

多方计算——打开区块链应用新场景

□ 杜 宁 陈 希

当今，全球主要国家都在加快布局区块链技术发展，想要确保我国占据区块链领域的创新制高点，需要加快区块链和相关前沿信息技术的深度融合，推动集成创新和融合应用。多方计算作为我国自主创新性新技术，可以使多个非互斥数据库在数据相互保密的前提下进行高效数据融合计算，其和区块链技术有效结合，将加速区块链场景落地，推动我国区块链应用发展。

把握区块链应用落地的新趋势

下一阶段的区块链应用发展应完成以下两个转变：一是单一技术转向多种技术综合应用。区块链技术与云计算、人工智能、5G、物联网等新一代信息技术结合更为紧密，初步形成“区块链+”应用解决方案。如“区块链+云计算”基于云资源可创建更简便高效的区块链云上环境，并能提供部署、运行、监控的一体化运维解决方案，降低区块链的使用门槛；“区块链+人工智能”提升区块链对复杂业务的支持能力，扩大区块链的使用价值。“区块链+5G+物联网”为区块链提供高效的数据采集能力，并能大幅提升数据传输速度、减少网络拥堵，使得区块链性能得以大幅提升。未来区块链与多种技术结合应用的解决方案也将完全取代单一技术，成为技术创新与发展的重要引擎。

二是单一场景转向多场景融合应用。区块链技术现已从金融领域扩展到政务、医疗、教育、物流、食品安全等多个领域，也在跨行业场景融合应用中显现出价值。如“政务+金融”通过区块链打通政府部门与金融机构数据共享通路，实现资金的透明使用及有效监管。未来，区块链在跨领域多场景的融合应用也将重塑当前社会商业模式，成为产业浪潮的重要推手。

随着区块链应用范围的不断扩展，四个问题也逐渐凸显：一是数据隐私保护问题。区块链目前在隐私保护方面的技术处于早期发展阶段，仍存在诸多隐私泄露风险。二

是性能效率的局限性。区块链的运行机制依赖于大量实时的数据通信。随着数据量的膨胀使得链上节点数量不断增长，区块链的系统性能和处理效率问题也将直接影响其进一步商用普及。三是链上链下数据打通的挑战。目前链上数据有限，还需与链下系统打通解决信息孤岛问题，而目前国内外链上链下协同技术仍处于早期研究阶段。四是上链数据真实性问题。区块链可在技术上实现难以篡改，但如何保证其上链数据真实性，也是当前区块链应用中的一大难题。

推进区块链结合多方计算的新探索

多方计算理论是由图灵奖得主姚期智院士于上世纪80年代率先提出和创立，是中国原创性的计算机底层技术，其突出特征是可在密文状态下实现数据计算并能得到与明文计算同样的结果。近两年，随着算法和工程设计的重大突破与改进，多方计算产品初步落地商用化，也为区块链的应用发展瓶颈提供了新的解决思路。

区块链难以篡改、可追溯的优点，结合多方计算能实现数据“可用不可见、按规定的用途和用量使用”的强项，可实现数据隐私保护、数据存证、数据核验、联合计算、联合建模等多种功能，开拓区块链应用的崭新局面。

“区块链×多方计算”解决链上隐私、跨链协同及性能效率问题上。区块链记录和存证技术解决了传统模式中数据流转时常发生的造假问题，但由于多节点共同参与区块链系统的数据验证、存储和维护，使得数据隐私泄露风险增大。现结合多方计算技术可有效应对数据隐私泄露问题。具体应用如在政务领域，政务数据上链有助于推动数据共享和流通，然而政务数据中有些高敏感的信息直接上链将极有可能被不法分子在某单点攻破截获，因此通过结合多方计算技术，对政务部分敏感数据在上链前先做关联处理，用合约的方式将数据授权、用法用量控制等业务审批权限

放于链上，链下则通过多方计算平台实现数据的隐私计算及结果反馈。通过这样的模式能有效解决区块链上敏感数据隐私泄露问题，并且这样的方式也解决了大量数据上链导致的多节点共识行为影响性能效率问题，同时也降低了链上数据的存储成本。此外，在调用政务数据进行计算时，如涉及链下或跨链数据，可通过多方计算的最新技术——密文协同计算技术进行融合计算，为链上链下数据打通也提供了有效的解决方案。

“区块链+多方计算”核验链上数据真实性。通过区块链技术可实现数据的一致存储和难以篡改，由此大大增加了上链数据造假的难度和成本，也打消了大部分人群及机构对数据信心的顾虑。然而，仅靠区块链技术并无法保证上链数据的绝对真实，通过结合多方计算，可从当前链上难以获得的信息中对上链数据信息真伪进行有效核验。具体应用如在金融监管领域，金融机构将相关交易数据上传至区块链便于监管机构对链上数据进行审查分析和行为监管，但有些大额高风险交易数据为了不被监管机构察觉，金融机构很有可能在上链前就作了修改，为避免金融交易数据造假导致行业风险扩散，监管机构可通过多方计算技术从金融机构提供的交易信息对手方或上下游行业获取相关的数据，再与金融机构所提供的链上交易数据进行对比对，可及时发现金融机构是否有交易数据造假行为，从而有效增强金融监管的穿透性和专业性。

“多方计算+区块链”实现数据可溯源、可监管。多方计算为区块链应用提供了有效的解决方案，而区块链也对多方计算应用落地提供了有益的补充。如多方计算由于使用的是密文计算模式确保数据计算参与方都无法看到其他方的数据，如果参与方恶意输入错误数据将影响整体计算结果，通过区块链对参与计算的数据以及计算过程进行加密存证，可有效追踪恶意输入，同时也有利于监管部门对敏感数据流通及融合计算等场景进行有效监管。多方计算开创了区块链应用新境界，两者的紧密融合将产生更多

相互促进的积极效果，为数字社会治理、交易和数字经济发展提供重要支撑。

积极探索社会治理新模式

基于区块链与多方计算融合技术可创建更安全可信的数据共享流通平台，减少信息不对称，使得社会治理组织能及时获得更准确、更高质量、更全范围的社会行为信息，让社会治理变得更加公平、更加灵活和更加高效。同时，也能帮助监管机构有效挖掘出隐藏在海量数据中的风险趋势，实现风险早识别、早预警、早发现、早处置，从而更好地完善现有监管体系，并提升对新技术应用风险的把控能力，推动监管机构实现从“事后监管”走向“实时监管”，从“旁路监管”走向“主动干预”。

此时，区块链与多方计算结合能有效推动数据确权 and 流通，区块链技术使得数据权属得以确认，而多方计算技术使得数据的可见价值与使用价值剥离，在保护数据隐私同时也能让数据的使用价值进行流通交易，为更多数据资源成为可交易的资产提供关键技术支撑。区块链与多方计算还能推动数据交易市场的发展，区块链技术能让数据资产交易的平台透明度提升，多方计算技术则能规定数据的用途用量，避免数据被滥用，加速数据价值变现步伐，为我国加快培育数据要素市场奠定基础。

总之，区块链与多方计算结合可搭建更安全、更灵活的数字基础设施底座，基于该底座可与大数据、人工智能、5G、物联网等多种新一代信息技术有机结合，并能充分激发新技术的应用潜力与价值，也将催生出全新的数据产业生态，促进数据与产业的深度融合创新应用，有效推动数字经济的高质量发展。



数字经济赋能城市治理

□ 李国正 迟远英 艾小青

改革开放以来，伴随城乡二元体制机制壁垒消弭，大规模农业转移人口开始从乡村涌入城镇，中国的常住人口城镇化率从1978的17.92%飙升到2019年的60.60%。人口向超大城市（城区常住人口1000万以上）、特大城市（城区常住人口500万以上、1000万以下）集聚，对城市承载力提出了巨大的挑战，考验着城市治理能力。

数字经济为超大、特大城市提供了新的治理路径。数字技术的跨时空关联性使得经济能以较低的成本和多样化的方式建立起新的连接，数字经济因其线上优势，使得经济活动和社会行为可以更容易地打破时空界限，从而最大限度地减少了人口的集聚。具体而言，第一，基于新一代信息技术的数字经济导致产业中的上下游企业在地理空间中的依存度降低，使得企业与企业之间的地理空间关联与纽带变得没有那么紧密，促使企业与企业之间从原先地理空间集聚模式变成以数据和信息实时交换为核心的网络虚拟集聚模式，从而推动区域内产业转移。第二，数据要素能够促进技术、人才等其他生产要素的跨地区协同联动，有助于实现产业链上下游之间以及企业内部不同职能部门之间的跨地区合作与沟通，从而进一步推动区域内产业转移和人口疏解。第三，数字经济改变了居民的消费习惯、消费行为与消费结构，“在线消费”“移动支付”等发展迅速。一方面，互联网平台消除了消费信息不对称问题，使生产和服务的供求信息更加精确；另一方面，由于信息在网络上的共享性，网络消费产品可以复制，不会引起边际成本增高以及市场交易量的增加。第四，数字经济减少了劳动密集型企业对劳动力的依赖，一方面，工业机器人的投入会显著提高工业劳动生产率，从而替代一部分劳动就业；另一方面，随着大数据、云计算、人工智能技术的进一步发展，机器主要可以实现自我监督和自我调节，智能化的生产过程进一步加剧了物化劳动替代活劳动的过程。第五，数字经济有助于促进地区间公共服务均等化，尤其是伴随“在线教育”“远程医疗”等新模式、新业态发展，高质量的公共服务资源可以更高效地实现跨地区共享。第六，数字经济与农村经济深度融合，提升了农业附加值和农村经济发展，在推动乡村振兴的同时也增加了乡村对劳动力的拉力。综上所述，数字经济在促进中国经济动能转换的同时，也极大改变了城镇经济结构以及居民生活、工作习惯，成为破解中国发展难题的重要战略选择。

以“虚”“实”深度融合提升未来中国数字经济的承载力和包容力。信息技术是数字经济发展的基础，自主创新是数字经济发展的生命线。我们应该发挥制度优势，集中力量推动新一代信息技术的研发。与此同时，重视推进“数字中国”建设，发展分享经济，支持基于互联网的各类创新，通过发展跨境电子商务、建设信息经济示范区等，促进世界范围内投资和贸易发展，推动全球数字经济发展。此外，面对虚拟经济过度发展导致实体经济空心化的隐忧，在加快发展数字经济的同时也应该推动实体经济和数字经济融合发展，其核心任务是加快中国互联网基础设施体系建设，努力提升信息数据链的完备性。



企业数字化转型要找准切入点

□ 李东红

面对蓬勃发展的数字经济，推进企业数字化转型成为必然趋势，将数字技术数字化思维与数字化管理工具引入生产经营活动中，以求降低成本、提高效率、改善客户体验、增加产品与服务价值，进而建立起新的市场竞争优势，使企业谋求更好的生存与发展。那么，企业该如何有条不紊、卓有成效地推进其数字化转型呢？企业转型的切入点，成为其中重要一环。

企业数字化转型要点面结合

本轮企业数字化转型呈现出三大显著态势。第一，数字化与企业全面融合。数字化不仅在传统的财务、人力资源、内审、行政办公等职能管理领域与企业更为紧密地融合，而且深入到了技术创新与产品开发、物流与仓储、生产过程与设备维护、销售与售后服务等业务发展的各方面。企业生产经营过程中的每个环节、每项行为活动，都有数字技术与管理参与其中，甚至发挥主导作用。第二，数据全面汇集成为新的生产要素。企业内部各部门与人员、机器设备、零部件与产品、生产与作业现场，以及企业外部的供应商、客户与横向合作者，都在生产、协作与交易中源源不断地产生出以文本、图像、声音、视频等多种方式呈现的信息，在实现数字化转换后，形成海量数据。这些数据在经过标准化清洗后进行存储，成为企业的“主投入”或“辅助投入”，从而具有了突出的企业生

产要素特性，甚至成为支撑企业未来发展的战略资源。第三，智能化决策全面显现。大数据、云计算、边缘计算等技术广为应用，带来了企业对消费者更为精准的画像与预判，企业决策更多地依赖企业的数字化、智能化系统作出分析。

信息科技的发展要求企业必须全面部署数字化转型工作。首先，企业内部需要对此形成广泛的共识，管理团队需要充分认识到全面推进数字化转型的必要性和紧迫性，认同企业向数字化转型工作的持续资金投入及新型团队建设，高度关注并愿意带领员工一起投身转型的工作之中。其次，企业要制定出全面推进数字化转型的战略方案。企业要有较为明确的数字化转型的总体目标与核心任务，特别是要建立的数据库、数据治理机制、数据模型的整体架构及其功能、数字化系统的预期成效，各部门转型工作粗线条的任务分工与协作，主要时间节点的工作进展，各数字化模块的内在联系与相互支撑机制等。这些共同构成企业有计划、有步骤、有系统地推进其数字化转型的行动纲领。再次，企业要把推进数字化转型的每一项具体工作视为全面推进转型的有机组成部分。以内部立项的方式推进数字化转型——形成一个或多个项目，确立项目的目标、任务与场景，组建项目团队，划拨资金，监控项目执行过程，项目完成后验收并投入运行。每个项目的建立与执行，都要有全局视野，要有统一的基础标准。单个项目所形成的子系统一定要避免各自为战、互为孤岛和低下

平重复建设，要能在遵循一定治理准则的要求下顺畅地实现相互连通和数据共享、相互赋能并能共同对企业的全面转型形成强有力的支撑。对于项目推进中暂时无法实现充分连通的子系统，要预留出足够的接口。

企业全面部署数字化转型，实现全面转型的目标，需要从某个领域切入，然后再以更大的力度推进全面转型。这主要是由如下三个方面的现实条件所决定的。其一，数字化转型要建立数字化人才队伍。数字化转型迫切需要重塑一支既懂数字技术与管理、又深悉具体业务的员工团队，很难一蹴而就、应从某个点出发，以点带面，持续累积。其二，大量的资金投入有助于企业数字化转型。建设企业的数字化前台、中台与后台，建立私有云或使用外部的公有云，因应数字化要求改造现有的生产场地与办公场所，依据场景要求进行模型开发与应用等，都要求企业持续投入大量资金。

甄选数字化转型切入点的若干准则

第一，着眼于消除痛点。每个企业，都会面临一个或多个制约其发展的痛点。企业选择数字化转型切入点时，可以首先考虑从企业痛点入手施行数字化转型。

第二，格外关注价值点。企业推进数字化转型，不是赶时髦，而是为了谋求持续发展。为此，企业在选择切入点时，有必要充分考虑

在哪个或者哪些关键点率先推进数字化转型能够带来可观的价值。这样的价值，可以从两个维度来衡量。一是为客户带来性价比更优的产品或服务、更好的体验；二是为企业带来收入和利润的增加。

第三，高度重视成熟点。企业分阶段、分职能或业务领域、分模块推进的数字化转型，应该走先易后难的道路，率先把相对成熟的领域作为切入点。这里所讲的成熟领域，包括两层含义：一是就企业自身而言，以往的信息化、自动化等工作已经为数字化转型作了不少积累、基础较好；二是就全社会的数字化进程来看，产业中已经有较为成熟的技术手段和软硬件作支撑，有清晰的实施步骤与办法和不少成功范例、易于落地。

第四，优先考虑牵引点。企业的数字化转型的最终目标是全面数字化，切入点只是最初的关键一步。既然如此，能够发挥牵一发而动全身、对企业其他组成部分的数字化转型具有较强引领和带动效应的领域，显然应该优先作为数字化转型的切入点。

显然，具体到特定的企业，选择数字化转型的切入点时并不需要同时满足上述四个方面的要求，重要的是：企业可以从这四个维度进行深度分析和推演，更好地甄选出切入点，从而更为从容和有效地推进数字化转型工作。



（上接1版）

有效防控百年未有之大变局中的风险挑战，需要始终保持理论上的清醒。要深入学习马克思主义基本理论，真学真懂真用习近平新时代中国特色社会主义思想，切实掌握贯穿其中的辩证唯物主义的世界观和方法论，提高战略思维、历史思维、辩证思维、创新思维、法治思维、底线思维能力，善于从纷繁复杂的矛盾中把握规律，善于透过复杂现象把握本质，始终做到心中有数，通过早防控、严防控、智能防控和联动防控等手段，真正实现防患于未然，

有效防控百年未有之大变局中的风险挑战，还必须制度化作保障，建立完善风险防控机制。“要突出问题导向，建立健全风险研判机制、决策风险评估机制、风险防控协同机制、风险防控责任机制，主动加强协调配合，形成齐抓共管的合力。”要加强对各种风险源的调查研判，提高动态监测、实时预警能力，推进风险防控工作科学化、精细化，对各种可能的风险出手及时有力，力争不出现重大风险或在出现重大风险时能够有效应对。

勇于担当作为，提高化解能力

应对重大挑战、抵御重大风险、克服重大阻力、解决重大矛盾，必须进行许多新的历史特点的伟大斗争。要充分认识到这场斗争的长期性、复杂性、艰巨性。既要高度警惕“黑天鹅”事件，也要防范“灰犀牛”事件；既要有效防范风险的先手，也要有应对和化解风险挑战的高招；既要打好防范和抵御风险的有准备之战，也要打好化险为夷、转危为安的战略主动战。这是我们在应对百年未有之大变局中风险挑战的重要遵循，领导干部务必要做到“准确识变、科学应变、主动求变”，“既善于积势蓄势谋

势，又善于识变求应变”，勇于担当作为，在斗争实践中，不断强化斗争意识，增强斗争本领，敢于和善于斗争，并做好斗争的充分准备，从最坏处着眼，向最好的结果努力，自觉把职责使命扛在肩上、干在实处、走在前列，绝不能把问题和风险推给上面、留给后面，切实做到守土有责、守土担责、守土尽责。

化解风险挑战，必须清醒认识到我国依然处在社会主义初级阶段、依然是世界上最大的发展中国家的国情，充分认识到自身的短板，充分认识在深化改革开放中凸显出的深层次矛盾问题。发挥中国特色社会主义制度优势，发挥我国众志成城、聚合国力、攻坚克难的体制优势，发挥我国市场容量大、经济承压韧性强的优势，努力把我们的事情办好，夯实应对风险挑战的基础。

化解风险挑战，必须不断提高化解风险挑战能力。要精准施策、靶向发力，落实好中央各项决策部署。坚决贯彻总体国家安全观，确保我国政治安全；持续巩固壮大主流舆论阵地，落实意识形态工作责任制，创新思想政治工作内容和形式；下大气力解决好人民群众切身利益问题，切实做好“六稳”“六保”各项工作，等等。要克服“本领恐慌”，不断提高综合素质和驾驭能力，遇到重大风险挑战、重大工作困难、重大矛盾斗争，能够做到第一时间进行研究、拿出切实可行的预案、有效推动工作。

“暮色苍茫看劲松，乱云飞渡仍从容”，无论国际风云如何变幻，只要我们牢牢把握全球大发展大变革大调整时期和平与发展的时代主题，高举和平、发展、合作、共赢的旗帜，锐意推进构建人类命运共同体，切实提高防范化解风险的能力，就能够在应对大变局中，实现既定的发展目标。

（作者系全国社会保障基金理事会副理事长、党组成员）