用区块链算法本身的容错性，简化功能单元设计，从而提升计算通量。

五、政策建议

当前我国投资界、产业界、学术界以及政府给予了热炒的区块链技术以高度的关注。然而，很

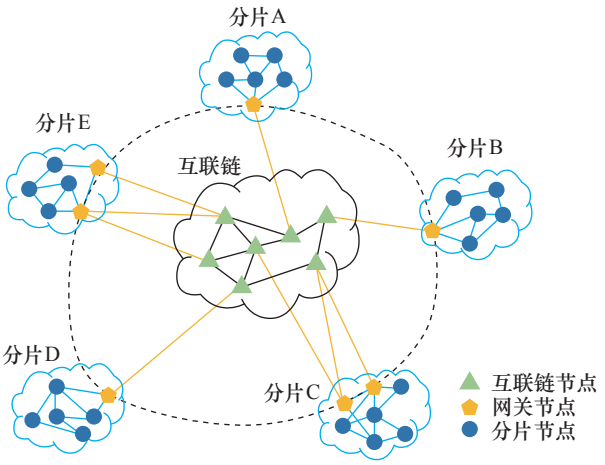

图 1　InterChain 跨分片通信架构

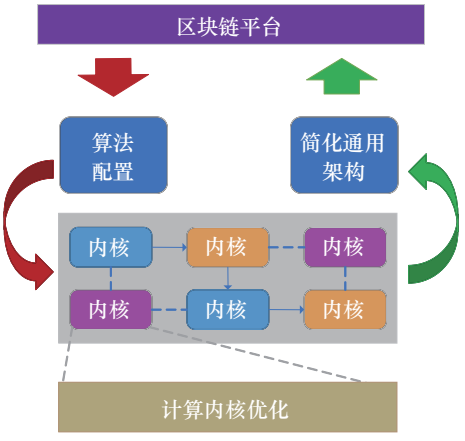

图 2　高通量区块链芯片架构优化

多项目只是披着区块链的“外衣”，犹如当年互联网发展初期一样，鱼龙混杂。著名信息技术研究和顾问机构 Gartner 每年都发布的技术成熟度曲线（the hype cycle）显示，任何一项技术的发展必经过 5 个阶段：最初的兴起期，热炒的膨胀期，幻灭的低谷期，稳步的爬升期，以及成熟的实质产业期。云计算、大数据、虚拟现实等是这样，区块链技术也不例外。经过这两年热炒之后的区块链技术，必须经过各方面扎实的技术研发、准备和铺垫，才可能大规模形成产业，影响社会进步、经济发展，以及人们的生产生活，最终“飞入寻常百姓家”。

因此，对待区块链技术，不能盲目跟风，需要理性看待。既要看到区块链技术的优点和可能带来的变革，也要认识到当前区块链技术存在的不足和挑战。从技术层面，要加大区块链底层和基础技术的研发和优化；从治理层面，要适时跟进制定法律法规，创新监管模式；从人才层面，要加大交叉学科人才培养的力度，补充人才空缺。

（一）应重视区块链底层技术的研发

应该清醒地认识到，国内区块链产业风风火火发展的背后隐藏着区块链底层技术研发投入不足的现实。目前，大多数区块链项目、区块链团队都是基于比特币、以太坊、超级账本等国外提出的区块链平台，或进行二次开发，或直接探索在特定领域、特定行业的应用。

为了应对上述性能、安全性等区块链技术发展和大规模应用面临的挑战，区块链底层技术的创新才是重中之重。应该加大在体系结构、共识算法、验证签名机制、（跨链）通信协议、专属硬件等方面的研发投入，耐心地从底层研发做起，做到技术自主可控，引领全球区块链技术发展。

（二）需要发展创新监管模式

不同于传统互联网应用有专门的运营单位，可以作为特定的监管对象，秉承分布式、去中心化思想设计的区块链应用（DAPP）一旦部署，就是所有自由接入的节点和参与者共同负责，没有中心化节点和存储，不存在某个特定机构对其负责，这给区块链应用的监管带来巨大的挑战。

因此，一方面，国家在鼓励区块链技术和应用发展的同时，要从立法层面积极跟进，引导区块链的应用方向，规范区块链应用的审查和部署；另一方面，要从信息技术工具层面，加大针对区块链平台和应用的监测、分析、判别、预警等信息技术工具的研发投入和力度，引入人工智能、大数据、信息安全等先进技术，从而实现对区块链平台和应用的科技监管。

（三）加强交叉学科人才

智能合约（Smart Contract）是运行在区块链上的计算机程序。区块链技术让人们可以在去中心化的情况下达成共识，而智能合约则决定了可以达成什么样的共识。换言之，区块链只是一个分布式的记账方式形成的公共账本，智能合约则进一步结合千千万万个不同的应用场景和经济活动，约定了谁与谁、在什么情况下记账，进而产生什么样的账本。

未来，区块链体系基础架构搭建完成，在商业应用场景中，所谓广泛应用区块链技术，很大程度上就是利用区块链编写智能合约。参与各方进行谈判和协商，形成合约条款，再编写计算机程序形成智能合约，并保证准确无误，方能部署运行。编写、审核智能合约需要精通计算机通信和其他专业领域的大量跨界人才，需要加强这些交叉学科人才的培养工作。

参考文献

[1] 中华人民共和国工业和信息化部. 中国区块链技术和应用发展白皮书(2016) [R]. 北京: 中华人民共和国工业和信息化部, 2016.
Ministry of Industry and Information Technology of the PRC. White paper on the development and application of blockchain technology in China (2016) [R]. Beijing: Ministry of Industry and Information Technology of the PRC, 2016.

[2] Castro M, Liskov B. Practical byzantine fault tolerance [C]. New Orleans: USENIX OSDI, 1999.

[3] Yossi G, Rotem H, Silvio M, et al. Algorand: Scaling byzantine agreements for cryptocurrencies [C]. Shanghai: ACM SOSP, 2017.

[4] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: A scalable blockchain protocol [C]. Santa Clara: USENIX NSDI, 2016.

[5] Bender A, Katz J, Morselli R. Ring signatures: Stronger definitions, and constructions without random oracles [C]. New York: Springer TCC, 2006.

[6] Ben-Sasson E, Chiesa A, Tromer E, et al. Succinct non-interactive zero knowledge for a von Neumann architecture [C]. San Diego: USENIX Security Symposium, 2014.