隐私计算：构建金融数据安全共享的新范式

基于隐私计算的数据安全共享新范式，将逐步改变整个金融行业数据流通的模式，撬动金融行业更大范围、更深层次的数据应用。

文 | 宋益昶

当前，随着数字经济的发展，信息化与数字化浪潮加速推进。作为数字时代最重要的生产要素之一，数据成为推动数字经济深化发展的核心引擎，也为数字经济发展提供不可或缺的动力源泉。如何在保障各参与方数据安全的前提下实现流通共享和协作应用，是合规、安全、充分地挖掘和释放数据价值的关键。

根据 2021 年 9 月正式实施的《中华人民共和国数据安全法》条文，数据是指任何以电子或者其他方式对信息的记录；数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等；数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

金融业是数据密集型行业，掌握大量身份、财产等重要数据信息，这些数据信息在金融机构经营发展中一直发挥着基础、全局、引领作用。在依法合规的前提下，金融机构对数据要素合作共享、融合应用的需求尤为迫切。中国人民银行今年年初发布的《金融科技发展规划（2022-2025 年）》提出了八大重点任务，其中格外注重“数据”，明确提出从强化数据能力建设、推动数据有序共享、深化数据综合应用、做好数据安全保护方面充分释放数据要素潜能，并陆续出台了金融数据安全相关标准，对金融数据安全与共享应用的重视程度与日俱增。

金融数据融合应用面临挑战

我国金融数据融合应用正处于起步阶段，金融机构已在内部数据价值挖掘方面取得诸多成果，但受自身数据维度单一、实时性不足等影响，各类市场主体在金融数据融合应用领域尚未形成统一的应用模式，不同类型的数据融合共享平台呈现出多元化、分散式等特征。同时，由于具有高敏感性、隐私性等特点，金融数据应用正面临一系列挑战。

数据安全问题突出。随着大数据、云计算、移动互联网、人工智能等新技术的兴起，各类型数据应用层出不穷，数据价值日益提升。但与此同时，围绕数据的泄露、滥用、违规交易等风险事件也时有发生，侵犯了公民的隐私及财产安全。因此，构建隐私数据安全防护体系，已成为金融行业实现数据要素融合应用必须直面的难题。

合规审查日趋严格。金融数据的安全与风险防范一直是监管部门关注的重点内容，国家层面也多次出台相关政策与法律法规，如《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等，对金融数据安全保护与合规审查的要求日趋严格。

“数据孤岛”问题凸显。众多企业在开展业务的过程中积累了海量数据，但由于物理和逻辑上的孤立性、合规监管以及隐私保护等方面的原因，不同系统、组织、行业之间的数据安全壁垒日渐增加，导致数据共享开放程度较低、数据流转不畅，也逐步形成大量的“数据孤岛”，阻碍了数据要素价值的挖掘和流通。

如何让“数据可用不可见”

如何在满足合规要求、保护各方隐私的前提下将自有数据和外部数据融合运用，如何建设安全的金融数据生态，已成为金融行业亟待解决的共性问题。对此，“隐私计算”技术的发展为内外部数据融合应用提供了全新路径。

隐私计算，是指一种由两个或多个参与方联合计算的带有隐私机密保护功能的技术和系统，参与方在不泄露各自数据的前提下通过协作对数据进行联合机器学习和分析。在隐私保护计算框架下，参与方的数据不出本地。隐私计算将数据所有权和使用权分离，从技术上对数据的共享使用形成刚性约束，确保数据安全合规共享，以“数据可用不可见，数据不动价

隐私计算将数据所有权和使用权分离，从技术上对数据的共享使用形成刚性约束，确保数据安全合规共享，以“数据可用不可见，数据不动价值动”的形式保障数据安全。

值动”的形式保障数据安全，发挥数据的价值，进一步提升金融核心业务能力。

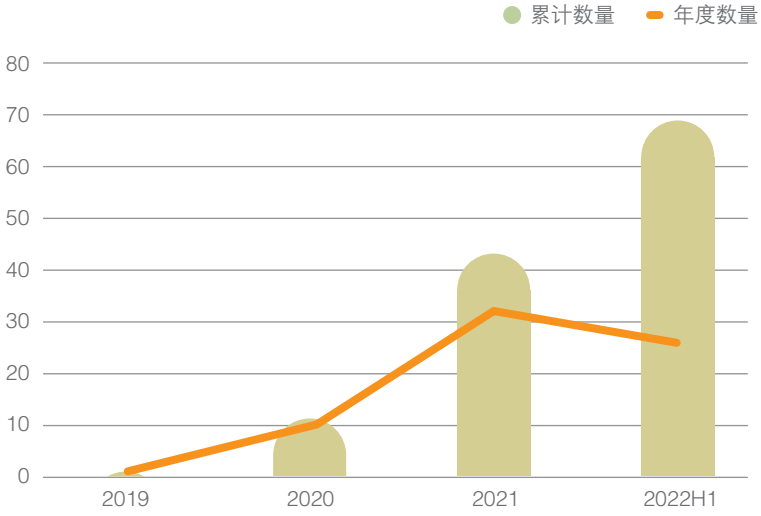
隐私计算体系共涉及三个关键技术：区块链、联邦学习和多方安全计算。

区块链技术可以构建数据互信的机制，有效实现分布式协作模式。区块链本身具有多中心、分布式以及不可篡改、智能合约的特性，能够更好地应用于数据确权、行为追踪、数据使用、人员管理以及全生命周期授权管理等。

联邦学习则可以将分布在多个机构的数据，在不出库的情况下进行联合学习、建模和预测，充分应用多方异构数据建立更好的模式，为用户提供优质服务。比如在营销场景中，有些金融机构手中的营业数据较为单一，但结合电商的采购数据、社交数据，则可以更好地为用户建模。

多方安全计算是一种基于多方数据协同完成计算目标、实现除计算结果及其可推导出的信息之外不泄露各方隐私数据的密码技术，通过一系列经过严格证明的密码学协议，实现了互不信任的多个参与方在不泄露自身原始数据的前提下，得到准确的计算结果，从技术上限定了数据的使用形式和使用范围，达到“可用不拥”“不可还原”“不可重标识”的合规性要求，为破解数据安全共享难题提供了技术解决方案。

2019 ~ 2022 年上半年隐私计算招标数量



> 数据来源：中国通信院

新场景培育新业态

隐私计算通过综合运用密码学、统计学等方法，实现了数据“可用不可见”与“可控可计量”，不仅在保证数据安全和隐私的前提下推动了数据共享，同时也化解了数据价值流通与隐私安全保障之间的矛盾，从而推动我国金融数据融合应用迈入快速发展的新阶段。目前，隐私计算技术已广泛应用于普惠金融、联合风控、精准营销、金融监管等业务场景，随着数据融合需求的进一步释放，应用场景正快速拓展至金融产品定价、反洗钱、运营管理等领域。主要业务场景如下。

一是供应链金融信用信息流通。“供应链金融”通过核心企业评估上下游配套中小企业的还款能力，解决其融资难问题。如何在保守各自商业秘密的同时实现企业间、企业与银行间的信息传递，使得银行可以有效评估企业的还款风险，是供应链金融面临的一大挑战。“区块链 + 隐私计算”能够将企业的经营信息形成不可篡改的数据记录，实现实时信息共享。其他参与者无法获知具体经营信息，但可以利用其进行信用评估计算。该解决方案十分契合供应链金融业务发展痛点，缩小了企业授权范围，避免了数据在使用的过程中被留存，有利于解决供应链金融场景下服务提供方与核心企业、小微企业间价值不对等、信息孤岛、信息泄露等问题。

二是丰富用户画像，服务精准营销。在存量用户挖掘、异业交叉营销等场景中，由于单一金融机构拥有的数据资源有限、数据特征单一，通常难以精准、实时地分析用户偏好，最终被迫采取“广而告之”的营销方式。对此，基于隐私计算技术支持数据价值和原始数据分离的特性，金融机构可在保障数据融合应用安全、合规的前提下，全方位刻画用户画像，构建“千人千面”的精准营销模式，从而更好地了解用户需求、提升用户满意度，并构建起由数据驱动、模型驱动的精准营销模式，以产品精细化营销助力业务精细化发展。

三是融合多方数据，提升风控水平。“数据孤岛”现象使金融机构在贷前、贷中、贷后各环节都存在风险识别难的痛点问题，且多头借贷风险较难规避。通过隐私计算技术与合作机构展开政务、企业等多维度数据融合共享，银行等金融机构将可以实现数据安全融合，在贷款全周期流程中实时、精准、全面地分析用户。通过采用纵向联邦学习、多方安全计算等技术，将多方数据共同用于训练联邦风控模型，能够在保护用户隐私数据的前提下实现模型优化，进而更好地支持普惠金融和消费金融发展，提高风控能力，且数据样本和模型效果的提升还可有效节约传统信贷的审核成本。

四是金融联合反欺诈、反洗钱。随着银行业、保险业、证券业线上业务占比的不断上升，金融欺诈渗透线上申请、交易、营销等各个环节，欺诈手段也越发防不胜防。鉴于单一来源数据构建的反欺诈模型效果较差，各机构具有很强的反欺诈合作意愿，但在具体合作过程中又会担心用户的隐私数据和机构的商业机密遭到泄露，造成重大不利影响。通过隐私计算技术，可以整合内外部收集到的各种数据，尽可能消除申请及交易等环节的信息不对称问题，并与用户行为建立关联，从而更全面地了解用户、评估用户。基于多方数据源还可建立丰富的反欺诈模型、规则以及反欺诈知识库，对用户进行持续识别和监控，增强反洗钱风险洞察及溯源核查能力。

隐私计算通过密码学、统计学、人工智能等科技手段的交叉融合，有效解决了数据共享交易过程中所存在的数据保护问题，为数据安全提供有力的技术支撑。但是，隐私计算的应用在技术实现、性能等方面仍存在诸多挑战：在技术实施方面，存在异构隐私计算平台无法互联互通、性能效率低、产品化能力不足等局限；在业务方面，传统业务与隐私计算平台的结合与改造需要大量的时间和人力成本，同时业务价值难以体现；在操作方面，数据安全法等法规实施后，相应的实施细则和指南仍未出台，隐私计算的落地缺乏指导依据。

展望未来，隐私计算技术通过与人工智能、区块链、边缘计算等技术进行融合创新，将能够形成体系化的技术解决方案，助力金融机构加快实现数字化转型。同时，通过实现计算性能与效率的平衡，以及不断增强计算模型有效性和稳定性，将可以构建更加成熟、易用的隐私计算服务体系，进一步赋能金融机构释放多源数据的融合价值。相信在不远的将来，通过使用隐私计算技术贯通各主体、各领域、各行业的数据资源，可形成一个完整、安全的数据共享生态体系，从而将数据要素的市场化红利分享到各行各业。

虽然复杂的实践现状对隐私计算应用构成了不小的挑战，但长期来看，对于银行、保险、信托等诸多金融机构，与外部机构开展数据共享交易的金融科技赋能需求一直存在。随着技术不断成熟和市场认知逐渐提高，基于隐私计算的数据安全共享新范式，将逐步改变整个金融行业数据流通的模式，撬动金融行业更大范围、更深层次的数据应用，提升数据应用效能，为数字经济形态的向好发展提供稳健助力。

（作者供职于英大集团股份有限公司）

目前，隐私计算技术已广泛应用于普惠金融、联合风控、精准营销、金融监管等业务场景，应用场景正快速拓展至金融产品定价、反洗钱、运营管理等领域。