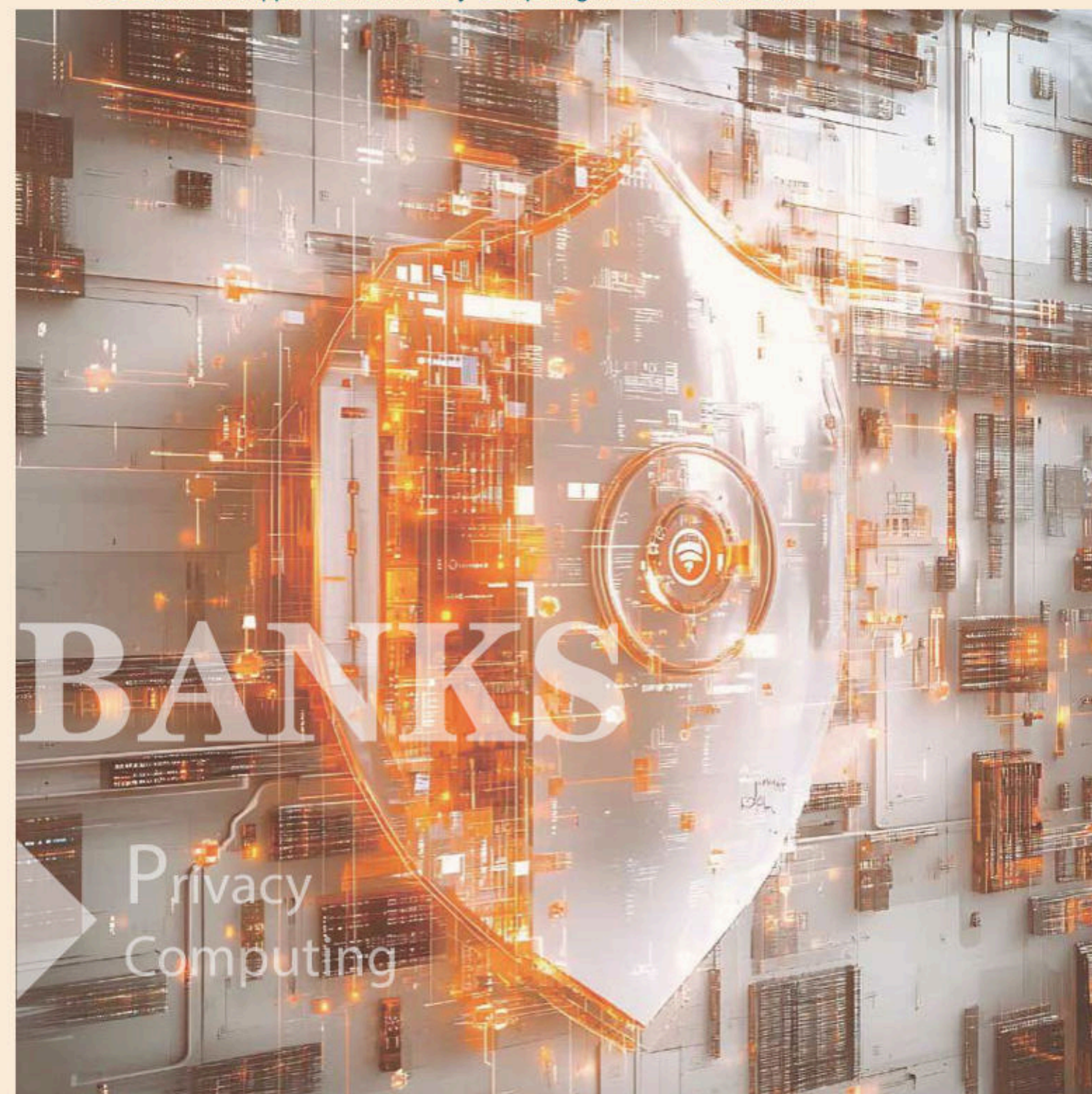


商业银行隐私计算技术 研究与应用

Research and Application of Privacy Computing in Commercial Banks



联合发布

交通银行 瞭望周刊社

撰写单位

交通银行 瞭望智库

课题组成员

课题指导

张路 刘旸辉

课题负责人

钱菲 万一 聂欧

撰写团队

谢谨 郭坚 谭培强 王光中 陈文捷 沈心艺 吴铭德 童蕙

曹嘉欣 王丽娟 王亭亭 敖祥菲 马天平 张世建 王岩岩

高翔 包红霞 何祖琳 林韵祺

外部顾问

梅建平 何宝宏 王学德 高胜

前言

我们身处数字时代，回望人类文明的演进，始终与两项核心能力的拓展相伴相生：其一是连接与协作的广度，其二是信任与保密的深度。从威尼斯银行的复式账簿催生现代金融，到今天全球金融网络中奔涌的数据洪流，我们社会的历次飞跃，都伴随着更广范围内，以更低成本建立的可靠信任关系与风险应对网络。

商业银行，作为这种信任关系的集大成者，其核心职能逐步强化：疏通社会经济血液的枢纽，通过汇聚闲散资金并将其配置给最具活力的生产部门，完成价值的跨期交换与风险的优化配置。历经农耕文明和工业文明，商业银行在数字文明时代需要面对新的挑战：

一方面，数据已成为驱动金融行业提质增效的“新石油”。精准的信贷决策、高效的欺诈识别、个性化的财富管理，无不依赖于对海量、多维数据的融合分析。传统的、局限于财务报表和集中征信的“小数据”风控模式，在瞬息万变、风险隐匿的数字经济中或有力不从心之感。连接与共享，是银行迈向智慧金融的必由之路。另一方面，数据隐私已成为捍卫公民权利和商业机密的“新边界”。随着2016年我国网络安全法、2021年我国数据安全法及个人信息保护法的相继落地，数据的收集、处理与流转被套上了隐私保护的“紧箍咒”。合规与安全，是银行生存发展不可逾越的红线。

数据价值释放对于手握海量敏感信息的商业银行而言，这一矛盾尤为突出：不推动数据融合，无异于在数字经济的竞争中“自缚手脚”；但若共享数据不合规，则不仅是巨额罚单的合规与声誉风险，更是颠覆信用基石的生存风险。那么，能否在数据“不出域”、隐私不泄露的前提下，实现其价值的“跨域”流动与融合应用？答案，正从理论走向现实，隐私计算与相关安全技术有可能成为解决问题的“金钥匙”。

隐私计算，可追溯至1982年图灵奖提出的“百万富翁问题”。历经数十年理论积淀与算法优化，在算力飞跃与数据危机的双重催化下，多方安全计算(MPC)与联邦学习(FL)、可信执行环境(TEE)的技术路径共同构成了隐私计算的主流技术路线，辅助金融机构破解数据价值与数据安全相互纠缠的“博弈谜题”。

当前，全球科技巨头与金融领军机构已纷纷押注于此。从谷歌应用联邦学习优化安卓手机输入法模型，到微众银行等机构开源联邦学习框架FATE推动技术普惠；从英特尔硬件级安全技术SGX的持续迭代，到多家国际银行联合开展基于MPC的反洗钱协作试点——隐私计算的燎原星火，已在全球主要经济体的金融、医疗、政务等领域此起彼伏。这不再是一场单纯的技术探索，更是关乎未来金融安全与高质量发展的战略制高点之一。

中国的商业银行是中国金融体系的压舱石，“服务实体经济”的根本宗旨离不开数据这一关键生产

要素的高效安全配置。

然而，正如本白皮书将深入剖析的，商业银行在拥抱隐私计算的征程中，正面临着一系列挑战：从技术路线的甄选与融合，到性能瓶颈的突破；从业务场景的价值验证，到跨机构协作模式的建立；从应对快速演进的监管要求，到复合型人才的极度匮乏。因此，系统性研究隐私计算技术，并为其在银行业的落地绘制一幅清晰的航图，不仅具有紧迫的现实意义，更具备深远的前瞻价值。这正是撰写本白皮书的核心宗旨。

本白皮书并非一份简单的技术介绍，而是一次面向银行家、监管者、科技从业者的系统性战略思考。接下来的五章中，我们将致力于：

（1）厘清脉络：在第一章引言中，我们将深度解析数据共享与隐私保护矛盾激化的时代根源，阐明隐私计算对于商业银行不仅是技术工具，更是破解发展困局的战略支点之一。

（2）技术前瞻：在第二章隐私计算发展图谱与监管态势中，我们将梳理国内外技术演进的关键里程碑与最新监管态势，帮助银行在纷繁复杂的信息中把握全局。

（3）直面挑战：在第三章商业银行隐私计算的痛点与难点中，白皮书不回避问题，坦诚地剖析在技术、业务、监管层面遇到的“硬骨头”，为后续寻找解决方案奠定基础。

（4）聚焦实践：在第四章商业银行隐私计算应用实践中，我们将呈现核心应用场景图谱，并辅以国内外先锋银行及科技企业的典型案例，从联合风控、精准营销到跨机构合规协作，展现隐私计算相关技术正在实现的创新价值。

（5）倡议与展望：在第五章，我们将从发展战略、生态建设、趋势倡议等维度，提出实施路径与战略建议。继而基于技术如何支持业务的趋势为判断，为商业银行制定自身的隐私计算战略蓝图提供前瞻性指引。

业界的共识是，隐私计算不只是生产工具，更可能孕育一种新的生产关系，它有望在数据的“拥有权”“使用权”与“收益权”之间建立均衡、可信的价值实现模式。国家数据局于2026年6月发布的《关于推进行业高质量数据集建设行动的实施方案》，明确提出以“场景牵引数据、数据驱动模型、模型赋能应用”，构建数据飞轮良性循环，这为隐私计算技术在金融领域释放数据价值、赋能人工智能创新指明了方向。对于商业银行而言，率先理解、布局并驾驭以隐私计算为代表的数应用与安全技术，不仅将会在新一轮竞争中获取优势，更是其在金融强国事业中，巩固自身作为社会重要信任枢纽这一角色的难得机遇。

本白皮书愿作一盏微光，与所有同行者一起，探寻通往未来数智银行之路！

目 录

第一章 引言

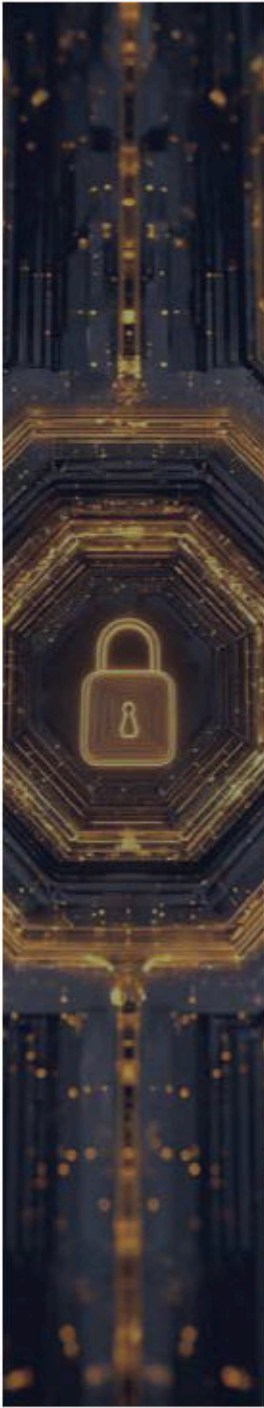
1.1 研究背景与现实意义.....	01
1.2 概念界定.....	06
1.3 研究范畴与全文框架.....	09

第二章 金融行业隐私计算发展图谱与监管态势

2.1 核心技术趋于成熟、融合应用逐步深化、产业落地有序铺陈.....	15
2.2 全球视野与中国路径：金融隐私计算的监管环境与政策驱动.....	21
2.3 从试点到基建：金融行业隐私计算应用发展图谱.....	30

第三章 商业银行隐私计算业技融合实践难点与合规要点

3.1 多重约束下，隐私计算技术面临的痛点和难点.....	34
3.2 业务与管理层合作意愿低、实施周期长、商业模式成熟度不足.....	37
3.3 监管规制与合规要点：数据匿名、流通授权、技术可控、跨境传输.....	39



第四章 商业银行隐私计算应用新近发展与实践亮点

4.1 全景探析：商业银行隐私计算核心应用场景.....	44
4.2 价值解构：隐私计算破解业务痛点的赋能机理.....	45
4.3 业界纵览：国内外隐私安全计算应用案例.....	47
4.4 实践路径：商业银行与科技企业典型应用场景案例.....	51

第五章 隐私计算技术趋势、合规路径与发展倡议

5.1 技术趋势：驶向未来的航线图.....	60
5.2 建议商业银行战略先行、合规引领、场景突破、生态协同.....	63
5.3 面向行业协同：共建可信数据空间生态.....	67

第一章 引言

1.1 研究背景与现实意义
1.2 概念界定
1.3 研究范畴与全文框架

CHAPTER 1

1.1 研究背景与现实意义

金融行业正处在数字化转型的十字路口。一端，是由数据驱动、互联互通的数字文明曙光，数据被誉为“新时代的石油”，其流动与共享蕴含着解锁经济增长、社会福祉和科技革命的无限潜能。另一端，则是矗立多年的个人隐私与商业秘密的堡垒，“个人隐私的权利观念在数字空间同样面临着多维挑战。**数据共享的澎湃浪潮与隐私保护的坚固堤坝，在交互碰撞中考验金融机构的取舍与平衡。**

正是在这种张力达到顶点的时刻，一类技术应运而生，它并非要重塑颠覆任何一方，而是旨在补充一座沟通的桥梁。**这便是隐私计算安全技术，它并非凭空出现，而是集成了千年权利思想演变、数十年互联网技术发展，以及近年来全球监管与信任危机共同作用的沉淀。**理解其兴起的背景，不仅是理解一项技术，更是理解我们如何从一个数据权利模糊的时代，走向一个有望实现“数据可用不可见”的新时代。

1.1.1 隐私意识的觉醒

1万年前的农业社会，人们生活在“熟人社会”中。个人的信息在狭小的社群内几乎是透明的，但与此同时，信息的传播范围也极其有限。隐私作为一种普遍的权利观念并未觉醒。随着城市化进程和文艺复兴、启蒙运动的推进，个体主义开始抬头。人们从封建依附关系中解放出来，对私人空间、个人事务不受干涉的权利要求日益强烈。1890年，美国律师法学家塞缪尔·沃伦（1852-1910年）和大法官路易斯·布兰代斯（1856-1941年）在《论隐私权》一文中正式提出了“隐私权”的概念，将其定义为“独处的权利”。这标志着隐私权从一种朦胧的感觉，上升为一种明确的法学诉求和文明社会的基石。

进入20世纪下半叶，尤其是互联网普及之后，互联网技术实现了从“信息匮乏”到“信息过剩”的跨越，但同时也带来两方面的悖论：一是便捷与监控的悖论。人们享受在线购物、社交网络、搜索引擎带来的便利，其代价却是个人偏好、社交关系、行为轨迹被服务商持续地、大规模地记录。二是免费与商品的悖论。我们使用“免费”的数字服务，但“如果你没有付费，那么你就是商品。”我们的注意力和个人数据似乎已被动成为科技公司谋利的资产。

过去，人们努力划定的公私边界，在数字世界中有的将变得模糊。物理世界的“墙”无法阻挡数据的“光”，人们仿佛置身于一个全透明的数字圆形罩笼，而看守者却无处不在又难以名状。这种权利被侵蚀的焦虑，是隐私保护的出发点。

1.1.2 数据洪流与信任危机

当前，全球共识已经形成，我们正处于数字时代，数据是数字经济时代的“石油”，数据已经成为关键生产要素。

数据的价值在于驱动创新与效率提升。首先是驱动创新，人工智能，特别是机器学习，其性能高度依赖于海量、高质量的数据。单一机构的数据是孤岛，只有跨机构、跨行业的数据融合，才能训练出更精准的风控模型、医疗影像分析模型或智能推荐系统。其次是效率提升，在供应链金融、精准营销、联合反欺诈等领域，数据共享能带来显著的效率提升和成本节约。对于商业银行而言，在不暴露各自客户隐私的前提下，与同业或电商平台联合风险识别，具有巨大的商业价值。

与数据驱动经济并行的，是频频拉响的数据警报，数据安全事件频发，造成信任崩塌。雅虎用户信息泄露、Facebook剑桥分析事件、万豪酒店数据泄露……这些轰动性事件警示我们：粗放的数据共享模式如同在沙地上建塔，脆弱不堪。每一次数据泄露，都是对用户信任的一次重击。企业开始意识到，数据安全不再是IT部门的成本中心，而是企业生存的生命线和社会责任的体现。缺乏可靠技术保障的数据共享，无异于饮鸩止渴。

面对市场失灵、行业需要和立法呼应，全球隐私保护立法出现。2018年，欧盟实施了《通用数据保护条例》（General Data Protection Regulation，简称GDPR）。GDPR以其严格的处罚条款和“设计即隐私、默认即隐私”的原则，为全球数据立法树立了标杆。例如一旦违法，则可以罚款企业全球年营业额的4%或2000万欧元，取较高者。

随后，全球掀起数据立法潮，美国的《加州消费者隐私法案》（California Consumer Privacy Act，简称CCPA）、中国的个人信息保护法（Personal Information Protection Law，简称PIPL）、数据安全法等相继出台。这些法律明确要求，在处理个人信息，尤其是进行数据共享、转让时，必须获得用户明确授权，并确保安全。它们从根本上改变了游戏规则，使得过去那种随意买卖、交换用户数据的粗放模式成为违法。企业突然发现，数据金矿就在眼前，但却被一种无形的“玻璃墙”隔开，无法触碰。这种“数据孤岛”合法化、常态化的困境，需要一种能够“穿墙而过”的技术解决方案。

1.1.3 隐私计算思想

当经济的推力、法律的压力、信任的拉力汇聚于一点，一场技术变革便已箭在弦上。隐私计算

(Privacy Computing) 的兴起,正是多种技术思路在时代召唤下的集中爆发。

隐私计算的核心思想,是在处理数据时保持数据的“加密”或“分散”状态,实现“数据可用不可见”。

不只是技术层面,当前国际标准组织、各国央行、行业协会正在积极制定隐私计算的技术标准和应用规范,解决不同系统间的互操作性问题,标准与生态建设正在加速。大型科技公司积极拥抱,谷歌、苹果、微软等巨头均已将隐私计算作为其重要战略,并将其广泛应用于广告、医疗、金融等业务线。

在中国、欧盟等推动数据要素市场化配置的背景下,隐私计算正被普遍视为未来数据交易所不可或缺的底层信任技术。隐私计算正成为数据要素市场的重要基础设施,引领我们迈向“数据文明”新纪元。

1.1.4 隐私计算因何成为商业银行的战略选择

全球各个企业正航行在数据海域,商业银行也不例外。一侧是“数据金矿”,另一侧则是“合规风暴”,任何不当的触碰都可能引发致命的监管风险。数据共享的迫切需求与隐私保护铁律之间的矛盾,在商业银行这个数据天然聚集地,表现得更为尖锐和激烈。

商业银行,自诞生之日起,其核心功能就是基于信用充当借贷双方的中介。这份信用建立在两大基石之上:一是对客户信息的掌握,了解你的客户(Know Your Customer,简称KYC),二是对客户信息的保护,这是商业银行的保密义务)。在过去千百年里,客户的账目信息被锁在银行厚重的账本中,保密性通过物理隔离和严格的内部制度来实现。数据的收集是局部的,常常只是基于面对面关系,数据使用是受限的,风险是可控的。

然而,数字时代破坏了这种物理隔离,带来了一个两难困境:一方面,业务创新要求数据“流动”,客户数据要求在网络中以光速流动,要提供精准的信贷评估、个性化的财富管理、高效的联合反欺诈,必须打破银行内部各部门之间的“数据孤岛”,甚至要与外部生态伙伴,如政府、电商、运营商进行数据融合。但另一方面,合规与信用要求数据“静止”,个人信息保护法、数据安全法等法律,以及银行的保密传统,要求银行必须将数据牢牢锁住,未经授权不得移动、使用、共享。这个悖论正摇撼着银行长期以来的信用基石。一旦发生数据泄露,银行损失的不仅是金钱,更是最宝贵的资产——客户信任。因此,商业银行正陷入一种“数据窒息”状态:明知数据是“石油”,却不敢轻易开采,生怕引发爆炸。

中国银行业面临的上述挑战,也是全球金融业共同面临的困境,且因中国的监管环境和市场阶段而更具复杂与多样性。中国的个人信息保护法等法律法规也展现出高的标准和严厉的处罚力度。这意味着,数据“野蛮生长”时代的终结,过去那种通过无限度收集、使用用户数据来驱动业务增长的模式已行不通。任何跨机构、跨境的数据合作都必须有法可依、有据可查。法规在保护个人的同时,也客观上使得机构间的数据壁垒从“技术问题”变成了“法律红线”,极大地增加了数据要素市场化配置的难度。

就在银行受困于合规枷锁之时,新的竞争者却利用技术手段在合规框架下实现了“弯道超车”。以某大型科技企业为例,其推出的相关移动支付、信用卡等服务,将自身定位为“数据管道”的维护者而非所有者,通过设备端智能和差分隐私等技术,在提供个性化服务的同时,最小化对用户原始数据接触。这种“隐私优先”的设计哲学,正成为吸引用户的核心竞争力。与此同时,在欧洲PSD2等法规推动下,开放银行模式迫使传统银行在用户授权下,通过API与金融科技公司共享数据。这本质上是一场“数据控制权”的转移革命。银行如果不掌握隐私计算这类能在共享同时保护秘密的技术,将在开放生态中沦为单纯的“数据管道”,价值被大幅削弱。

可见,商业银行面临的已不是一场单纯的业务竞赛,而是一场基于技术实力的合规能力竞赛。能否在合规前提下盘活数据资产,将直接决定其未来在金融格局中的地位。

在全球共性挑战的背景下,中国商业银行的数字化发展之路呈现出独特的复杂性。其核心任务并非在“业务创新、数据合规、经营效益”三者之间进行艰难取舍,因为数据合规是必须恪守的法律底线和经营前提。如何将合规要求从看似制约创新的“成本项”,转化为驱动高质量发展的“赋能项”?工欲善其事,必先利其器,这要求银行从根本上转变发展范式。如图1所示。

目标层

业务创新与经营效益

赋能层

以隐私计算与安全技术为代表的数字技术

基石层

数据合规与安全

图1 商业银行在数据时代的发展范式转变:
从合规成本到创新效益

图1中，基石层代表刚性约束、业务前提。赋能层代表隐私等相关安全技术将合规约束转化为赋能工具，是破局的关键。目标层代表“精准营销”“智能风控”“普惠金融”“供应链金融”等具体业务创新场景，以及“降本增效”“收入增长”“风险降低”等经营效益目标。

可以说，传统的粗放式数据应用模式将合规视为“枷锁”，归为成本单元，导致创新与效益目标在合规红线前止步不前，形成事实上的发展瓶颈。

而基于隐私计算的新范式，则可以内化合规要求，通过“数据可用不可见”的技术内核，将合规底线重塑为业务创新的安全引擎。在此新范式下，合规不再是限制数据融合的“红灯”，在隐私计算与相关安全技术和制度支持下，有望成为数据价值安全、可控释放的“绿灯”。银行得以在合规的框架内，通过隐私计算等一系列安全技术的赋能，积极推进数据驱动的业务创新，最终实现经营效益的可持续增长。

因此，商业银行面临的真正挑战，是完成从“规避合规限制”到“利用合规赋能”的战略思维升级，并通过引入隐私计算等关键技术，将合规、创新、效益三者从看似冲突的目标，整合为相互促进的协同体系。

当前，中国商业银行的信贷风控，特别是对中小微企业和长尾个人客户，严重依赖央行征信等有限数据。由于缺乏安全的数据融合手段，银行难以引入税务、电力、物流等更丰富的维度来精准刻画客户风险，导致要么“惜贷”，要么“错贷”，制约了服务实体经济的能力。财富管理、精准营销等业务亟须对用户画像进行深度洞察。但在现行法规下，银行即使内部调用数据也需谨慎万分，更不用说与第三方合作平台进行联合建模。这导致产品同质化严重，难以满足客户个性化的需求。**无论银行是与政府合作“普惠金融”，与核心企业合作“供应链金融”，还是与同业合作“联合反欺诈”，都迫切需要数据协同。**但传统的“原始数据出域”方式风险极高，金融机构面临诸多技术约束和合规要求。这使得银行构建开放生态的战略举步维艰。例如政府希望与银行合作，利用企业的社保、税务数据发放普惠贷款。但因无法解决数据安全与隐私保护问题，项目难以落地。有意愿、有需求，但缺乏安全可行的技术工具保障支持。

从时代背景看，研究隐私计算技术对商业银行而言，已不只是简单“降本增效”的技术工具，有望成为支持高质量发展核心竞争力。鉴于隐私计算允许商业银行在不移动、不暴露原始数据的前提下，完成数据的计算与分析。这意味着，商业银行的角色发生了转变：**银行不再仅仅是存储数据的“金库”，而是转变为提供“保密计算服务”的枢纽。**数据所有权和使用权得以分离，银行可以

在客户授权和合规框架下，让数据“价值”流动起来，而“信息”不被泄露。

从这个意义上讲，在数字文明时代，商业银行“信用”的内涵正在从“保管财富的安全”扩展到“处理数据的安全”。隐私计算，正是商业银行在数字时代重塑和巩固其信用基石的重要技术，关乎未来银行的形态。那些能率先深度应用隐私计算技术的银行，将能够在合规的轨道上，解开数据安全羁绊，释放数据要素的巨大生产力。在创新的战场上，构建差异化的核心竞争力，提供既智能又让人安心的金融服务。

1.2 概念界定

隐私计算既要做到用户数据被计算、运用，成为企业的生产要素，又要做到用户数据保持隐私状态，这种“既要又要”的状态，使得隐私计算不限于单一技术，而是一个技术体系。从当前主要技术路径看：

1.2.1 隐私计算与密码技术相关概念背景

1982年，由图灵奖得主、中国姚期智院士提出“百万富翁问题”：两个百万富翁想在不袒露各自财富的前提下比较出谁更富有，这一思想催生了多方安全计算（Multi-Party Computation，简称MPC）的理论基石。MPC通过复杂的密码学协议，使得多个参与方能够在无需公开各自输入数据的前提下，共同完成某个函数的计算，并只输出最终结果。

打一个通俗比喻，MPC是一种“共拼藏宝图”的思路。如果一份标有宝藏位置的完整地图被撕成几份，分由几人保管。MPC就像一种神奇的规则，允许这几个持有碎片的人在把各自碎片拼凑成完整地图，即不泄露碎片信息的情况下完成拼凑。密码学协议通过一套复杂的协作指令，共同指引“盲人”走到宝藏的确切地点挖宝，最终宝藏被找到时，却没有任何人看到完整的地图，甚至不知道宝藏具体在哪个人的碎片上。

可以看出，理论意义上隐私计算可以不暴露数据本身，核心理念是“数据可用不可见”。隐私计算的密码学的角色也因此发生了历史性转变：从传统上专注于保障数据在存储、传输等静态环节的安全，如加密存储、安全传输，演进为保障数据在联合分析、建模计算等动态使用过程中的安全。密码学技术，特别是基于MPC的协议，构成了实现隐私计算这一目标的理论基石与核心方法论。除了纯密码学的软件方案，硬件技术的进步提升也为隐私计算提供可信执行环境（Trusted Execution Environment, 简称TEE）。

1.2.2 隐私计算的主要技术路径

隐私计算并非单一技术，而是一个技术体系，其核心目标是在保障数据隐私的前提下实现数据的计算与分析，即“数据可用不可见”。在此核心理念下，隐私计算逐渐形成了多条不同的技术实现路径。不同技术在安全性、效率、适用场景与信任机制方面各有侧重，共同构成当前隐私计算的技术体系。

当前，主流的技术路径主要围绕四大方向展开：以分布式机器学习为核心的联邦学习（FL）、以密码学为基础的多方安全计算（MPC）、以硬件安全技术为支撑的可信执行环境（TEE），以及以数据扰动为手段的差分隐私（DP）。

首先，2016年，美国谷歌公司系统性地提出“数据不动模型动”理念。各参与方在本地用自己的数据训练模型，只将模型的参数更新（而非原始数据）加密上传到中央服务器进行聚合，得到一个更强大的全局模型，这被称为联邦学习（Federated machine learning, Federated Learning, 简称FL）。联邦学习极大地契合了AI时代的需求，为打破“数据孤岛”训练联合AI模型提供了极具可操作性的工程框架，特别是在移动互联网和物联网场景下优势明显。

联邦学习的核心在于，各银行方上传的不是原始数据，而是模型训练过程中的参数更新。如果想用这些更新后信息来反向推导出原始数据，难度极大。而且在实际应用中，通常还会结合差分隐私（DP），即在更新中加入精心设计的噪声，或融合MPC，来进一步增强联邦计算的隐私保护。

如果打一个通俗比喻，一次联邦计算就像一次协作学医。假设多家医院想共同训练一个能诊断某种疾病的AI模型，但出于法律和伦理，不能共享患者数据。那么，可以由一位专家（中央服务器）设计一套诊断规则（初始模型），分发给每家医院。每家医院用自己的病人数据，各自对这套规则进行微调和优化，实现本地训练与本地学习。当学习完成，各个医院不汇报任何病人的具体信息，只向专家汇报：“根据我医院的经验，您医院制定的第X条规则的权重应该提高一些，第Y条应该降低一些”，这样就实现了模型更新。当中央服务器的专家收集所有医院的“心得”之后，可以整合成一套新的、更完善的诊断规则，从而实现全局模型的更新。而且，新规则可以继续下发，重复过程，直到模型变得非常精准，实现循环迭代。最终，AI模型诊断能力很强，但专家从未接触过任何一家的病人数据。

对于商业银行，通过联邦学习技术，多家银行可以合法合规地共建反欺诈或信贷风控模型，共享“知识”（模型参数）而非“数据”（客户隐私），共同提升识别风险的能力，提升风控精度。

除了联邦学习，还有多方安全计算MPC（Secure Multi-Party Computation）。MPC通过设计复杂的密码学协议，如秘密分享、混淆电路、不经意传输等，使多个参与方能够在不泄露各自输入数据的前提下，共同完成对某个函数的计算，并仅获得正确的计算结果。在商业银行领域，MPC适合对安全性要求极高、但数据量相对可控的联合计算场景。例如联合反欺诈，多家银行可以基于MPC，在不暴露各自黑名单客户具体信息的情况下，共同查询某个客户是否存在于任何一家的黑名单中，从而识别潜在的欺诈风险。又如联合信贷评分，银行可以与税务、电力等机构合作，通过MPC协议综合计算企业的多维数据，得出一个更精准的信贷评分，而各方均无法窥探其他方的原始数据。还比如隐私集合求交（PSI），允许银行双方计算出共有客户的集合，而不泄露各自客户名单中非交集的部分，可用于精准营销的客群匹配。

MPC的优势是提供了高安全性，因为其安全性基于严格的密码学假设，不依赖于对硬件或第三方的信任，信任根源在于数学和密码学本身。但MPC协议存在较大的性能开销和通信延迟，尤其是在参与方众多或计算逻辑复杂时，对网络带宽和计算资源的要求较高。

与此同时，可信执行环境TEE（Trusted Execution Environment）也是一条技术路径，依托于硬件安全技术，在中央处理器中构建一个隔离的、受硬件保护的区域，可以称为“飞地”或“安全区”。数据在这个“飞地”中进行计算时，即使是操作系统内核、虚拟机监控程序乃至云服务提供商，都无法窥探其内容。TEE可以用于敏感数据查询与分析，银行内部不同部门之间，或银行与可信第三方之间，需要对加密的敏感数据进行联合分析时，可部署在TEE环境中，保证计算过程可信，也可以用于密钥管理与数字资产托管，TEE是保护加密货币私钥、进行数字资产安全交易的环境。TEE能够处理大规模、复杂的计算任务，提供高计算效率，性能损耗低于纯密码学方案，但TEE的信任建立在硬件制造商之上，存在遭受侧信道攻击的风险。

最后，差分隐私DP（Differential Privacy）。在隐私计算中，经过添加经过精确数学设计的噪声，使得攻击者无法通过查询结果判断任何一个特定个体的数据是否存在于数据集中。这一特性使其适合商业银行数据发布和统计查询场景，只是噪声过大可能导致分析结果失真。

总体来看，在当前技术时代背景下，隐私计算在全球呈现出技术融合趋势，表1展示了隐私计算这四种技术路径的类型及核心思想。

表1 隐私计算的技术路径类型及核心思想

技术名称	英文简称及全称	核心思路	通俗比喻	需要信任的基础
多方安全计算	MPC: Secure Multi-Party Computation	密码学协议,分散计算	共拼藏宝图	数学和密码学
联邦学习	FL: Federated Learning	数据不动,模型动,交换参数	协作学医	算法与加密的更新
可信执行环境	TEE: Trusted Execution Environment	硬件隔离,创建安全飞地	银行金库	硬件科技企业和芯片
差分隐私	DP: Differential Privacy	在数据查询与模型训练中量化隐私损失	刻意扰动使数据先失真	密码学

1.3 研究范畴与全文框架

本白皮书立足于全球数字经济浪潮与中国数据要素市场化改革的双重背景，聚焦于商业银行这一数据密集与监管严格的典型领域，分析隐私计算技术的应用现状、核心价值、典型案例与未来演进路径。

研究将探讨隐私计算如何助力银行在合规前提下，破解数据孤岛困境，激活内外部数据要素潜能，从而在智能风控、精准营销、开放银行、供应链金融等核心业务场景中实现赋能与创新。

本白皮书旨在为商业银行的战略决策者、科技部门负责人及业务运营团队提供一份兼具前瞻视野与实操指引的参考，同时为政策制定者与行业生态伙伴提供启发，共同推动构建安全、可信、高效的新生态，赋能金融业高质量发展。

1.3.1 研究对象：聚焦于商业银行的隐私计算应用

商业银行在金融体系中举足轻重，作为金融系统的信息中枢和信用创造的主体，商业银行在业务开展过程中汇聚了海量、高敏感度的个人金融数据与企业金融数据。这些数据既是其核心资产，也构成了其风险管理和业务创新的基础，同时也使其成为数据安全与隐私合规压力最为集中的领域。据此，商业银行对隐私计算技术的需求最为迫切和典型。

当前，商业银行面临着《巴塞尔协议》系列、国内外隐私保护法规，例如中国的个人信息保护法、网络安全法、商业银行法，以及国家金融监督管理总局、中国人民银行的多重严格监管。其业务模式，如信贷风控、反洗钱、财富管理等，对数据融合与协同计算有着内在的、强烈的需求。这

种“高压”与“刚需”并存的局面，使得商业银行成为研究隐私计算落地的最佳样本。

在监管环境与业务需求之下，商业银行的隐私计算应用场景需要深度挖掘。从商业银行的具体业务条线看，零售金融业务中，精准营销、智能化信贷审批、信用卡反欺诈、客户生命周期管理均涉及隐私计算。对公金融业务中，供应链金融、中小企业信贷、贸易融资真实性核查也涉及隐私计算。而同业等金融市场业务中，如何联合反洗钱、合规监管报送、同业机构间的风险信息共享，是隐私计算的重点场景。即使是商业银行内部管理，在跨部门数据合规使用、绩效分析时，隐私计算也有一定的价值潜力。

1.3.2 研究范围：贯通商业银行业技融合的供需两侧

隐私计算在商业银行的应用，涉及从技术供给到业务需求，乃至整个产业链生态的完整价值链。

从供给端看，隐私计算落地需要考察不同类型的隐私计算解决方案，方案中往往涵盖技术路线，如MPC,FL,TEE或其融合体，也包含产品形态，如软件、硬件及一体化平台状态，还包括服务模式、商业模式及市场竞争格局等内容。

如果深入到核心技术细节，则需要跟踪分析隐私计算底层技术的演进，包括新型密码协议、硬件TEE技术的更新，如Intel SGX,AMD SEV、联邦学习算法的优化等。当然，本研究的重点是商业银行如何运用，而不是对技术模型、参数的详解解释。部分群体关注国内外、行业内外相关的隐私计算技术标准、interoperability（互操作性）规范的制订进展，这些技术性的细节，本研究主要结合与商业银行相关度更高的部分。

从需求端看，中国商业银行当前的现状与规划如何，是本报告的一个关注点。我们通过调研与访谈，试图摸清不同类型商业银行，如国有大型商业银行、股份制商业银行、头部中小银行（互联网银行）在隐私计算技术上的认知程度、试点方向、应用实践情况以及未来规划等。对于商业银行当前的业务驱动力、隐私计算面临的痛点与难点，也是本报告的关注点。商业银行引入隐私计算的核心驱动力，是合规压力、业务创新需求，还是竞争态势所迫，哪一方面需求更强，以及在技术选型、概念验证、系统集成、人才培养、成本收益衡量等方面遇到哪些困难，是行业较为关注的问题。

由于隐私计算涉及产业链与生态圈，必然涉及商业银行上下游关联方，隐私计算的应用绝非商业银行的单方面行为。商业银行在应用隐私技术时，需要打交道的各类生态伙伴较多，一般有数据源方，例如政府机构中的税务、社保、海关，又如运营商、电商平台、核心企业等。也有合作金融机构，包括同业银行、保险公司、证券公司等。还包括第三方服务商，例如咨询公司、系统集成商、

测评认证机构等。这些机构与商业银行形成生态协作模式，例如“数据要素化”市场可能形成隐私计算的协作模式，如数据信托、联合数据运营平台等。本研究无法对这种全景式的每个链条覆盖，但旨在为读者勾勒出一幅总体画像，助力商业银行清晰地定位自身在隐私计算生态中的角色，并制订有效的合作与实施方案。

1.3.3 价值输出：为商业银行提供战略思考与落地启示

本白皮书的核心价值在于提供商业银行的战略思考与落地指引，而非单纯的技术介绍。为确保本研究结论的科学性、客观性与可信度，我们将采用多元化的分析视角进行交叉验证。

首先是文献与政策解析。本研究系统性地梳理了现有知识体系，包括隐私计算、数据要素市场等内容，重点关注技术原理在商业银行的新突破、性能优化方案，也考察了主流隐私计算技术提供商公开发布的一些技术文档、产品文档，包括各科技企业的技术路线、产品特性和市场定位，以便能充分把握隐私市场的趋势和行业共识。

在中国，对政策法规的理解尤为必要。本报告关注与数据安全、隐私保护、金融科技创新相关的法律法规、监管政策、国家标准和行业规范，特别是对网络安全法、数据安全法、个人信息保护法以及金融行业监管细则进行梳理，明确其对商业银行数据应用的合规指引与发展导向。

其次是开展针对性的调查研究与专家访谈。为获取关于隐私计算在商业银行领域采纳情况的定量、可统计的一手数据，调查内容涵盖多个维度，包括商业银行基本信息，受访银行类型、资产规模、数字化投入等，也包括各商业银行对隐私计算的认知与态度，例如对隐私计算技术的了解程度、价值认可度。还包括应用现状，例如是否已开展或部署应用，投入规模怎么样、应用场景怎么看待、技术路线如何选择等。被调查者面临的挑战，在技术、成本、人才、合规等方面遇到的主要障碍，未来的采购或合作意向等，也是关注点。

多轮半结构化访谈的线下专家，覆盖了隐私计算生态中的关键角色，包括需求方专家，尤其是大型商业银行的首席信息官、首席数据官、数据安全负责人、特定业务部门。也包括供给方专家，主要是领先隐私计算企业的创始人、首席执行官、首席技术官等。还包括部分“中立方专家”，例如金融监管机构的政策研究者、行业协会专家、高校及科研院所知名学者、第三方咨询机构的资深顾问。

访谈提纲核心围绕几个主题展开，一是对隐私计算技术成熟度及未来发展的判断。二是在具体项目实施过程中遇到的实际困难与成功经验。三是对政策环境、行业标准、商业模式、生态合作的看法与建议。专家访谈为本研究提供了鲜活、深入的案例和前瞻性的观点，是报告内容具有“洞察力”的关键来源。

第三是进行案例研究与比较分析。选取数个具有代表性的商业银行隐私计算应用案例，进行细节剖析分析。对每个案例，白皮书力图从项目背景、技术选型、实施路径、合作模式、面临的挑战、取得的成效以及经验教训等多个维度进行解剖，旨在将抽象的理论和趋势转化为具体、生动的实践参考，为其他银行提供可借鉴的样板。

总体上，为保障研究过程的严谨与结论的可靠，采取了多方面的质量控制措施。由兼顾金融行业背景、技术研究能力和市场分析经验的成员尽量从多角度剖析问题。对于重要结论，力求通过文献研读、专家调查访谈和案例，至少两种的来源进行交叉验证，避免单一来源的偏差。研究力求所呈现的事实客观、数据翔实、分析深入、结论可靠，能为商业银行及相关从业者提供一份有价值的操作指南。

1.3.4 研究思路与全文框架

本研究按照“问题导向→现状分析→实践验证→破解之道→未来规划”的递进式结构组织开展。逻辑如下图：

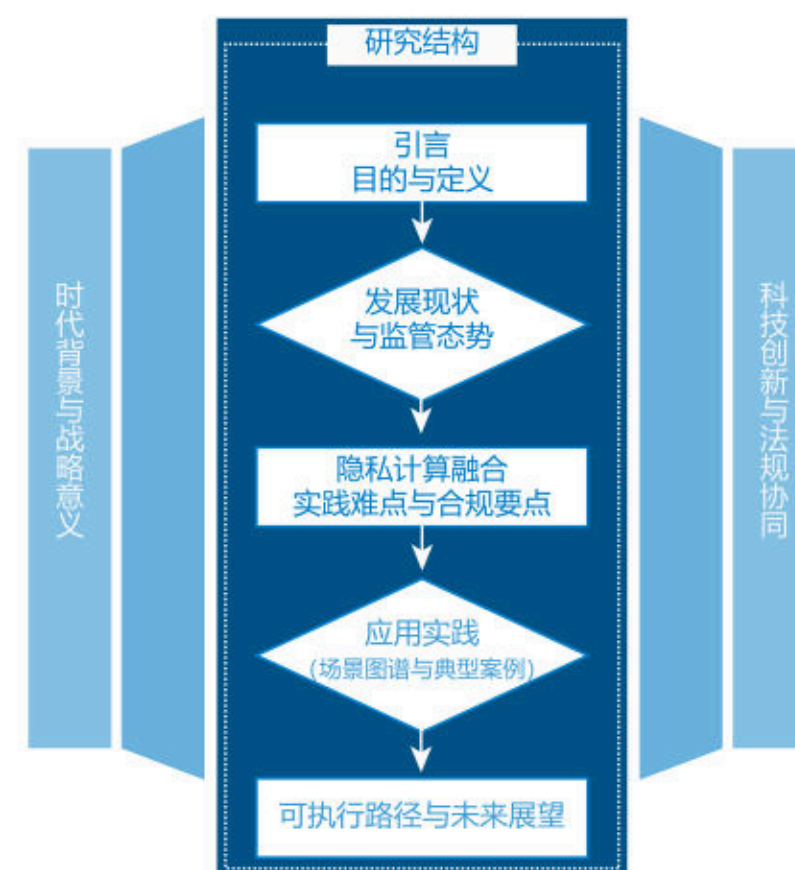


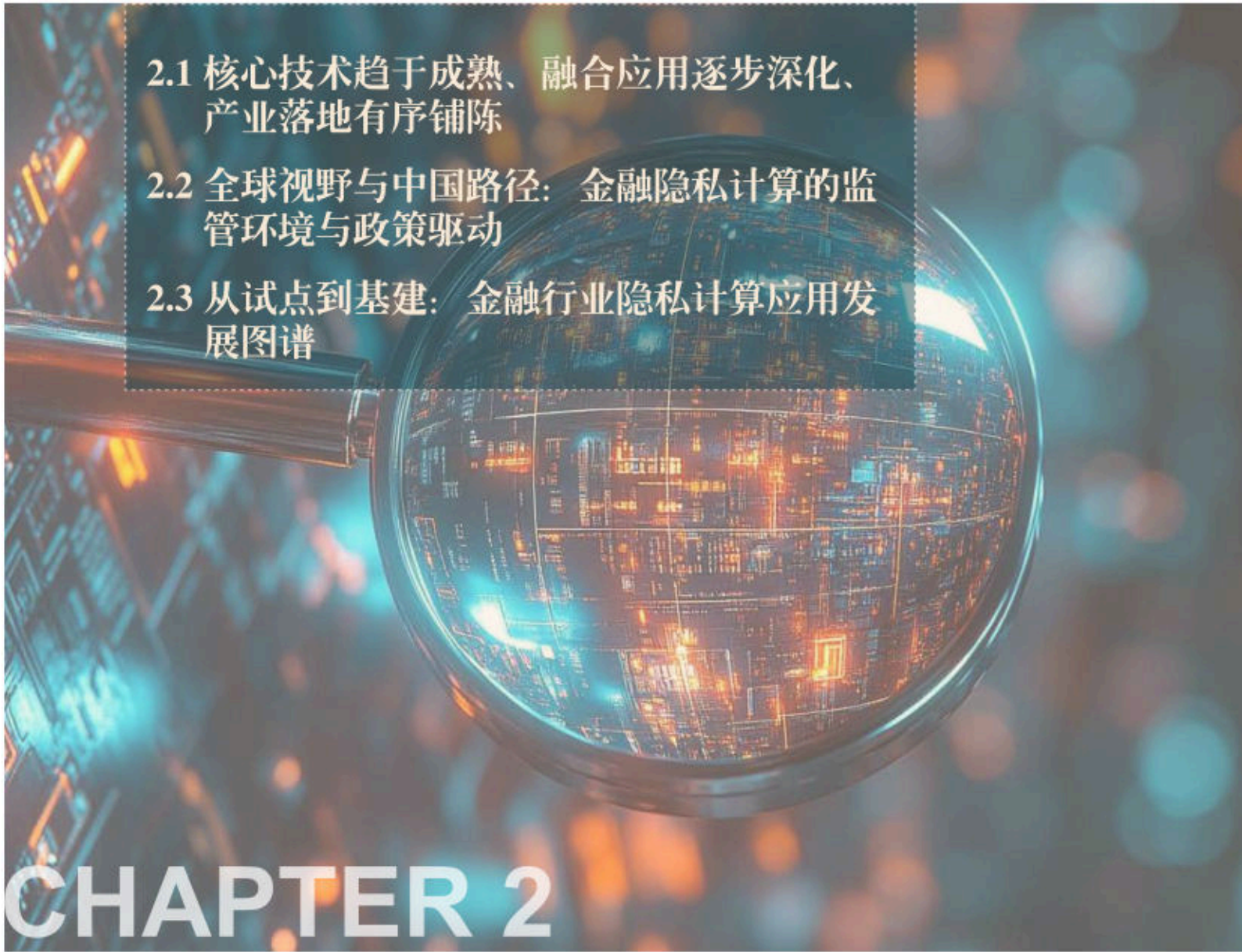
图2 全文逻辑框架

首先在开篇中，本研究从千年权利观念演变到现代法规体系，深度解析矛盾产生的历史与制度根源，说明隐私计算是数字时代信任重构的必然选择，然后现状扫描，系统梳理技术发展脉络与全球监管态势，同时提出商业银行面临的现实约束，即数据价值释放与隐私合规的冲突，确立隐私计算作为破局关键的战略地位，为银行提供决策基础。再次是结合工商银行、建设银行、交通银行等案例，实证隐私计算在风控、营销等场景已实现的价值，解析技术性能、合作模式、合规认定等现实瓶颈，为解决方案提供针对性靶点。最后是路径规划，提出技术选型与生态共建的参考方案，最终形成可落地的战略蓝图，指引银行从被动合规转向主动赋能。这一框架体现了从宏观到微观、从理论到实践、从问题到方案的研究思路，尝试为商业银行拥抱隐私计算，提供行动指南。

研究各章的逻辑按照“发展趋势—现实困境—破局实践—建议展望”的递进顺序铺排。从第二章开始，首先展示隐私计算技术的巨大潜力以及全球监管的引导方向，勾勒出应用蓝图。说明“我们应该去哪里”以及“理论上我们能做什么”。第三章直面“现实鸿沟”的挑战，坦诚地揭示商业银行在近几年的实践探索中，在通往“理想”道路上遇到的痛点与难点、技术瓶颈、业务协作难题、合规不确定性等重重障碍，说明“我们当前身处何处”，反映与“理想”之间的差距。从第三章“现实难点”到第四章“实践亮点”，再到第五章“解决方案与未来展望”，尝试形成了一个逻辑链：“问题痛点是什么？有人成功了吗？他们是怎样做到的？那么，我们系统性地应该怎么做？”，力图识别问题，到寻找实证，再到提炼方法论，层层递进。

第二章

金融行业隐私计算 发展图谱与监管态势

- 
- 2.1 核心技术趋于成熟、融合应用逐步深化、产业落地有序铺陈
 - 2.2 全球视野与中国路径：金融隐私计算的监管环境与政策驱动
 - 2.3 从试点到基建：金融行业隐私计算应用发展图谱

CHAPTER 2

当前，隐私计算技术已从概念验证阶段迈入规模化应用初期。技术的快速发展和应用场景的持续迭代，加之政策支持与数据要素市场需求扩张的双重驱动，隐私计算技术正成为金融机构打破数据孤岛、实现安全协作的关键基础设施。其中，商业银行逐步成为隐私计算技术价值实现的主要阵地，后者在其普惠金融精准风控、零售业务获客营销及跨机构反欺诈等业务场景持续创造价值，构建出“多点开花”的应用生态。

当前，隐私计算正处在技术深化与产业落地的关键过渡期，开源生态逐步成为推动技术普惠的重要支撑。对此，各国在监管政策方面努力厘清隐私计算的应用边界，以期实现“隐私保护与价值释放”的适度平衡，如欧美、新加坡等陆续通过法规与沙盒机制引导隐私计算的合规应用。而我国则通过网络安全法、数据安全法、个人信息保护法划定的安全底线，辅以“数据二十条”等一系列政策鼓励，推动隐私计算加速成为“原始数据不出域、数据可用不可见”的理想解决方案。

综合来看，隐私计算技术应用正从单点尝试向平台化、体系化演进，其产业图谱已初步形成，涵盖了互联互通标准、技术开源、场景融合等多项环节，应用深度更是渗透风控、营销等核心业务。行业建设模式呈现出平台化与互联互通并进的特点，伴随相关技术规范的不断出台，隐私计算的跨平台协同与生态成熟度不断向系统化阶段迈进。

2.1 核心技术趋于成熟、融合应用逐步深化、产业落地有序铺陈

2.1.1 隐私计算技术发展的四个关键阶段：从理论奠基到生态成熟

隐私计算的发展已形成从理论奠基到生态成熟的清晰脉络，可简要概括为四个关键阶段（如图3）。1949年至1982年的萌芽期，以密码学领域的理论突破为核心，为现代隐私计算相关技术奠定了早期基础；1983年至1999年的探索期，聚焦技术方法层面的创新，进一步完善了隐私保护相关的技术路径；2000年至2019年的成长期，推动技术从实验室研究逐步走向工程化实践，加速了技术落地的进程；2020年至今的应用深化期，在数据要素市场化需求的驱动下，隐私计算突破研发局限，深度融入各行业场景，同时各类厂商崛起倒逼技术实用化提升，推动整体生态走向成熟，为数据安全合规流转提供核心支撑。

萌芽期（1949年至1982年）以密码学理论突破为核心。香农在1949年发表了《保密系统的通信理论》，开启了现代密码学的时代；1976年Diffie和Hellman提出了公钥密码学框架；1977年RSA算法的诞生，奠定了非对称加密基础；1982年，姚期智提出的“百万富翁问题”，首次把安全计算的概念引入隐私保护的领域，为后续发展埋下了伏笔。

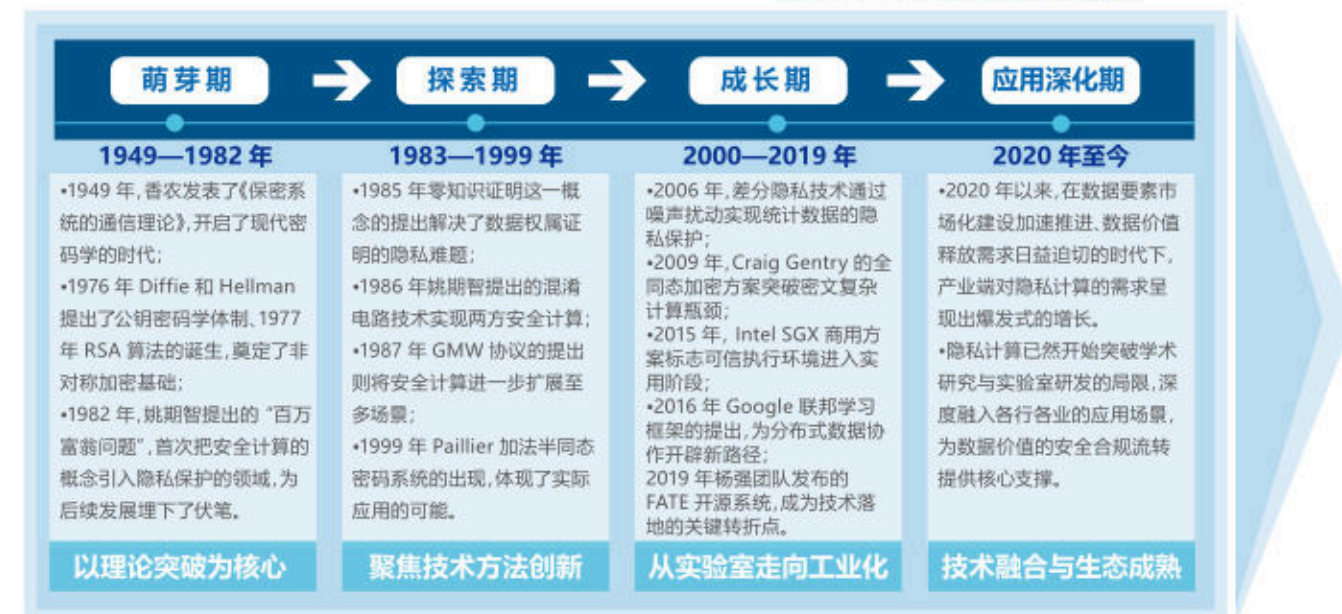


图3 隐私计算技术发展关键阶段

探索期（1983年至1999年）聚焦技术方法创新。1985年零知识证明这一概念的提出解决了数据权属证明的隐私难题；1986年姚期智提出的混淆电路技术实现两方安全计算；1987年GMW协议的提出则将安全计算进一步扩展至多场景；1999年Paillier加法半同态密码系统的出现，体现了实际应用的可能。

成长期（2000年至2019年）标志着技术从实验室走向工程化。2006年，差分隐私技术（DP）通过噪声扰动实现统计数据的隐私保护；2009年，Craig Gentry的全同态加密方案突破密文复杂计算瓶颈；2015年，Intel SGX商用方案标志可信执行环境进入实用阶段；而2016年Google联邦学习框架的提出，为分布式数据协作开辟新路径；2019年杨强团队发布的FATE开源系统，成为技术落地的关键转折点。

应用深化期（2020年至今）标志着隐私计算走向技术融合和生态成熟。2020年以来，在数据要素市场化建设加速推进、数据价值释放需求日益迫切的时代背景下，产业端对隐私计算的需求呈现出爆发式的增长。其中，中国人民银行出台首个金融应用规范指引跨主体协作，为金融机构的跨主体数据协作提供了关键指引。隐私计算已然开始突破学术研究与实验室研发的局限，深度融入各行各业的应用场景，为数据价值的安全合规流转提供核心支撑。在此过程中，各类隐私计算厂商纷纷崛起，进一步倒逼技术的实际可用性得到提升。

2.1.2 隐私计算核心技术全景梳理：发展脉络、技术体系与实践落地

在数字经济深度发展的当下，数据作为核心生产要素，其安全合规与跨域协同价值释放需求的

矛盾日益凸显，这也驱使隐私计算技术成为平衡数据可用与隐私保护的关键支撑。其中，多方安全计算（MPC）、联邦学习（FL）、可信执行环境（TEE）、与差分隐私（DP）四大技术，构成了隐私计算领域的核心支柱。它们从不同维度切入隐私保护需求，既各有技术侧重，又能协同互补，共同构建起“可用不可见”的数据流通与价值挖掘体系。

四类主流技术并非孤立存在：MPC聚焦无信任场景下的多方协同计算，通过密码学协议实现数据不共享却能联合计算；FL侧重分布式模型训练，让数据留在本地、仅流转模型参数，适配大规模终端与跨机构协作；TEE依托硬件级隔离环境，为敏感计算提供可信执行空间，解决软件层面难以规避的安全风险；DP则通过可控噪声注入，在数据查询与模型训练中量化隐私损失，保障个体数据不被逆向识别。下文将围绕这四大核心技术，分别**梳理其发展脉络、拆解核心技术体系、呈现行业实践路径**。

(1) 多方安全计算（MPC）：经典技术演进与行业落地实践

多方安全计算（MPC）研究在近年呈现多维度深入推进的态势，从经典课题的技术深化到特殊场景的问题探索，从理论复杂度的突破到行业应用的高效落地，形成了完整的研究与实践生态。在经典研究课题方面，门限加密/签名算法、混淆算法作为MPC的核心支柱，持续吸引大量研究关注。门限方案的设计逻辑是让一组参与方共享密钥，仅当超过预设阈值的参与方协同操作时，才能完成对消息的解密或签名，这一机制在金融跨机构密钥管理、政务多部门权限控制等场景中具有关键价值；混淆算法则源于姚期智院士提出的经典姚氏混淆电路，通过将计算逻辑转化为加密的布尔电路，实现参与方仅能获取结果而无法窥探输入的隐私保护效果。其中，Schnorr、BLS、BBS+、ECDSA等签名算法的研究尤为集中，各类研究围绕签名的轮数复杂度（即协议执行的通信轮次）、抵御适应性敌手的能力（面对动态攻击时的安全性）、底层假设的可靠性（如离散对数难题的有效性）及实际场景的健壮性展开深入探索；而混淆算法的研究则聚焦于算法性能的优化，以及算术电路、算术-布尔混合电路等更适配复杂计算场景的混淆算法设计，例如在金融风控的数值运算场景中，算术电路的应用可大幅提升密文计算效率。

MPC的技术价值通过多行业落地与工程化工具得到充分验证。场景应用方面，MPC在机器学习/深度学习领域的应用最为活跃；此外，时间序列分析、身份认证、网络服务、密钥管理、动态数据库分析等场景均有成熟的MPC应用案例。

(2) 联邦学习（FL）：隐私协同范式、技术链路构建与多场景落地

联邦学习是隐私保护机器学习的核心范式之一，核心逻辑是让多方在不直接共享原始数据的前提下，仅通过交换模型参数或梯度来协同训练全局机器学习模型，以此达成数据协同计算与隐私保护的平衡。它的核心优势在于，一方面打破数据壁垒，推动跨机构数据融合并释放价值；另一方面，通过将原始数据留在本地，结合差分隐私（DP）的噪声注入、同态加密的密文计算以及多方安全计算的协议设计，构建多层防护体系，从根本上规避训练数据的隐私泄露风险。

在应用场景上，联邦学习已广泛落地：例如在智慧城市交通领域，多个城市的公共交通系统利用联邦学习，在不共享原始出行数据的情况下联合训练出行流量预测模型，提升高峰调度与应急响应能力；智能风控场景中，银行与电商平台通过联邦学习，在样本对齐基础上联合训练反欺诈模型，提升风险识别能力且数据不出本地，保障隐私与合规；广告转化预测场景里，广告平台与品牌广告主借助联邦学习联合构建转化预测模型，精准定位高价值用户。

(3) 可信执行环境（TEE）：技术演进脉络与融合应用生态

可信执行环境（TEE）是软硬件协同构成的隔离环境，可保护敏感数据并执行隐私计算，常用技术包括Intel SGX、Intel TDX、AMD SEV 和ARM TrustZone，涵盖攻击、防御、应用、构建四大方向。可信执行环境（TEE）的技术发展已完成从架构构想到规模化应用生态的完整跃迁，其脉络清晰呈现为“**隔离可信—虚拟化可信—融合可信**”三个递进阶段，实现了从硬件根基构建到系统工程突破，最终迈向业务生态集成的演进。

第一阶段为隔离可信，核心聚焦在不可信操作系统下能否构建可信计算路径的基础问题，致力于奠定硬件安全根基。这一阶段确立了以硬件为信任根基的隔离执行范式，并借助GlobalPlatform等组织形成标准化框架。第二阶段进入虚拟化可信，随着云原生架构普及，应用级TEE（如SGX）暴露出编程复杂、兼容性差、I/O通路缺失等问题，研究重心转向如何将TEE无缝嵌入现有虚拟化基础设施的系统级工程突破。第三阶段迈向融合可信，TEE不再是孤立安全模块，而是作为隐私保护基础设施的核心组件，与云原生、隐私计算深度融合形成规模化应用生态。此外，在硬件层面，TEE在Intel和AMD之外，也同样支持融合RISC-V的多种体系架构。技术协同方面，TEE与联邦学习、同态加密、MPC等技术构建“可用不可见”数据流通体系。

(4) 差分隐私（DP）：技术发展路径及业务落地与合规

差分隐私（DP: Differential Privacy）是一种具备数学严谨性的严格隐私保护技术，其核心逻辑是向原始数据或数据查询结果中，添加遵循特定概率分布、强度精准可控的精心设计噪声。这

种方式能有效抵御攻击者借助背景知识反推个体信息，最终实现在个体数据不可识别的情况下，整体数据仍可用的目标，平衡隐私安全与数据统计分析价值。差分隐私的发展动态呈现出清晰的三阶演进脉络，从抽象理论逐步走向业务化、规模化部署，形成了“**理论奠基—工程突破—生态融合**”的完整发展路径，其技术体系与应用价值持续深化。

第一阶段为“隐私可证—奠定理论根基”，差分隐私的发展始于对隐私严格定义与量化的追问。2006年Dwork首次提出其数学定义，使隐私保护具备可量化、可组合的理论基础，后续经系列机制设计，确立了可证明隐私保护的标准框架。第二阶段进入“高效可用—实现工程突破”，理论完善后研究转向实用化探索。2014年Google RAPPOR项目验证了大规模落地可行性，后续通过隐私损失度量、隐私会计框架等的发展，解决了隐私与效率兼顾的关键挑战，推动其从理论安全迈向工程可行。第三阶段迈向“面向业务—融合部署与合规落地”，差分隐私已升级为数据处理的内生能力，深度嵌入业务流程。工业级部署案例涌现，且与多种技术融合形成隐私基座，同时纳入国家标准体系，成为合规法定技术路径。

在此基础上，差分隐私已广泛渗透至统计分析、机器学习、大规模数据挖掘等关键领域。通过科学配置噪声机制与隐私预算，它既能筑牢敏感数据的安全屏障，又能完整保留数据的宏观统计特征与分析价值，实现隐私保护与数据利用的动态平衡。在金融风险评估场景中，银行、保险、证券等机构借助该技术开展信用风险研判、违约率测算时，可安全披露客户分布、平均信用评分等宏观结论，有效规避个人账户信息、交易细节的泄露风险；金融科技平台也能通过其防范合规审计、二次数据挖掘中的内部滥用与第三方泄露问题。

面对全球范围内严苛的金融数据监管要求，差分隐私不仅能助力机构落实数据最小化、个人信息去标识化等合规要求，构建“隐私友好”的运营模式以增强客户信任，其严谨的数字化隐私保障特性，还能为跨境金融业务中的多法域合规审查提供透明可审计的技术支撑。凭借可量化的隐私界定、灵活适配的噪声机制及广泛的场景适用性，差分隐私为大数据时代搭建了坚实且具备延伸性的隐私保护体系，持续为数据合规流通与价值释放注入核心动力。

综上，隐私计算主流技术路线各具特点：秘密分享、不经意传输、混淆电路均为多方安全计算（MPC）的典型实现，安全性高且无需可信第三方，但通信开销大、开发难度高；联邦学习性能与安全性中等，部分需可信第三方，适用于联合建模与预测；可信执行环境性能与安全性高，但依赖硬件厂商；差分隐私性能安全性中等，无需可信第三方，主要用于统计计算。总体来看，不同技术在性能、安全性、信任假设间存在权衡。

2.1.3隐私计算技术深化与产业落地过渡期：开源生态支撑技术普惠

当前，隐私计算正处于技术深化与产业落地的关键过渡期，学术研究聚焦效率突破，产业应用在垂直领域形成标杆，但规模化复制仍面临着挑战，**开源生态则成为技术普惠的重要支撑**。

隐私计算典型开源项目可按核心技术方向分为多方安全计算（MPC）、联邦学习（FL）、可信执行环境（TEE）、差分隐私（DP）四大类，另有覆盖多技术的综合型项目。这些开源生态围绕隐私计算核心技术方向，均构建起适配多元需求的支撑体系，无论是匹配主流技术栈以降低适配成本、覆盖不同产业场景的差异化诉求，还是兼容多类基础设施环境、平衡功能覆盖与计算效率，本质都是通过技术组件的模块化复用、开发门槛的系统性降低，让不同规模的机构能低成本获取成熟技术能力。这类开源布局打通了技术从研究、试点到产业落地的链路，推动隐私计算逐步走向更广泛的行业普惠。

技术 领域	项 目 类 别	典 型 项 目	核 心 特 点
多方安全计算（MPC）	工业应用类	TF-Encrypted、Meta CryptTen、矩阵元 Rosetta、OpenMined SyMPC、蚂蚁 SPU	基于 PyTorch/TensorFlow 等深度学习框架开发
	学术研究类	MP-SPDZ、FudanMPL、EzPC、ABY/ABY3/Cheetah	MP-SPDZ 支持多协议且优化通信效率；FudanMPL 支持多机器学习模型；EzPC 专注神经网络安全推理；部分为论文协议实现，常作底层集成
	专用协议类	OPRF-PSI、MultipartyPSI(隐私集合求交)；XPIR、SealPIR(匿踪查询)	聚焦特定隐私计算场景，提供专用协议支持
	基础组件类	libOTe、EMP-toolkit、Obliv-C	提供不经意传输、混淆电路等密码学原语，支撑上层应用开发
联邦学习（FL）	横向联邦	Google TensorFlow-Federated、USC FedML、CMU LEAF	欧美项目为主，面向 C 端千万级参与方
	纵向联邦	微众银行 FATE、百度 PaddleFL、阿里 EFLS、京东 FedLearn	国内项目为核心，适配 B 端少参与方、大数据量场景
可信执行环境（TEE）	硬件适配类	蚂蚁 Occlum、Intel Gramine（前 Graphene）、OP-TEE、百度 Teaclave、Google Asylo	适配不同硬件架构（SGX、ARM TrustZone 等），提供安全计算环境或开发支持
同态加密（HE）	布尔电路类	TFHE、FHEW、OpenFHE、Concrete、HEhub	支持任意运算，国内首个同态开源项目 HEhub 在此列，效率待提升
	算术电路类	微软 SEAL、IBM HElib、OpenMined TenSEAL	基于多项式环，支持 SIMD，计算效率较高
	综合类	OpenFHE、HEhub	可实现布尔电路与算术电路转换
	硬件加速类	cuHE、cuFHE、cuYASHE	基于 GPU 加速，计算效率提升 1 个数量级
综合技术型	多领域覆盖类	OpenMined PySyft、蚂蚁 SecretFlow、原语科技 PrimiHub	包含 MPC、FL、TEE、HE 等主流技术，具备完善社区生态

图4 隐私计算开源生态典型项目解析

2.2 全球视野与中国路径：金融隐私计算的监管环境与政策驱动

在技术趋势趋于成熟的同时，法规政策和监管环境也在同步助力隐私计算的落地应用。金融隐私计算的应用深化与落地推进，得益于全球与国内层面日趋完善的监管政策和外部环境。从全球视野看，国际监管普遍秉持隐私保护与价值释放的双重导向，通过法律规范界定技术义务、创新赋能举措优化落地环境，推动隐私计算成为破解数据利用与隐私保护矛盾的合规刚需。从中国路径而言，以“三法”为核心的法律体系划定了合规底线，在此基础上，数据要素战略引领下的多层次政策从顶层设计、金融专项落地到多部门协同保障逐步推进，既延续安全内核，又破解应用难题。全球与国内的监管政策形成合力，为金融领域应用隐私计算提供了充分的法律支撑与政策指引。

2.2.1 国际视角：隐私保护与价值释放的双重导向

国际监管以“隐私保护 + 价值释放”的双重导向，底层逻辑是引领技术升级锚定合规目标，助力隐私计算成为满足跨域数据融合要求的通用解法(如图5)。欧美借法规强制明确技术义务:美国《加州消费者隐私法案》(CCPA)界定去标识化、假名化标准，强制研究数据处理流程，推动隐私增强技术成合规刚需。欧盟通过《支付服务指令》(PSD2)、《监管技术标准》(RTS)与《通用数据保护条例》(GDPR)层级协同，《通用数据保护条例》(GDPR)“设计默认保护”条款催生需求，《人工智能法案》(AI Act)适配 AI 场景技术诉求。新加坡以《个人数据保护法案》(PDPA)、《银行法》构建刚性约束，借隐私增强技术 (PETs) 沙盒、《隐私增强技术 (PETs) 采纳指南》等赋能，推动技术规模化落地。

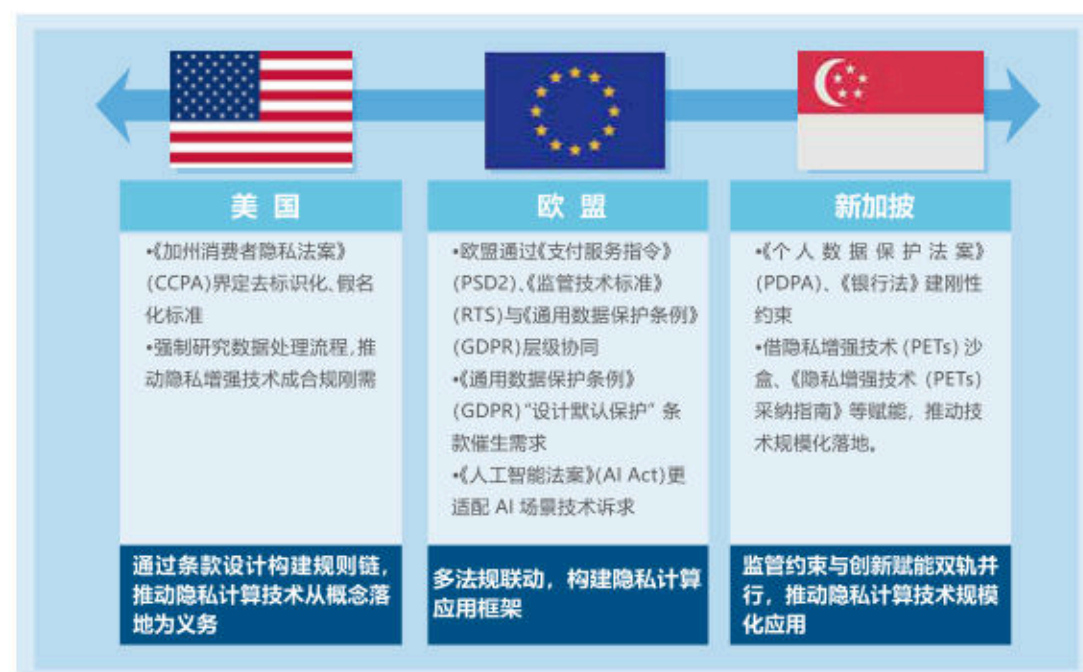


图5 隐私计算技术国际监管框架概览

(1) 美国：通过条款设计构建规则链，推动隐私计算技术应用落地

美国《加州消费者隐私法案》CCPA体系通过精准的条款设计，完成了隐私增强技术从概念到义务的转变，形成从定义到要求再到保障的完整规则链。

在核心技术界定上，加州民法典明确“去标识化”需满足三重条件：技术层面实施防重识别措施、组织层面建立泄露防控流程、法律层面放弃重识别尝试，同时要求通过合同约定接收方行为，实质将隐私增强的全流程管控纳入法定标准。

对“假名化”的界定更具操作性，要求将身份映射信息与主体数据分离存储，并施加技术与组织防护，直接为隐私增强技术的典型实践提供法律依据。针对于研究应用的条款设计则实现了隐私增强技术的流程化强制。明确要求用于研究的个人信息必须先假名化再去标识化，且需同步落实三项技术保障：技术性防再识别机制、业务流程层面的重识别禁令、研究目的专属访问控制，将隐私增强技术从单一技术工具升级为系统性处理方案。数据最小化原则的条款化进一步扩大隐私增强技术的适用范围，规定个人信息的收集、使用与共享必须合理、必要且成比例，推动企业采用数据脱敏、字段过滤等隐私增强技术。

(2) 欧洲：多法规联动，构建隐私计算应用框架

欧洲通过《支付服务指令》PSD2、《监管技术标准》RTS与GDPR的层级协同，构建了隐私增强技术在金融数据共享中的强制应用体系，实现从原则到技术标准的全维度覆盖。

PSD2作为业务基础法规，首先以数据约束划定隐私增强技术的应用边界，其相关条款明确禁止支付发起服务商存储敏感支付数据及超范围使用数据，并对账户信息服务商作出同等要求，将数据最小化与数据使用的目的限定转化为硬性义务，而这些义务的落地必须依赖数据脱敏、访问权限管控等隐私增强技术。

RTS（委托法规(EU)2018/389）则将技术标准条款化，形成可执行的安全规范。其中明确要求全流程保障个性化安全凭证的机密性与完整性，禁止明文存储密钥材料，直接指向加密存储等隐私增强技术的强制应用；并对凭证全生命周期的安全控制提出要求，推动了动态加密、安全销毁等技术的规模化部署；相关条款要求采用通用且安全的开放通信标准，并确保会话的保密性与完整性，这些都是端到端加密、安全接口与安全会话的强制规范，对应着典型的隐私增强技术实践。这些条款使欧洲开放银行的技术合规有了明确的指标。

GDPR 作为顶层法律框架，为隐私增强技术提供了原则性支撑与强制力保障。GDPR 确立了全球最为系统的数据保护规则，即合法性、透明度、目的限制、数据最小化与完整性保密等原则。凭借着严苛的数据处理规范、高额的处罚力度以及对数据主体权利的全方位保障，GDPR 成为了驱动隐私计算技术在欧洲落地应用的最关键动力。例如，GDPR，数据保护需要是内生且默认的（Data protection by design and by default），要求企业需要采取适当的技术或措施来落实数据最小化原则。因此，企业选择隐私计算保障数据“可用而不可见”成为了必要的合规方案；数据处理的安全性（Security of processing），列出了数据假名化、数据加密、定期测试评估等安全措施的有效性。这与隐私计算的密态存储、同态加密等高度契合。企业若想在跨境数据传输、多方数据协作等场景中满足 GDPR 的合规要求，就必须借助技术方案突破隐私保护与数据利用的矛盾，隐私计算成为必要方案。

随着人工智能技术的发展与应用普及，欧盟人工智能法 AI Act 应运而生，进一步延伸了这一监管逻辑。该法案推动 AI 系统数据治理的刚性监管框架成为隐私计算技术合规落地的关键制度支撑。例如，该法条有明确规定，高风险 AI 系统的训练、验证和测试数据需满足相关性、代表性和准确性要求，同时在偏见检测与纠正场景中，允许例外处理种族、健康等特殊类别个人数据，但必须严格遵循“数据不传输、使用后删除”等保障措施。这种既要数据质量用于模型优化，又要严防敏感数据泄露的合规需求，恰好为隐私计算技术提供了用武之地，联邦学习可实现多源数据协同训练而不暴露原始信息，同态加密能支持密态数据直接运算，多方安全计算则能在分布式场景中完成数据聚合分析，这些技术特性匹配了对数据“可用不可见”的核心诉求。此外，该条款要求的数据全生命周期治理，如标注、清洗、偏差纠正等，也推动企业采用隐私增强技术构建合规体系，进一步巩固了隐私计算的应用价值。

（3）新加坡：监管约束与创新赋能双轨并行，推动隐私计算规模化应用

作为东南亚数字经济的枢纽，新加坡构建了以《个人数据保护法案》（PDPA）为核心的数据隐私监管体系，确立了数据处理的核心规则：数据收集需基于合理目的并获取同意、明确个人访问更正数据的权利、要求全生命周期的数据安全与及时删除，跨境传输需确保同等的隐私保护标准。配套的《个人数据保护（数据泄露通知）条例》等法规进一步细化执行标准，提供了落地化的流程、判定标准与沟通模板，形成了刚性的合规约束框架。此外，新加坡的《银行法》（Banking Act）对客户信息披露设置了严格的限制，严禁银行及职员随意披露客户信息，仅允许在法律规定的个别目的、对象和条件下合规披露，且接收方需承担永久保密义务，违规者将面临监禁或罚款。

在严格监管的基础上，新加坡资讯通信媒体发展局（IMDA）与个人数据保护委员会（PDPC）于 2022 年 7 月联合推出首个隐私增强技术沙盒（PET Sandbox），其核心目标在于激发隐私增强技术的创新活力，探索更具通用性的操作模式与标准规范。该沙盒将为市场主体提供多维度支持，涵盖技术支撑、资金扶持与法规层面的专业指引，以此推动隐私增强技术的规模化应用。同时，作为安全的试验载体与实践空间，它能助力企业筛选适配的隐私增强技术方案，鼓励其开展技术试验与应用优化，最终实现数据安全共享的核心目标。该沙盒既回应了监管对隐私保护的要求，又为隐私计算技术的试验、优化与规模化应用提供了关键支撑，成为连接监管框架与隐私计算发展实践的重要纽带。

在“人工智能+”的背景下，新加坡于 2025 年推出的新版全球 AI 保障沙盒、《隐私增强技术采纳指南》及《新加坡数据保护标准》三项举措，构建了规范边界与创新赋能并重的监管态势，为隐私计算技术发展提供了明确方向与实践支撑，深刻推动其从技术探索走向规模化应用。《PETs 采纳指南》作为核心赋能工具，直接降低了隐私计算的落地门槛。该指南基于 2022 年 PETs 沙盒积累的实践经验，精准回应企业在隐私计算部署中的核心痛点，通过 PETs 用例评估工具帮助企业匹配适配自身业务的隐私计算方案，如 AI 训练或跨行业数据共享场景的技术选型；借助实施检查清单规范从评估到部署的全流程，确保技术应用的安全性与有效性。更关键的是，指南作为动态文档将随沙盒新增用例与业界反馈持续更新，使隐私计算技术能灵活适配不断变化的业务需求，减少企业试错成本。新版全球 AI 保障沙盒则为隐私计算提供了针对性的试验场景与风险适配空间。沙盒扩展后覆盖具代理能力的 AI（Agentic AI）、数据泄露风险等新范式与风险，且结合“大型语言模型安全测试入门工具包”提供标准化测试路径，这使得企业可在安全环境中试验隐私计算技术在新型 AI 场景中的应用效果。同时，沙盒向监管机构开放收集实测反馈，其产生的洞察既能优化隐私计算的技术参数，又能为监管政策提供实践依据。

《新加坡数据保护标准》的升级则从合规层面强化了隐私计算的技术价值。其明确涵盖第三方管理、跨境数据传输等关键合规领域，而隐私计算恰好是满足这些要求的核心技术方案。企业为获取新版认证以彰显合规能力，将更主动地采纳隐私计算技术，这不仅创造了刚性市场需求，更使隐私计算成为企业践行数据保护承诺的显性名片，增强大众对技术应用的信任。三者形成的监管合力，推动其成为新加坡构建可信 AI 与数据生态的核心支撑技术。

2.2.2 国内基石：以“三法”为核心的安全合规底线

近年来，国内监管对数据的跨域流通划定了明确的合规红线，同时又在隐私计算领域构建起安

全与发展并重的鲜明态势，推动隐私计算从此前数据应用的可选项升级为满足数据安全与个人信息保护核心底线的必然要求。以《中华人民共和国网络安全法》（简称网络安全法）《中华人民共和国数据安全法》（简称数据安全法）《中华人民共和国个人信息保护法》（简称个人信息保护法）（“三法”）为核心的安全线，为隐私计算划定合规边界的同时，也明确了其技术价值的合法施展空间（如图6）。



图6 中国隐私计算监管规制框架

网络安全法要求网络运营者采取技术措施保障数据安全，隐私计算通过多方安全计算、联邦学习等技术逻辑，实现数据“可用不可见”，在金融跨机构风控等场景中，既满足了企业对数据价值挖掘的需求，又落实了法律对数据安全的要求；数据安全法确立的数据分类分级、流通合规等制度，让隐私计算成为政务数据共享、数据交易所交易的关键技术，实现“数据不动价值动”；个人信息保护法的“告知—同意”“最小必要”原则，而隐私计算的联邦学习、差分隐私等技术，在互联网用户行为分析等场景中，达成了个人信息权益保护与商业需求的平衡。

以网络安全法、数据安全法、个人信息保护法为核心的“三法”体系，清晰划定了合法空间，让“原始数据不出域、数据可用不可见”的隐私计算模式，成为破解数据共享需求与安全合规要求矛盾的现实路径，这为隐私计算从实验室走向产业实践，尤其是进入对合规性要求极高的金融领域，奠定了核心基础。

2.2.3 政策驱动：数据要素战略下的金融发展指引

金融业对隐私计算的应用与采纳逐步深化，这推动了隐私计算从被动满足合规底线到主动利用数据创造业务价值的战略转向。这一过程中，国家政策的明确鼓励成为隐私计算释放数据要素价值、驱动金融创新的安全底座。金融业对隐私计算的应用主要依托两大背景展开：一是“数据要素”作为生产要素的定位逐步明确，二是监管层面对跨主体数据合作、金融领域专项落地到多部门协同保障三个层面逐步推进，既延续了“三法”的安全内核，又兼顾商业银行应用隐私计算时的合规顾虑、技术门槛与业务协作难题，推动隐私计算在金融领域实现从合规试点向规模化普及发展。

（1）顶层政策为商业银行隐私计算注入信心

数据要素市场化配置改革是当前数字经济发展的核心任务，隐私计算技术作为数据流通的关键基础设施，在政策层面得到了顶层设计的强力支持。这些政策文件精准切中商业银行在数据应用中的核心痛点，为商业银行探索应用隐私计算，实现数字化转型与业务赋能提供了根本遵循（见图7）。

在合规层面，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”）明确提出“鼓励公共数据在保护个人隐私和确保公共安全的前提下，按照‘原始数据不出域、数据可用不可见’的要求，以模型、核验等产品和服务等形式向社会提供”。此前，银行在对接公共数据（如政务、税务、社保数据）或跨机构共享客户信息时，多因担心触碰数据隐私保护红线而不敢尝试，如结合企业纳税数据优化普惠贷款授信，顾虑直接获取原始数据违反个人信息保护法的规定；尝试联合同业构建反欺诈模型，顾虑泄露客户隐私的风险。“数据二十条”出台后，隐私计算成为公共数据社会化利用的主流路径，使得商业银行逐步从“不敢用”隐私计算，转向主动拥抱和探索合规应用场景。

文件名称	发布时间	发布机构	主要内容
《多方安全计算金融应用规范》	2020 年 11 月	中国人民银行	金融行业第一个隐私计算相关技术的标准
《金融科技产品认证目录(第二批)》	2022 年 1 月	金融监管总局、中国人民银行	目录共包含 14 个产品种类：多方安全计算金融应用、移动终端可信执行环境(TEE)、可信应用程序(TA)、客户端软件、安全芯片、区块链技术产品等
《金融科技发展规划(2022—2025 年)》	2022 年 1 月	中国人民银行	探索建立跨主体数据安全共享隐私计算平台,在保障原始数据不出域前提下规范开展数据共享应用,确保数据交互安全、使用合规、范围可控,实现数据可用不可见、数据不动价值动
《中国人民银行业务领域数据安全管理办法(征求意见稿)》	2022 年 7 月	中国人民银行	数据处理者采用隐私计算等技术促进数据融合创新应用时,应当确保原始数据未离开自身控制范围,且多个数据提供方被关联后,暴露约定范围外信息的风险可控.采用隐私计算技术提供数据时,应当建立统一的技术风险评估和控制策略,明确安全可验证性、性能可接受性等风险对应的缓释措施
《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》	2022 年 12 月	中共中央、国务院	鼓励公共数据在保护个人隐私和确保公共安全的前提下,按照“原始数据不出域、数据可用不可见”的要求,以模型、核验等产品和服务等形式向社会提供
《十六部门关于促进数据安全产业发展的指导意见》	2023 年 1 月	工业和信息化部、中国人民银行等十六部门	加强隐私计算、数据流转分析等关键技术攻关.加快发展数据资源管理、资源保护产品,重点提升智能化水平,加强数据质量评估、隐私计算等产品研发
《个人信息保护合规审计管理办法(征求意见稿)》	2023 年 8 月	国家网信办	专业机构应当采取相应技术措施和其他必要措施,保障数据安全
《“数据要素 x” 三年行动计划(2024—2026 年)》	2024 年 1 月	国家数据局	打造安全可信流通环境,深化数据空间、隐私计算、联邦学习、区块链、数据沙箱等技术应用
《银行保险机构数据安全管理办法(征求意见稿)》	2024 年 3 月	金融监管总局	银行保险机构应当建立数据安全技术架构,明确数据保护策略方法,采取技术措施,保障数据安全
《国家数据标准体系建设指南》	2024 年 9 月	国家发展改革委、国家数据局、中央网信办、工业和信息化部、财政部、国家标准化管理委员会	数据流通安全标准主要规范数据流通安全合规相关要求.包括数据交易服务安全、数据流通脱敏和匿名化、隐私计算、数据传输安全、数据流通安全能力、数据来源合规评估等标准
《关于促进数据产业高质量发展的指导意见》	2024 年 12 月	国家发展改革委、国家数据局、教育部、财政部、金融监管总局、中国证监会	加快可信数据空间、区块链、隐私计算、匿名化等可信流通技术研发和应用推广
《关于促进企业数据资源开发利用的意见》	2024 年 12 月	国家数据局、中央网信办、工业和信息化部、公安部、国务院国资委	鼓励企业采用可信数据空间、区块链、隐私计算、匿名化等技术模式,促进数据安全流动和开发利用
《银行保险业科技金融高质量发展实施方案》	2025 年 3 月	金融监管总局办公厅、科技部办公厅、国家发展改革委办公厅	鼓励金融机构加大数字化转型投入,运用云计算、大数据、人工智能、机器学习、隐私计算等技术,研发数字化经营工具,集成展示科技型企业评价、评估结果,增强企业识别和筛选能力,提升经营管理质效和风险防控水平

图7 国内隐私计算重点政策概览

在业务赋能层面，政策支持商业银行“数据+金融”的价值空间，隐私计算成为破解业务痛点的利器。国家数据局《“数据要素x” 三年行动计划（2024—2026年）》进一步细化落地路径，提出“打造安全可信流通环境，深化数据空间、隐私计算、联邦学习、区块链、数据沙箱等技术应用”，隐私计算与其他可信技术融合，共同构建“技术+制度”双轮驱动的数据流通体系，有助于银行在合规前提下突破数据瓶颈，实现对业务的实际增益。

在基础设施层面，国家同样有战略级部署。2025年1月6日国家发改委官网公布，为贯彻落实党的二十届三中全会关于建设和运营国家数据基础设施，促进数据共享的部署要求，国家发展改革委、国家数据局、工业和信息化部联合印发《国家数据基础设施建设指引》，具体阐述了国家数据基础设施概念内涵、发展愿景、总体功能、总体架构，从数据流通利用、算力底座、网络支撑、安全防护等四个方面指明具体建设方向。这一指引聚焦于数据流通利用的基础设施底座与算力支撑体系，为隐私计算提供了规模化落地的底层承载能力。在此基础上，2026年6月3日，国家数据局印发《关于推进行业高质量数据集建设行动的实施方案》（国数科基〔2026〕25号），进一步将隐私计算纳入国家数据基础设施的顶层设计。该方案明确提出，“鼓励依托国家数据基础设施，充分运用隐私保护计算、可信数据空间等能力，开展数据集安全存储、可信流通、高效应用，推动数据集从分散持有向集约化、标准化供给转变。”同时要求“构建数据集全生命周期的管理体系……依托数据基础设施，强化隐私保护计算、区块链等技术应用，确保数据可管、可控、可追溯。”这标志着隐私计算已从技术可选项升级为国家数据基础设施建设中的核心安全能力，为商业银行等行业主体参与高质量数据集建设提供了政策指引与合规路径。

（2）金融领域政策多维度护航，推动商业银行隐私计算应用落地

在合规层面，中国人民银行2020年11月发布的《多方安全计算金融应用规范》是金融行业首个隐私计算标准，明确了多方安全计算在金融领域的应用场景、技术要求与合规边界，为银行、证券、保险等机构开展跨主体数据协作提供了应用指南。

在技术层面，国家市场监督管理总局与中国人民银行联合发布的《金融科技产品认证目录（第二批）》《金融科技产品认证规则》的公告，将多方安全计算金融应用、移动终端可信执行环境（TEE）等隐私计算相关产品纳入认证范围，通过产品认证的机制推动技术标准化与商业化，加速了隐私计算技术在金融机构的规模化部署。在业务场景层面，2022年11月中国人民银行发布的《金融科技发展规划（2022—2025年）》提出探索建立跨主体数据安全共享隐私计算平台，要求在保障原始数据不出域的前提下，实现数据可用不可见、数据不动价值动，推动金融机构在供应链金融、反

洗钱、保险精算等场景的隐私计算应用实践。规划中提及的供应链金融、反洗钱等场景，正是商业银行的核心业务领域，例如在供应链金融中，银行可通过隐私计算整合核心企业、物流、仓储数据，更精准评估中小供应商信用；在反洗钱场景中，能联合多机构共享风险特征却不泄露客户隐私。

(3) 政策协同破局：技术、规范、业务齐发力，激活商业银行隐私计算应用动能

在技术供给层面，2023年1月工业和信息化部、中国人民银行等十六部门联合发布的《十六部门关于促进数据安全产业发展的指导意见》，将隐私计算列为关键技术攻关重点方向，要求加强隐私计算、数据流转分析等关键技术攻关，同时提出加快发展数据资源管理、资源保护产品，重点提升智能化水平，加强数据质量评估、隐私计算等产品研发，从技术研发到产品落地全环节提供政策支持。政策的落地实施方面，引导产业链上下游的科技公司、科研机构聚焦该领域，加速成熟技术产品的供给：一方面，技术厂商会基于政策导向加大研发投入，推出更适配金融场景的隐私计算平台；另一方面，政策鼓励的数据保护产品智能化升级，会让隐私计算工具更易用、更贴合业务需求。这将大幅提升行业供给能力，降低技术应用门槛与试错成本，实现技术普惠。

在规范统一层面，2024年9月，国家发展改革委等部门印发的《国家数据标准体系建设指南》将隐私计算纳入数据流通安全标准体系，明确“数据流通安全标准主要规范数据流通安全合规相关要求，包括数据交易服务安全、数据流通脱敏和匿名化、隐私计算、数据传输安全等”，通过标准建设推动隐私计算技术的规范化、规模化应用，为全行业划定了通用标准：无论是银行间的协作，还是银行与政务、企业等外部机构的对接，都可依据统一标准设计隐私计算流程，避免了重复开发、反复适配的无效模式。

在业务协作层面，国家数据局等部门于2024年12月发布的《关于促进企业数据资源开发利用的意见》鼓励企业采用可信数据空间、区块链、隐私计算、匿名化等技术模式，促进数据安全流动和开发利用，为企业级数据要素市场的发展提供了技术路线指引。一方面，银行可更主动地与政务部门、核心企业、第三方数据机构沟通，以数据可用不可见的模式获取关键数据支持；另一方面，政策也推动外部机构更愿意与银行共享数据，核心企业无需担心泄露风险，共同打造银行、企业、供应商三方共赢的生态。

在国家政策持续鼓励与支持下，隐私计算的应用价值与发展潜力正持续释放，成为激活数据要素价值、助力数字经济高质量发展的关键支撑。随着数据托管、经纪、认证等新业态在政策支持下加

速兴起，隐私计算有望成为这些业态的技术底座：既支撑数据经纪企业完成合规流通、收益分配等全流程服务，又助力第三方机构实现数据空间安全能力标准化评估。同时，在企业数字化转型与数据空间互联互通需求下，隐私计算正探索统一技术规范与交互协议，为跨空间数据协同提供技术支撑，让高价值数据在可控范围内安全流动。

2.3 从试点到基建：金融行业隐私计算应用发展图谱

伴随技术的日趋成熟与融合应用、法规政策和监管框架的包容引领，隐私计算在金融领域正经历从局部试点到成长为重要技术基础设施的关键阶段，这一进程以成熟产业生态为支撑，逐步实现应用阶段的跃升与落地模式的体系化构建。

2.3.1 产业情况：多头并进的产业图谱初步形成

全球隐私计算产业已构建起多主体协同、全链条覆盖的完整产业图谱（见图8），在产业生态层面，隐私计算已形成覆盖需求、制度、产品、基础设施、算法、治理及AI扩展的多层次协同发展格局。



图8 全球隐私计算图谱

需求牵引层聚焦金融、医疗、政务、能源、科研及跨境数据等场景，参与方包括银行、保险、运营商、广告平台、药企等，为技术落地提供真实业务驱动力。

制度与数据流通层依托国家数据局体系、地方数据集团、行业主管部门及数据交易所、数据授权运营机构等，构建可信数据空间与数据沙箱，为数据安全流通提供制度保障与基础设施。

协同计算产品层汇聚了蚂蚁、微众、华控清交、蓝象、洞见等隐私计算平台厂商，以及 AWS、Snowflake、Google、Microsoft 等云服务商，提供联邦学习、数据洁净室、密态计算等产品能力。

机密基础设施层由 Intel、AMD、NVIDIA、ARM 及国产芯片厂商（海光、鲲鹏、昇腾、飞腾）提供 TEE、机密虚拟机、机密容器及远程证明等硬件级安全能力，并依托 AWS、Azure、阿里云、谷歌云等实现云端部署。

密码与算法内核层涵盖 MPC、PSI、HE/FHE、DP、ZK、PIR、安全聚合等核心技术，典型开源与商业项目包括 OpenFHE、SEAL、Zama、SecretFlow、FATE、OpenMined 等，由高校及密码团队持续贡献。

治理与审计层通过使用控制、数字合约、数据计量、收益分配、区块链存证及合规审计等机制，支撑数据交易与可信数据空间运营，参与方包括区块链厂商、交易所、监管科技公司等。

AI 扩展层聚焦机密 AI、隐私大模型评测、模型 IP 保护、隐私 RAG 及联邦微调等前沿方向，参与方有 OpenMined、NIST CAISI、NVIDIA、Google Cloud、华为昇腾及金融机构 AI 平台等。

整体来看，从需求牵引到制度流通、从产品协同到硬件支撑、从密码内核到治理审计再到 AI 扩展，各层级相互联动，共同推动隐私计算走向规模化产业应用。

2.3.2 发展阶段：从单点试点迈向规模化应用

隐私计算相关理论和工程技术的成熟推动其走出实验室，稳步实现其在风控、营销等核心场景中的规模化落地，成为打破数据孤岛、激活数据要素价值的关键技术，其成熟度主要体现在场景渗透、技术适配、协作生态及价值转化四大维度。

从场景覆盖来看，其应用已深度渗透金融核心业务领域，形成以风控与营销为核心的规模化落地格局。在风控领域，跨机构联合计算模式已成为行业共识，银行通过与政务、同业、运营商等多方合作，构建全流程风险管控体系，解决了单一机构数据维度不足的痛点；在营销领域，依托跨行业数据融合的精准运营模式，实现从获客到留存的全链路效能提升，场景覆盖从零售金融延伸至普惠

金融、科技金融等重点支持领域和金融服务薄弱环节。

技术适配性已实现业务需求与技术能力的深度匹配。多方安全计算、联邦学习等主流技术经过实践验证，能够满足金融业务对数据隐私保护与计算效率的双重要求，企业级隐私计算平台的搭建进一步解决了技术落地的工程化难题，支持海量数据处理与实时响应，适配信贷授信、反欺诈等高频业务场景。

协作生态呈现多元化、体系化特征。参与主体已涵盖国有大行、股份制银行、互联网银行等各类金融机构，且与政务、支付清算、电商等外部机构形成稳定合作链路，对等平台部署、联合建模等合作模式已标准化，头部机构牵头的行业生态初步形成，推动技术应用从单点试点走向批量复制。

价值转化成效显著，有望成为政策落地与业务增长的关键抓手。通过打破数据壁垒，有效支撑数字金融、科技金融等政策落地，同时在风险识别准确性、营销转化率等核心指标上实现量化提升，证明隐私计算已从合规工具升级为金融机构提升核心竞争力的基础设施，应用成熟度处于各行业前列。

2.3.3 建设模式：平台化建设与行业互联互通标准

金融业正逐步构建形成“平台搭建—场景运营—监管协同”三位一体推进路径。在平台建设层面，银行正从购买单一软件转向主动构建统一平台，工商银行、建设银行、交通银行等机构均通过自主搭建隐私计算平台，整合多元技术路径，在联合风控、普惠授信、反欺诈及精准营销等高频业务场景实现技术落地与实效转化。与此同时，各类市场主体（如银行、支付机构等）自主搭建或外部采购部署隐私计算平台的尝试，进一步推动了上述场景的技术落地。

在互联互通层面，行业逐步探索制定统一执行标准。2024年3月，北京金融科技产业联盟发布团体标准《金融业隐私计算互联互通平台技术规范》（T/BFIA 031—2024），由中国银联牵头、50余家单位参与，明确了多方安全计算、联邦学习、可信执行环境等异构技术路线下的平台架构、接口、安全与验证要求，为跨平台作业与跨机构协同提供了统一规则，推动行业从单平台试点转向跨平台协作。2025年启动的《数字金融隐私保护计算互联互通技术规范》金融行业标准等正在研制中；另一方面，行业级互联互通能力并行推进，监管沙箱与行业组织主动搭建跨机构互联互通基础设施，着力破解技术孤岛等实践难题，各地方金融科技创新监管工具也多次纳入隐私计算方案。

第三章

商业银行隐私计算 业技融合实践难点与合规要点

3.1 多重约束下，隐私计算技术面临的痛点和难点

3.2 业务与管理层合作意愿低、实施周期长、 商业模式成熟度不足

3.3 监管规制与合规要点：数据匿名、流通授权、 技术可控、跨境传输

CHAPTER 3

尽管前景广阔，隐私计算的规模化应用并非一片坦途。本章将审视商业银行在拥抱这一技术时，在技术、管理及合规层面临的普遍性挑战与关键节点。

3.1 多重约束下，隐私计算技术面临的痛点和难点

在“人工智能+”的战略背景下，隐私计算在业技融合时面临多维度痛点，既包括规模效率与安全的平衡、技术平台异构、信创适配与性能平衡等技术难题，也涵盖数据供需互信缺失、AI可信度与数据治理衔接缺口、合规认定不匹配等困境。



图9 隐私计算落地应用中的技术融合痛点

3.1.1 规模、效率与安全的平衡难题

在隐私计算技术的实际应用中，如何在规模、效率与安全之间取得平衡始终是一个核心挑战。其主要痛点集中体现在三个方面：首先，以多方安全计算为代表的技术存在显著的通信开销瓶颈，其多轮交互协议在面对海量数据时会产生指数级增长的成本，严重制约了规模化部署。其次，计算过程本身存在效率与精度的双重损耗，如同态加密的密文运算效率较明文低数个数量级，而部分联邦学习方案为保障安全不得不牺牲模型精度。最后，随着节点规模扩大，动态环境下的安全风险日益凸显，包括恶意节点检测、算力异构等复杂因素不断削弱原有的安全假设，使得系统的可信验证与协同管理变得异常复杂。这些痛点相互交织，共同构成了技术迈向大规模产业化落地的关键障碍。隐私计算与区块链这一数字世界的隐性基础设施深度绑定可以突破单一加密技术的一些局限，而二者融合过程中，规模、效率与安全的平衡难题突出：一方面，区块链需从单链向聚链成网升级

以支撑多机构协同，但当前架构下，大规模网络的互通兼容性、跨链数据流转的顺畅性尚未有效突破，难以形成统一的数据共享协作网络；另一方面，网络规模扩大易导致计算时延增加、算力消耗上升，若为满足高隐私需求采用零知识证明、多方安全计算等密码学技术，又会进一步加剧效率损耗，形成安全强度与计算效率的对立；此外，安全风险还涵盖区块链网络本身的节点安全、应用接口防护等层面，且技术研发容易陷入脱离场景谈指标的误区，若过度强调单一技术参数，反而会脱离数据流通与安全计算的实际需求，削弱融合技术的落地价值。

技术融合的规模化应用还面临信创适配与性能平衡的潜在挑战。如某大型银行在新技术引入过程中需满足信创标准，隐私计算与AI融合所依赖的TEE等硬件、算法工具均需完成相应的信创适配，而信创生态内不同科技企业的技术成熟度存在差异，可能影响融合方案的稳定性与效率。同时，AI模型的训练对计算性能要求较高，隐私计算的加密解密过程往往会带来性能损耗，二者的性能平衡需在实践中持续优化，在越大规模数据、越复杂AI模型的融合场景中，性能损耗与计算效率的矛盾可能越突出，成为技术落地的隐性制约。

3.1.2 技术不足以支撑信任基础

从技术应用信任基础来看，数据供需双方的互信缺失、数据供给需求的适配性不足构成基础障碍。如AI的核心竞争力依赖于海量、高质量数据的持续输入，尤其是金融领域的垂直AI模型，更需要多维度、跨主体的数据支撑才能实现精准洞察。而隐私计算的核心价值在于通过联邦学习、多方安全计算等技术实现“数据可用不可见”，其应用前提是多方数据的协同参与。过去部分银行在实践中，发现计算场景下普遍存在数据持有方共享意愿偏低的问题，大家都不愿意主动开放核心数据，导致AI模型训练所需的跨机构、跨领域数据池难以有效构建。

金融行业尤其是银行间的信任壁垒显著，同业机构对核心业务数据的安全保障存在天然顾虑，即便隐私计算技术已能实现数据不出域、参数可交互，仍难以打消核心业务信息被间接推断的担忧。这种信任缺口并非技术本身能完全填补，若缺乏权威第三方或政策层面的公信力赋能，即便技术成熟，跨机构的AI+隐私计算融合项目也易陷入落地难的僵局。

AI可信度建设与隐私计算的数据治理衔接也存在着缺口。AI模型的可信度高度依赖于输入数据的质量与合规性，而隐私计算场景下的数据来源更为复杂，涵盖政府、企业、专业服务机构等多个主体，数据标准、质量参差不齐。但隐私计算的技术特性使得数据预处理与质量校验难度显著增加，传统数据治理中可直接开展的清洗、比对工作，在“数据不可见”的隐私计算框架下需通过多方的协调，不仅流程更为繁琐，也难以保证质量管控的全面性。此外，AI模型的迭代优化需要持续的反馈数据，

而隐私计算场景下的数据交互多为单次、特定场景的授权调用，缺乏长期、稳定的反馈数据闭环，导致AI模型难以通过持续学习实现精度提升，进一步制约了两者融合应用的深度。

3.1.3 平台间存在差异，提升落地成本

技术平台的异构性加剧了融合落地的成本与复杂度。如同人工智能技术本身存在多样的模型架构与开发框架，当前隐私计算市场尚未形成完全统一的技术标准与接口规范，不同科技企业的产品和技术架构、核心算法与安全模型上呈现显著差异：有的基于可信执行环境（TEE）搭建底层框架，有的以多方安全计算（MPC）或联邦学习（FL）为核心技术路线，其支持的算子库、密文传输协议及性能参数千差万别。不同科技企业的产品之间实行互联互通的技术难度较大，即使能够实现往往效果较差。更棘手的是，即便同一科技企业的不同版本平台也可能存在代际鸿沟，早期版本多聚焦基础数据对齐，新版则扩展了联合建模、隐私查询等高级功能，这样的局面直接冲击人工智能对多源数据的集成需求。人工智能模型训练往往需要联动政务、通信、金融等多领域数据，而跨科技企业平台对接时，常常出现密文协议不兼容、算法库版本不匹配等问题。技术团队往往需耗费数周调试接口，甚至被迫重构适配层，不仅推高实施成本，更导致人工智能模型的训练数据接入效率大打折扣，难以实现多源数据协同赋能的核心目标。这种异构性的背后是行业缺乏统一的技术对接标准，使得AI模型与隐私计算工具的融合难以形成规模化复制能力，即便是具备较强技术实力的机构，在跨主体合作中仍需为适配成本买单。

3.1.4 技术落地进程面临法规约束，短期效果受限

隐私计算的深度应用还面临法规认定与技术实践不匹配的痛点。如隐私计算与AI融合应用，隐私计算的核心价值是实现数据可用不可见，而人工智能模型的训练与迭代依赖海量数据，但二者融合产生的计算结果隐私性、模型参数的合规性界定仍处于模糊地带。隐私计算作为技术工具，仅能在数据质量把控、应用优化等层面发挥作用，无法解决所有法律问题，尤其是涉及个人数据的敏感场景，法律风险的判断需结合具体场景逐一评估。例如，在开展联邦学习时，虽通过参数交换避免原始数据出域，但模型训练过程中数据授权的边界、参数传递的隐私风险等，尚无明确的行业标准与法律细则。这种合规模糊性迫使金融机构不得不采取保守策略，例如，某大型银行对多数融合场景需申请进入中国人民银行监管沙盒，在监管指导下开展试点，且对公场景因合规要求相对较低更易推进，个人场景则因敏感性高而进展缓慢，这在一定程度上限制了“隐私计算+AI”融合应用的场景广度。同时，隐私计算与AI的融合应用可能涉及数据跨境、个人信息保护、算法伦理等多重法律监管议题，而当前监管环境对这类新型技术组合的认定标准尚未明确。在AI应用场景中，隐私计

算的加入使得数据流转路径更为隐蔽，进一步增加了法律监管的判断难度。例如，通过隐私计算获取的政务数据、个人征信数据用于AI模型训练后，其模型输出结果的责任界定、数据使用痕迹的追溯等问题均缺乏明确法规。这种监管不确定性使得金融机构在推进技术融合时趋于谨慎，往往需要投入大量精力应对法律风险，难以集中资源突破技术融合瓶颈，一定程度上延缓了融合应用的创新进程。

综上所述，隐私计算在规模化落地进程中面临多重交织的困境：技术层面，规模、效率与安全的平衡难题尚未根本破解，平台异构导致的高昂适配成本与互联互通壁垒依然突出；信任层面，数据供需双方的互信缺失与 AI 可信度治理的衔接缺口，使得跨机构协作难以有效展开；合规层面，法规认定与技术实践的不匹配进一步加剧了应用的不确定性。需要正视的是，部分隐私计算技术的安全性依赖于特定技术假设（如 TEE 对硬件厂商的信任、密码学方案对数学难题难解性的依赖），这些假设在实际环境中难以完全验证，且存在侧信道攻击、协议漏洞等潜在风险，并非绝对无风险。尤其值得关注的是，隐私计算对中小企业而言技术复杂、参与成本较高，部署和运维门槛远超其资源能力，可能导致其在数据协作生态中逐渐被边缘化，长此以往或将加剧“强者愈强、弱者愈弱”的生态失衡。这些痛点的叠加，构成了隐私计算从技术可行迈向大规模产业应用的关键障碍。这些痛点也表明，隐私计算与 AI 的技术融合并非简单的工具叠加，需要信任机制、标准体系、法规框架与技术实践的协同推进，需要破解信任壁垒、完善统一标准、明确法规边界。

3.2 业务与管理层合作意愿低、实施周期长、商业模式成熟度不足

在业务与管理层面，隐私计算落地面临多重现实挑战，既存在跨机构信任缺失、数据收益分配机制不明导致的合作意愿不足，也面临项目成本高、周期长、复合型人才稀缺的实施难题，还受成熟商业应用模式尚未形成的制约。



图10 隐私计算业技融合面临的难点

3.2.1 业务合作意愿的核心障碍：跨主体信任缺失，协同动力不足

商业模式构建与合作意愿激发的核心障碍集中于跨主体的信任缺失与协同动力不足。作为数据密集型行业，金融领域的数据持有方普遍存在信任缺失与动力不足的问题，银行在交易数据、政务数据等核心数据的利益主体是谁、利益如何分配等关键问题尚未形成共识，数据持有方既担心核心数据经隐私计算交互后存在隐性泄露风险，又对数据共享可能产生的收益缺乏明确预期，导致“数据孤岛”现象在隐私计算技术框架下仍难以有效打破。

“数据孤岛”现象的背后，本质是缺乏有效的信任联结机制。银行间同业合作中，即便隐私计算技术能实现“数据不出域、参数可交互”，各方仍对核心业务数据可能被间接推断、敏感信息泄露存在深层顾虑，难以形成主动共享的动力。即便与互联网企业、银联等开展联合营销、风控建模等合作，也需耗费大量精力进行前期沟通与风险评估，且合作范围往往局限于非核心业务场景。这种信任壁垒并非单纯依靠技术优化就能破解，跨主体合作的推进离不开外部权威力量的公信力支撑，若缺乏这种支撑，即便技术方案成熟，合作也易陷入停滞。此外，目前行业尚未形成清晰的利益分配机制，数据价值的贡献度难以量化，进一步削弱了机构间主动参与数据共享与合作的积极性，使得“数据孤岛”的破解陷入想合作却不敢、想合作却无从下手的困境。银行间、银行与政府及企业间的信任壁垒难以快速消融，使得隐私计算本应具备的跨主体数据协同优势难以充分发挥。

3.2.2 项目实施的阻力：成本高，周期长，复合型人才稀缺

在项目实施过程的中，另一重困难是较高的成本投入与较长的推进周期。隐私计算作为融合了密码学、分布式技术等多领域的复杂技术，其基础设施部署与系统搭建往往需要显著的资源投入。众多银行在自建数据交易平台、搭建隐私计算技术平台的过程中，平台的研发、部署与维护必然涉及高额的技术采购与硬件投入。而更大的成本与周期压力来自与外部对接的复杂性：由于行业缺乏统一的技术接口标准，外部数据引入需面临逐一对接的困境。这种基础设施建设成本高、外部对接适配成本高、项目推进周期长的现状，使得众多具备较强资源实力的机构，相关项目也仍处于起步阶段，难以快速规模化复制。

人才层面的制约也是不容忽视的问题，隐私计算的落地需要既懂密码学、数据安全等技术，又熟悉金融业务场景与合规要求的复合型人才，而当前市场上这类人才相对稀缺。人才缺口使得隐私计算项目从技术选型、场景适配到系统上线的全流程周期显著延长，尤其在需要与 AI、数据中台等现有系统融合时，技术对接与流程磨合往往需要额外的时间成本，进一步推高了项目实施的整体门槛。

3.2.3 商业应用模式不成熟：可复制的成熟模式待构建

隐私计算的应用场景虽在逐步拓展，但技术价值向商业价值的转化路径仍在探索中。目前隐私计算的应用多聚焦于内部价值提升，尚未找到清晰的盈利切入点。某大型银行的实践显示，其数据交易平台目前以引入外部数据、服务行内应用为主，暂不对外提供数据服务，核心价值体现在规范数据应用流程而不是使其成为创收工具，多数应用仍服务于内部业务效率优化或风险控制，尚未形成可对外输出的、能直接产生收益的标准化产品，未实现数据价值变现的直接盈利模式。某大型商业银行与互联网科技企业的风控合作、与社保部门的数据交互、与子公司的营销协同等场景中开展实践，且取得了效果不错的初步成果，但这些应用多聚焦于内部效率提升或特定合作场景的需求满足，尚未形成可复制、可盈利的成熟商业模式。

从行业现状来看，多数银行的隐私计算应用仍停留在成本投入阶段，如何通过技术应用实现直接盈利或显著降本的问题尚未得到有效解决。一方面，隐私计算的投入主要体现在基础设施与合规成本上，短期内难以通过业务收益直接覆盖；另一方面，适合隐私计算规模化应用的高价值场景仍在探索中，目前的应用多集中在风控、营销等传统数据应用领域的延伸，尚未挖掘出能够充分体现隐私计算独特价值的创新商业场景。隐私计算技术的商业价值仍需时间验证，也让部分机构对其投入持谨慎态度。

3.3 监管规制与合规要点：数据匿名、流通授权、技术可控、跨境传输

隐私计算技术作为实现“数据可用不可见”的核心手段，在平衡数据开发利用与安全保护方面展现出巨大潜力。然而，其创新特性也需要监管包容与合规保障。在匿名化合规、授权机制、技术可控性、跨境传输及行业适配等关键维度面临的合规要点值得关注。

3.3.1 数据匿名化与去标识化的合规边界

隐私计算技术处理个人数据时常援引匿名化作为合规基础，然而如何匿名化、匿名化的具体标准如果不明确，容易触犯合规要求。个人信息保护法规定，经过匿名化处理的个人信息不再属于个人信息，可以在不经个人同意的情况下流通使用，但相关标准规范尚待细化。实践中，匿名化与去标识化的法律界限模糊，可能导致隐私计算输出结果仍被认定为个人信息，从而触发完整的个人信息保护义务。

(1) 再识别风险与责任分配：隐私计算环境下，数据接收方可能通过辅助信息、多次查询或算法推理等方式重构原始信息，导致再识别风险。现行法律框架尚未清晰界定这种情况下发生数据安

全事件时的责任分配原则。特别是当多方参与计算时，如何确定匿名化失败后的责任主体、归责原则和处罚标准，都存在法律上的不确定性。湖南省通信管理局与网信办在专项治理行动中，明确将“通过技术手段绕过用户授权机制，强行收集数据”列为整治重点，这表明监管部门对技术规避行为的态度，间接反映了对匿名化技术被滥用的担忧。

(2) 匿名化效果的认定分歧：不同技术路径下的匿名化效果评估缺乏统一标准。例如，联邦学习中的模型参数、多方安全计算的中间结果，可能包含残留的可识别信息，这些技术衍生物的法律定性直接影响到整个处理活动的合规基础。目前国家标准《数据安全技术个人信息匿名化处理指南及评价方法》、《数据匿名化流通实施及评估指南》已立项推进，但尚未发布。由于缺乏明确的匿名化操作规范、技术指标和流通环境要求，这种不确定性使得企业在采用隐私计算技术时面临合规判断的困境。

3.3.2 数据流通与授权同意的法律冲突

隐私计算技术在多方数据协作场景中，面临与传统个人信息保护原则如何协调的挑战，尤其是在授权机制适配性和多方处理责任界定方面。

(1) 授权机制的适配性挑战：根据个人信息保护法，处理个人信息通常需要获取个人的明确同意，且应当充分告知处理目的、方式和个人信息种类。然而，隐私计算环境中，原始数据不离域，数据处理目的可能在计算过程中动态变化，这使得传统的特定、明确授权较难及时覆盖全流程。特别是当多个数据源融合计算产生未预见的分析结果时，既有的授权基础可能无法支撑最终数据使用行为。

针对这一挑战，这在隐私计算的多方参与场景中尤为重要，技术应用方须审慎评估授权范围是否覆盖了整个计算过程，避免因授权缺陷导致合规风险。

(2) 多方处理模式的责任界定：隐私计算技术涉及多方主体，包括数据提供方、算法提供方、计算平台运营方和结果使用方等，这些主体在个人信息保护法下的法律定位可能随技术架构而变化。例如，联邦学习中的参与方可能同时构成“共同处理者”而非单纯的“技术提供方”，从而需承担更严格的法律责任。根据《个人信息保护合规审计管理办法》要求，共同处理需明确各方权利义务、安全机制及事件报告流程，这种责任划分在技术复杂度高的隐私计算环境中实施难度较大。

3.3.3 技术可控与可解释性备受关注

隐私计算技术的复杂性和“黑箱”特征引发了监管部门对其可验证性和可解释性的高度关注，这些将直接关系到法律合规要求的落实效果。

可验证性不足与监管审计障碍：隐私计算技术的内在复杂性使得传统安全审计方法难以适用，而《个人信息保护合规审计管理办法》要求处理超过 100 万个人信息的个人信息处理者定期开展合规审计。在隐私计算环境下，如何验证数据输入、计算过程和结果输出的完整合规性，存在技术挑战。这样无法为监管机构提供足够的透明度和可验证性，可能难以满足合规审计要求。

金融领域的规定尤为严格，《中国人民银行业务领域数据安全管理办法》明确要求“使用隐私计算技术提供业务数据时，应当建立技术风险评估和控制策略，明确安全不可验证、性能不可接受等风险的应对措施”。这反映了监管部门对隐私计算技术风险可控性的高度重视，技术应用方须建立相应的风险评估框架和应对预案，以符合行业监管要求。

算法黑箱与自动化决策规制：当隐私计算与人工智能技术结合用于自动化决策时，其算法不可解释性可能违反个人信息保护法关于自动化决策透明度和公平性的要求。隐私计算环境的复杂性使得实现上述要求面临技术挑战，特别是如何向数据主体通俗解释决策逻辑的同时不泄露商业秘密或削弱隐私保护效果。

3.3.4 跨境数据传输的合规壁垒

隐私计算技术在跨境场景中的应用，面临着一个核心挑战：如何与现行数据出境监管框架实现有效协调。具体而言，其合规要点主要集中在以下两个方面——监管认定与合规路径。

技术方案与跨境监管的适配性：数据出境监管通常以数据跨境流动为规制对象，而隐私计算技术可以支持“数据不出域”但“价值跨境”。目前，监管机构尚未明确认可隐私计算技术可以替代传统的数据出境合规路径。例如，即使采用联邦学习等不出境原始数据的技术，其模型参数、中间结果或最终洞察的出境，仍可能被认定为数据出境行为，从而需要通过安全评估、认证或标准合同等法定机制。《中国人民银行业务领域数据安全管理办法》对跨境传输采取了严格立场，规定“重要数据出境需申报安全评估，且不得通过技术手段（如数据拆分、格式转换）规避监管”。这表明监管部门对技术规避行为的重视，技术应用方需审慎评估隐私计算在跨境场景中的法律地位，避免因错误认定而导致的合规风险。

国际规则对接与司法管辖冲突：隐私计算技术的跨国应用还面临不同法域监管要求差异的挑战。例如，加州消费者隐私法案 (CCPA) 的最新修订引入了针对风险评估的新要求，与国内规定存在差异。当隐私计算技术涉及多个法域时，如何同时满足不同司法辖区的合规要求，成为企业面临的实际难题。特别是在执法调取、司法协助等场景下，不同法域对隐私计算环境下数据的访问权和控制权

可能存在冲突，以至于相关机构陷入两难境地。

综上所述，隐私计算技术作为数据要素市场化的关键赋能技术，其稳健落地需要在技术创新与合规稳健之间寻求到平衡点以后，创造商业价值。面对匿名化标准不明、授权机制适配困难、技术可验证性不足、跨境规则不确定等挑战，商业银行应采取必要合规策略，在创新与规范之间找到平衡区间，真正实现其促进数据价值安全释放的潜力，为数字经济发展提供可持续动力。

第四章

商业银行隐私计算 应用新近发展与实践亮点

4.1 全景探析：商业银行隐私计算核心应用场景

4.2 价值解构：隐私计算破解业务痛点的赋能机理

4.3 业界纵览：国内外隐私安全计算应用案例

4.4 实践路径：商业银行与科技企业典型应用场景案例

CHAPTER 4

挑战虽多，须直面应对。当前，隐私计算在规模化应用的道路上面临着规模、效率与安全“三重张力”的严峻挑战，数据供需两侧的信任壁垒、异构平台的互联困境以及合规边界的模糊性，共同构成了技术落地的现实阻碍，但这并未阻挡商业银行技术创新与业技融合的步伐。

近年来，一些行业先行者们迎难而上，沿着战略先行、业务驱动、沙盒辅导的合规路径，在技术优化、生态共建与金融为民的数字化实践中寻找破局之道，在普惠金融、精准营销、联合风控等多个关键领域，将概念验证转化为具有显著业务价值的规模化应用。本章接下来将剖析这些典型案例，展示商业银行如何在迷雾中开辟可行路径，将挑战转化为机遇。

当前，部分商业银行正将隐私计算技术深度嵌入业务全链条：在普惠金融领域，通过与税务、工商等政府部门的安全协作，实现对中小企业信贷风险的精准评估；在零售银行场景，借助联邦学习技术与互联网平台共建营销模型，激活存量客户价值；在风控环节，运用多方安全计算构建同业反欺诈联盟，提升风险联防联控能力。这些实践不仅突破了传统数据合作的合规瓶颈，更创造了切实的业务价值。值得注意的是，技术落地的过程也推动着银行内部体系的升级。领先银行已着手构建融合多技术路线的隐私计算平台，通过标准化接口实现与外部生态的高效对接。同时，配套的数据安全治理体系持续完善，覆盖技术选型、合作方管理、合规评估等全流程，为技术创新构筑安全底座。

尽管在标准统一、商业模式等方面仍需持续探索，隐私计算技术已然成为商业银行数字化转型的重要基石。其发展轨迹证明：以解决实际业务痛点为导向，以安全保障为底线，以生态协作为路径的技术创新，终将在金融领域结出硕果。下面将深入探析隐私计算技术如何具体赋能银行业务，并全景式展现新近几年其覆盖核心业务链条的应用场景。

4.1 全景探析：商业银行隐私计算核心应用场景

纵观金融领域，聚焦商业银行近年来针对数据流通与应用方向的实践探索，整理隐私计算技术在商业银行的应用落地概览，可以将整体业务场景分为以下 5 种类型，分别为营销获客、客户画像、智能风控、授信审批以及其他综合服务。

隐私计算技术助力金融机构建立“可信供给—可控使用—合规分析”的全生命周期的防控体系，数据要素与安全技术协同，正在迸发推进数据要素流通的新活力。例如，某大型银行部署了隐私计算平台，在批量获客、反洗钱、风控审批等场景中实现了与第三方数据的安全融合。由于平台在设计之初即满足个人信息保护法的相关规定，后续数据引入与应用效率大幅提升。同时，安全引

入的数据使智能决策层模型的准确率有效提升。这一安全赋能业务的实践，正逐步改变金融机构对安全投入的价值认知。



图11 商业银行隐私计算核心应用场景

4.2 价值解构：隐私计算破解业务痛点的赋能机理

金融业是典型的数据密集型行业，其核心竞争力很大程度上依赖于对数据的深度挖掘和利用。数据的高效合规利用是当下找到业务增长点的核心路径。其赋能商业银行的核心机理在于，通过一系列创新技术架构，系统性重构数据协作的范式，面对“安全与效率”的平衡难题，联邦学习、多方安全计算与可信执行环境等技术路径提供了差异化的解决方案，使银行能够在特定场景下，于安全红线与性能要求之间找到最优解。针对“数据孤岛”与“信任不足”，其“数据可用不可见、计算可控可计量”的核心特性，为跨主体数据融合提供了不可或缺的技术背书的信任基础，使得在缺乏天然信任的环境下开展合作成为可能。对于“合规界定模糊”与“跨境传输”等监管关切，技术本身为实现匿名化处理、构建清晰的授权与审计链条、以及验证技术可控性提供了可验证、可审计的方法与工具，为合规实践提供了具象化的支撑。

隐私计算的赋能原理，正是将上述普遍存在的业务痛点，转化为可技术化解的模块化问题。聚焦上述金融行业典型应用的五个类型，其业务痛点以及破解方案汇总如下表：

表2 隐私计算在金融行业典型应用

业务场景	业务痛点	隐私计算技术的破解方案
营销获客	1. 潜在客户难寻，数据“荒岛”林立。 2. 客户画像模糊，营销策略粗放。 3. 数据融合的合规风险与客户隐私担忧。	1. 匿踪查询与隐私集合求交：银行可以在不暴露自己客户名单的情况下，向数据提供商（如大型互联网平台）发起匿踪查询，确认某些高潜客户是否在该平台存在，并获得其加密后的标签。或者使用 PSI 技术，安全地找到银行客户与平台用户的重合群体，用于联合建模。 2. 联邦学习建模：银行与媒体、电商平台等通过联邦学习联合构建客户响应模型或流失预警模型，在保护各方用户隐私的前提下，提升营销活动的响应率和客户留存率。
客户画像	1. 信息不全面：针对无信贷记录的“白户”客户，仅靠自身存款、理财等有限数据难以做出准确的风险判断。 2. 数据融合的“高敏感性”与“合规壁垒”，使得数据“碎片化”与“孤岛化”。	1. 利用多方安全计算（MPC）技术，多家金融机构可以在不泄露各自客户明细数据的前提下，安全地计算出一个客户在不同机构的总资产、总负债、平均现金流等关键指标。 2. 应用隐私保护技术。银行、工商、司法等部门可以将各自掌握的局部关系数据（如企业股东、担保关系、交易流水）在加密状态下进行融合与计算，共同构建一个安全的、全局的企业关联关系图谱。通过分析这个加密图谱，可以识别出隐藏的共同实控人、复杂的担保圈和潜在的风险传导路径。
智能风控	1. 黑产攻击跨机构流窜：欺诈分子和洗钱团伙通常会利用银行间信息不互通的漏洞，在不同银行间快速转移资金、分散交易，以规避单家银行的监控阈值。 2. 传统的“数据归集”或 API 直接查询方式，存在原始数据泄露、滥用或被合作方留存的核心风险。银行既担心客户隐私泄露引发法律纠纷，也担忧自身核心客户数据资产在合作中流失。	1. 多方安全计算与联合图计算：多家银行可以在隐私计算平台上，使用多方安全计算或隐私保护下的图计算技术，安全地计算跨机构的交易总笔数、总金额，或者共同构建一个加密的交易关系图谱，识别出隐藏在多家银行背后的复杂欺诈团伙或洗钱链条。 2. 提升侦测效率：从“单点防御”升级为“联防联控”，大幅提高对跨机构、隐蔽性强的金融犯罪的识别能力和效率，降低资金损失。 3. 合规共享情报：在满足匿名化、去标识化等要求下，仅输出风险标签或加密后的关联结果，而不泄露任何一方的原始明细数据，实现合规的情报共享。
授信审批	1. 银行内部的审批数据主要依赖于央行征信报告、历史信贷记录和客户提交的申请材料（如收入证明）。这些数据多为静态的、强金融属性数据，缺乏能反映客户实时信用状况、行为偏好和稳定度的弱金融相关数据（如消费、社交、税务、政务数据）用于模型预测。 2. 模型偏差：仅使用银行内部数据训练的模型，可能存在偏差，导致对某些客群的评估不准确。	1. 安全融合多方数据：利用联邦学习技术，银行可以与外部数据源（如互联网平台、其他金融机构）在不交换原始数据的情况下，共同训练一个更强大的风控模型。各方的数据保留在本地，仅交换加密后的中间参数（如梯度、权重），最终得到一个全局共享的、性能更优的模型。 2. 实现“数据不动模型动”：将银行的金融模型安全地部署到外部数据环境中进行计算，得出营销建议，而原始数据不发生转移。
综合服务	1. 例如银行的核心业务，代发工资业务，由于合规以及法规的要求，目前该部分数据无法激活，没有办法通过对工资分析对企业提供一定的洞察分析。 2. 再比如银行的投资理财业务，投后联合分析难以开展，银行（销售方）与资产管理公司（产品方）希望联合分析产品的表现和客户持有行为，以优化产品设计和客户服务，但双方都不愿或不能共享各自的客户明细数据。	1. 实现隐私保护的产品精准匹配：利用多方安全计算，将代发客户工资收支流水数据加密后的风险标签与理财产品加密后的风险等级进行安全匹配，在不暴露敏感信息的前提下，输出匹配结果，真正做到合规的“适当性管理”，用于精准营销等场景。 2. 安全进行投后联合分析：银行和资管公司可以通过隐私计算平台，安全地分析客户群体的行为模式（如哪些特征的客户容易赎回、产品收益与客户行为的关系），输出加密后的宏观洞察，共同优化投资策略和客户服务。

4.3 业界纵览：国内外隐私安全计算应用案例

隐私计算技术的价值，正是在尊重数据安全与合规边界的前提下，为破解上述困境提供可行的技术路径。相关安全技术能够在原始数据不出域的前提下，实现多方数据的联合建模与隐匿查询。这不仅有效回应了数据安全与隐私保护的监管要求，更为构建跨机构的数据信任协作机制奠定了基础。尽管在性能优化、平台互通和商业模式创新等方面仍需持续探索，但隐私计算已展现出推动数据要素安全流通的独特价值，也在全球范围内涌现出了一系列落地案例。

4.3.1 国内隐私计算典型应用案例

根据公开资料，商业银行等金融机构在隐私计算等安全技术领域的典型案例，如下表 3、表 4：

表3 隐私计算在商业银行典型案例概览

商业银行	应用场景	具体案例
工商银行	智能风控 反诈合规 资金流水核验服务	工商银行与银联合作，工商银行提供商户标签数据，银联提供收单商户特征数据，双方构建商户违约评分模型。与原有模型相比，小微商户业务模型性能以及户均授信均有不同程度的提升，另外工商银行与银联合作，融合工行的征信、流水等信息与银联支付交易信息，联合打造“刷单套现”精准识别模型，有效防范欺诈风险。
农业银行	集团内部协同 跨行业务风险	1. 农业银行以客户号作为 ID，利用隐私求交筛选出集团内开展共同业务、存在信用余额的客户交集，利用多方安全计算，实现境内外的信用总账计算。实现客户境内外信用总账统一管理，为贷前、贷中、贷后业务决策与风险管控提供支持。 2. 农业银行在信贷风控领域应用多方安全计算技术对行内外业务进行有效风险管控。针对对公客户跨行资金流水真实性验证需求，农业银行联合国家金融科技风险监控中心等机构，搭建基于多方安全计算的跨银行核验平台。该平台在确保原始数据不出域的前提下，通过加密查询值比对，验证客户在其他银行的资金流水数据真实性，辅助授信评估。
中国银行	精细化运营 精准风控 资金流水核验服务	1. 中国银行依托开放银行建设，试点隐私计算互联互通应用。其与京东分别部署隐私计算平台，采用手机号作为唯一的用户标识符，通过隐私求交将中行信用卡交叉销售白名单匹配京东渠道目标客户，赋能京东对目标客群进行营销触达。 2. 中行与支付宝通过互联互通隐私求交方式，采用手机号作为唯一的标识符，结合双方数据精准识别目标促绑、睡眠客群，通过支付宝收银台、充值、缴费等推广渠道完成目标客群的智能触达，宣传中行信用卡支付权益，吸引用户用卡并享受支付优惠。
建设银行	精准营销 信贷审批 反诈合规 精准风控	1. 建设银行上海大数据智慧中心牵头，建信金科提供技术支持，联合建信基金，利用隐私计算技术进行了集团一体化建模探索，参与联合建模的双方在生产环境中验证了隐私计算技术在金融产品智能营销场景的可行性。同时在生产环境中利用真实业务数据进行了基于用户特征维度拼接的纵向联合建模，针对“速盈客群价值提升场景”，实现跨双方隐私计算纵向模型建立，定位目标客群，助力建信基金侧的客户价值挖掘和提升。 2. 基于匿踪查询，隐私求交等隐私计算技术，建设银行应用总行与建信养老双方的客户数据，开展基于母子联邦的建信养老个人年金客户的个人养老金精准营销大数据项目，进行个人养老金精准营销。

商业银行	应用场景	具体案例
交通银行	普惠金融 精准营销 风控反欺诈 客户隐私保护	交通银行基于企业级隐私计算平台，积极推进数据要素跨机构融合，已经在交行总分行与政务机构、三大运营商、支付清算机构、金融机构、新型科技公司等多方的数据合作中得到了广泛应用，支撑数字金融、科技金融、普惠金融、养老金融、风控反电诈、人脸安防等多个领域成功落地应用。 1. 聚焦科技型企业融资需求，在全同态密文计算技术的加持下，融合公积金、水电气等行内外多方数据，对科技型企业客户开展多维度评价。 2. 将税务、销售、工商、司法数据和行内标签有机结合，通过多方安全联合统计决策技术，实现“主动授信”+“主动营销”的技术方案。 3. 采取“全匿随机群体相似度计算”技术，融合了外部相关数据，获得相似客群包，由交行进行营销投放，进一步提升基础客群客户的经营效率。 4. 在风控反欺诈领域，交通银行与运营商合作，运用隐私计算技术，通过联邦学习训练数据构建诈骗人群模型和易感人群模型，建立识别电诈交易新手段，加强机构间反欺诈生态建设，维护金融秩序，保护人民群众财产安全。 5. 将人脸信息等隐私数据分片后分别存储在交行与其他机构节点，并通过多方安全计算的联合查询判断技术进行验证，使得双方无需交换存储的特征即可完成特征比对，在不改变现有流程和运行体验的前提下，提升客户端图像识别验证的隐私保护能力，降低了信息泄露风险。
邮储银行	精细化运营	邮储银行通过隐私计算技术与外部机构（如通信运营商、互联网渠道商）共享欺诈特征，构建联合风控模型。例如，利用匿踪查询技术实时校验可疑账户，降低涉案账户数量。以及与支付宝合作进行隐私求交，针对交集客户分级营销，匹配营销资源进行促活。
招商银行	精细化运营 反诈合规	招商银行通过银联云闪付生活营销活动促活睡眠用户。与支付宝进行隐私求交，在支付宝平台引导客户绑卡。与字节跳动基于联邦建模对客户价值精确识别，并制定更加合适的 RTA 出价策略，实现信用卡广告的精准投放、广告费用降本增效。用客户手机号作为 ID，利用匿踪查询共享交易信息及黑名单、风险等级标志等信息，通过联邦学习构建反欺诈模型，提升银行反欺诈反洗钱、防范多头抵押多头贷款等领域能力。
民生银行	精准营销 精细化运营	民生银行与中国银联使用各自隐私计算平台，基于开源算法实现互通。构建联邦客户资质分层模型，采用前置策略模式进行客群前筛，择优导流。前筛模型上线后，导流贷款申请通过率提升，件均授信增加。民生银行与某互联网机构合作，落地了隐私计算安全求交功能的算法互通，应用于支付权益投放等场景，促进睡眠户激活、客户潜力提升。探索公域流量联合运营，助力营销资源精准投放。
浦发银行	精准营销	浦发银行波塞冬隐私计算平台与银联隐私计算平台，基于开源算法实现互通。浦发与银联基于隐私求交、联合分析算法，实现双方数据的安全撞库和联合分析，挖掘银联侧用户资产特征、消费特征类数据，结合浦发侧用户金融资产、交易表现类数据，针对资产等级、消费规模、经营者标签等特征，产出高潜客户名单。通过专属营销活动配置，叠加线上渠道触达，开展有针对性的线上经营。
浙商银行	反欺诈 风控审批	浙商银行与某电信运营商利用联邦学习的隐私计算技术，在保护用户数据隐私、原始数据不出本地的前提下，合法合规地从多源数据中训练出更加准确的联合风控模型，用于小微企业信贷风控建模，为供应链融资中风险防控等场景的模型补充数据内容，打造用于供应链金融的动态风险监控产品，进一步增强小微企业信用评估能力，扩大银行普惠金融服务半径，切实提升小微企业获得融资服务的效率。
微众银行	信贷审批 精准风控	为了解决小微企业贷款风控数据不足的问题，微众银行联合对家外部合作伙伴一起搭建基于联邦学习的风控模型。以微众银行和发票信息服务公司的合作案例为例，微众银行具有标签 Y 和央行信贷特征 X3，发票信息服务公司拥有发票相关数据 X（例如 X1、X2）双方基于开源的联邦学校系统 FATE 进行纵向联邦建模，多个机构可以构建联合模型而无需共享其数据。通过联邦建模，扩大了可用的数据特征，随着模型效果的改善，贷款不良率明显下降。

表4 隐私计算在相关机构典型案例概览

机构名称	应用场景	具体案例
北京国际 大数据交易所	数据资源流通 生态体系	北数所数据交易平台 IDeX 系统，该系统融合应用隐私计算、区块链、测试沙盒等技术，构建全链条交易服务体系，在保障数据隐私安全前提下交易流通跨域数据。基于多方计算技术的数据安全融合平台可作为各行业数据的归集、处理和共享的支撑平台，在保障数据安全的同时，充分释放其计算价值。
工银安盛	精准营销	工银安盛应用联邦学习方案，在不泄露原始数据前提下，有效融合自身数据与工商银行数据进行联合建模，精准分析了集团客户投保偏好、投保能力，有效挖掘了健康险潜在投保客户群体。实际成效方面，该保险营销模型较集团现有模型准确率提升约 16 个百分点，为集团协同构建精准营销体系有效探索了先行示范路径。
美团	精细化运营	基于美团企业版与银联在支付生态与本地生活服务的战略互补性，以及银联多个支付及认证服务等已有合作基础，双方通过隐私计算平台实现商户与支付解决方案的精准对接，推动线上线下服务融合，既给餐饮商户带来更多补贴和流量，也同时满足了企业消费场景下的支付诉求。
蚂蚁	精细化运营	蚂蚁与平安蜂巢基于隐私计算安全技术构建数据要素流通平台，基于蚂蚁提供的隐语算法镜像实现互通。车险市场饱和，利用隐私计算融合双方数据构建车险联合定价模型，提升市场竞争力。双方基于同一算法镜像，集成至各自平台侧，通过调用算法镜像的接口进行联合计算，分阶段对新能源车、燃油车车险构建联合定价模型。
字节跳动	广告投放	字节跳动同多个股份制行通过联邦建模的方式对客户精确识别，并制定更加合适的 RTA 出价策略，实现广告的精准投放、广告费用降本增效。经过联邦建模精准识别的目标客户，广告投放成本降低了。
腾讯	普惠金融平台	腾讯作为中国领先的科技公司，在隐私计算领域进行深耕，腾讯和顺德区政府紧密合作，建立了一套基于联邦学习的普惠金融平台，促进营商环境持续优化项目。 (1) 腾讯侧：提供联邦学习平台，融合顺德区的政务数据，申请企业数据，银行业务数据，建立实时进件分析和风险控制模型。 (2) 政府侧：提供政务数据，用于联邦建模特征，再通过政务云部署进件审批模型，实际应用。 (3) 企业侧：前端申请注册，业务信息通过政务云输出联邦建模特征。
洞见科技	隐私计算 智能风控平台	洞见科技建立了贯穿普惠金融信贷全生命周期的大数据隐私计算智能风控平台，与国内多家银行合作，将银行的行内信贷用户申请信息、存款、理财、行为偏好等数据和工商、运营商等其他合作方数据进行了安全融合，极大丰富了普惠金融信贷用户风控数据特征维度，扩大了其他合作方数据开放程度，从安全融合到智能发现，再到决策应用，全面提升了多方大数据在行内的普惠金融风控应用价值和效率。
国家金融科技 风险监控中心	金融行业 隐私计算平台	北京国家金融科技风险监控中心有限公司、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、交通银行股份有限公司、华控清交信息科技（北京）有限公司运用多方安全计算技术搭建金融行业隐私计算平台，在确保各方原始数据不出域的前提下，验证对公客户提供的他行资金流水数据真实性，并将对公客户提供的他行资金流水数据与该客户在行内历史数据进行关联和分析，辅助开展对公客户授信评定、融资需求评估等，提升银行智能化风控水平。

4.3.2 国外隐私计算典型相关实践

国际方面，隐私计算应用主要集中于欧盟，英国、美国、澳大利亚、葡萄牙，新加坡等的部分银行。例如，一些跨国银行利用联邦学习技术开展反洗钱模型联合训练，以及欧美银行业在开放银行框架下采用共享数据的案例等。这些案例体现了隐私计算在国际银行业应用的成效和价值。

表5 国外隐私计算技术相关实践概览

机构	应用类型	具体实践
SWIFT与13家 全球银行联盟	跨境支付 联合反欺诈	在与 13 家全球金融机构合作的试验中，团队采用了隐私增强技术，使各机构能够安全地跨境共享欺诈情报。Swift 与 13 家国际银行在 1000 万笔测试交易的试验中，将实时欺诈检测能力提高了一倍。其中应用到的隐私增强技术使各机构在保持端到端隐私和安全的前提下，实现交易数据共享。大规模应用该技术可构建全球金融联合防欺诈体系，高效打击犯罪行为，显著降低行业欺诈成本。
澳大利亚交易 报告与分析中心， 联合28家银行	跨机构反洗钱 与反金融犯罪	澳大利亚交易报告与分析中心牵头，28 家金融机构参与，包括澳新银行等，通过隐私增强技术连接不同机构的数据库，识别跨两个或多个账户的可疑资金链接，追踪资金在不同金融机构账户间的流动，同时保护客户隐私。项目旨在从上亿账户中获取洞察。该项目提升了各参与机构在欺诈和反洗钱调查中的筛查效率，快速识别出需要优先调查的案件。
富国银行	AI 客服数据安全	富国银行的 AI 助理“Fargo”是银行业将隐私计算理念大规模应用于生成式 AI 的典型案例。其核心在于通过一套“隐私优先”的系统架构，在调用外部强大 AI 模型的同时，确保客户敏感数据全程不外泄。AI 助理“Fargo”年互动超 2 亿次。主要用到的隐私安全技术是隐私优先设计，在数据接触外部 AI 模型前，在银行内部完成清洗和匿名化。后续 AI 编排层通过内部系统先清理和标记客户语音中的个人信息，仅将匿名化意图传给外部 AI 模型，防范原始数据泄露。 法国兴业银行主导的 DANIE 联盟案例，该项目 2020 年左右启动，是一个由重要金融机构推动的行业级协作实践。应用的核心技术是，可信执行环境（TEE）结合加密技术，多家银行通过隐私计算技术，在可信执行环境的保护下共建数据平台，以应对欧盟的严格数据合规要求。项目主要应用于以下两个方向： 1. 提升数据质量：协同核对和修正数据，以满足监管报告要求。 2. 联合反洗钱与欺诈检测：在保护客户隐私的前提下，跨机构识别可疑模式。
葡萄牙中央银行	运用隐私计算技术 为外部研究人员提 供敏感微数据访问 支持	葡萄牙中央银行的案例，是其微数据研究实验室（BPLIM）为解决“研究需要数据”与“隐私法规严格”之间的矛盾而设计的创新方案。其核心在于通过一套“脚本准备 - 后台执行”的工作流程，让外部研究人员能在不接触原始机密数据的前提下进行分析。其核心流程创建了一套安全数据环境与匿名化处理后的合成数据，创建与原始机密数据结构、统计特性一致的匿名化伪数据集供研究准备，研究人员编写的脚本经审查后在原始数据上运行，确保数据在分析中不被直接接触。
金融数据交换 (FDX) 联盟	数据集成	金融数据交换（FDX）联盟：这是一个非营利组织，汇集了超过 200 家金融机构、金融科技公司和数据聚合商。FDX 制定了一套通用的开放金融 API 标准，从基于隐私计算技术的安全数据接入，到集成式的 API 输出，让消费者可以安全、便捷地授权第三方应用访问其银行账户数据，从而享受个性化的财务管理服务。
新加坡金融 管理局（MAS）	金融科技沙盒监管	允许金融科技强化技术水平，严格执行隐私计算技术，在数据流通安全可控的情况下可以在完全符合传统监管要求的情况下进行创新测试，旨在促进金融科技企业的发展。

4.4 实践路径：商业银行与科技企业典型应用场景案例

案例一：工商银行以隐私计算赋能业务创新，构建数据生态

工商银行作为全球资产规模领先的商业银行，其在隐私计算技术领域的实战应用，已从早期聚焦于内部或单点场景的试点验证迈向多场景、趋于规模化的业务深度融合与广泛生态连接，形成了涵盖多方安全计算、联邦学习、机密计算3大技术路线的行业标杆性技术体系，取得了显著的业务成效与良好的社会效益：对内，它将隐私计算技术能力封装为通用服务供数据运营平台等内部系统调用；对外，一方面牵头参与行业级“跨银行资金流水核验”项目，链接十余家主要同业，破解银行业共同的企业信贷风控难题；另一方面，基于隐私计算深度融合公积金、税务、产业链等跨领域公共数据，赋能联合风控、普惠金融等多业务领域场景落地，每年避免潜在损失、助力普惠信贷融资达数百亿元。这些实践共同描绘出一幅以技术驱动数据价值安全流转、以平台思维构建协作生态的清晰图景，标志着中国大型商业银行在数据要素时代的前沿探索。

（一）科创企业评分授信场景

科创企业大多属于轻资产型企业，企业核心通常是技术、人才等，银行在对其进行贷款授信时面临授信额度评估维度少、资产评估难、授信效率低等问题。利用隐私计算技术密态融合科创局的高新企业经营数据，根据原创的针对科技中小型企业融资产品预授信额度测算模型，进行联合计算得到企业评分，实现对科创企业的授信评分，并同步对目标企业开展精准营销。

成效上：业务在试点省份上线半年即获得千余户目标客户清单及其参考预授信额度，其中超一半非存量结算客户，累计发放贷款数十亿，极大助力对高新企业的拓户拓新工作，提升科创金融服务效率；建立了原创科创企业信用评价模型，支持科创企业良性发展，做好“科技金融”大文章。

（二）普惠金融场景

一是小微企业普惠信贷。传统“被动拓户”模式严重影响了普惠贷款的投放效率，外部数据的匮乏导致“拓新户”成本高，无法满足“精准、批量拓客展业”的发展目标；优质小微企业的资金需求远高于分行传统风控模型的授信上限，不能完全满足目标客户的资金需求，致使部分优质小微企业客户损失。应用隐私计算技术，安全融合北京金控的企业数据，从企业经营状况多个维度进行建模，排除高风险、低收益的小微企业，针对目标企业展开精准营销和贷款发放。最终实现了加大对小微企业的信贷投放，做好“普惠金融”大文章。

二是普惠创业贷。长期以来银企信息不对称问题始终制约小微信贷发展，小微客户自身财务不健全、抗风险能力较弱、公开数据源信息较少。针对小微企业线下提供的相关经营材料，商业银行缺乏信息交叉验证验真渠道，导致商业银行不敢贷、不愿贷。工行依托隐私计算技术，在获得客户完全授权情况下，采集客户个人及企业公共数据开展联合建模，为上海地区小微企业主、个体工商户等群体提供小额融资服务。运营至今，新增普惠有贷户以及放款金额大幅度增加；客户到店贷款操作效率提升70%，实现高效便捷的贷款服务体验。

（三）外汇风险联合防控

在“宏观审慎+微观监管”的监管框架下，工商银行利用隐私计算技术，建立监管机构和工商银行之间的数据融合通路，构建提前精准预警、由点及面完整追溯、名单信息高效共享的本外币一体化外汇合规风险联合防控体系，实现外汇合规风险联合评分模型，精准、全面、及时反映个人客户的外汇业务合规风险。

在结售汇资金的追踪方面，隐私计算平台基于黑名单标签传播的图联邦算法，外管局提供可疑结汇节点、工行基于人民币交易计算风险传导和可疑社区，从“合理性”角度切入，通过交易数据和海量外部数据的逻辑勾稽关系甄别其交易的真实性，以“数据不动、模型梯度动”的联邦学习技术训练二分类有监督模型，找到团伙性外汇资金转移线索，解决外汇合规风险防控精准性问题。

案例二：建行隐私计算平台的生态化演进

为突破单一技术范式限制、拓展数据协同边界，建设银行构建了基于隐私计算技术的数据平台，并于2022年对其隐私计算技术底座进行了关键性升级。平台支持联合建模、联合统计分析、匿踪查询、安全求交等多元化计算范式。这一平台的建成，从根本上解决了在原始数据不出域的前提下，进行更广泛、更深入数据价值挖掘的难题，为激活内外部数据要素、解锁复杂业务场景奠定了核心技术基础。

基于“数据与业务深度融合”的理念，建行构建了层次清晰、自主可控的企业级隐私计算安全平台，其架构自上而下可分为四层：

应用层：直接赋能业务前线，支撑精准客户画像、场景化获客、自动化审批授信及智能风控等核心业务应用。

服务层：作为能力中枢，将隐私计算能力封装为标准服务，与行内模型管理平台、数据管理平

台等系统对接，实现能力集成与调度。

算法层：提供强大的计算引擎，全面兼容联邦学习、多方安全计算等多种隐私保护计算框架，灵活支持查询、统计运算与联合建模等各类计算范式。

数据层：构筑坚实的数据基座，通过标准化接口，安全接入行内各业务系统数据以及外部合作方的多元化数据源。

该架构体现了“能力平台化、服务组件化”的设计思想，确保了技术对业务需求的敏捷响应与高效支撑。

平台能力也一定程度上转化为了业务价值，驱动了集团内外协同的创新浪潮。开展了诸多业务：

（1）与建信基金合作：通过安全求交锁定目标客群，并利用联邦建模构建客户转化模型，成功引导客户从货币基金向收益更高的非货币基金配置，提升了客户价值与 AUM。

（2）综合金融深化：为建信人寿、建信养老等子公司赋能，通过安全求交技术，在严格保护客户隐私的前提下，合法合规地将行内高净值或养老需求客群精准推荐给相应子公司，实现了个人养老金业务等战略领域的客户转化与综合开发。

（3）信托业务赋能：支持建信信托通过匿踪查询技术，在无需暴露具体客户信息的情况下，验证特定客户群体的行内信用评级分布，为产品设计与风险定价提供数据智能支持。

（4）小微金融服务创新：与美团开展深度合作，基于联邦建模技术，融合银行金融数据与互联网平台商业流水数据，共同构建商户信贷的准入与额度模型，为海量小微商户提供“快贷”等普惠金融服务，有效破解了小微企业融资中的信息不对称难题。

（5）零售业务促活：同样基于联邦学习，与美团在支付客户激活与促活场景进行建模，精准提升零售银行业务的活跃度与黏性。

（6）普惠金融与乡村振兴领域：在此领域，建设银行的核心目标是解决乡村客群缺乏有效信贷数据的痛点，通过与地方政府合作，安全引入政务数据，实现批量、精准的信贷投放。

建行山东省分行与新泰市政府合作，共同设立“裕农快贷—信用贷”信用大数据实验室。项目通过隐私计算技术，在保障数据安全的前提下，深度融合了当地的社会信用信息与银行的金融数据。通过对农户、个体工商户、新型农业经营主体等进行精准画像和信用评价，项目成功输出了 14 类细

分客群，最终实现了覆盖全市的“整县授信”。这一实践将社会信用数据有效转化为信贷依据，是金融服务乡村振兴的典范。

案例三：交通银行构建基于隐私计算的数据流通基础设施，重塑数据价值融合新范式

交通银行积极践行国家数据要素战略，立足数字化转型业务发展需要，充分调研各行业数据应用诉求，率先研究探索搭建基于隐私计算的数据流通基础设施，推进数据要素产业安全、健康发展。

2020 年初，交通银行启动建设隐私计算平台，平台采用开放式架构，支持快速部署、互联互通和场景定制，可以基于国产化集群，处理海量数据，灵活适配多种业务需求和快速对接异构平台。

在技术架构层面，平台研制了统一的数据资源、任务资源管理能力，实现不同数据类型、不同数据来源的配置化接入，支持应用系统对隐私计算能力的快速对接。平台研制了统一的任务管理能力，支持不同机构间快速实现隐私计算加密连接，同时支持项目管理、数据管理、任务管理、模型管理等能力，实现大型集团、机构间的单点接入，以及多层架构总分模式接入后的全局合作。平台通过开放式架构设计，实现算法模型与平台的解耦，可自定义算法组件，进行任务编排，进而更好满足多元业务场景的协同计算与建模需求，灵活适配多种模式及应用场景。

在核心技术方面，平台不仅全面集成了多方安全计算、联邦学习等当前主流的隐私计算技术，还在此基础上完成了全匿踪联邦建模、基于混淆能力的统计隐私集合求交、隐私保护的图节点、基于椭圆曲线的乘法三元组生成方法等多项技术创新：首创全匿踪联邦建模方案，实现隐私计算全流程匿名化，在不泄露交集 ID 的基础上完成联邦学习，确保数据的完全匿名性和保密性，该方案荣获了 2022 年度金融密码杯一等奖；首创基于混淆能力的统计隐私集合求交算法，使得参与方在不泄露任何一方在交集之外的任何信息的前提下，获得加密混淆后的交集集合；首创隐私保护的图节点的嵌入方法，使用多个参与方图节点 ID 进行联邦化的图嵌入训练，支持多方之间基于隐私保护的图融合需求；首创基于椭圆曲线的乘法三元组生成方法，实现加密算法国产化，可以根据多方安全计算的客体数据规模来灵活选择乘法三元组的取值空间大小。后两项已获发明专利。

在性能方面，平台设计了适用于全场景应用的隐私计算技术集群架构，支持亿级数据的求交和查询，千万级的数据联合建模，在此基础上能够支撑海量数据批量、准实时、实时预测，联机响应时间控制在较低水平，缓解了隐私计算工程化难题及性能困境，满足金融等行业对效率的要求，为推进数字数据要素流通发挥价值潜力奠定了坚实基础。

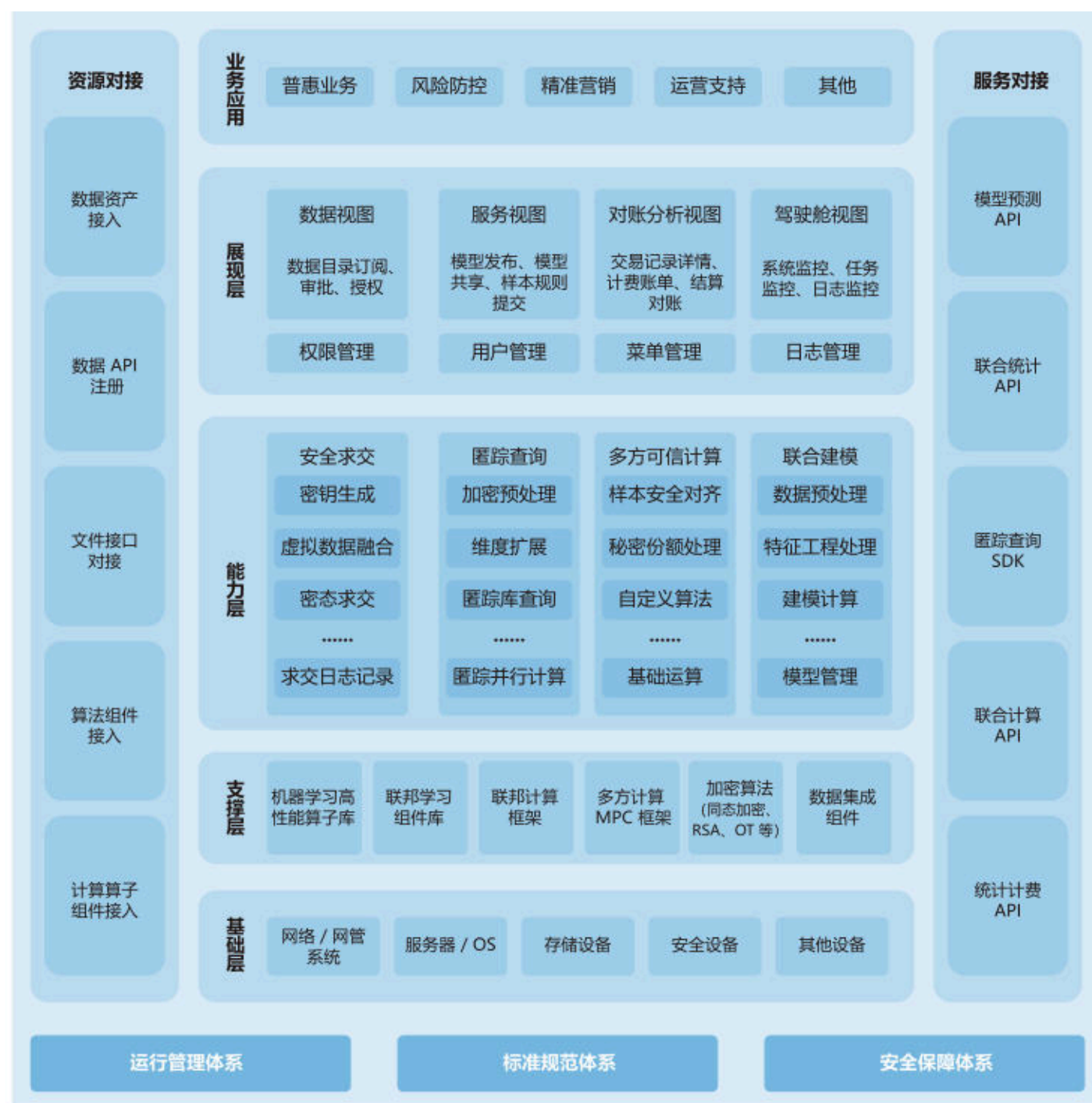


图12 交行异构平台架构示意图

交通银行基于企业级隐私计算平台，积极推进数据要素跨机构融合，已经在交行总分行与政务机构、三大运营商、支付清算机构、金融机构、新型科技公司等多方的数据合作中得到了广泛应用，支撑数字金融、科技金融、普惠金融和养老金融等领域成功落地多项业务应用，实现了跨机构、跨

行业的数据要素安全流通和价值挖掘，让数据“可用不可见”，充分显示隐私计算在金融行业应用的巨大潜力。

（一）科技金融

在科技金融领域，交通银行大力响应“科技—产业—金融”的良性循环，聚焦科技型企业融资需求，在全同态密文计算技术的加持下，融合公积金、水电气等行内外多方数据，对科技型企业客户开展多维度评价，实现“主动授信+精准触达”的普惠金融业务模式创新升级。该项目入围了辽宁省人民银行金融科技监管工具创新应用项目。该项目成效显著，大幅提高了科技类企业评价的及时性与准确性，触达覆盖度和效率实现从“零星营销”向“智能批量”转变。

（二）普惠金融

在普惠金融领域，交通银行针对缺少客户了解、预授信额度不准确等痛点问题，将税务、销售、工商、司法数据和行内标签有机结合，通过多方安全联合统计决策技术，对科技型小微企业开展多维度评价并实现“主动授信”+“主动营销”的技术方案。本项目形成“数据筛—精准选—预核额—在线办—线上管”的普惠金融授信业务模式，作为全行主动授信策略的标杆场景，在全行多个分行开展推广。

（三）数字金融

在数字金融领域，针对“基础客群资产提升识别场景”，交通银行首次创新“全匿随机群体相似度计算”技术，融合了外部相关数据，对借贷需求待识别存量客群进行借贷意向评估，并根据评估结果进行精准营销，进一步提升交通银行基础客群客户的经营效率。在本场景中应用的全匿踪随机群体相似性算法实现了混淆求交组件，相比传统安全求交，整个计算过程中无任何个人信息泄露的风险，实现了合规增强的效果。

（四）养老金融

在养老金融领域，交通银行与外部合作伙伴基于隐私计算平台技术，得到潜在用户样本群进行营销。除了对潜在用户样本群扩大营销曝光力度，提供权益服务外，前端营销页面还嵌入了客户经理企微添加步骤，在提高个人养老金账户开通量的同时，进一步为目标客户提供交通银行后续增值服务。该项目有效提高了个人养老金账户开通量和缴存金额，扩大了养老金融服务的覆盖面。

（五）风控反欺诈

2021 年以来人民银行相继出台多项法律法规、通知、办法打击反电信诈骗。交通银行与运营商开展合作，运用隐私计算技术，通过联邦学习训练数据构建诈骗人群模型和易感人群模型，建立识别电诈交易新手段，加强机构间反欺诈生态建设，服务实体经济服务普惠民生，维护金融秩序，保护人民群众财产安全，构筑反诈高地。该项目针对“易感用户+欺诈人群+可疑银行卡账户”，构建了“事前+事中+事后”全流程体系，并且通过“高风险止付、中风险介入、低风险提醒”的模式全面防控欺诈事件，从而保护客户利益减少客户损失。

案例四：某科技企业推出基于隐私计算的数据智能应用一体机

某科技企业自成立以来深耕隐私计算领域，通过软件定义硬件，推出数据智能应用一体机（InsightBox）融合了计算、网络、存储等硬件资源与洞见 InsightOne 隐私计算软件服务。科技企业深度优化 InsightOne 平台隐私计算算法，与高性能加速卡统一整合、调动，实现大规模分布式加密计算或训练，突破网络传输的通信瓶颈，提供十亿级别数据量的隐私计算业务应用能力，满足政府与企业在数据协同、共享、交换等场景的高性能计算需求。

该应用一体机内置“隐私计算+区块链”的数据平台，即可用于一站式交付又可助力于各机构上线大数据智能风控产品，平台有效联合工商、税务、水电、司法、运营商、征信机构等外部大数据，构建风控用户画像、风险规则和信用评分模型，帮助银行更加安全、智能地评估信贷用户的风险状况。

基于该平台的能力，科技企业助力雄安数融通共创平台首发上线，探索城市级可信数据空间新范式，为构建典型应用场景牵引，发挥公共数据的引领作用，推动公共数据、行业数据、企业数据的深度融合与创新应用，雄安新区城市可信数据空间综合服务平台——雄安数融通共创平台首发上线。

该平台作为国家数据局可信数据空间创新发展试点的重要组成部分，是全国首批城市可信数据空间创新发展试点中率先上线的技术平台之一，为雄安新区进一步构建全域融合、动态更新的城市数据资源体系，以及城市建设、运营和治理体制改革提供了有力支撑。

在运营模式上，平台创新采用专区化的运营模式，中国雄安集团数字城市科技有限公司联合中矿大数据、星网数科、联通数智、中移集成、电信数城、洞见科技等龙头企业共同运营。截至目前，已有 17 家头部企业签约入驻，并启动城市规划与交通出行、空天信息、地理信息、通信等 11 个重点领域专区的运营工作，上架遥感影像产品、高精地图、水体检测数据服务、道路检测数据服务等 50 余款典型数据产品与服务，有效促进了跨领域数据汇聚、流通与价值释放。

在技术支撑方面，平台深度融合隐私计算、数据沙箱、数字身份、使用控制、区块链等先进技术，打造“全程可控、安全可信、多方接入、全域可感、融合共创”的城市数据流通环境，构建全域融合、动态更新的城市数据资源体系。通过强化可信管控、资源交互、价值创造等能力，为数据要素的安全有序流通与价值转化提供保障，助力城市精细化管理和智能化发展。

作为全国城市数据要素流通与市场应用的重要探索，雄安数融通共创平台致力于形成可复制、可推广、开放包容的“雄安范式”。未来，平台将立足雄安，面向全国，持续发挥其作为数据要素流通关键枢纽的核心功能，与各方共同构筑数据产业生态，加速数据价值释放，助推数字经济高质量发展。

第五章

隐私计算技术趋势、 合规路径与发展倡议

5.1 技术趋势：驶向未来的航线图

5.2 建议商业银行战略先行、合规引领、 场景突破、生态协同

5.3 面向行业协同：共建可信数据空间生态

CHAPTER 5

本章基于前述实践，围绕技术、合规两大核心支柱，展望隐私计算实施路径与未来图景。需要明确的是，破解前述痛点困境、赢得数据要素竞争的关键，并非依赖于单一技术突破，而是一场关乎战略定力、组织韧性与生态格局的全面考验。未来的竞争，是数据协作生态的竞争。金融机构需要坚持以真实业务价值为导向，以可信安全合规为底线，以科技引领与业技融合为发展动力，方能在隐私计算的深化应用中行稳致远，克服当前的诸多挑战与瓶颈，形成可持续的核心竞争力。

5.1 技术趋势：驶向未来的航线图

隐私计算技术经过多年技术发展与应用试点沉淀，形成了以多方安全计算（MPC）、联邦学习（FL）、可信执行环境（TEE）、差分隐私（DP）4大技术流派为核心的多技术路径体系，目前处于从“技术可行”向“规模化商业应用”及“融合发展”的过渡阶段。

技术层面，各项技术均实现针对性突破：MPC通过SPDZ2k等优化协议将复杂计算效率提升10倍，可支持超千节点协同运算；FL借助FedProx等算法优化解决非独立同分布数据引发的模型收敛问题，在金融联合风控场景中可使违约识别准确率提升18%；TEE通过硬件升级与远程证明机制强化安全隔离，性能损失控制在2%-6%以内，同时支持TEE的国产信创硬件迅速普及，华为、曙光等均实现商业项目落地；差分隐私（DP）方面，基于f-DP的分析框架在去中心化联邦学习中将所需噪声量大幅度减少（NeurIPS 2025），自适应噪声机制与动态隐私预算分配也在统计查询场景中有效降低了精度损失。更显著的是技术融合成为主流，如FL+MPC通过加密参数交换提升隐私强度；谷歌2025年发布的PPI系统（arXiv:2510.21684）即采用AMD SEV-SNP和Intel TDX等TEE技术进行硬件隔离计算，并对聚合结果应用差分隐私添加噪声，实现了计算过程安全隔离、发布结果匿名保护的双重防护机制，已成功部署于Pixel Recorder等应用的生产环境。

随着更多的商业化项目及更广泛应用需求的落地，隐私计算技术与区块链、量子计算等外部技术的互补式融合发展展现出强大生命力，在可预见的未来，“芯片-系统-平台”全栈软硬协同将加速发展，向智能制造、车联网、医疗保险等领域纵深渗透，跨行业、跨领域协作案例将不断涌现。隐私计算正从单一的数据安全技术升级为人工智能和可信数据空间等数字经济的基础技术手段，推动数据要素价值与隐私保护的协同发展。

5.1.1 隐私计算与区块链、量子计算、人工智能、可信数据空间等前沿技术的双向赋能融合

5.1.1.1 隐私计算与区块链技术融合

隐私计算技术强化了隐私数据保护，但数据在流转过程中的确权、定价、存证监管、可验证性等是困扰其发展的显性问题。另一方面，区块链技术由于上链数据的分布式存储特性，也存在隐私保护和数据安全的隐忧。

隐私计算与区块链技术的互补融合能较好地解决上述问题。区块链通过采用智能合约、共识机制、密码学等技术，实现难以篡改、可追溯、去中心化、公开透明等特性，较好地解决了隐私计算的过程监督及双方互信问题，而隐私计算则可以解决区块链上链数据的隐私增强和安全保护问题。例如，在联邦学习与区块链的融合案例中，隐私计算的密钥生成与分发、模型的聚合、模型贡献度计算等，通过区块链的智能合约，使逻辑公开透明，增强隐私计算任务的计算信任。任务信息、数据申请信息、授权信息、参与计算的数据信息、流程信息、过程数据、计算结果等，也可通过区块链进行记录与存储，上链信息可通过签名确认并与哈希值验证匹配，实现信息的不可篡改性。

5.1.1.2 隐私计算与量子计算技术融合

量子计算与隐私计算的结合可有效解决各自技术路线的防御性前瞻问题。以广泛应用的隐私集合求交（PSI）为例，当前的 PSI 协议多采用基于 RSA 或 ECC 等公钥密码算法，或融合不经意传输（OT）及不经意伪随机函数（OPRF），并辅以对称密码算法进行构造。然而，RSA 和 ECC 等公钥密码算法无法满足抗量子安全性，已成为抗量子时代潜在的安全隐患。在此背景下，结合抗量子密码学的安全特性与隐私计算的应用需求，发展具备抗量子能力的隐私计算协议显得尤为重要。随着新型密码技术的多方安全计算、联邦学习等隐私计算协议探索持续推进，涌现出一批具有代表性的研究成果，在安全协议、软硬结合、安全硬件等多个领域，抗量子密码算法的隐私计算关键技术取得了显著进展，尤其是基于格的隐私计算协议的突破，为技术实现提供了高效路径。一些金融机构已开始尝试将这些新技术应用于实际业务场景，比如银行间通过整合政府机构金融黑名单数据，采用基于抗量子加密技术的多方安全计算、隐私信息检索等，实现跨机构的黑名单共享能力。

目前量子计算与隐私计算的融合应用方式主要有二：一是使用高效、可靠、安全的后量子密码及数据签名算法，替代或结合现有的基于数论难题的传统密码算法，以确保数据在计算和传输过程中的安全；二是使用适用于量子计算环境的隐私增强技术，如差分隐私、后量子多方安全计算、后量子联邦学习等，以在量子计算环境下实现数据的“可用不可见”。抗量子密码迁移不仅仅是简单的算法替换，还涉及协议安全性分析、安全强度评估和资源消耗量化等复杂问题。尽管这些挑战存在，隐私计算作为一种新兴技术，其技术迭代空间较大，应用范围也在不断扩展。相较于传统信息系统，隐私计算领域进行抗量子密码迁移时，业务影响相对较小，迁移成本也较低，同时行业从业者对新

技术的认知程度较高。因此，隐私计算也被视为抗量子密码迁移的理想实践场景。

5.1.1.3 隐私计算与人工智能前沿技术融合

隐私计算同人工智能技术融合存在天然的需求，联邦学习等技术方案充分发挥了隐私保护同机器学习算法的各自优势。当前，人工智能技术快速发展，生成式人工智能在人类生产生活中的渗透率逐步提升，其隐私保护需求也逐步显现：一是在大模型训练过程中，往往需要多机构数据合作，如何在保证数据安全、隐私的前提下，确保模型效果和建模效率；二是在大模型推理过程中，如何确保个人和企业客户包含隐私信息的问题不被大模型所学习利用，同时又能获得高质量的答案；三是在大模型生态的外部插件、Agent、工具等调用过程中，如何保护数据信息、隐私安全。目前部分开源生态、研究机构、科技企业提出了基于隐私保护框架的大模型应用方案，主要技术路线有两种：一种是采用联邦学习机制进行模型训练及微调，构建联邦大模型（FedLLM）；一种是基于 TEE 机制构建分布式模型，或基于 TEE 进行不信任机制下推理。

与此同时，大语言模型在代码生成、数据分析等领域的突破进展，可赋能隐私计算技术应用的便捷化。在用户侧可分别基于本地大模型的 NL2SQL、数据分析智能体等能力，提供高效的代码编写、数据处理、数据分析服务，提升隐私计算平台的使用体验。

5.1.2 隐私计算作为可信数据空间的基础技术作用愈发显著

可信数据空间作为数据资源共享共用的一种数据流通利用基础设施和数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体，正日益成为推动数据要素市场化配置改革的核心力量，而隐私计算，正是可信数据空间的核心技术之一。自《可信数据空间发展行动计划（2024—2028年）》印发以来，全国可信数据空间发展提速，龙头企业、地方数据集团、专业服务机构、科研创新平台等各类主体积极开展布局，加快推进可信数据空间探索实践。可信数据空间形成的以数字合约、使用控制为核心的技术体系，具备以下典型特征：安全可信的数据流通使用，跨域跨空间的数据互联互通，多方参与的数据价值共创。

隐私计算与可信数据空间并非两个独立的生态，而是底层技术能力与上层架构的有机整体。隐私计算为可信数据空间提供“计算可信”与“数据可用不可见”的技术保障，解决数据在流通与计算过程中的隐私保护问题；而可信数据空间则在此技术基础上，构建涵盖规则、合约、治理与生态协同的完整体系，解决“流通的生态可信与合规”问题。简言之，隐私计算是可信数据空间不可或缺的基础技术能力，而非与之对等的并行生态。

二者之间的关系具体体现在以下三个方面：

一是技术嵌入：隐私计算成为可信数据空间的安全底层。当数据在可信空间内进行交换与联合分析时，联邦学习、多方安全计算、可信执行环境等隐私计算技术将被内嵌为标准化的安全选项，确保流通与计算过程始终处于加密或脱敏状态，从而将安全能力从可选配件升级为原生组件。

二是生态支撑：隐私计算赋能可信数据空间下的服务新业态。在可信数据空间的治理框架下，数据托管、合规认证、算法审计、价值评估等第三方专业服务得以发展，而隐私计算为这些服务提供了可验证、可审计的技术基础，形成了“技术 + 规则 + 服务”的完整产业生态。

三是标准统一：以可信数据空间战略推动隐私计算互联互通。国家推动的可信数据空间战略，其核心任务之一是形成互联互通的统一标准。这为当前碎片化的隐私计算市场提供了统一的“插座和接口”，降低了不同技术平台之间、以及平台与空间之间的对接成本。

5.2 建议商业银行战略先行、合规引领、场景突破、生态协同

当前，隐私计算在规模化、计算效率与商业模式上的挑战依然严峻，但这并未阻碍先行者的探索与创新。领先机构以实践证明：破局之道，藏于细节之中。本节在总结前期案例经验的基础上，从单一机构落地实践角度，提炼可参考的经验和模式，其核心点在于：将解决特定痛点的项目智慧，升华为可规模复制的体系能力。从长远看，从单点破冰到体系制胜，是技术价值兑现的必由之路。通过战略选择、组织协同与实施路径，跨越从“验证可行”到“推广可用”的鸿沟。

基于上述洞察，报告总结了五大核心支柱，系统性地回应了前期实践中的各项挑战，并以此构成落地行动框架。其具体内涵与相互关系见下图模型。

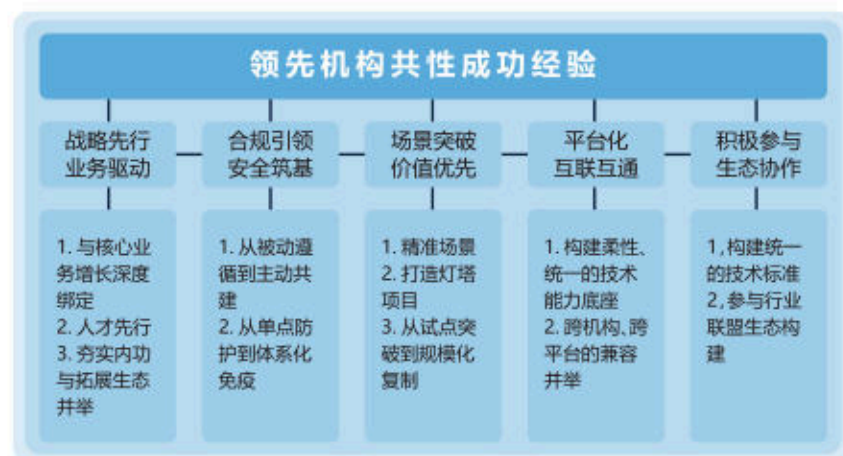


图13 领先机构共性成功经验五维图

战略先行决定了方向，业务驱动确保了价值，合规引领奠定了基础，平台化与互联互通提供了规模化能力，而最终的生态协作与标准共建则决定了价值天花板。五大维度协同互补，助力隐私计算从技术构想转化为商业现实。

5.2.1 战略先行、业务驱动

隐私计算的成功落地，根本上取决于其能否从一项前沿技术转化为驱动业务增长的助力引擎，秉持战略先行，业务驱动的顶层思路，实现从技术导向到价值导向的根本性转变。

第一，战略锚定：在推进隐私计算落地的进程中，需要战略引领，确保技术部署与银行核心业务增长深度耦合。从根本上摒弃“为技术而技术”的实验室思维，将隐私计算定位为支撑业务发展的战略能力，而非孤立的技术项目。成立由业务部门如零售、对公、风控、科技部门、数据管理部门共同参与的专班，将隐私计算置于银行发展的主航道上，获得持续的战略投入，促使技术投入转化为业务增长的动力。

第二，业务驱动：隐私计算的落地须坚持业务价值导向，将技术部署深度融入银行的主营业务链条。其成功不取决于算法的复杂度，而在于能否为实际业务场景创造可衡量的价值。建立从业务痛点出发、以价值验证为导向的工作机制，将技术能力转化为业务语言，打造从场景挖掘到价值回馈的标准化操作流程，业技联合开展方案共创、MVP 最小可行性产品验证、价值度量、迭代反馈等流程，进而打造具有示范效应的价值案例。

理想的隐私计算应用策略将体现在，它不再被视为特殊技术，而是成为支撑银行日常运营和创新发展的基础能力，在金融机构的数字化转型中不可或缺。

5.2.2 合规引领、安全筑基

隐私计算的落地，必须在创新与风控之间找到平衡。将合规引领，安全筑基作为行动准则，意味着企业需从被动的规则遵循者，转变为主动的信任构建者，为此，合规与安全不应被视为单纯的“成本项”，而是支撑可持续发展的核心能力与关键基石。

第一，合规引领：从被动遵循到主动共建。合规不应是阻碍创新的红线，而应是引导创新安全落地的航标。如前述章节案例所示，部分机构会采取一种前瞻性、对话式的合规策略，主动沟通，寻求共识，例如积极参与监管部门指导的金融科技创新监管试点等，在项目早期设计阶段，就主动与监管部门沟通，阐明技术原理、业务价值及风险控制措施。这不仅是为了合规报备，更是为了增进理解、

寻求指导,在前沿地带共同探索合规应用范式。在企业内部,设立“合规—科技—业务”融合工作组,研读网络安全法、数据安全法个人信息保护法等法规条文,在每个重要隐私计算项目启动前,将合规性要求逐条拆解为具体的技术约束和业务操作要求,形成项目的《合规性设计 Checklist》。

第二,安全筑基:从单点防护到体系化免疫。安全不能仅仅依赖于隐私计算技术本身,而应构建一个覆盖数据全生命周期的、纵深防御的治理体系。通过体系化治理,建立一个横跨数据采集、传输、存储、处理、销毁各个环节的安全策略与控制措施。确保即使在复杂的跨机构协作中,各方也能在预设的安全边界内放心地进行数据价值交换,从而为数据驱动业务创新提供坚实基础。不仅要确保隐私计算算法和协议本身在理论上的安全性,还应通过第三方算法审计、代码审查和安全认证来验证技术可信;同时,需要保障计算任务的发起、执行和结果输出的整个流程是可追溯且不可篡改,实现过程可信。

合规引领为隐私计算的应用提供了适用空间,而安全筑基则在这一空间内构筑了坚固的堡垒。二者相辅相成,共同将隐私计算从一项有潜力的技术,转变为企业可以依赖的、安全可靠的基础能力。

5.2.3 场景突破、价值优先

隐私计算的规模化应用,绝非一蹴而就的大跃进,而应遵循场景突破,价值优先的精益原则。通过精心选择的种子场景快速证明技术的商业价值,以实实在在的成果驱动内部共识与持续投入,实现从点到面的稳健扩张。

第一,场景选择:在信任沃土上播下高价值种子。成功的试点始于精准的场景选择,应优先聚焦同时具备高信任基础与高业务价值的领域,直接解决一个明确的、迫切的业务痛点,其价值可衡量、可感知。信任基础是前提,能将讨论重点从能否信任直接转向如何创造价值。例如,与政府平台(如税务、社保、海关)或集团内子公司合作,能极大降低跨组织协作的沟通与信任成本。

第二,价值验证:根据历史场景,对模型、数据进行价值模拟验证。由点及面进行技术验证、价值证明与信心建设,有效化解业务部门对技术实用性的质疑,可为规模化推进奠定基础。在审慎评估后,试点运行并逐步扩大范围,实时监督业务价值创造情况,建立动态反馈—迭代优化机制,对数据质量、模型效果进行实时监测与跟踪,并及时根据市场最新情况进行调整。

5.2.4 统一平台、互联互通

隐私计算的竞争力,将不再取决于对单一技术的掌握深度,而在于其作为连接器与枢纽的生态位技术价值。推动技术的平台化与互联互通,是破解当前应用瓶颈、释放数据网络效应的核心课题之一。

第一,平台化:构建柔性、统一的技术能力底座。通过构建企业级统一平台,告别分散、孤立的项目制烟囱,将隐私计算能力转化为可被业务随时调用的标准化服务。设计支持多种技术路线共存与融合的“技术中立、分层解耦”架构,通过模块化与可插拔设计,将核心算法、通信协议、资源调度、安全管理等组件解耦,提升平台可扩展性,降低后续的升级维护与技术迭代成本。将复杂的隐私计算技术封装成简单、稳定、可靠的数据协作服务,允许通过可视化配置,使企业可以根据不同合作场景的安全、性能与信任需求,灵活选择最优的技术组合,降低业务方的使用门槛,加速技术的内部普及与价值渗透。

第二,互联互通 迈向规模化生态协作的必由之路。平台不应是封闭的“城堡”,而应是开放的港口。应主动打破因技术标准不一而形成的计算孤岛,增强外部适配能力,优先对接并遵循行业或国家级数据流通的互联互通标准规范。通过互联互通能力建设,开发多协议转换网关和标准化适配器,实现与市场上主流的隐私计算平台及国家级数据流通基础设施(如数据交易所、可信数据空间)进行高效、低成本的对接。

5.2.5 积极融入、共建生态

隐私计算的价值实现,依赖于一个繁荣、可持续的数据协作生态。对于商业银行而言,静观生态成熟是一种战略被动,主动融入、积极共建才是掌握发展优势的关键。这要求银行从独立建设者转变为生态参与者乃至规则共建者,在开放协同中放大自身价值。

第一,拥抱技术生态,加速能力落地与迭代。通过采纳或贡献行业公认的通信协议、算法接口与数据格式,确保自身平台与外部系统、主流技术同频共振。降低与不同机构进行技术对接的成本与复杂性,利用生态中成熟的通用组件、安全插件和开发工具,实现本地化应用的快速部署与跨机构合作场景的敏捷扩展,将技术生态的协同性转化为自身发展的加速度。

第二,融入多元业务生态,实现数据与场景的协同增值。在业务层面,主动寻求跨机构、跨行业的协作网络。一方面,应积极探索与政府部门、核心企业、互联网平台及同业机构的数据融合,在合法合规前提下,将政务数据、产业链数据、消费行为数据等多维信息与金融数据有机结合,通过隐私计算技术刻画更立体、真实的客户与市场画像,发挥“1+1>2”的数据协同价值。另一方面,

发掘和设计跨机构的业务流程协作场景。利用隐私计算实现关键业务信息在保护隐私前提下的安全核验与流转，从而创新服务模式，将技术能力直接转化为新的业务链路。例如，在供应链金融中，与核心企业及物流平台共同设计基于多方安全计算的动态货值监控与融资模型；在联合风控中，与同业机构共建反欺诈联盟，通过联邦学习迭代黑产识别模型。

5.3 面向行业协同：共建可信数据空间生态

技术筑牢安全底座，生态定义价值天花板，站在隐私计算从技术验证迈向规模应用的关键转折点，单纯依靠市场自发探索已较难应对技术融合与生态构建的系统性挑战，为此可从以下三个方面进行前瞻性布局与系统性引导：一是以权威合规框架破解协作权责痛点，建设完善健康、包容开放、规范有序的环境，为创新提供清晰稳定的预期；二是以统一标准体系打通技术互联壁垒，降低规模化应用成本；三是牵头共商共建行业级可信数据共享平台，推动形成协同共生的数据流通新生态。

5.3.1 确立合规框架：划定安全创新边界，提供包容审慎的发展环境

隐私计算在金融业的深入应用，正面临跨机构协作中权责规则模糊、安全信任不足、技术标准不一的痛点。破解这一困境，需监管层面主动引领，通过制定清晰、可操作的权威细则，明确各方权责；进一步丰富完善监管沙盒等机制，提供包容审慎的试验空间，从而系统性降低协作的制度性成本，激发市场主体的协同意愿与创新活力。

一方面是研制可实施的操作细则，明晰数据共享权责边界。

当前，跨机构数据协作（如联合风控、反欺诈）难以规模化的首要障碍，在于数据“如何使用、由谁负责”缺乏官方、统一的实施细则，导致机构因权责不清、操作方式不明而顾虑重重。建议监管部门或相关行业协会牵头组织，针对金融业高频协作场景，尽快出台金融业隐私计算数据共享操作指引相关专项细则，为数据流通过程划定清晰的合规边界与操作红线，将数据安全法、个人信息保护法的原则性要求细化落到金融数据融合应用垂类领域。

我们倡议，在制订相关细则时，应着力从以下三个维度构建核心权责框架：

一是强化数据使用的目的限定与原则。从数据分级分类、业务场景分类等维度明确数据使用边界，遵循合法、正当、必要原则，将共享范围限定于完成特定业务目标所必需的最小数据集与最小计算结果集，并数据分级分类、业务场景分类等维度，对可共享的数据、允许的计算任务及可输出的结果形式作出明确界定，从源头杜绝数据滥用。

二是健全数据全生命周期的安全管理机制。建立覆盖数据评估、接入、计算、存证、使用到销毁的闭环管理制度，提供匿名化、去标识化等要求的技术指引，合理规定数据在计算过程中的有效留存期限与使用次数上限，并明确任务完成后数据的处置方式、处理技术要求，降低非法留存与隐私泄露风险。

三是清晰界定多方参与下的法律责任划分。在细则中明确数据提供方、使用方、技术平台方等在数据传输、联合计算、结果使用及安全事件等环节中的法律责任、安全责任与合同责任，建立可追溯、可定责的治理体系，提升协作的规范性与可预期性。

通过上述制度设计，将法律原则转化为可落地的操作手册，为隐私计算环境下的多方数据协作奠定合规基础，促进数据要素安全、高效、有序流通。

另一方面是优化“监管沙盒”机制，提供包容审慎的创新环境。

在明确基本规则的前提下，为鼓励前沿技术在真实场景中的探索与验证，建议进一步优化和扩大金融科技创新监管工具（监管沙盒）的应用领域，为隐私计算等技术的复杂应用提供风险可控的安全试验场。

具体建议包括：

（1）扩大试点范围与场景：在现有基础上，将“监管沙盒”试点从单点业务，拓展至跨省级行政区、跨金融子行业等场景，进一步激发金融创新活力。

（2）建立弹性容错机制：在严守安全底线的前提下，对沙盒内测试项目设定合理的容错空间。允许参与机构在模拟真实环境或有限真实业务中测试技术方案与商业模式的稳健性，对于非主观恶意、未造成重大风险且已主动报告的探索性偏差，可采取约谈指导、限期整改等柔性监管措施，鼓励机构大胆探索。

（3）推动试点成果转化：建立沙盒内成功试点项目的快速推广机制。对经过验证有效的技术方案、合规流程与协作模式，及时总结并形成行业最佳实践或标准化建议，依托监管平台、渠道开展相应成果宣贯，加速其在全行业的合规应用，打通从试点到推广的路径。

5.3.2 推动标准建设：研制共性技术规范，打通互联互通的实践路径

建议由金融监管部门联合国家数据局等管理机构，组织行业领先机构共同发布前瞻性、体系化

的标准建设顶层指引，并推动行业协会与产业联盟据此研制覆盖技术全生命周期的具体操作规范与评估体系，为行业提供清晰、统一的路线图，指导各机构实现安全、高效的对齐与对接，破解当前隐私计算应用面临的平台孤岛、接口不一等生态壁垒，推动技术从分散建设迈向规模化、可互操作的产业协同，

一是发布顶层设计指引，明确标准建设方向与框架。

建议由银行、监管、数据等业务主管部门，研究制定金融业隐私计算技术应用与标准化发展指引，从产业协同和生态构建的高度，明确标准化的总体原则、核心目标、关键领域与推进路线图，统一行业认知，为后续各类具体标准的研制提供权威的顶层依据，确保标准建设工作有章可循、方向一致。

二是指导研制全链路操作规范，覆盖关键环节。

在顶层指引下，鼓励并授权全国性金融标准化组织、行业协会及产业联盟牵头，组织市场机构共同研制一系列操作性强的具体规范，重点覆盖以下四个维度：

(1) 数据资源质量标准：制定金融场景下用于隐私计算的数据分类分级指南、数据质量评估模型与认证规范。明确不同业务场景（如信贷、反洗钱）对数据字段完整性、准确性、时效性的最低要求，从源头上保障数据可用性与计算有效性。

(2) 平台互联接口规范：制定金融机构自建平台与国家级、区域级数据交易所、公共数据平台以及不同合作方平台之间进行安全连接和数据服务调用的通用技术接口标准。统一身份认证、任务调度、数据传输与结果返回的协议与格式，实现一次开发，多处对接，大幅降低生态连接的技术复杂度与成本。

(3) 隐私计算技术互联互通规范：这是当前较为紧迫的环节。建议尽快出台金融行业的隐私计算互联互通专项标准，聚焦于不同技术框架之间算法协议的兼容互认、安全参数的协调一致以及联合计算任务的协同管理，实现跨平台算力与数据价值自由组合。

(4) 安全与合规评估规范：制订统一的隐私计算系统安全评测指南、算法合规性审计指引以及全流程存证溯源规范。为第三方测评和机构自评估提供方法论，确保技术应用始终满足数据安全与个人信息保护的法律底线。

三是以标准牵引产业实践，加速生态化落地。

通过顶层指引、行业研制细则的模式，将监管要求与产业实践高效结合。通过统一的接口与质量标准，指引金融机构、科技公司与数据服务商进行标准化研发，使其产品与平台天生具备互联互通的基因。牵引隐私计算生态从定制化点对点连接，迈向标准化网络协同，为数据要素在金融领域的安全高效流通提供规范指引。

5.3.3 共建共享平台：构建行业级可信基础设施，拓展数据协同网络

建议由金融监管部门倡导或指导、行业主体共同建设可信数据共享平台，作为中立、可信、开放的协同枢纽，为市场提供超越单一机构的公信力与标准化服务，从而系统性降低生态协作的信任与技术门槛，激发网络效应。

一是平台定位，可信协同枢纽破解核心信任痛点。

行业级平台的首要价值在于其公信力。由监管部门指导或认可的设立模式，能有效弥补纯商业主体间的信任缺口。平台应定位于规则的执行者与过程的鉴证者，而非数据或业务的直接经营方。其核心功能包括：为参与机构提供统一身份认证与合规准入核验；对数据协作的全流程进行不可篡改的存证与审计追溯，确保所有计算任务严格限定于经授权的最小必要范围；执行标准化的数据安全与隐私保护基线要求。通过将监管规则内嵌于平台运行机制，可为金融机构参与复杂生态协作提供坚实的信任锚，敢于、乐于共享和运用数据价值。

二是平台核心功能，统一标准的载体与网络协同的基石。

在提供可信环境的基础上，平台应成为推动技术标准化与生态网络化的核心载体。作为统一技术标准的孵化器与试验场：建议平台应率先采纳并验证前述章节所倡导的互联互通接口、数据质量等标准。各类机构在平台上开展的实际协作，将为金融行业隐私计算技术标准的迭代与完善提供最真实的反馈，加速从标准文本到产业实践的转化。

作为跨域生态协同的连接器：平台的终极目标是成为连接金融与政务、产业、科技等多元生态的桥梁。通过平台，金融机构可安全、合规地触达经认证的政务数据（如社保、税务）、产业数据（如供应链、物联网）和商业数据，极大丰富风控与营销的数据维度。

三是以平台赋能生态拓展，从金融内生到赋能千行百业。

行业级平台的建成，将推动隐私计算应用实现双向赋能的跃迁。向内深化金融业务创新，金融机构可更放心地探索科技金融、绿色金融、普惠金融、养老金融与数字金融等复杂业务的联合建模

与数据核验，催生新的金融服务模式。向外赋能实体经济发展，通过平台，金融数据能力可以安全、可控地服务于更广阔的国家战略与产业需求。同时，平台通过提供标准化、低成本的隐私计算服务，显著降低中小企业、科创公司的接入门槛，使其能够便捷地融入金融数据协作网络，破解融资与发展中的数据孤岛问题。例如，在智能制造领域，平台可支撑银行基于加密后的企业生产、能耗、物流数据，与核心企业协同开发更精准的供应链金融模型；在乡村振兴领域，可促进涉农数据、政府补贴数据与金融数据的融合，助力整村授信等普惠金融模式规模化、高质量发展。这种金融赋能产业、产业反哺金融的良性循环，将真正释放数据要素乘数效应。

前瞻来看，一个健康、稳定的行业级可信数据共享平台，不仅是金融业数据协作的基础设施，更将成为未来全国一体化数据要素市场网络中的关键节点。平台通过实践验证规则与标准，通过服务连接多元主体，最终推动形成规则互认、网络互联、价值共享的跨区域、跨行业数据流通枢纽，为数字经济高质量发展提供节点支撑。

本白皮书系统探讨了隐私计算在金融业从技术验证到规模应用的完整图景，其发展已形成清晰脉络：前沿技术的快速融合（算法、架构、跨域）是引擎，领先机构的业务驱动与实践范式是车轮，而监管引领的规则与生态建设则是支撑整个系统稳健前行的路标与道路。三者环环相扣，共同指向一个愿景：隐私计算已不仅是一项可选技术，它将成为金融业在数据要素时代构建核心竞争力、实现数字化转型的关键基石。

展望未来，隐私计算的深化应用将驱动金融业发生三重深刻变革：一是业务范式的变革，从基于封闭数据的内部优化，转向基于开放生态的协同创新；二是风险范式的变革，从被动防御合规风险，转向主动构建覆盖全链条的可编程信任；三是产业范式的变革，金融机构将从数据的重要使用者演进为可信数据生态的关键构建者与价值赋能者，更紧密地服务于实体经济千行百业的数字化进程。隐私计算的发展将与国家数据要素市场化进程同频共振。金融机构将通过筑牢安全底座、共建协作生态、释放要素价值，助力全国一体化数据市场的建设，为数字中国的高质量发展注入强劲而可靠的金融动能。这不仅是技术的胜利，更是一场关于信任、协作与增长的数字时代商业文明的开始。

国内参考文献：

1. 郭宇. 隐私计算技术：拓展多方数据联合应用链路 [J/OL]. 金融电子化, 2025-08-08=2009.<https://mp.weixin.qq.com/s/uUtC-183YmOb7TEWGV8vyg>.
2. 鞠鑫, 曹京, 陈佛忠, 等. 隐私计算在卫生健康行业的应用与安全研究 [J]. 信息通信技术与政策, 2023,49(2):43-48.
3. 中共中央、国务院. 中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见 [EB/OL].(2022-12-19) [2024-10-01].
http://www.gov.cn/zhengce/2022-12/19/content_5732695.htm.
4. 国家数据局 中央网信办 科技部 工业和信息化部等十七部门. “数据要素 ×” 三年行动计划 (2024-2026 年) [EB/OL].(2023-12-31).
https://www.cac.gov.cn/2024-01/05/c_1706119078060945.htm.
5. 中国人民银行. 多方安全计算金融应用技术规范 (JR/T 0196-2020) [EB/OL].(2020-11-24)[2024-10-01].
<https://std.samr.gov.cn/hb/search/stdHBDetailed?id=B7BA9DE9181993F3E05397BE0A0A1FD2>.
6. 国家市场监督管理总局 中国人民银行. 关于发布《金融科技产品认证目录 (第二批)》《金融科技产品认证规则》的公告 [EB/OL].(2022-02-09).
https://www.samr.gov.cn/zw/zfxxgk/fdzdgknr/rzjgs/art/2023/art_b7334e5dad48404a986c76e3bdd39d53.html
7. 中国人民银行. 关于印发《金融科技发展规划 (2022-2025 年)》的通知 (银发〔2021〕335 号) [EB/OL].(2022-01-21).
<http://www.pbc.gov.cn/zhengwugongkai/4081330/4406346/4693549/4470403/index.html>.
8. 工业和信息化部 中国人民银行等十六部门. 关于促进数据安全产业发展的指导意见 (工信部联网安〔2022〕182 号) [EB/OL].(2023-01-03).
https://www.gov.cn/zhengce/zhengceku/2023-01/15/content_5737026.htm.
9. 国家发展改革委 国家数据局 中央网信办 工业和信息化部 财政部 国家标准委. 关于印发《国家数据标准体系建设指南》的通知 (发改数据〔2024〕1426 号) .(2024-09-25).
https://www.gov.cn/zhengce/zhengceku/202410/content_6978809.htm.
10. 国家数据局 中央网信办 工业和信息化部 公安部 国务院国资委. 关于促进企业数据资源开发利用的意见 (国数资源〔2024〕125 号) [EB/OL].(2024-12-25).
https://www.gov.cn/zhengce/zhengceku/202412/content_6994570.htm.
11. 张莉. 隐私计算技术在银行业的应用及商业银行策略思考 [J], 银行业经营管理, 2025-08.
12. 交通银行. 隐私计算金融应用白皮书 [R], 2021-12.
13. 中国工商银行股份有限公司金融科技研究院. 隐私计算推动金融业数据生态建设白皮书 [R], 2021-11.
14. 中国工商银行软件开发中心. 工商银行大数据技术及应用白皮书 [R], 2024-10.

国外参考文献：

1. 源于苹果在其官网的隐私介绍以及产品发布会 (WWDC)。苹果全球营销高级副总裁格雷格·乔斯维亚克认为“隐私是基本人权”，同时 Apple Pay 使用了“Tokenization”技术。