北京金融科技产业联盟
BEIJING FINTECH INDUSTRY ALLIANCE

金融业隐私计算应用风险与问题研究

北京金融科技产业联盟

2023 年 12 月

版权声明

编制委员会

编委会成员：

何　军　　聂丽琴　　强群力

参编人员：

陈　俊	郭　林	强　锋	魏博言	徐安滢	司忠平
邱晓慧	胡师阳	何东杰	王　雪	李武璐	王云河
时　代	王煜惠	高善博	李克鹏	张　雄	卞　阳
黄翠婷	方　竞	彭宇翔	傅致晖	薛瑞东	陈　剑
傅跃兵	姚　明	何　浩	靳　新	王　磊	殷　山
严守孟	昌文婷	冯博豪	许海洋	张志慧	金银玉
单进勇	蔡超超	周岳骞	张亚申	陈浩栋	卢春曦
刘　姝	龚自洪				

编　审： 黄本涛　　郭　栋　　刘宝龙

参编单位：

网联清算有限公司

中国工商银行股份有限公司

中国农业银行股份有限公司

北京银联金卡科技有限公司

中国银联股份有限公司

建信金融科技有限责任公司

华控清交信息科技（北京）有限公司

深圳市腾讯计算机系统有限公司

上海富数科技有限公司

同盾科技有限公司

北京融数联智科技有限公司

深圳市洞见智慧科技有限公司

蚂蚁科技集团股份有限公司

北京百度网讯科技有限公司

北京数牍科技有限公司

北京冲量在线科技有限公司

深圳壹账通智能科技有限公司

目 录

前 言

2016 年发布的《隐私计算研究范畴及发展趋势》正式提出“隐私计算”一词，并将隐私计算定义为：“面向隐私信息全生命周期保护的计算理论和方法，是隐私信息的所有权、管理权和使用权分离时隐私度量、隐私泄露代价、隐私保护与隐私分析复杂性的可计算模型与公理化系统。”

隐私计算本质上是在保护数据隐私的前提下，解决数据流通、数据应用等数据服务问题。根据目前市场上隐私计算技术的主要相关技术，可分为三类：多方安全计算、联邦学习和可信执行环境。

本课题基于隐私计算技术在金融行业的典型应用案例，从监管、安全、技术、参与者等角度多方位分析隐私计算应用的风险及所面临的困境，并针对上述问题提出有效的解决方案，同步给出政策建议，为应用隐私计算的金融机构提供参考和指导。

一、 隐私计算典型金融应用案例

(一) 联合风控与营销

目前行业主要有三种实现该功能的技术路线：多方安全计算、可信执行环境和联邦学习。

1. 多方安全计算

由于安全性上的优势，多方安全计算技术是金融业务联合风控场景最为常用的技术。金融机构在进行风控模型建模时，需要通过引入外部数据来增强风控模型效果，以便对申请贷款的用户或小微企业进行更准确的授信判断，基于多方安全计算的联合风控技术框架如图 1 所示。

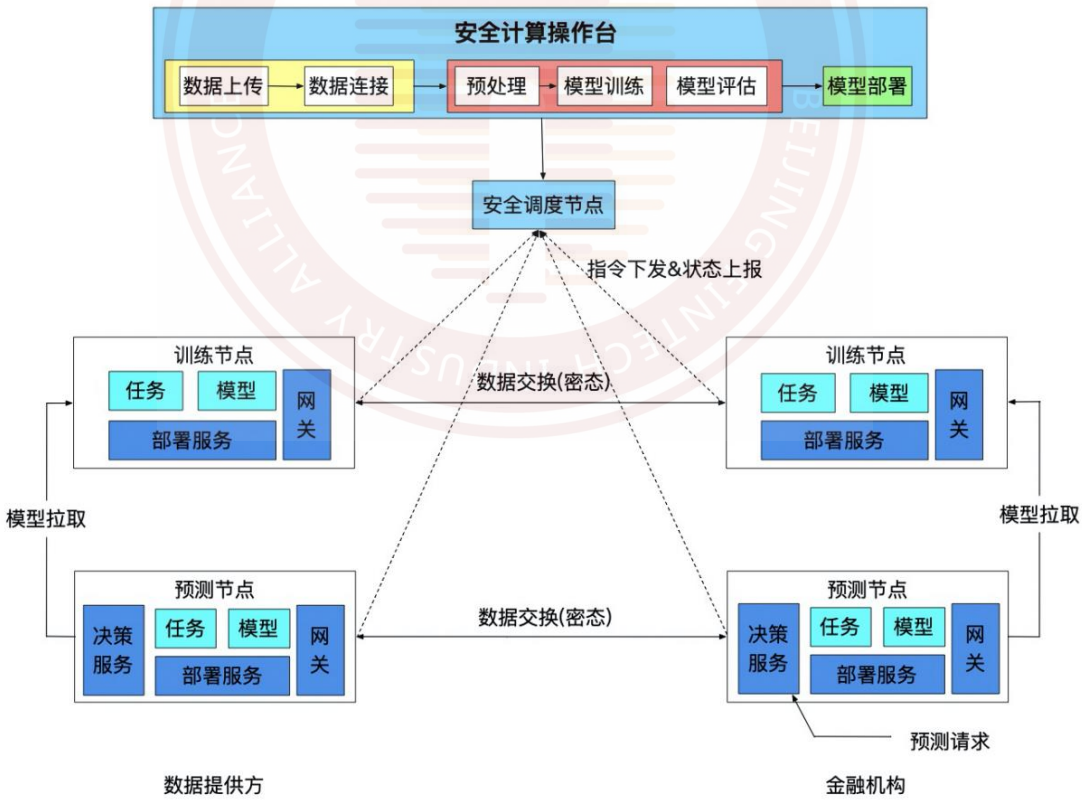

图 1 基于多方安全计算的联合风控技术框架

多方安全计算训练流程如下:

步骤一: 参与方（金融机构和数据提供方）将训练数据样本上传至各自的数据存储服务。

步骤二: 建模人员在多方安全计算平台通过可视化页面构建数据融合、特征工程、模型训练、模型评估等工作流。

步骤三: 工作流以任务形式下发到协调器，后者将任务调度到对应节点的训练引擎。

步骤四: 训练引擎根据任务描述，读取本地样本数据

步骤五: 训练引擎使用多方安全计算协议与对端协同完成一次训练任务。

步骤六: 训练任务完成后，训练引擎将模型文件保存至各自的模型存储服务。

多方安全计算预测流程（一次预测过程）如下:

步骤一: 决策服务作为预测请求统一入口，金融机构从本地向它发起一次预测请求。

步骤二: 决策服务根据模型 ID，请求预测引擎。

步骤三: 预测引擎从金融机构本地的特征服务获取在线特征，利用本地的模型参数计算预测分数。

步骤四: 金融机构预测引擎向数据提供方预测引擎发起预测请求。

步骤五: 数据提供方预测引擎从特征服务获取在线特征，利用本侧的模型参数计算预测分数，并返回给金融机构。

步骤六: 金融机构预测引擎将两侧预测分数相加得到最终的预测结果。

2. 可信执行环境

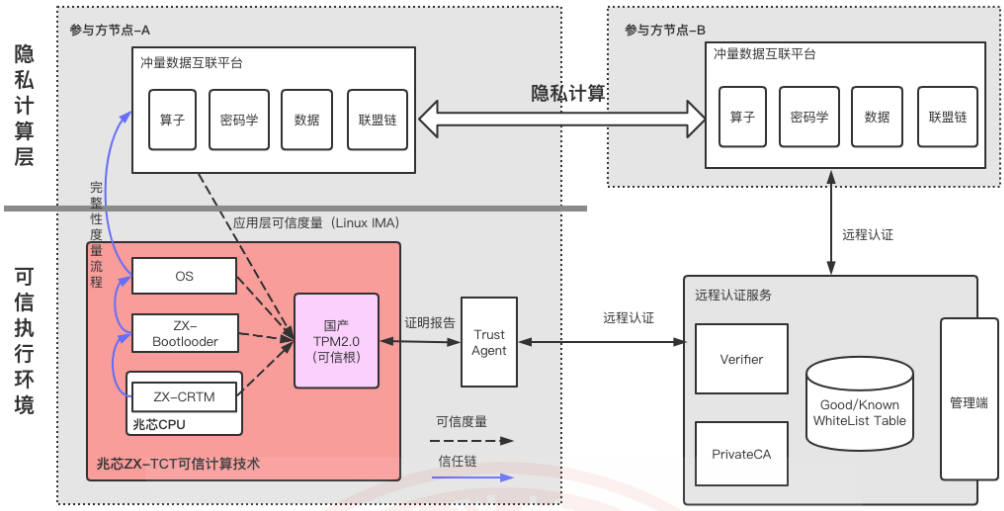

图 2　基于可信执行环境的联合风控技术框架

本案例为基于可信执行环境（TEE）的联合风控与营销方案，具体技术框架如图 2 所示。金融机构在进行金融产品销售之前，需要融合来自不同数据提供方的大量不同维度的用户数据，构建出用户风险评估和精准营销模型，以便于更好地对产品销售进行风控管理以及精准营销。

步骤一：金融机构，发起风控营销建模任务，同时选择参与任务的数据提供方和执行该任务的计算节点（计算节点只能是任务发起方或参与该任务的数据提供方）。

步骤二：风控营销数据的提供方也是某个计算任务的参与方，它可以选择是否参与任务。

步骤三：风控营销数据的提供方同意任务后，任务开始执行，此时数据会经过加密后上传到计算节点里，数据的上传过程是基于 TEE 的数据封存服务保证数据在域内安全、加密存储，通过 TEE 端到端构建的 TLS 通信保证数据在跨域流

通中一次一密传输并支持多协议层多重加密，用于保证数据的“可用不可见”。

步骤四：任务执行完成后，会对融合的数据进行销毁处理，保证数据不沉淀，并且任务结果仅作为任务发起的金融机构可见。

3. 联邦学习

本案例为基于联邦学习的联合风控方案，具体技术框架如图 3 所示。当银行客户向银行提出借贷申请时，银行需要整合各种方面的资讯来评估违约风险。传统做法一定程度上会泄露客户隐私，也会违背监管要求，因此未能普遍采用。银行现在利用联邦学习技术，可以联合其他数据方进行联合建模，在保护客户隐私数据不泄露的情况下，利用外部数据建立模型，不仅发挥了外部数据价值，而且提升模型预测的准确性。

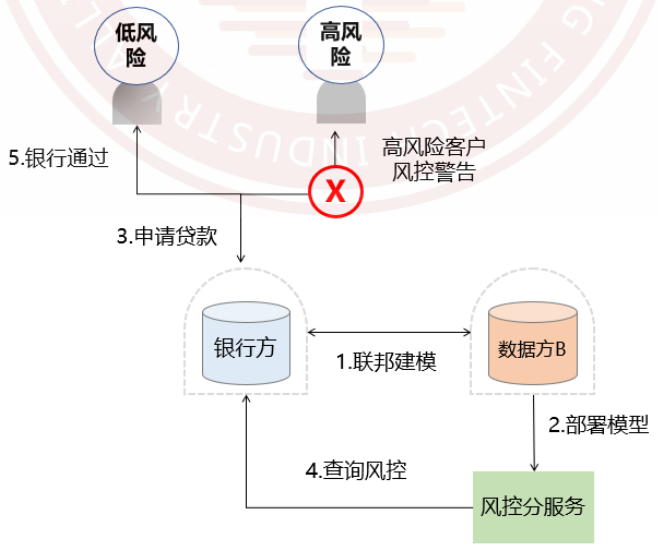

图 3 基于联邦学习的联合风控技术框架

(二) 智能运营

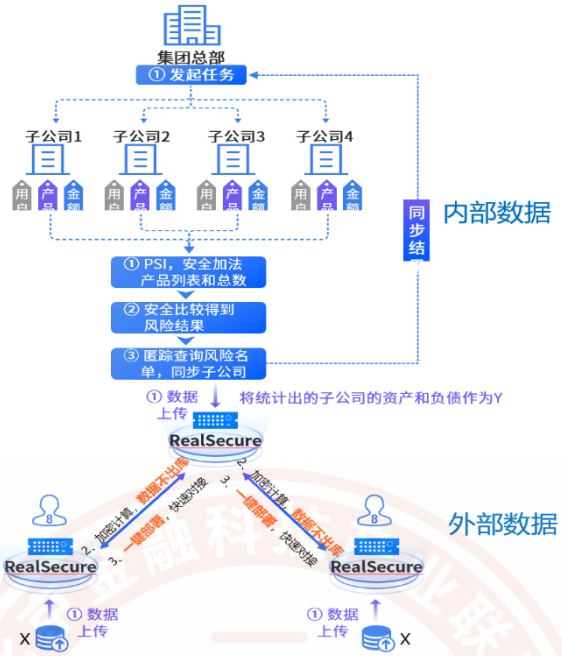

图 4 基于联邦学习和多方安全计算的智能运营技术框架

本案例为基于联邦学习和多方安全计算（MPC）的智能运营方案，技术框架如图 4 所示。银行业机构通过联邦学习、多方安全计算等手段安全合规地利用外部数据源，实现对客户的精细化管理、客户分群、客户特征描述、产品需求偏好分析等。同时针对不同类型的客户制定不同业务策略，改善服务，提高效率，降低成本，实现对客户全场景智能化运营。需要注意的是，相关客户信息以及高价值客户特征数据信息的采集需要获得个人信息主体的同意。

步骤一：在银行业机构集团内部各个子公司部署隐私保护计算节点，实现集团内部各子公司的信息互联。

步骤二：同外部高价值客户特征数据源利用隐私保护计算平台对接，对客户特征进行建模交叉匹配，精准圈定目标客群。

步骤三：针对目标客户制定不同业务策略，提升服务体验。

(三) 反欺诈

本案例为基于多方安全图计算技术的金融反欺诈方案，技术框架如图 5 所示。应用基于各自管控的多方安全计算系统平台，确保银行和运营商两方数据在不出库基础上联合构建多方融合关系网络，并应用于小微企业普惠金融业务，精准识别企业集群背后的复杂关系链条及欺诈风险，助力金融机构提高风控能力，解决中小企业融资难问题，安全高效服务实体经济。

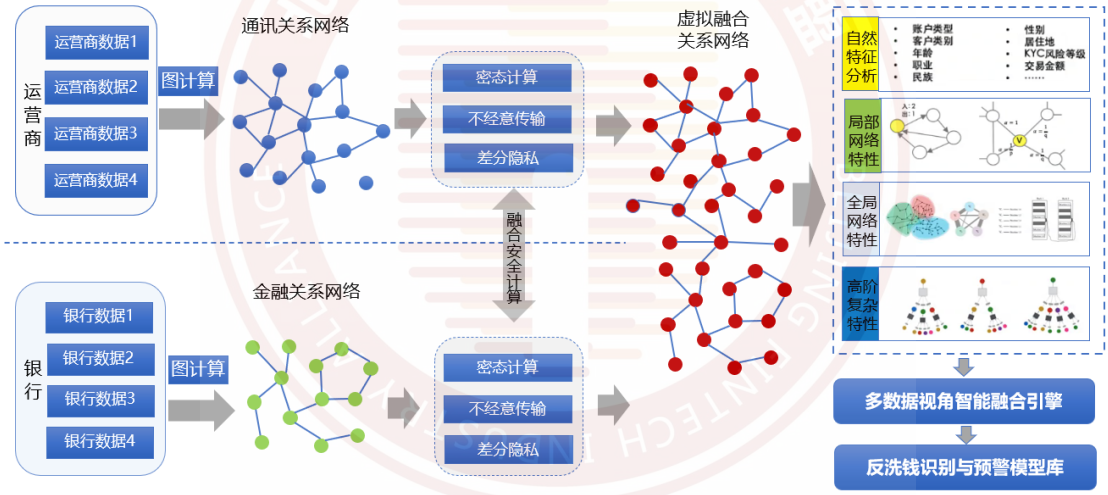

图 5 基于多方安全图计算的反欺诈技术框架

基于多方安全图计算的金融服务以多元技术融合突破应用边界，采用非对称、独立对称、融合对称三种安全图计算模式，结合差分隐私、密态计算、不经意传输等隐私计算技术，虚拟融合银行及运营商数据关系网络，通过对齐、扩充、传播、聚合等方法刻画关系图谱网络，进行用户自然特征、局部网络特征、全局网络特征和高阶复杂特征分析，在

多数据视角智能融合引擎基础上构建反洗钱反欺诈识别预警模型库，在金融反欺诈的识别效率和精确度方面均有大幅提升。

(四) 反洗钱

本案例为基于多方安全计算和联邦学习的反洗钱方案，技术框架如图 6、图 7 所示。针对金融机构和监管方在反洗钱领域面临的数据融合痛点，行业参与者可应用基于 MPC 的行业级数据安全融合平台，在保障各方数据隐私安全的前提下，掌握客户背景、交易性质、实体潜在关系、交易时序和全链路资金流向情况，实现对可疑洗钱行为的精准识别，降低样本误报比例，减轻监管方的成本负担。

1. 通过 MPC 有效识别洗钱高风险人群

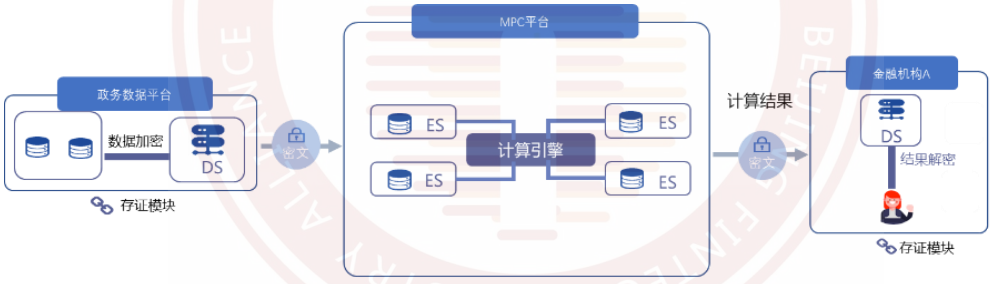

图 6 基于多方安全计算的反洗钱技术框架

步骤一：数据输入环节。政务数据平台和金融机构作为数据提供方，将客户身份证明及资产等相关数据通过计算节点以密文形式（输入因子）接入平台。

步骤二:计算环节。基于 MPC 的数据融合平台为计算方，执行联合统计及联合建模功能。其对输入因子进行预处理后分发至各计算节点，确保每个计算节点仅能获取到单个输入节点输入因子的部分“切片”。各计算节点完成各自计算后

将结果提交至计算引擎，由 MPC 计算引擎将计算结果切片后分发给若干个计算节点（每个计算节点仅能收到部分切片，即输出因子）。

步骤三：结果输出环节。平台将结果输出至金融机构的业务系统并解密为明文结果，即客户提供的身份信息是否为真以及客户洗钱风险预测。随后各计算节点销毁计算因子、计算中间结果和最终结果数据。

2. 使用联邦学习有效识别资金链路

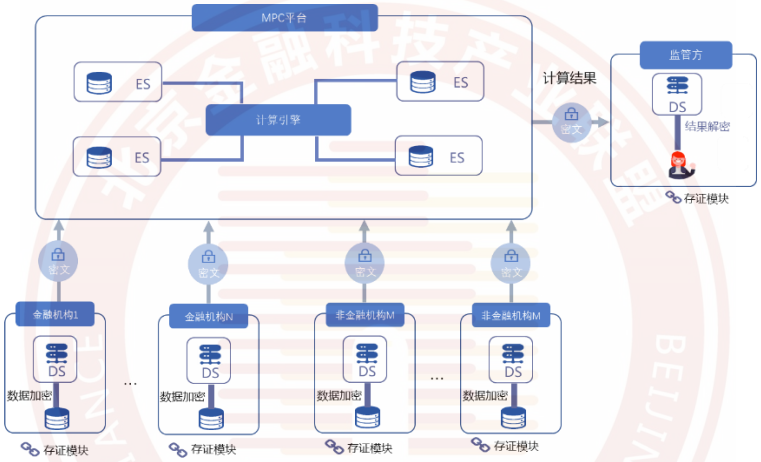

图 7 基于联邦学习的反洗钱技术框架

步骤一：银行、支付、保险、证券、期货、信托、财务公司等金融机构及工商企业、拍卖行等非金融公司作为建模参与方，在本地应用客户信息及其资金相关数据建立本地模型，随后将模型中间结果（如梯度和参数等）通过计算节点以密文形式（输入因子）输入平台。

步骤二：平台为计算方，对输入因子进行预处理后分发至各计算节点，确保每个计算节点仅能获取到单个输入节点输入因子的部分“切片”。各计算节点完成各自计算后将结果提交至 MPC 计算引擎，由引擎将计算结果切片后分发给若

干个计算节点（每个计算节点仅能收到部分切片，即输出因子）。

步骤三：平台将更新后的全局模型中间结果输出至各机构用于更新本地模型。

上述步骤迭代至全局模型收敛后，建模完成。训练后的全局模型应用不同机构的客户资金信息计算客户洗钱风险评分，并将其以密文形式上报至监管机构。监管机构的业务系统将其并解密为明文结果，用于筛选可疑洗钱分子。随后各计算节点销毁计算因子、计算中间结果和最终结果数据。

(五) 匿踪查询

本案例为基于多方安全计算的匿踪查询方案，技术框架如图 8 所示。查询方隐藏被查询对象 ID 如关键词或客户 ID，数据服务方提供该查询对象的数据却无法获知查询对象 ID，使其查询意图不会泄露。杜绝数据缓存、数据泄露或数据贩卖的可能。在广告营销的应用场景中，广告主希望获得自己的客户更多的标签，同时不会泄露自己有哪些客户。

图 8 匿踪查询流程图

广告主、投放机构和标签补充机构同时分布式部署隐私保护节点，所有的数据都在节点上运行，不同的标签提供机构可以进行多方安全计算，多方统计，在进行多方安全计算的过程中，即完成了标签补充的任务，同时标签补充方的数据得到了保护。通过匿踪查询，广告主在匹配自己存量客户的时候，保障了自己其他的客户隐私安全。

(六) 资产证券化

本案例为基于多方安全计算和联邦学习的资产证券化方案，技术框架如图 9 所示。资产证券化的核心能力是需要评判资产价格及个人偿还能力，传统的资产证券化所需要的相关信息是公开的，并不需要使用隐私计算技术。而随着资产证券化业务的发展，为了能够更准确地评判资产价格和个人偿还能力，相关机构引入了其他辅助信息（如征信信息），这些信息可能涉及企业或个人的保密信息，因此需要引入隐私计算技术加以保护。下述方案包括资产信用评估模型、现金流预测、增信咨询等功能。

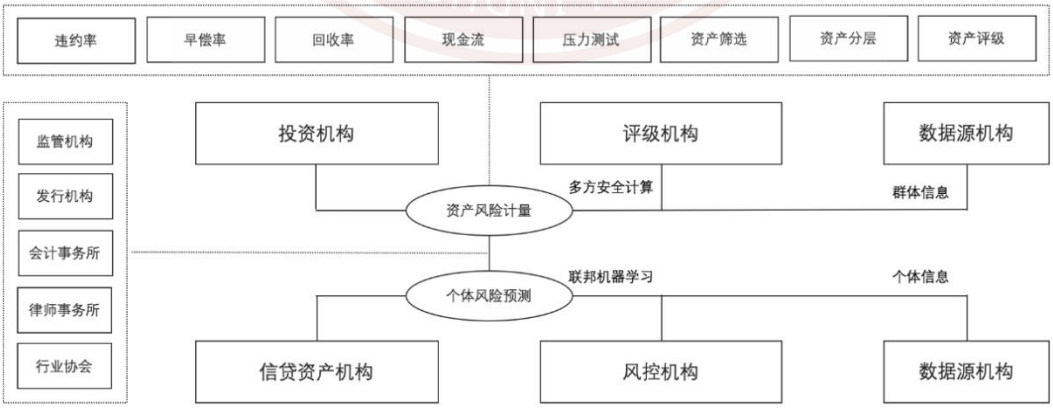

图 9 基于多方安全计算和联邦学习的资产证券化技术框架

步骤一：在底层资产评估环节引入独立的风控机构，风控机构利用资产方拥有的借款人还款表现数据、申请数据以及其他三方征信数据，通过联邦学习算法构建资产信用评估模型，得出资产信用评分，对底层资产做出筛选，依据违约率、早偿率、回收率等多个参数提供更有效的资产筛选，帮助投资人实现精准风控。

步骤二：基于资产信用评分，生成违约率、回收率和早偿率的分布，预测计算资产所产生的未来现金流，通资金端和风控端。

步骤三：基于资产信用评分的资产筛选，实现对标准静态池方法的优化，可以降低次级厚度，从而降低发行成本，提高资金周转率。

步骤四：在评级环节引入第三方数据对底层资产进行更真实准确地评估，增加评级结果精准性。结合隐私计算的资产证券化过程实现了资产信用可见，但个体数据不可见，同时避开了授权的复杂沟通及对接流程，加快了资产证券化业务的精准推进。

(七) 供应链金融

本案例为基于多方安全计算和联邦学习的供应链金融方案，技术框架如图 10 所示。传统供应链金融重点关注核心企业经营情况，监控供应链（进销存）数据和票据信息，这些信息可以是公开的，并不需要进行隐私计算。然而核心企业的经营情况并不能代表供应链上下游每一个企业的经营情况，供应链（进销存）数据和票据信息也难免存在杠杆率

过高或造假情况。供应链金融中如引入第三方数据，增强对核心企业上下游每家企业经营情况的监控，将更有利于控制供应链金融风险，但这些高价值数据的拥有者并不希望其他参与者获得相关数据，因此隐私计算技术在此场景中可以得到有效应用。

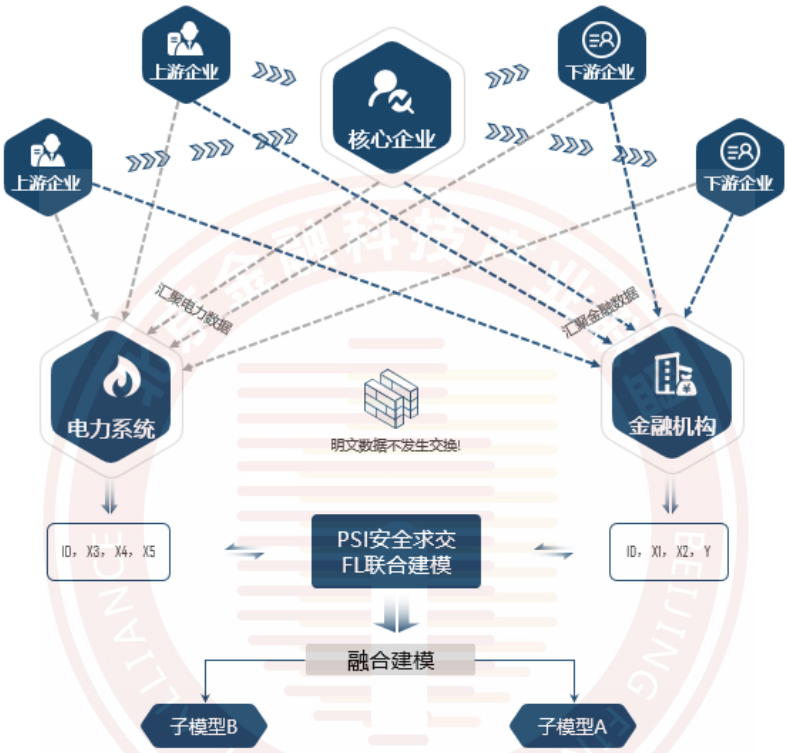

图 10 基于多方安全计算和联邦学习的供应链金融技术框架

现在双方对数据进行隐私求交技术，实现了各自明文数据不出本地的数据域，再应用联邦学习技术联合建模，实现双方数据可用不可见，可算不可知。从业务视角实现了对供应链相关企业更准确的风险评价。

(八) 跨行业数据流通与融合

本案例为基于多方安全计算和联邦学习，并结合了区块链等技术的跨行业数据流通与融合方案，技术框架如图 11 所

示。该大数据交易所采用了以 MPC 为核心、其他隐私计算技术及区块链存证功能相结合的组合型技术，构建了具有创新的数据交易模式和规则的数据融合平台，在保障数据安全的前提下实现了金融、政务等数据计算价值的跨域流通。该平台还支持交易过程中的第三方服务，以及关键信息上链等操作，便于监管部门对数据交易过程的审计及监管。

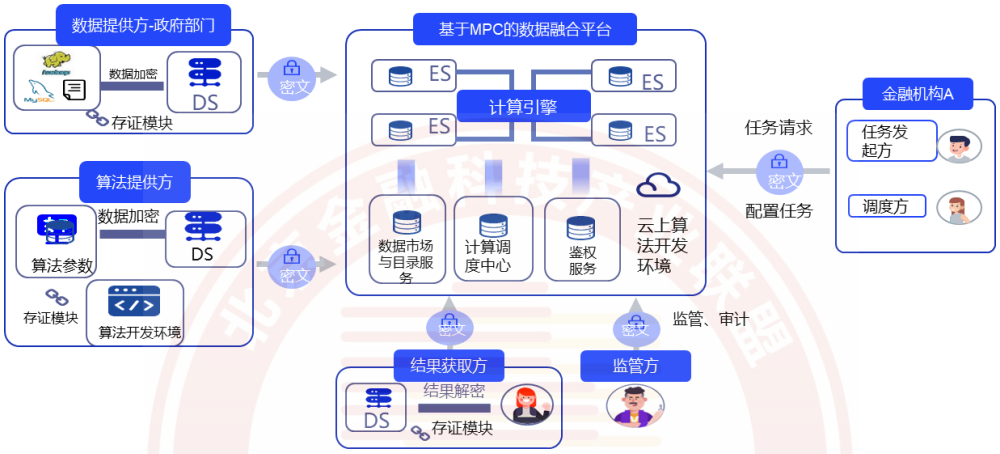

图 11 以 MPC 为核心的数据交易平台技术架构

步骤一：数据和算法输入环节。数据提供方（如金融及互联网公司）将需求方所需数据通过输入节点以密文形式（输入因子）提交至 MPC 计算引擎；算法提供方将算法参数加密提交至 MPC 计算引擎。同时，需求方（如金融机构）在平台发布需求并提交数据应用申请，随后根据自身需求在平台上选择相应的数据和算法，形成计算合约。

步骤二：数据计算环节。MPC 计算引擎将输入因子切分为若干随机切片，并分发至各计算节点，每个计算节点仅能获取单个输入节点计算因子的部分“切片”。各计算节点完成各自计算后将结果提交至 MPC 计算引擎，由其将计算结果

切片后分发给若干个计算节点（每个计算节点仅能收到部分切片）进行计算。

步骤三：数据输出环节。金融机构为结果获取方（即需求方），其输出节点对计算因子进行解密，获取明文融合结果。随后各计算节点销毁计算因子、计算中间结果和最终结果数据。

二、 隐私计算技术通用问题分析

(一) 隐私计算应用呈发散性发展

1. 路线多样

多方安全计算（Secure Multi-Party Computation, SMPC）是一个密码学定义。它是可证明安全的，即它有一个严格的安全定义，要保障双方除了最终的计算结果以外，中间的任何步骤都是不能泄露任何数据明文的。其目的是解决一组互不信任的参与方（数据持有者）协同计算一个既定函数的问题。该概念是由图灵奖获得者姚期智于 1982 年正式提出的。多方安全计算常用的实现有以下几个关键技术：秘密共享(Secret Sharing, SS)、混淆电路(Garbled Circuit, GC）和不经意传输(Oblivious Transfer, OT)。

联邦学习（Federated Learning, FL）是近代为了进行多方协同机器学习训练全局模型而诞生的概念，于 2016 出现并应用于改进用户手机输入法的场景中。它实现了在不直接获取用户隐私数据的情况下，从多个分布式手机用户中分别进行训练后获取各个模型梯度（间接收集用户输入法行为），并执行安全聚合，迭代优化全局输入法模型从而利益模型使用者（输入法用户）。联邦学习在参与方的数据不离开本地的情况下，通过多轮聚合各个参与方中间梯度的方式实现多方协同训练模型。

可信执行环境(Trusted Execution Environment, TEE)是一种基于硬件的安全技术，实现了机密计算。它的安全风险是来自对基于硬件的可信执行环境的各类侧信道攻击，从

而推导其内部的机密数据内容。其次，它必须被确认其可信执行环境厂商是可信的。例如可信执行环境方案中的远程通信需要可信执行环境厂商参与远程证明。最后，如果部署此方案，需要购买指定的硬件，这在某些场景中会显著提高使用成本。目前有 ARM 的 Trust Zone 和 Intel 的 SGX(Software Guard Extensions, SGX）为主流的 TEE。一般而言，在 TEE 中开发和运行软件需要专业的知识和工具，而且部署也需要特定的硬件环境绑定。

除了上述三种主流路线之外，还有较多相关隐私计算技术辅助或配合应用于主流路线之内，拓展了主流路线的应用场景，增强了主流路线的各项功能，如同态加密、差分隐私、区块链等。

同态加密（Homomorphic Encryption, HE）是一种基于数学难题的密码学技术。其特点是对经过同态加密后的数据进行计算得到一个输出，将这一输出进行解密后，其结果与未进行加密的原始数据进行同样计算的输出结果是一样的。这意味着数据处理权与数据所有权进行了分离，从而实现了保护数据隐私的能力。例如企业可以防止泄露自身数据的同时，利用云服务的算力。

差分隐私(Differential Privacy, DP)也是密码学的一种手段，旨在提供一种当从统计数据库查询时，最大化数据查询的准确性，同时最大限度减少识别其数据的机会。顾名思义，差分隐私的目的是用来对抗差分攻击，通常其应用场景是统计查询。对于两个相似的数据集，攻击者可以通过

两次返回的统计结果进行推理进而得到差异数据的隐私信息。其具体的解决方法是，在原始数据中加入一定的噪声，从而达到对于相似的数据集的两次统计返回的结果，攻击者无法推断出具体的隐私信息，从而保护了差异数据的安全性。

区块链(Blockchain)技术以其去中心化、不可篡改性、可追溯性、高度可扩展性、匿名性等特点被应用于包括金融行业在内的重要领域。本质上区块链是一种分布式账本（Distributed Ledger），目的是解决交易信任问题，其可有效保护信息的透明性，能够在不同机构共享信息。区块链可以和隐私计算技术结合，用于实现审计、存证、追溯等功能，更好地实现金融业务场景落地。而且，许可链也可以实现在对经审核的组织或个体进行授权，实现一定范围内的隐私信息共享。

表 1 隐私计算路线对比

技术分类 对比维度	多方安全计算	联邦学习	可信执行环境
第三方/协调方/可信方	有无均可	有无均可	是（需要可信硬件）
保密性	★★★★★	★★★★ （未结合密码学） ★★★★★ （结合密码学）	★★★★★
准确性	★★★★	★★★	★★★★★
高效性	★★★	★★★★	★★★★★
通用性	★★★★★	★★★★	★★★★★
自主可控	★★★★★	★★★★★	★★★ （主要依赖 Intel 国际芯片；芯片本身存在漏洞）

注: 自主可控主要指金融业机构在应用隐私计算的过程中从技术层面对该技术路线的自主可控性。

TEE 主要依赖 Intel CPU，但是国内海光 x86 CPU、华为 ARM CPU、飞腾 ARM CPU 等 TEE 芯片都也有了较好的发展，TEE 国产化可以实现自主可控。同时，目前针对芯片的典型漏洞业界已有对应的补丁，但仍可能存在潜在未知漏洞的风险。

隐私计算路线对比如表 1 所示，上述表格不建议单独作为金融机构技术或产品选型的决策依据，仅作为学术参考。

2. 架构多样

不同隐私计算技术的原理和特性不同，其适用的金融应用场景也不同。当技术落地为具体的金融产品时，不同的产品架构在安全性、通用性、计算效率和可扩展性等方面也会有差异。存在多个维度对隐私计算技术的产品架构进行划分，如根据参与方个数划分，有两方计算架构、三方计算架构等。这里根据数据提供方（简称：数据方）之间是否有交互计算，即数据方是否同时也是提供算力的计算方，将隐私计算架构分为直连架构与代理计算架构。这也是目前隐私计算领域常用的两种架构方式。

（1）直连架构

直连架构中，数据方直接参与隐私计算过程，即数据方同时担任计算方的角色。该架构有两种常见的形式，一种是对等（peer to peer）网络架构，另一种是客户端-服务器（client-server）架构或主-从（master-worker）架构。

对等网络的典型例子是一种两方隐私集合求交（Private Set Intersection）的实现架构。两方 PSI 问题

指两方各有一个样本集合，希望求解两个集合的交集，但每一方不向对方暴露自身不属于交集的样本子集。该问题的典型架构如图 12 所示，两个计算参与方 A 和 B 分别部署有一个计算节点，彼此通过网络互连，在隐私计算过程中进行数据交互，从而实现双方数据参与协同运算。

图 12 直连架构：对等网络示意图

客户端-服务器架构常用于特定场景的两方或多方计算，各客户端和服务器端通过网络互连，即多个客户端在服务器的协调帮助下，共同协作完成计算任务。其中，服务器也可以是数据方之一，如图 13 所示。

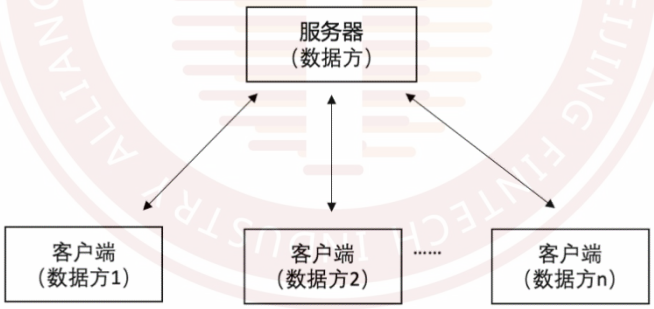

图 13 直连架构：客户端-服务器示意图

直连架构模式比较适用于计算时参与方数量相对较少的情况，在应用时能够快速部署，具有“短平快”效应，有利于快速推广隐私计算技术在金融领域的应用。

从可监管性上来看，直连模式下参与方之间的数据互通像一个完全封闭的管道，流通的数据类型、数据敏感度等难以被外部察觉，对其进行监管的方法（之一）是将监管探针

直接放在数据方一侧。因此监管的有效性取决于探针所获数据的真实性。

（2）代理计算架构

在代理计算架构中，数据方不是计算方，数据方之间没有连接。即，数据方将数据计算功能代理给了其他节点（计算方）完成。该架构常见的方式是由一套分布式集群执行密码学协议，如一些多方安全计算框架[12],采用代理计算模式实现直接在加密后的数据上进行计算，常见的框架中通常由 2 至 4 个代理计算节点完成协同计算，其架构如图 14 所示。这种将数据和计算解耦合的架构可以实现高可扩展性：支持数据源持续不断的动态接入。

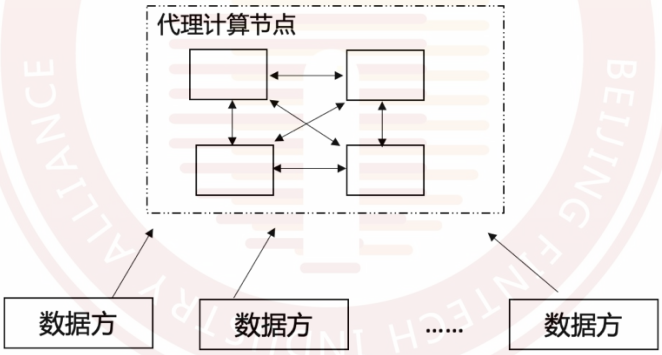

图 14 代理计算架构

可以将这类架构中分布式的代理计算节点统一视为一个“虚拟的中心计算节点”，如此则这种模式也形似某种形式的客户端-服务器架构——数据方作为客户端，向服务器

[1] Dan Bogdanov, Sven Laur, Jan Willemso. Sharemind: A Framework for Fast Privacy-Preserving Computations. ESORICS 2008: Computer Security - ESORICS 2008.pp 192-206.

[2] Yi Li,Yitao Duan,Yu Yu,Shuoyao Zhao,Wei Xu. PrivPy: Enabling Scalable and General Privacy-Preserving Machine Learning.KDD,2019.

提供输入数据，而虚拟的中心节点作为服务器，完成计算任务。但不同的是，“虚拟的中心计算节点”在计算时不提供数据。

代理计算架构适用于基础设施或平台建设，为大量数据方提供接入条件，具备规模化经济效益。

从可监管性上来看，代理计算架构将算力独立出来，监管方可借助这种独立于数据方（往往是利益方）的“虚拟的中心计算节点”，配套相关的技术手段直接实施监管职能。

在现实世界中当然存在以上两种架构的混合模式，也就是说，部分数据方提供了算力，但同时又需要其他计算方来辅助计算；或者在执行某些计算任务时是直连模式，当执行另外的任务时又是代理计算架构。这里不再一一赘述。

（3）架构差异性造成的影响

首先，两种架构的差异会给架构间的互联互通带来困难。需要进一步明确不同架构平台（产品）间的互联互通接口，求同存异，统一互通方式。

其次，两种计算架构并存会在短期内给市场应用造成一定困惑。市场应用方（如金融机构）需要针对不同的应用场景综合考量可扩展性、可监管性、成本、长期规划等各方面因素，从而选择最匹配的架构类型。

隐私计算是解决跨机构数据联合计算和联合建模的重要技术手段，在金融、电信、医疗、政务、工业互联网、智慧城市等方面需求迫切。目前技术厂商已开发出一些较为成型的算法和平台产品，主流的技术路线包括联邦学习、多方

安全计算、可信执行环境等，而底层实现技术包括同态加密、混淆电路、秘密分享、不经意传输等，可实现安全的多方联合查询、联合统计、联合建模、联合预测等应用。

但目前各个厂商的隐私计算平台由于技术路线多样性，算法的不统一，具体技术实现的差异性，以及安全标准、算法接口规范、通讯协议等方面不统一，导致行业用户建设平台后，底层算法与其他合作方无法互联，不同平台所托管的数据在实际应用中无法跨平台交互，必须部署多套系统才能进行多源数据联合计算或建模，而且这些基于异构隐私计算系统的数据源也无法同时参与到同一个模型训练或联合统计的任务。这样势必会增加隐私计算技术使用方的平台建设复杂度和建设成本，而且把“数据孤岛”问题转化成“技术孤岛”问题。隐私计算跨平台互联互通成为实际落地应用的新挑战。

隐私计算跨平台互联互通问题，一方面是由于算法的多样性造成，实现某一特定的应用功能，可采用不同的算法。举例来说，单单实现隐私集合求交（PSI）应用功能，就可以采用不同的技术路线和算法，包括基于公钥体系的 PSI、基于不经意传输的PSI、基于同态加密的PSI、基于电路的PSI、基于可信执行环境的PSI 等。在具体技术实现中，可进一步采用不同的算法，例如在公钥体系的PSI 中，可基于 RSA 的盲签名协议，或基于椭圆曲线协议、基于布隆过滤器协议等。不同厂商开发的隐私计算平台往往根据自身的技术优势来采用不同的算法协议来实现，这就导致了平台间算法协议不

一致，从而无法共同来完成一个跨异构平台的联合安全计算任务。

另外一方面，隐私计算跨平台互联互通问题，在于目前缺乏统一的技术规范，除了算法协议上的差异，在平台架构、接口、报文、安全标准等方面，各个厂商之间都是相互割裂、独立开发，造成即使是节点、数据资源等基础层面，目前都无法直接互联。

(二) 隐私计算的计算效率有待提高

隐私计算的底层技术虽然各异，但性能低下是它们的统一特征。以 3 万行、100 列的结构化样本为例，非隐私版本的建模，一般几秒就可以迭代一轮，但在隐私计算技术领域，通常需要几分钟甚至几小时。造成这个局面的原因多样，以下三个方面展开讨论。

1. 物理世界的制约

隐私计算的参与方通常分布在地理上的各端，需要通过公网通信，即使有专线的情况下，带宽一般都难以突破 1000Mbps。在这样的网络条件下，延时和带宽都大大制约隐私计算的性能。以某开源秘密分享计算为例，在对 100 万量级数据进行若干次简单的乘法、比较操作，需要耗费几分钟，在这样的计算性能情况下，进行稍复杂的隐私建模任务，耗时是以小时计的。

目前市面上没有专门的隐私计算设备，无论 CPU、GPU 都没有对隐私计算进行专门的定制优化。尤其是同态加密的技

术方案，设计专用的加解密、同态运算的芯片，是大有想象和实践空间的。

2. 底层技术原理的制约

为了保护隐私，需要付出额外的代价。这个代价反映在不同技术路线上的表现形式不同。

（1）在以混淆电路为蓝底的技术路线下，有以下三个制约性能的因素。

第一是复杂的电路，一个业务的算术计算逻辑，可能会编译出来规模大而庞杂的电路。

第二是混淆电路的大通信量，在目前的混淆电路优化技术中，一个与门的混淆表需要 2 个密文，32 字节，电路中大量与门混淆表的通信可能会受限于网络带宽，影响整体性能。

第三是加解密，混淆电路路线的实现中，一个元电路，需要对不同布尔值的输入、输出进行加密、解密操作。

第四是不经意传输的使用，混淆电路执行方（Evaluator）需要使用不经意传输来获得其输入线的标签，如果混淆电路执行方有大量输入线，就需要使用大量不经意传输，构建不经意传输也需要占用网络带宽。

（2）以秘密分享为蓝底的技术路线，不管是基于布尔电路、算术电路或者混合电路的实现方案，其加法本地计算，乘法及其他计算需要网络通信，均可能受限于网络带宽。

（3）以同态加密为蓝底的技术路线下，加解密和密文运算均制约计算性能。

第一，以 Paillier 为代表的半同态方案，加解密需要进大整数模幂计算，是耗时操作;

第二，全同态的方案，多项式相乘、Bootstrapping、模转换、重线性化均为复杂运算;

第三，对 Sigmoid 等数学函数进行高精度和高效的模拟计算也是很大的挑战。

3. 架构的制约

受限于技术路线或者发展水平，分布式隐私计算尚在起步阶段，较多的分布式计算的既有经验无法迁移到分布式隐私计算领域。这个现状使得隐私计算在算力上无法快捷地扩展。

4. 其他制约

各参与者计算环境和算力、网络环境和带宽、数据规模和质量不对等，协作计算性能和稳定性保障困难。

(三) 应用部署的硬件成本和人力成本较高

1. 技术复杂性带来的共识成本

隐私计算技术本身包含很多密码学知识，技术理论由学术界传导到技术公司转化为产品，再由技术公司传导到应用方转化为金融业务系统（的一部分），技术传导带来的共识偏差很难避免。并且隐私计算包括多种技术类型，技术之间存在嵌套、层次关系，而主流产品一般包括多类技术以期达到最优性能，因此，让最终的应用方理解技术原理并选择最适配自身应用场景的技术或产品，需要相当的人力成本。

2. 密文计算性能带来的算力成本

对于同一个计算需求，目前基于密文的计算量要比基于明文的计算量高一个或几个数量级（具体量级和计算类型、密文计算方案有关）。因此，密文计算一般需要更高的算力支持，除了更多的硬件数量，有时也需要专用于密文计算的硬件芯片。

3. 多方应用带来的部署调试成本

隐私计算的一个重要目的是通过数据有序流通实现多方数据融合，以期望最大化释放数据价值。因此，隐私计算在应用时就会涉及多个实体组织，在调试环节需要协调各方，使各方在人力投入、网络开通、机器使用等各方面能够保持时间上的一致性。

4. 未来异构产品互联互通带来的附加成本

目前隐私计算领域各科技公司的产品架构、技术类型都有一定差异，即使同一家公司在两个不同应用中部署的产品技术类型也会不同。当前为迅速占领市场，很多科技公司和金融机构往往采用最便捷的模式部署产品。在缺少统一规范和互联互通的约束下，这必将给未来建立行业级数据流通基础设施乃至全国数据流通网增加额外升级成本或改造成本。

(四) 国密暂不支持同态加密

随着金融安全上升到国家安全高度，近年来国家有关机关和监管机构站在国家安全和长远战略的高度提出了推动国密算法应用实施、加强行业安全可控的要求。摆脱对国外

技术和产品的过度依赖，建设行业网络安全环境，增强我国行业信息系统的“安全可控”能力显得尤为必要和迫切。

2010 年底，国家密码管理局公布了我国自主研制的“椭圆曲线公钥密码算法”。为保障重要经济系统密码应用安全，国家密码管理局于 2011 年发布了《关于做好公钥密码算法升级工作的通知》，要求“自 2011 年 3 月 1 日起，在建和拟建公钥密码基础设施电子认证系统和密钥管理系统应使用国密算法。自 2011 年 7 月 1 日起，投入运行并使用公钥密码的信息系统，应使用国密算法。”

当前行业联邦学习主要面临的问题是，现有的联邦计算在实现过程中依赖同态加密算法，而国密算法中并不包含同态加密，公私钥体系也不具有同态性。未来如何对联邦学习算法进行改造并与国密算法统一从而实现行业规范，保障互联网金融市场的安全仍然是行业中需要深入研究的问题。

(五) 参与者预期的风险

1. 隐私计算技术安全性评估不足带来的数据泄露风险

隐私计算技术尚且处于前期发展阶段，其依赖的底层原理多涉及前沿的密码学技术以及可信硬件技术。仅仅是其相关的密码协议就有同态加密、混淆电路、不经意传输、秘密分享等几种。不同的隐私计算技术方案所采用的底层原理不尽相同，其安全性本身也有高低之分，而金融行业的特殊性决定了其对数据安全有着极高的要求。

作为隐私计算业务发起方和使用方（如金融机构），对相关技术的理解和认知较为缺乏，不够深入，故难以结合自身情况对隐私计算的数据安全性做出有效评估。其次，隐私计算技术的不成熟和相关产业的不完善，导致其在金融应用落地场景数量较少，整体市场缺乏对隐私计算技术安全性的有效验证，作为参与方，缺少可参照的案例，对数据泄露的风险无法做出准确判断。

作为隐私计算技术提供方，为业务发起方和数据提供方提供数据、算法选择和建模等服务。在与多方数据融合建模过程中会对数据进行加密处理，这使得整个隐私计算流程对所有人是一个黑盒，并具有不可衡量与不可检测的特性，导致发起方和数据提供方担心隐私计算在执行数据融合的过程中，是否对其数据进行了完全保密，以及结果是否真的仅对其自己可见，这些问题使得业务相关方对隐私计算技术的接受程度较低。

2. 异构平台的互联互通造成的数据泄露风险

隐私计算的底层原理复杂多样，当前市场上的隐私计算产品通常采用了不同的技术方案。为了能使数据在不同隐私计算产品间流转，最大化利用数据要素价值，异构平台的互联互通必将成为隐私计算发展的趋势，事实上，确实有机构已经投入异构平台互联互通方案的研发中。异构平台互联互通的风险主要有两个原因，一是市场缺乏统一的异构平台互联互通协议标准，因此参与方缺少对异构平台互联互通的数据安全评级标准和实施方案。二是互联互通的两个平台中涉

及多个隐私计算参与方，每个参与方对于数据共享的范围和权限需要做出控制，目前难以评估互联互通方案是否能够保证数据在各参与方的规定范围内进行流转。

3. 参与方未有效或违规使用隐私计算技术

数据提供方在参与数据融合应用过程中，可能会存在自身数据在名义上通过隐私计算技术进行流通，而实际上仍然以明文形式共享，即部署了隐私计算功能但没有真正使用。同时，由于隐私计算涉及多方参与，即使金融机构自身合规使用隐私计算技术，也很难保证其他参与方不违规或者违反协议进行计算（以套取其他机构隐私数据）。例如，推理攻击，即传输到中心服务器的中间结果有可能被恶意的中心服务器进行反推导计算，从而推理出各参与方的隐私信息；投毒攻击，恶意的参与方可能会将被篡改的数据或权重发送给服务器，从而影响全局模型。这需要技术提供方和使用方之间对技术能够达成的目标和前提有清晰的认识，并选择合适的技术类型。

4. 隐私计算高复杂度和高成本将带来投资风险

部分隐私计算路线所采用的技术由于其加密机理复杂、交互次数多，当流通的数据量较大、结构较为复杂、参与方过多时，需要更多的硬件数量，有时也需要专用于密文计算的硬件芯片，增加了实现成本，并且实时计算的效率也会受到相应影响；此外，目前大部分企业的数据规范性和数据质量可能难以支撑隐私计算，由于其算法敏感度较高，因此对参与方的数据规范性和数据质量要求也较高。

因此隐私计算的算法复杂、通讯数据量大、时效性低、效率低、需拥有可承载大数据量的算力，导致参与方前期建设和沟通成本较高，在对预期收益不明确的情况下，需要承担相关投资风险，将阻碍参与方落地应用隐私计算技术。

5. 隐私计算数据权责难以界定

在以数据流转为“新常态”的场景中，数据使用场景更加开放，业务生态更加复杂，数据处理的角色更多元，系统、业务、组织边界更模糊，数据生产、流动、处理等过程更加丰富。一方面，当数据生产、采集、存储、分析、使用等环节闭环运作时，责任主体将变得不清晰，责任边界将变得模糊，数据的处理活动将变得难以控制。另一方面，参与方在数据使用场景中存在越权的风险，参与方数据授权后，无法有效监控真实的使用场景，无法防止数据被滥用。当数据泄露后，无法有效追责。

因此，应以细粒度权限、脱敏加密、分级分类、安全审计、行为追溯等技术为手段，全面防控数据活动（如数据收集、传输、存储、处理、共享、开放、销毁等）安全风险。

(六) 参与者面临的困境

1. 难以获得完整的数据授权链条

隐私计算应用应确保数据协同使用过程中授权链条的完整性。根据《中华人民共和国网络安全法》第四十一条及《中华人民共和国民法典》第一千零三十五条规定，“收集、使用个人信息应当公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。”《个人金融

信息保护技术规范》规定了“金融业机构应遵循合法、正当、必要的原则，向个人金融信息主体明示收集与使用个人金融信息的目的、方式、范围和规则等，获得个人金融信息主体的授权同意”。由此可见，从个人信息的收集、使用到金融机构和其他参与方的协同使用均需获得授权。从技术上来说，隐私计算给原来不能融合的数据提供了联合计算的机会，但在业务应用的过程中，仍然需要确保用户授权链条的完整性，即用户既需要授权给金融机构查询其外部数据的权限，也需要授权给数据生产方在不泄露隐私的前提下，应用和分享其数据的权利。

2. 现有法律未对隐私计算地位进行明确定位

《中华人民共和国网络安全法》中规定“未经被收集者同意，网络运营者不得向他人提供个人信息”，同时设置了“经过处理无法识别特定个人且不能复原”的例外条款。隐私计算仅仅避免了原始数据转移的过程，但完成了基于多方数据的计算，所以仍然涉及个人信息的提供和使用。目前，将个人信息用于隐私计算，以及如何在符合个人信息保护的要求下使用隐私计算技术，现有法律法规及相关标准等并无明确界定。

金融机构含有大量的个人金融信息。首先，企业在使用隐私计算技术进行数据融合应用时若涉及这些个人信息，目前尚没有明确的正向依据来确定其是否符合《个人信息保护法》。其次，我国尚无关于应用隐私计算技术进行数据交易

的政策法规，金融机构即便具备隐私计算技术能力，依旧不敢、不愿应用隐私计算技术交易自身数据。

3. 数据流通市场不成熟，数据价值难以衡量

隐私计算作为一种支撑数据流通的技术，其大规模应用的前提是参与方具有数据交易的意向，而数据作为一种新型资产，其价值是促成数据交易的关键因素之一。但是，当前市场正处于快速发展的早期阶段，明确的数据资产定价方法、合理的激励机制、利益分配机制等模式尚未落地，难以支撑商业化数据流通和交易市场。而不成熟的交易市场，会导致隐私计算参与方难以估计数据交易、数据流通带来的收益，大大削弱参与方的积极性。

因此奖励机制是必要的，在理想状态中，每个参与方都应该有相似的贡献度，然而现实情况中，有些机构拥有优质的数据和算力，而有些机构数据量和算力稳定性都有可能有所欠缺，然而在经典联邦学习架构中，所有的参与方都有权利拿到最终的全局模型，所以如何定义奖励机制也是需要考虑到的现实问题。

4. 不同隐私计算平台间难以互联互通

随着隐私计算技术的发展，越来越多的技术服务厂商研发了自己的隐私计算平台，或服务于自有生态，或服务于金融机构，或服务于政府机构，将原本独立存在的数据孤岛连接了起来，实现了“数据的可用而不可见”。但是因为不同的隐私计算平台基于自有知识产权的算法原理和系统设计实现，且目前闭源的平台居多，平台之间原生无法完成信息

的交互，将“数据孤岛”变成了“计算群岛”。金融机构作为数据的应用机构，往往面对着和不同的数据提供机构合作时，需要部署不同隐私计算平台的情况，存在着严重的系统建设和运营成本浪费，因此“互联互通”成了隐私计算应用的参与者面临的新困境。例如，当前隐私计算平台无法兼容老模型的风险，联合建模的模型文件无统一格式规范，当金融机构替换第三方隐私计算平台后，新平台无法快速兼容老模型，同时还要承担模型迭代、升级、推理的职责。

隐私计算平台的互联互通指基于不同设计原理和功能实现的隐私计算平台之间协同完成某一项隐私计算任务的能力，具体指不同隐私计算平台间通过统一规范的系统接口、算法协议、操作流程等实现数据资源和计算能力的交互与协同，解决使用不同隐私计算平台的数据提供方和数据应用方之间的协作问题，实现资源与价值的跨平台互联互通。

隐私计算跨平台互联互通以求同存异为原则，关注跨平台协同能力基础环节的标准化，也保留了个性化和可扩展性。在经过业务驱动的厂商之间的一对一对接，厂商自己定义自有的互通规范的两个发展阶段之后，目前金融行业的标准制定组织——北京金融科技产业联盟也在组织金融行业互联互通标准的起草和撰写，隐私计算参与者之间也在标准框架的指导下进行积极的互通落地实现，解决参与者之间互通的难题，共同推动隐私计算行业的良性发展。

5. 隐私计算非万能，需与其他技术融合

隐私计算可以很好地解决用户业务数据流通中的安全合规问题，但无法解决所有问题。当隐私计算落地应用至某些用户所需的业务场景时，面临如何衡量与检测、如何基于加密数据进行智能化处理、如何快速部署等一系列问题，如果这些问题不得到解决，会让业务需求方难以选择使用隐私计算技术。

因此，可以融合区块链、容器云和人工智能等多种技术，利用区块链技术可追随、可审计的特性、人工智能技术可以提供智能的数据挖掘分析能力和容器云技术具备快速部署和便于开发的优势，为用户提供了可信、安全、隐私、公平与高性能的数据互联解决方案，支持用户与多个外部机构进行安全便捷的数据流通与生态协作，解决了用户在使用隐私计算技术中面临的一系列问题，保证隐私计算技术能够更好地服务用户的业务。

6. 技术安全性缺乏统一的行业共识

隐私计算是保护数据隐私的同时实现数据价值的挖掘，即实现数据内容的安全性和数据价值的开放性的统一。目前，隐私计算的三种主流技术路线：多方安全计算技术、联邦学习技术、可信执行环境技术，实现安全性的核心思路都是基于数据内容的机密性保护，从而减少数据的暴露面。然而，三种主流技术路线保障安全性的理论基础、架构思路、实现框架均存在较大差异，必然导致数据隐私安全性存在高低程度的不同。

多方安全计算技术本身仍然存在不同的算法或者协议设计方案，不同的多方安全计算方案的安全性采用不诚实门限、统计安全参数、计算安全参数等安全参数进行度量。

联邦学习的部分基础算子通过密码学方式实现，能够采用可证明安全性理论度量安全性。联邦学习的更多高级算子则仍然采用分布式人工智能方式实现，仍然面临人工智能模型的数据投毒、模型投毒、对抗攻击甚至导致隐私泄露问题。如何衡量联邦学习技术的安全性仍有待进一步的研究。

目前，支持可信执行环境的主芯片被暴出安全漏洞的事件仍然多发频发。同时，可信执行环境是一种具有可信第三方的技术路线，其可信第三方主要是支持可信执行环境的主芯片硬件厂商或者硬件平台厂商，在我国自主可控能力尚且薄弱的客观背景下，可信第三方的安全可信性必将大打折扣。如何客观公正评价可信执行环境技术的安全性仍然是仁者见仁、智者见智。

安全性是应用隐私计算技术的根本出发点，也是针对不同的场景需求选用隐私计算技术和产品的核心权衡点之一。然而，目前仍然缺乏对隐私计算技术安全性的统一认识，即缺乏统一的安全性量化度量框架或者统一的安全性定性分级框架，影响行业应用隐私计算技术的信心，进而影响上层制度体系对隐私计算技术合规性的论定。

隐私计算可应用于各类场景，但是业内对于不同隐私计算技术提供的数据隐私保护维度和可能面临的安全风险和威胁缺乏统一的认识。与其他信息安全类产品和系统类似，

隐私计算产品和系统在设计、开发、部署、使用中若缺乏相关安全要求认知，会造成严重安全风险，甚至引发数据泄露事故。

三、 隐私计算技术金融应用风险与安全分析

(一) 金融应用合规性亟待提高

目前，各国对于数据流通、协作等方面的立法正逐步完善。2018 年欧盟委员会《通用数据保护条例》、2020 年美国《加州消费者隐私法案》明确了个人数据可应用的范围及应用中用户的知悉权；在发展中国家，印度、巴西等国也已为个人信息保护立法；我国也相继出台了《民法典》《网络安全法》《数据安全法》《个人信息保护法》等法律法规，对个人信息传输和使用过程中的安全问题都提出了明确的要求。由此可见，数据安全、个人隐私保护的法治化已迈向全新阶段。

金融领域在个人信息保护的立法和实践已实行多年。在《中华人民共和国中国人民银行法》《中华人民共和国商业银行法》《中华人民共和国证券法》《中华人民共和国保险法》中，均明确提出了保护个人金融信息的要求。金融标准化技术委员会也于 2020 年 2 月发布了《个人金融信息保护技术规范》，对个人金融信息全生命周期提出了安全防护要求，包括事先告知金融数据主体共享或转让其金融数据的目的，并已征得主体同意；对数据进行去标识化处理，且确保数据接收方无法复原并重新识别数据主体。同时，根据金融产品或服务的需要，将收集的个人金融信息委托给第三方机构处理时，对第三方机构等受委托者也提出了明确的要求；对委托行为进行个人金融信息安全影响评估，并确保受委托

者具备足够的数据安全能力，且可以提供足够的安全保护措施。

综上所述，个人信息数据的共享、开放、交易，应遵循数据“不可还原”“不可重标识”的基本原则；在已授权数据或无需授权数据的使用合规性方面，相关的法律法规及技术规范明确要求了数据协作过程涉及的各个环节中，各参与方需要承担相应的职责。

(二) 对应的政策与标准仍需完善

1. 政策及标准的必要性

隐私计算作为一种涉及安全的新兴技术，在金融行业的应用需要相应政策和标准来确保应用的合规性与安全性，同时政策及标准的出台也可在一定程度上加快相关产品落地与推广。隐私计算相关政策的出台能够提升用户及消费者对隐私计算的信任度和接受度，引导机构合理应用隐私计算技术，促进隐私计算在金融行业健康有序发展。隐私计算作为一种全新的金融科技新技术，传统技术规范不再适用于隐私计算。为保证隐私计算金融应用的有序推进、健康发展和安全合规，应制定相应的标准规范。相关标准的出台能对不同公司、不同路线的隐私计算产品起到规范及标准化作用，解决技术应用合规性的问题，在最大程度上确保其安全性及可用性。此外，标准的出台也能够在大大降低监管方的工作量，在加快审核流程的同时提高监管的质量。

2. 政策及标准现状

在政策方面，早在 2016 年底，工信部就在《大数据产业发展规划（2016-2020 年）》中提出要“加强大数据安全技术产品研发，要突破差分隐私技术、多方安全计算、数据流动监控与溯源等关键技术”。到了 2019 年，工信部发布的《工业大数据发展指导意见（征求意见稿）》中指出为激发工业大数据市场活力应当指导建设国家工业互联网大数据中心，鼓励企业、研究机构等主体积极参与区块链、多方安全计算等数据流通关键技术攻关和测试验证，降低工业大数据流通的风险。而到了近两年，随着对数据隐私问题的关注增加，越来越多涉及隐私计算的地方性政策也相继出台。比如山东省政府出台的《山东省推进工业大数据发展的实施方案（2020-2022 年）》中指出“加强工业数据安全产品研发。推动重点高校、科研机构和骨干企业联合开展多方计算、差分隐私、同态加密等安全技术攻关，提升数据安全防护能力。建立安全可信的数据安全产品体系，增强数据安全防护能力。到 2022 年，打造一批具有全国影响力的优秀产品与解决方案。”

可以看到，最早随着大数据产业的发展，数据的安全性逐渐被人所重视，出台的政策中也会提及隐私计算等技术。而到了近两年，可以看到更多的政策开始着重强调隐私计算技术，这也说明隐私计算技术逐渐成为行业内的潮流和热门方向。

而政策作为技术发展的风向标往往要起到未雨绸缪的作用，故而在某项技术大规模落地之前就往往已经有大量的相关政策。而标准则不然，对于某项新技术而言，其发展初期往往都还处于技术探索阶段，难以制定较为统一规范的标准来对其进行约束，只有当技术发展到可以商业化落地的阶段，标准的制定才具有意义。到了 2020 年，随着疫情的到来，数字化进程明显加快，银行等金融机构迫切地需要进行数字化转型，隐私计算也来到了开始商业化的阶段。在这种关键的节点上，标准的制定就至关重要。

2020 年 11 月 24 日，中国人民银行发布了《多方安全计算金融应用技术规范》，这也是金融领域有关隐私计算的第一个标准，为隐私计算开始大规模落地部署打响了第一枪。

3. 加紧标准制定的紧迫性

尽管我国已经注意到了隐私计算在金融市场的巨大潜力和发展前景，但在标准制定方面仍有所不足。目前，仅有涉及多方安全计算的一个标准出台，在联邦学习、同态加密等方面都没有相关的统一标准。这也为这些产品的落地带来了困难。以联邦学习为例，国内已有多家厂商推出了相关产品，但标准的缺失使得客户对厂商产品的安全性存在质疑，推广面临困难。另一方面，由于这些厂商之间的技术路线互有差异，在缺少标准指引的情况下，厂商与厂商之间的产品也很难做到互通，技术孤岛的问题也会再度显现。对于隐私计算这种新兴的技术而言，一旦开始进入商业化场景其发展

速度往往是很迅速的，而相关标准的缺失不应成为制约其快速发展的阻碍，及时跟进相关标准就显得尤为重要。

(三) 传统监管手段难以有效实施监管

随着大数据、云计算、人工智能以及区块链等新兴技术的飞速发展，金融科技（FinTech）已经成为金融业发展的新标志。金融科技的发展大大促进了金融创新，但也带来了诸如滥用数据资源与侵犯个人隐私等网络安全问题。如何监管这些新的金融产品和模式，实现金融科技业务和产品合规创新，已成为政府、监管部门、金融机构以及科技金融公司各方关注的焦点问题。

一方面，由于金融科技的科技创新性，传统的监管措施在防范金融科技的潜在风险方面显得捉襟见肘，将高科技应用于监管领域的“监管科技”应运而生，其本质是采用技术手段，在被监管机构与监管机构之间建立一个可信、可持续与可执行的“监管协议和合规性评估、评价和评审机制”。金融行业中全面的监管，对于保护投资者利益、维护市场公平尤为重要，而搭建统一的隐私计算协同平台能够为监管提供新的可能性，同时又为市场带来前所未有的细粒度隐私保护。

另一方面，隐私计算技术在金融领域的应用给监管科技带来新的挑战。隐私计算技术本身是中性的，但是在应用时可能存在风险，特别是当使用这种技术能够给相关参与方带来可观的商业利益时，这种风险会被加大，比如相关利益方可能以隐私计算为幌子非法进行个人金融信息买卖等。应对

传统的数据应用技术，通常的监管方式（之一）是直接将应用方的数据提走，通过对数据审计、核验发现其中的违规现象，或者在应用方的业务流中尝试增加监管探针，监测其数据使用情况。而对隐私计算技术应用进行监管的难点在于，隐私计算往往涉及多参与方共同计算，需要对多方同时监管，在时间一致性、数据真实性上有更高要求:

第一，需要对多个参与方的数据在时间上找出关联的内容，进行比对、核验;

第二，需要防止利益方之间相互串谋制造相互关联的假数据。

为应对这些难点问题，需要监管科技在顶层设计（如监管规则数字化）时就提前进行考虑，并建议金融机构使用监管友好型的隐私计算产品或技术架构，并辅助使用探针、存证、审计等技术手段。

(四) 较难验证或检测数据可用不可见

各个参与方能够以数据不出本地的形式分享数据的“价值”“知识”“信息”而不是原始数据，做到数据“可用不可见”，从而既让潜在的数据价值被挖掘释放，又不损害数据所有者的权益和隐私权。由此，各方才有动力和能力通过数据流通协作来进行深度合作，用户也才能最大程度减少将个人数据放在各种互联网平台上的隐私泄露忧虑，有助于促进数据经济深度发展演化。

技术服务提供商在算法建模或计算过程中，一般会用较为专业的检测手段来衡量一个模型的好坏，如测试集的准确

率与召回率等。但是技术服务商与其客户之间存在技术鸿沟，也即仅凭检测指标可能无法说服客户信任相关产品的“数据可用不可见”特性，这就要求技术服务商可以对规则、模型进行解释。但不是所有的模型都是规则模型，一些黑盒模型（比如神经网络）有着更高的准确率，但是无法给出具体的规则，无法让普通人理解和信任模型的预测结果。尤其当模型应用到银行业等金融领域时，透明度、可解释性、规则简单是隐私计算模型是否值得信任的重要考核标准。

尽管隐私计算技术声称能保护数据，使其“可用不可见”，但是不同的技术服务提供商所提供产品的底层技术可能不尽相同，由于涉及金融机构的机密数据，参与各方若要完全信任隐私计算相关系统，代码开源可能是较好的获取信任的方法。特别是当安全可控成为我国当前信息技术创新主旋律的背景下，代码透明的信任更加重要。但是开源产品的盈利难度较大，可能需要公司内其他产品的交叉补贴，否则盈利周期会变得更长。

(五) 参与者安全技术与管理水平存在差异

在真实的网络环境中，模型反演攻击、成员推理攻击、模型推理攻击层出不穷，参与者需要建立完善的安全管理制度，采取一定等级的安全技术措施来保证隐私计算过程的安全。

由于缺乏标准化建设指引，各金融科技企业采用的隐私计算技术各异、算法各异、数据格式和接口不统一，导致各隐私计算平台之间安全技术要求不一致，从而让不同参与者

之间在互联互通时，无法排除安全隐患。甚至同一金融机构内，由于采用不同厂商的隐私计算平台产品，也无法实现安全技术要求的完全统一，无法实现数据价值的有效融合，发挥隐私计算技术最大价值。

隐私计算多用于跨机构、跨部门的数据融合，甚至跨行业的数据流通，对参与方的安全管理一致性也提出了较高要求。部分中小机构本身科技力量较弱，自身的数据安全管理水平有欠缺，在参与隐私计算过程时，不仅难以发挥其隐私计算相关价值，还可能会影响隐私计算的可靠性和准确性。

(六) 对金融用户的隐私保护意识和措施有待加强

目前，金融业蕴藏着巨大价值的数据能够以极低的成本复制和无限使用，产生了滥用数据资源与侵犯个人隐私等网络安全问题。拥有用户数据的隐私计算参与者，可能存在忽视用户具有隐私使用知情权，以及其自身应具有的保护用户隐私的义务，从而导致各种各样数据泄露、盗用、滥用等问题案件频频发生，给人们带来了不少困扰。

隐私计算技术解决的是让数据分享流通过程中的隐私保护问题，然而，使用隐私计算的前提是数据提供方和使用方都必须征得用户同意。隐私计算的“可用不可见”并不能替代“信息主体告知同意”，隐私计算参与者应在自身的隐私政策中明确告知用户，会对其收集的信息在去标识化后用于研究、统计、分析，并为第三方合作伙伴的商业决策提供支持，尊重个人信息主体的意志。否则机构无权将数据用于联合计算。同时，隐私计算参与者应制定个人信息保护相关

制度和管理办法，定期开展自身和合作方的个人信息安全影响评估工作。

(七) 防范恶意攻击安全性仍需加强

1. 当前技术发展局限性

近年来，多方安全计算、联邦学习等理论和技术不断发展，隐私计算平台产品不断涌现，功能和性能都有明显提升。然而，目前绝大多数隐私计算平台产品所使用的底层算法和密码技术都依赖于半诚实模型（Semi-Honest Model），即假设隐私计算各参与方忠实执行隐私计算算法，不进行篡改、重放、伪造、合谋等恶意攻击。

各家隐私计算厂商使用半诚实模型隐私计算方案的原因主要是以下两点:

（1）性能原因: 相较于半诚实模型的算法框架，抵抗恶意攻击算法框架的性能低 5-10 倍，且会随着参与节点数量的增加进一步增加性能损耗，在实际场景落地中会造成较长的等待时间和较差的用户体验;

（2）理论原因: 相较于半诚实模型的算法框架，抵抗恶意攻击算法框架发展仍不成熟，除部分秘密分享和混淆电路算法存在抗恶意攻击 UC-安全性证明（Universal Composable），具备可证明安全性结论。联邦学习、可信执行环境、差分隐私等技术路线尚缺乏完备的抗恶意安全性定义和论证框架，在实际应用中难以抵抗投毒、逃逸、篡改、合谋、伪造、重放等攻击手段。

2. 抵抗恶意攻击的必要性

对于以政府机关、金融机构为代表的国有机构，数据安全管理规定更为严格，对于隐私计算的安全性和可靠性要求更高，在对外通过隐私计算进行数据融合协作过程中需要着重考虑当对方作恶时造成的不利影响，避免关系到国家利益、企业利益的重要数据或模型被攻击者掌握。虽然能够通过合作协议明确各方的权利和义务，但是仍不能从根本上解决防止恶意攻击的问题。

3. 基于区块链进行存证审计

针对当前技术现状，在不断完善抗恶意攻击算法框架的同时，一个切实可行的方法是通过区块链存证技术将隐私计算过程中的数据，包含随机数、密文、梯度等信息进行存证上链，在审计过程中通过隐私计算任务重新运行等途径与链上存证进行实时比对，进而确认各方在隐私计算过程中是否发生过篡改、投毒等行为，能够在一定程度降低各方的作恶动机，是在抗恶意算法框架成熟之前的一个备选方案。

四、 发展建议

(一) 完善相关法规与标准

建议继续完善国家的法律法规，明确如何在符合个人信息保护的要求下使用隐私计算技术，出台完善隐私计算相关标准，标准体系建议如下:

1. 隐私计算数据协同平台技术规范：包含隐私计算协同平台架构、功能模块、交互流程、安全要求等内容。

2. 隐私计算安全评估规范：包含针对隐私计算金融应用相关的技术、业务、数据和服务安全要求规范。

3. 隐私计算技术应用指南:包含应用场景、应用策略、演进路线等，适用于金融领域隐私计算应用的规划、设计、建设和维护。

4. 隐私计算平台检测认证规范：包含隐私计算平台基本能力、增强能力、安全能力、隐私保护能力、风控能力等内容。

5. 隐私计算异构平台互联互通规范：包含隐私计算异构平台技术架构、系统功能、数据交换等内容。

6. 隐私计算数据价值评估指南：包含统计各参与方调用其他参与方数据、模型、算法等相关数据指标，给出合理的数据资产定价方法、激励方法等。

7. 隐私计算数据共享合规指南：包含隐私计算应用中数据共享所应具备的技术与管理能力，以及应满足的隐私保护相关的合规要求。

8. 隐私计算的可解释性应用指南:包含可解释性概念、评估指标、评估方法、应用案例等内容。

建议下一步工作可以首先明确与制定隐私计算安全评估规范、应用指南、检测认证等规范，以初步指导金融机构应用隐私计算技术；其次逐步制定互联互通、数据价值评估、可解释性等规范，用以进一步完善隐私计算的用户体验。

(二) 开展相关评测认证

建议金融业第三方检测认证机构针对产品的技术能力、安全能力等开展统一的、公认的、权威的评测认证，为隐私计算各参与方提供行业公信力强的安全评测报告或认证证书，扫除各参与方对隐私计算平台的安全风险与问题的担忧。

若由中立的权威机构搭建了第三方平台，则该平台需要具备同时审核所有参与方数据安全水平的技术能力和对应的实施方案，各参与方在符合该平台的基本安全要求后才可以加入平台的隐私计算过程。

(三) 开展应用试点

国内目前传统的粗放型数据经济模式（明文数据买卖）仍有延续性，数据灰色交易依然存在，建议管理部门可以依据相关政策法规，进一步规范隐私计算市场的违法或违规行为，完善识别、评估、惩罚等机制和手段，引导隐私计算技术在金融领域融合应用。同时，行业组织可以开展隐私计算法律法规宣讲，以及相关的技术、数据安全、隐私保护等培训，增强参与者的合法合规意识，降低违规几率，促进市场健康发展。

金融业管理部门应鼓励金融机构以及科技公司开展隐私计算相关试点探索，充分利用联邦学习、多方安全计算等技术，快速推动并形成适合行业数据发展的路径。

(四) 建立可信媒介作为协调方

在传统的商业市场中，信任有着至关重要的作用，交易通常由参与方信任的权威机构监督执行。例如，市场监督管

理局以及消费者协会，其存在的本身就是对商品交易流程的监督和把控，以及对交易中的违法行为进行惩罚。也就是说，权威机构在商品交易的过程中起到了“可信媒介”的作用，为市场交易保驾护航，其中，市场监督管理局还对商品的质量、价格等细节均有十分详尽和标准化的管理方案。同样地，数据交易市场中，隐私计算技术的应用，是为了数据在安全的前提下进行交易和流转，实现数据要素价值化发展，因此可以在其中引入权威的第三方作为协调或管理节点。

该协调方可以具备以下能力:

第一，在多个相对平等的机构进行数据融合计算时，承担任务调度、资源管理和监管职能，也可以作为算力主要承担方协助缺乏计算能力的金融机构开展隐私计算应用，以确保隐私计算过程的完整性以及计算功能在各个金融机构上对等分配。

第二，在使用隐私计算技术进行数据融合计算应用时，核实参与者使用隐私计算技术的真实性，防止“劣币驱逐良币”现象（如有些金融机构打着隐私计算的幌子进行数据明文交易）。

第三，监管数据要素在流通环节的定价，和在交易流程环节的合规，对恶意节点或不合规行为予以惩罚，从而进一步提高交易成功率，助力数据交易市场规模化发展。

第四，该协调方需要完全中立，建议由权威机构担任该角色。

(五) 建立可信媒介作为存证方

建议建立统一的存证中心，对数据使用进行全局管控，可有效避免参与者的数据使用合规风险、数据泄露风险、未有效或违规使用隐私计算技术等风险。

该存证中心可以利用区块链的不可篡改、可审计的特性，一方面将隐私计算执行的每个步骤都同步到链上，对任务参与方可见，从而保证隐私计算任务的可信性，并起到对隐私计算技术进行衡量与检测的作用，也可以根据在多方授权下开展事后审计，增加业务方对隐私计算技术的接受程度；另一方面，存证中心可以负责存储同行业业务领域交叠的参与方提供的客户信息，仅对此参与方自身可见，同业竞争对手方不可见，保证各参与方私有客户信息的隐私性。建议由中立的权威机构担任该角色。

(六) 建立数据价格与激励机制制定方

建议设立制定数据价格与激励机制的权威平台，负责统计在该平台上各参与方调用其他参与方数据、模型、算法等相关数据指标，并明确合理的数据资产定价方法、激励机制、利益分配机制等。举例如下:

1. 建模费

当某数据使用方 A 希望使用数据提供方 B 的数据进行联合建模时，A 需向 B 缴纳建模费用。B 获得的费用与其数据对模型的贡献强度相关，下面给出一种最基础的贡献度定义。

假设 A，B 两方完成了一个联邦学习，准确率是I_f。如果 A 只使用自身数据，得到的准确率是I_A，那么定义 A 的贡献度为：

$$C_A = \frac{I_A - I_{bm}}{I_f - I_{bm}}$$

其中是I_{bm}该问题的基准准确率，相应的，B 的贡献率为 $1-C_A$。

2．预测费

在横向联邦学习中，模型训练完成后，模型需求方会在本地保持一份完整的模型，后续的预测将在本地完成，此时不涉及到模型使用费。在纵向联邦学习中，模型训练完成后，参与方只会保留一部分模型，在线预测时，依然需要各参与方和平台配合。此时模型使用费应对每笔预测，支付给其他参与方一定的费用。

(七) 探索平台间互联互通

隐私计算跨平台互联互通的目的是实现基于不同设计原理和功能的隐私计算平台间协同完成某一项隐私计算任务的能力，建议建设行业关键基础设施，实现平台间互联互通，促进行业内以及行业间的数据流通，同时增强数据安全预警和溯源能力。具体从隐私计算平台的系统架构视角由上到下，从技术落地的视角由易到难，隐私计算平台互联互通的实现方式分为如下三个层次。

1. 管理系统互联互通

指不同的隐私计算平台可以在应用层完成系统的管理功能互通，如：节点发现、资源管理、存证管理和审计等，实现在不同的平台间业务层的互联互通。可包含如下功能：

（1）节点发现

不同的隐私计算平台之间可以通过预先定义的节点发现协议进行彼此节点的互认，可以建立节点间的网络连接，确认彼此身份，并在此基础之上实现机构之间合作关系的建立、暂停和结束等完整业务流程。

（2）资源管理

不同的隐私计算平台之间通过资源管理接口的统一定义和对接，实现对金融领域数据资源的命名空间统一定义、唯一确定，为计算任务的执行完成输入数据资源的标准化定义。

（3）存证管理

根据实际应用和安全性需求，存证组件可分为行为记录存证与计算过程存证两个子组件，行为记录存证组件实现了对各方操作和行为记录存证功能，计算过程存证实现了对于联合建模计算全流程的过程数据存证。

行为记录存证：行为记录存证组件记录并存储用户登录，数据使用，数据授权，任务发起，任务配置，模型使用，计费等信息，可使用区块链等技术存储存证信息，实现行为记录的存证功能。

计算过程存证：计算过程存证组件记录并存储联合建模计算任务中的随机数，秘密分片，密文，梯度数据，模型参数等计算过程数据，可使用基于哈希的 Merkle 树等技术途径确保计算过程数据存证隐私性，可使用区块链等技术保障存证数据不可篡改。

对于不同隐私计算平台间互联互通的技术方案，有必要确保存证系统互联互通，使得跨平台隐私计算任务全程留痕，便于监管审计，更好规范各个参与者的行为，如图 15 所示：

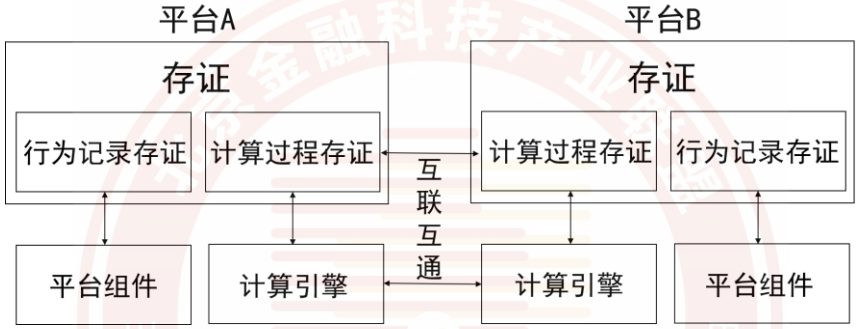

图 15 存证管理架构示意图

（4）审计

根据安全性和审计需求，审计组件可分为行为记录审计和计算过程审计，分别对应行为记录存证和计算过程存证组件，能够实现审计方对于用户操作行为的审计，以及对于联合建模计算过程的审计功能。

行为记录审计：行为记录审计组件对于已经完成的平台操作记录进行审计，用于查看相关用户的操作行为是否合规。

计算过程审计：计算过程审计组件对于联合建模计算任务进行审计，通过调用计算引擎对原始数据进行计算任务重现，并与计算过程存证组件的数据存整交互和匹配，进而确认计算任务的完成过程中是否存在异常或恶意行为。

对于不同隐私计算平台间互联互通的技术方案，有必要确保审计功能互联互通，使得跨平台隐私计算任务全程可溯源可复现，便于监管审计，更好规范各个参与者的行为，如图 16 所示:

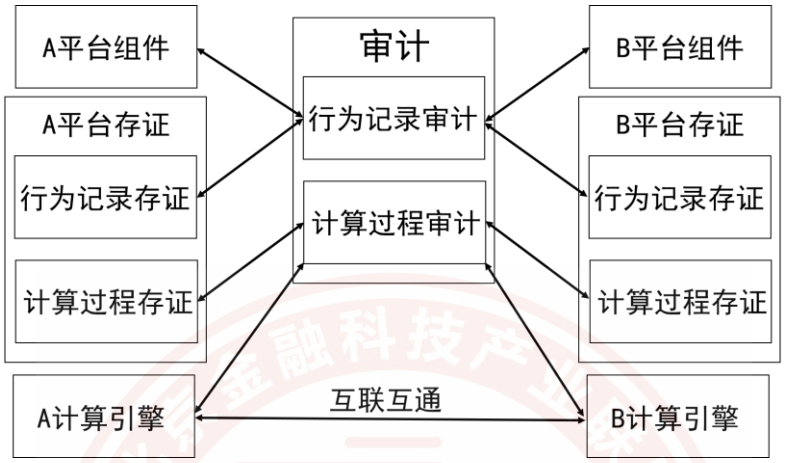

图 16 审计系统示意图

2. 算法协议互联互通

不同的隐私计算平台将“核心算法”作为一个黑盒，对算法本身的设计不做定义，而对算法的基本信息、输入、输出规范定义，使算法可以通过“算法插件”的形式由不同的技术服务厂商发布，在满足安全认证和授权要求的前提下，插件化集成到对方的隐私计算平台，进行同构化的算法插件之间的互联互通。

算法协议互通具体指约定不同隐私计算平台之间的通信规范，在此基础之上定义报文格式、参数内容等，完成后续的消息内容交互、协作指令执行等流程。统一支撑算法运行的功能组件定义包括:

（1）采用统一的通信协议: 如使用 HTTPS 进行隐私计算信令消息的同步，使用 GRPCS 进行数据内容的交互。

（2）采用统一的加密组件：使用预先约定好的高强度加密算法，使用满足安全性要求的随机数生成机制。

（3）采用统一的资源定义：使用统一的命名空间方式来定义不同数据集的标识，做到全局的唯一。

（4）采用统一的任务调度：对隐私计算任务定义统一的任务管理原语，控制任务的全生命周期运行。

（5）采用统一的模型格式：定义算法的模型封装格式，做到模型可以在不同隐私计算平台之间迁移部署，应用于批量预测和在线推理服务。

（6）采用统一的节点管理：规定统一的节点发现协议，节点认证机制，如：机构证书、机构签名等。

（7）采用统一的授权管理：制定统一的资源授权申请流程，以及授权操作类别、授权周期、授权次数等。

3. 计算原语互联互通

按照具体的计算协议，将不同隐私计算平台的算法或协议进行最小粒度的计算原语分解，实现计算原语的抽象和定义，在不同的隐私计算平台之间对计算原语进行各自的实现，在原语层实现互联互通，继而实现基于底层计算原语的中层算法实现、上层应用实现，完成平台的互联互通，如图 17 所示。

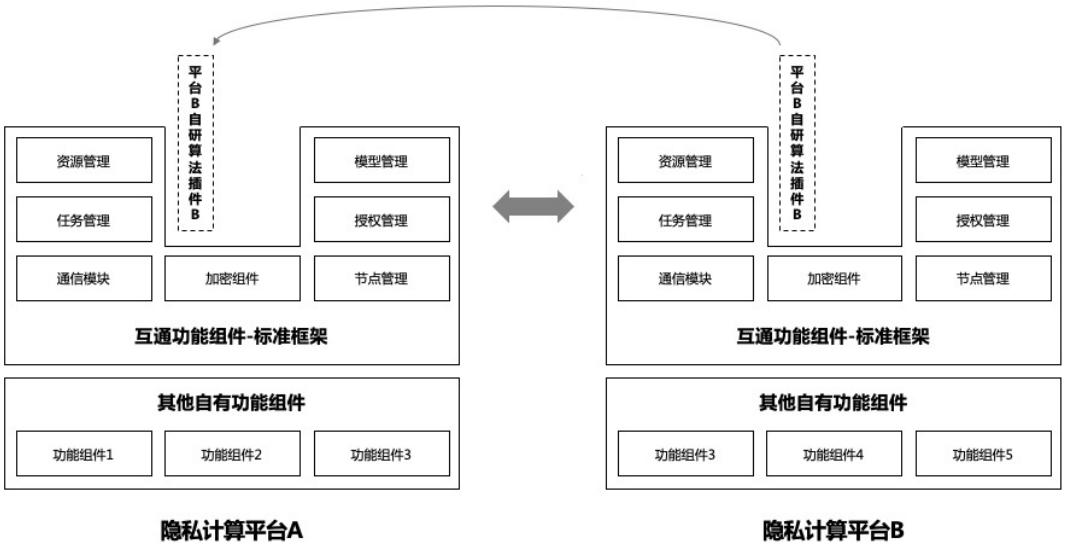

图 17 隐私计算平台间互联互通示意图

参考文献

[1] Miles N. Wernick，Yongyi Yang，Jovan G. Brankov，Grigori Yourganov，Stephen C. Strother， “Machine Learning in Medical Imaging”，IEEE Signal Processing Magazine，Vol：27，Issue 4，July 2010.
[2] Y Liu，A Huang，Y Luo，H Huang，Q Yang， “FedVision: An Online Visual Object Detection Platform Powered by Federated Learning”，Proceedings of the AAAI Conference on Artificial Intelligence, 34(08), 13172-13179.
[3] 杨强， 张宇，戴文渊，潘嘉林.《迁移学习》. 机器工业出版社，2020 年
[4] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. “Federated Machine Learning: Concept and Applications,” ACM Trans. Intell. Syst. Technol. 10, 2, Article 12 (February 2019), 19 pages.
[5] Y. Liu, Y. Kang, C. Xing, T. Chen and Q. Yang, "A Secure Federated Transfer Learning Framework," in IEEE Intelligent Systems, vol. 35, no. 4, pp. 70-82, 1 July-Aug. 2020
[6] D. Gao, Y. Liu, A. Huang, C. Ju, H. Yu and Q. Yang, "Privacy-preserving Heterogeneous Federated Transfer Learning," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 2552-2559
[7] S. Sharma, C. Xing, Y. Liu and Y. Kang, "Secure and Efficient Federated Transfer Learning," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 2569-2576
[8] H. Yang, H. He, W. Zhang and X. Cao, "FedSteg: A Federated Transfer Learning Framework for Secure Image Steganalysis," in IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2020.2996612.
[9] Y. Chen, X. Qin, J. Wang, C. Yu and W. Gao, "FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare," in IEEE Intelligent Systems, vol. 35, no. 4, pp. 83-93, 1 July-Aug. 2020, doi: 10.1109/MIS.2020.2988604.
[10] McMahan, B., Moore, E., Ramage, D., Hampson, S. & Arcas, B.A.y. "Communication-Efficient Learning of Deep Networks from Decentralized Data," Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, in PMLR 2017 54:1273-1282
[11] Yan Z, Wicaksana J, Wang Z, Yang X, Cheng KT. Variation-Aware Federated Learning with Multi-Source Decentralized Medical Image Data. IEEE J Biomed Health Inform. 2020 Nov 24;PP. doi: 10.1109/JBHI.2020.3040015. Epub ahead of print. PMID: 33232246.
[12] X. Li, Y. Gu, N. Dvornek, L. H. Staib, P. Ventola, and J. S. Duncan, “Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results,” Medical Image Analysis, vol. 65, p. 101765, Oct. 2020.
[13] Ligeng Zhu and Zhijian Liu and Song Han, “Deep Leakage from Gradients,” Advances in Neural Information Processing Systems 2019.

[14] Bo Zhao and Konda Reddy Mopuri and Hakan Bilen, “iDLG: Improved Deep Leakage from Gradients,” CoRR, arXiv:2001.02610, 2020
[15] Jonas Geiping and Hartmut Bauermeister and Hannah Dröge and Michael Moeller, “Inverting Gradients - How easy is it to break privacy in federated learning?” Advances in Neural Information Processing Systems 2020.
[16] Ong, Ding Sheng, Chee Seng Chan, Kam Woh Ng, Lixin Fan and Q. Yang. “Protecting Intellectual Property of Generative Adversarial Networks from Ambiguity Attack.” ArXiv abs/2102.04362 2021.
[17] Lixin Fan, Kam Who Ng and Chee Seng Chan, “Rethinking Deep Neural Network Ownership Verification: Embedding Passports to Defeat Ambiguity Attacks,” Advances in Neural Information Processing Systems,2019
[18] Bita Darvish Rouhani, Huili Chen, and Farinaz Koushanfar. "DeepSigns: An End-to-End Watermarking Framework for Ownership Protection of Deep Neural Networks,"" In Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '19). Association for Computing Machinery, New York, NY, USA, 485–497,2019.
[19] Shamir, Adi How to share a secret, Communications of the ACM*. **22** (11): 612–613, November 1979.
[20] Blakley, G.R. "Safeguarding Cryptographic Keys," Managing Requirements Knowledge, International Workshop on (AFIPS), 48: 313–317, 1979
[21] A. C. Yao, "Protocols for secure computations," 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Chicago, IL, USA, 1982, pp. 160-164, doi: 10.1109/SFCS.1982.38.
[22] A. C. Yao, "How to generate and exchange secrets," 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), Toronto, ON, Canada, 1986, pp. 162-167, doi: 10.1109/SFCS.1986.25.
[23] Dan Bogdanov, Sven Laur, Jan Willemso. Sharemind: A Framework for Fast Privacy-Preserving Computations. ESORICS 2008: Computer Security - ESORICS 2008.pp 192-206.
[24] Yi Li,Yitao Duan,Yu Yu,Shuoyao Zhao,Wei Xu. PrivPy: Enabling Scalable and General Privacy-Preserving Machine Learning.KDD,2019.
[25]周传鑫，孙奕，汪德刚，等. 联邦学习研究综述[J]. 网络与信息安全学报，2021，7（2）
[26]王健宗，孔令炜，黄章成，等. 联邦学习隐私保护研究进展[J]. 大数据，2021，7（3）：130-149.
[27]张艳艳. “联邦学习”及其在金融领域的应用分析[J]. 农村金融研究，2020，（12）：52-58.
[28]强锋，薛雨杉，相妹.隐私计算在金融领域的合规性分析[J]. 信息通信技术与政策，2021，47(06)：57-62.