云程发轫，精耕致远

中国隐私计算行业研究报告

概念界定

隐私保护计算

（Privacy Preserving Computing）

隐私保护计算（Privacy Preserving Computing），又称“隐私计算”，是指在提供数据隐私保护的前提下，对数据进行分析计算的一类技术。进而在保障数据隐私安全的基础上，可以让数据以“可用不可见”的方式进行安全流通。隐私保护计算是一个技术体系，而非一项单一的技术。

市场中主要采用“隐私计算”的表述形式，因此本报告中均以“隐私计算”作为统一的表达方式。

实际上，还有资料将“隐私计算”和“隐私保护计算”进行了分别定义与解释，可见目前关于“隐私计算”存在多样化的概念界定方式。

对于此类问题，报告不再过多赘述。**本报告定义仅用于统一读者理解，方便后文的相关研究论述。**

摘要及简介

行业发展分析

- 中国隐私计算在法律政策和市场需求的双轮推动下，实现了“产学研”协同发展。商用实践领先于国外，技术发展各有千秋。
- 2021年中国隐私计算市场规模为4.9亿元，预计至2025年将达到145.1亿元。目前隐私计算处于基建期，市场需求集中于基础产品服务，数据运营商业模式因拥有巨大市场发展空间而被广为看好。
- 2016年～2022年Q1，中国隐私计算行业共计发生55起融资事件，累计融资金额超30亿元人民币。

技术发展洞察

- **研究范围：**报告分别从“产品与技术选型、安全性问题、性能问题、软硬件结合、国产化、隐私计算跨平台互联互通”六个方面对隐私计算技术展开了分析。
- **市场调研：**研究团队面向金融、政务等领域的行业用户，重点对“产品与技术选型、安全性问题、性能问题、软硬件结合”等问题展开了市场调研，以定量的方式反映了行业用户的需求和关注点。
- **策略与建议：**分析师针对“产品与技术选型、隐私计算的安全性实践”等重点问题给出了相关策略及建议。

产业落地实践

- 分析师通过“iResearch：2021-2022年中国隐私计算效能发展象限”、“iResearch：隐私计算实践洞察雷达”等研究工具，对隐私计算的商用实践情况进行研究输出，并展开相应解读。
- 针对“用户所关注的隐私计算技术服务商能力”以及“行业用户的技术实践战略视角下：隐私计算应用的重要关注点”等相关问题，研究团队面向金融、政务领域的行业用户展开了调研。

行业趋势展望

- 分析师结合“iResearch：隐私计算发展周期洞察矩阵（对趋势的研究，中国市场）”对隐私计算行业的整体发展趋势进行了研究与分析，并针对“市场参与者发展格局、行业技术基础设施建设、应用层场景实践、隐私计算跨平台互联互通、算力加速需求”五大问题展开了细化解读。

来源：艾瑞咨询研究院自主研究及绘制。

法律政策驱动下的行业发展

三法联动及相关政策，推动了数据可信流通建设的发展

在《数据安全法》、《网络安全法》和《个人信息保护法》的三法联动推进下，中国数据市场迎来了安全合规发展阶段。同时，多项政策及发展规划也明确提出了对数据安全合规流通的发展建议与规划。这将推动着市场摆脱“数据包传输、API调用”等传统数据流转模式，进而构建安全合规的可信数据流通方式，让数据在隐私保护的前提下，发挥计算价值，全面推进数据要素流通。

数据安全合规流通的法律法规及相关政策

	时间	发布单位	文件名称	关键内容
三法联动	2021年11月1日	全国人大	《中华人民共和国个人信息保护法》	个人信息在数据流通过程中的安全合规性，确立了个人信息的“最小必要”原则。
	2021年9月1日	全国人大	《中华人民共和国数据安全法》	确立数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放相关法律法规。
	2017年6月1日	全国人大	《中华人民共和国网络安全法》	个人用户信息搜集的安全合规、网络数据的完整性、安全性、保密性等。
相关政策	2021年12月	央行	《金融科技发展规划（2022-2025年）》	提出在保障安全和隐私前提下推动数据有序共享与综合应用。
	2021年12月	国务院	《“十四五”数字经济发展规划的通知》	在创新数据要素开发利用机制中提到：在确保数据安全、保障用户隐私的前提下，调动行业协会、科研院所、企业等多方参与数据价值开发。
	2021年12月	国务院办公厅	《要素市场化配置综合改革试点总体方案》	建立健全数据流通交易规则。探索“原始数据不出域、数据可用不可见”的交易范式。探索建立数据用途和用量控制制度，实现数据使用“可控可计量”。
	2021年7月	工业和信息化部	《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》	通过隐私计算等数据安全技术的研究与应用促进数据要素安全有序流通。
	2020年4月	中共中央国务院	《关于构建更加完善的要素市场化配置体制机制的意见》	将数据作为一种新型生产要素写入了《意见》。

来源：公开信息、艾瑞咨询研究院自主研究及绘制。

市场需求驱动下的行业发展

传统的数据流通方式已无法满足合规要求，实现数据的可信流通是推进数据要素市场化配置的基础

大数据产业的迅猛发展，激发了数据要素流通的市场空间。中国大数据产业在“十三五”发展期间取得了显著的发展成效，产业规模年均复合增长率超过30%，2020年超过1万亿元。同时，《“十四五”大数据产业发展规划》发展目标提出：到2025年，大数据产业测算规模突破3万亿元，年均复合增长率保持在25%左右。

传统数据流通方式无法满足合规需求，需要通过创新的技术或模式来实现数据要素的可信流通。在大数据产业迅猛发展的背后，数据隐私安全相关问题也在逐渐暴露，传统“复制式”的数据流通方式让商业隐私信息、个人隐私信息等产生了泄漏，无法满足法律合规要求。而倘若在数据提供方处展开计算，虽然可以让数据不出域，但会暴露业务方的计算规则与计算模型，进而暴露业务方的商业隐私。因此，若想让数据要素实现良好的市场化配置，行业首先需要完善数据可信流通能力的建设。

行业用户对数据要素流通的关注点

Insight 1：面向业务需求者（数据使用者）的调研[1]

71.9%的受访者：**希望可以调用更加多元化类型的数据**

受访者较多的反馈是：目前所合作的数据源主要为通信运营商、大型互联网企业，但是对于部分业务，希望可以与更加多元类型的数据进行合作，如政务机构数据等。

64.7%的受访者：**对业务模型的安全性问题较为关注**

业务模型直接反映了业务逻辑与规则，在部分计算模型需要出域的情况下，受访者对模型泄露所带来的影响较为关注。

Insight 2：面向数据源（数据提供者）的调研[2]

87.4%的受访者：**在探索基于隐私保护的数据流通形式**

数据包传输、API调用等传统数据流通方式目前已经无法满足监管与合法要求，因此基于隐私保护的数据流通成为不可或缺的能力。

72.3%的受访者：**希望通过隐私保护技术，加强数据开放的深度与广度**

数据因计算才有价值，受访者一方面希望可以盘活数据价值，另一方面在积极践行数据要素开放流通战略，加强数据开放能力建设。

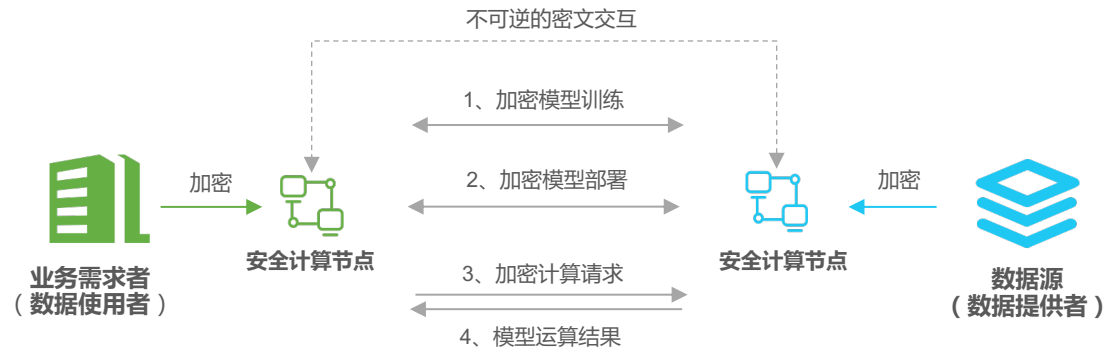
注释：1、面向业务需求者（数据使用者）的调研中，分析师对金融机构为主的139位技术应用者展开了访谈；2、面向数据源（数据提供者）的调研中，分析师对通信运营商、政务机构的159位技术应用者展开了访谈。
来源：艾瑞咨询研究院自主研究及绘制。

数据的可信流通

隐私计算可以构建“数据可用不可见，用途可控可计量”的数据可信流通范式

隐私计算通过在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算，可以保障数据以“可用不可见”的方式进行安全流通。除了“数据可用不可见”的特性外，隐私计算中的多方安全计算技术还可以控制数据的用途以及用量，进而做到数据“用途可控可计量”。在应用实践中，隐私计算还可以融合区块链技术来强化在“数字身份、算法、计算、监管”等方面的信任机制，进一步完善数据要素的确权、定价与交易的可信体系建设。

基于隐私计算的数据可信流通



该图（以多方安全计算为例）仅用作隐私计算应用实践的简单示意，不代表隐私计算的全部实践逻辑和技术方案。

来源：艾瑞咨询研究院自主研究及绘制。

中外隐私计算发展对比

iResearch 艾瑞咨询

国外隐私计算在技术研究方面持续耕耘，商业实践有限；中国隐私计算在“产学研”的协同推动下获得高速发展。

Section 1 整体差异对比

国外：企业布局早，更加专注于技术的研究，商业化实践有限。

- **技术研究的持续耕耘：**国外的隐私计算企业布局早于中国，并在不同技术层面取得了相应成果。如Intel SGX、TrustZone、AMD SEV等国外TEE技术方案经过多年的积累沉淀，目前相对成熟；微软、谷歌、Facebook（现改名为Meta）等大型科技企业分别在多方安全计算、联邦学习等领域持续探索多年。
- **有限的商业实践：**国外隐私计算企业虽然布局较早，但是整体的商用实践较为局限。在面向企业的服务中，医疗行业是较为活跃的领域之一。此外，谷歌、Facebook（现改名为Meta）等大型科技企业在探索面向C端的隐私计算应用，还有部分企业将隐私计算应用于数字货币相关场景。

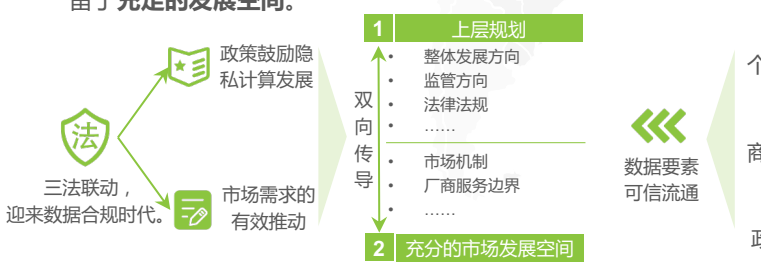
国内：企业布局晚，技术发展和商业实践协同并行，整体发展迅速。

- **起步虽晚，但市场格局千帆竞发：**国内在2016年开始出现垂直的隐私计算厂商，相对国外起步较晚。近年来，中国隐私计算行业的投融资事件数持续增加，2020年和2021年分别有14起和17起融资事件。此外，综合科技企业、区块链企业、人工智能企业等多种类型的技术公司也在纷纷入局。
- **产学研协同的高效发展：**中国的隐私计算在数据要素安全流通的市场需求和政策需求的推动下迎来发展契机，金融、政务、运营商等领域均在积极展开隐私计算基础平台建设，并逐渐开始在应用层展开场景实践。在产业需求的推动下，隐私计算跨平台互联互通建设、国产芯片厂商对可信硬件的研发、软硬一体机产品创新等均在如火如荼地开展。基于此，技术服务商还在探索基于数据运营商业模式下的更大市场机会。整体上，中国隐私计算在产、学、研的协同促进下取得了高效的发展。

Section 2 中外隐私计算发展模式对比分析

中国

中国正在**自上而下体系化**地推动解决数据隐私保护问题，同时也为市场预留了**充足的发展空间。**



欧美国家

随着《GDPR》和《CCPA》的正式生效，在2019～2022年间，欧美相关企业因数据隐私泄露等相关问题被处罚金累计达 **74亿+ 美元**

《CCPA》和《GDPR》都设置了较为严格的惩罚，国外用户对个人数据隐私保护意识较强，隐私保护问题直接被抛向相关企业，拥有大量用户数据的科技公司（如谷歌、Facebook（现改名为Meta）等）以合法合规为首要目标展开隐私保护计算的应用实践。

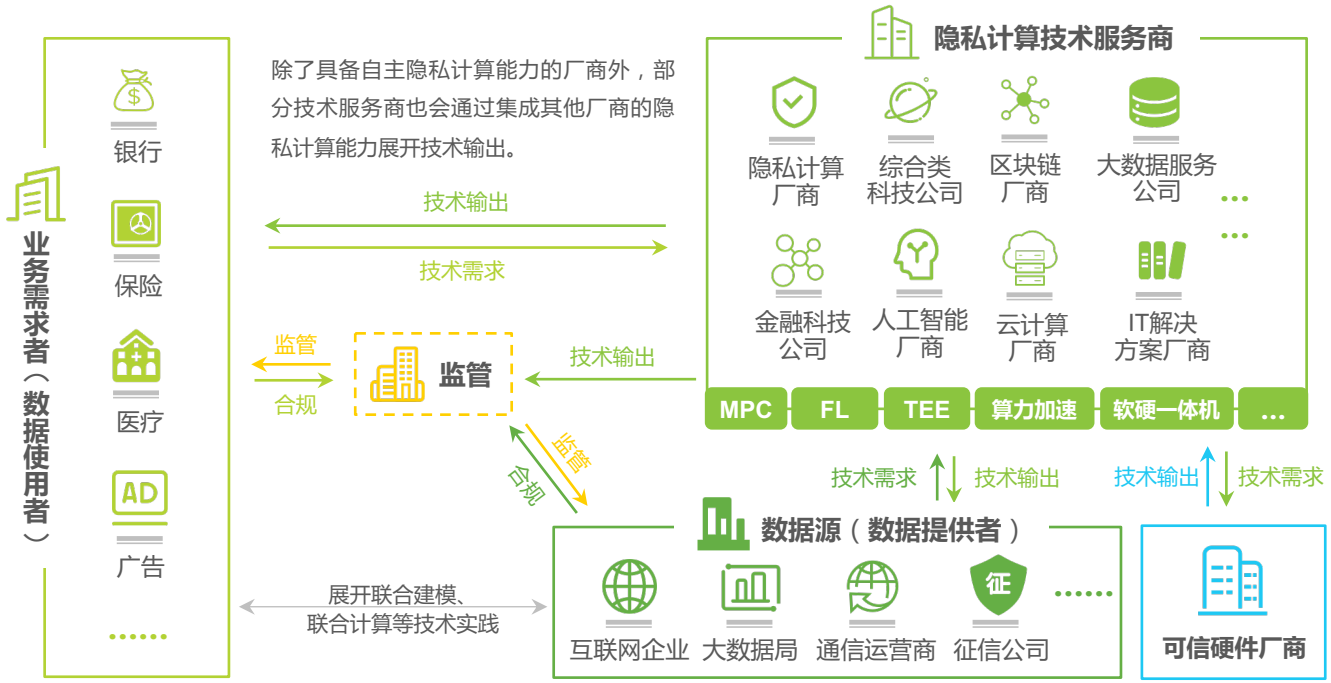
来源：艾瑞咨询研究院自主研究及绘制。

市场参与者类型

中国隐私计算市场呈现百舸争流、千帆竞发的市场格局

多方协同是隐私计算商用实践的一大特点，不同于其他类型技术，隐私计算在商用实践中，技术服务商除了提供平台建设外，还会为客户提供数据调用（寻找数据源）服务，且隐私计算也经常需要两方以上的参与者展开联合计算，因此多方协同特性十分明显。目前，中国隐私计算市场的参与者越来越多，除了垂直的隐私计算厂商外，各类技术企业纷纷入局，目前行业处于基础设施建设期，随着行业客户在应用层实践的逐步加深，数据运营、算力加速等需求也将不断涌现。对于中国隐私计算市场的发展，可谓是：百舸争流，奋楫者先；千帆竞发，勇进者胜。

隐私计算市场参与者类型（2022，中国市场）



来源：艾瑞咨询研究院自主研究及绘制。

产业图谱

2022年中国隐私计算产业图谱

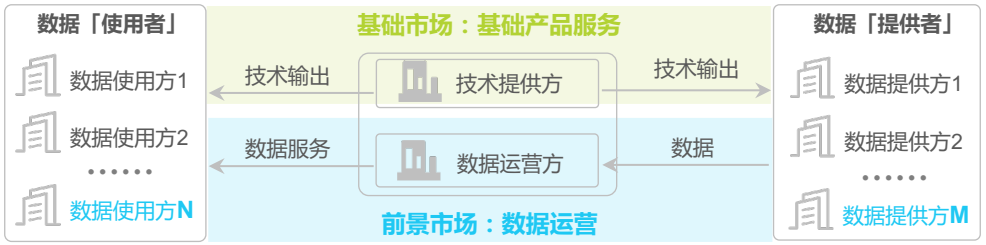
多数厂商布局了“MPC、FL、TEE”中的多项技术方案，且各具优势。艾瑞研究团队和产业专家团认为，应该鼓励企业进行多元化技术方案创新探索，因此产业图谱不对企业进行苛刻的“唯一性定位（每个企业仅展示自身「最优」的技术方案）”，而是采取了“最大兼容性”原则。但是行业用户在进行厂商选择时，需要考查并明确各厂商的具体技术优势所在。

注释：1、图谱中所展示的公司logo顺序及大小并无实际意义，不涉及排名。2、各种类型的市场参与者“上下/左右”位置并无实际意义，不代表排位。
来源：艾瑞咨询研究院自主研究及绘制。

商业模式及市场规模（1/2）

目前隐私计算正值行业基建期，市场需求集中在基础产品服务，数据运营服务将开启“隐私计算+”的蓝海市场

隐私计算的商业模式（2022，中国市场）



技术提供方和数据运营方既可以是同一类企业（如都是隐私计算技术服务商），也可以是不同类型企业。

基础市场：基础产品服务

- **产品销售**：对客户进行产品销售（产品形式可分为软件、硬件、软硬件一体机）。目前主要的实施方式为本地化部署。产品销售根据系统部署节点数量、功能模块等维度进行收费。如整体方案中含有硬件，也需涵盖硬件成本。
- **技术服务**：对系统更新维护等相关技术服务的费用。

前景市场：数据运营　　迈向“隐私计算+”时代

数据运营的理想模式是在M×N的数据运营网络（如上图）中，数据「提供者」通过与数据运营方合作，将数据接入数据智能产品，数据运营方向数据「使用者」提供数据智能产品的调用服务，我们可以框架性地将数据智能产品理解为封装了算法模型和多方数据的综合性产品，来为数据「使用者」提供“数据调用+算法模型”的一揽子服务。在这其中，数据运营方需要通过数据运营能力来持续创造价值[1]。基于此，衍生了两种商业模式：数据分润、业务分润。

数据分润　数据运营方为「数据使用者」提供数据源接入服务，技术服务商向「数据提供者」收取数据分润费用。

业务分润　数据运营方提供数据智能产品调用服务，按照业务实践效果收取业务分润的费用。如可按获客量、访问量等维度进行收取。

数据运营服务需要在行业用户完善隐私计算平台建设的基础上展开，目前的实践主要是满足客户的数据源接入需求，业务分润的模式相对较少，而各厂商的数据智能产品也处于建设之中。

注释：1、关于数据运营方该如何通过强化数据运营能力来持续创造价值，在报告“iResearch：隐私计算发展周期洞察矩阵（对趋势的研究，中国市场）”对「应用层场景实践」的解读中，给出了进一步的分析和实践策略建议；2、结合本报告对数据运营的定义，我们将「建模咨询」纳入数据运营范畴。

来源：艾瑞咨询研究院自主研究及绘制。

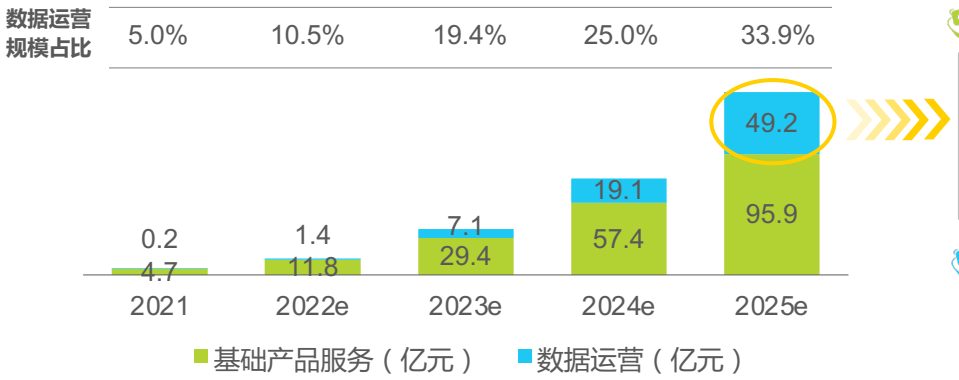
商业模式及市场规模（2/2）

2021年中国隐私计算市场规模为4.9亿元，预计至2025年将达到145.1亿元，数据运营占比持续升高

基础产品服务： 2021年中国隐私计算基础产品服务的技术采购中，金融、政务、运营商占据75%～80%的市场份额，医疗领域占比约为10%。结合对各领域行业用户的技术投入规划调研，我们发现金融、政务、运营商的核心投入期集中在2022～2024年，预计2025年将取得收官成果。以银行为例，预计至2025年，国有商业银行、股份制银行、40%～50%的城市商业银行均将完成隐私计算的平台建设。医疗领域将在卫健委政策和行业用户需求的推动下，预计在2023～2025年，在基础产品服务的投入上也会产生一定增速。

数据运营的市场空间将来自于两个方面：一是传统数据流通模式（数据包传输、API调用等）将被隐私计算的可信数据流通方案所重构；另一方面，传统模式下难以共享的数据（如政务数据等）将在隐私计算的加持下实现安全合规开放。

2021-2025年中国隐私计算市场规模



注释：1、2021年的市场规模统计了市场公开招投标信息+非公开招投标信息（通过对行业客户的调研、厂商营收调研等形式获取）；2、2022～2025年的市场规模发展，研究团队分别对金融、政务、运营商、医疗等领域的技术应用者展开了大规模调研，征询了其在未来3～5年的隐私计算投入规划。在此基础上，研究团队还参考了《“十四五”大数据产业发展规划》等相关政策中的大数据产业发展目标，进而对隐私计算市场的发展展开了综合预判。
来源：市场调研、行业专家访谈、艾瑞数据统计模型、艾瑞咨询研究院自主研究及绘制。

2026-2030年中国隐私计算市场规模发展分析

2026～2030年：数据运营市场的高速增长期

伴随着由“核心基建期”走向“隐私计算+”时期，应用层的差异化场景实践项目不断增加，数据智能产品的使用需求将大幅增加，数据运营市场将迎来**「极速发展期」，可参考报告第四章，对中国隐私计算行业的发展判断(2021~2033年)。**而基础产品服务将保持相对稳定增速，实现平稳发展。

2030年中国隐私计算市场规模将达：800～900亿元

该市场规模中，包含了隐私计算基础产品服务和基于“隐私计算+”的数据运营市场，后者将占据着**70%+**的比重。

数据运营市场方面，预计通过重构传统数据流通市场的规模占比约为**25%～30%**，基于隐私计算所带来的市场规模增量占比约为**70%～75%**。增量市场中，政务数据开放将发挥重要贡献。

注释：1、研究团队对政务机构的相关专家针对“数据开放规划和力度”进行了调研，综合评定了其对数据运营市场的影响。同时，我们也参考了其他领域的大量数理实证以及行业领导者意见，进而综合对2030年的「市场规模区间」和各项占比进行了研判。
来源：市场调研、行业专家访谈、艾瑞数据统计模型、艾瑞咨询研究院自主研究及绘制。

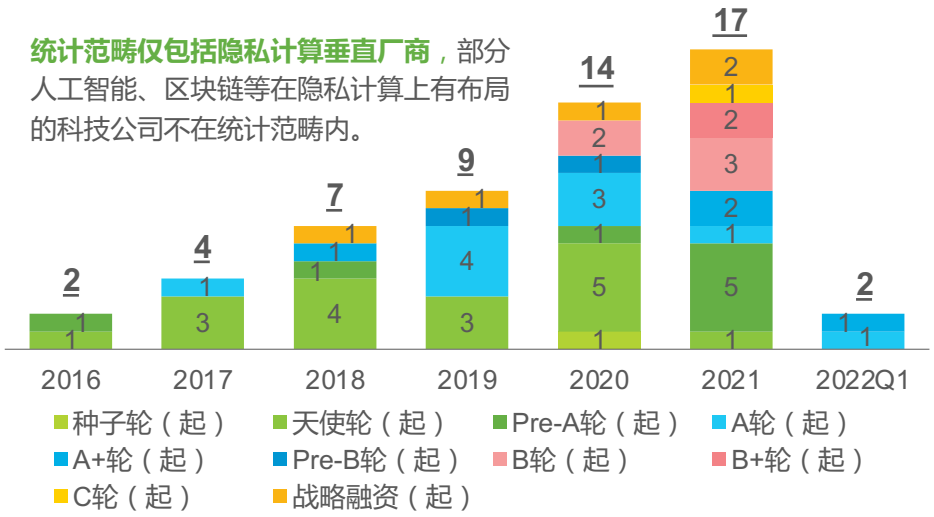
©2022.3 iResearch Inc. www.iresearch.com.cn

投融资分析

中国隐私计算行业共计发生55起投融资事件，累计融资金额超30亿元人民币

2016年–2022年Q1（截至3月9日），中国隐私计算企业的累计融资额超30亿元人民币，其中2021年占比超过60%。整体上来看，近年来的资本热度持续提升，大量初创型隐私计算企业纷纷入局。2020年和2021年是近年来资本热度最高的两个年份，2020年参与融资的隐私计算企业主要集中于种子轮～A+轮，2021年参与融资的隐私计算企业集中于Pre-B轮～C轮，在2022年，资本热度将持续保持。目前的投资机构呈现出多元化的状态，创投机构、产业基金、国有企业、各类科技公司等纷纷入局，分别从财务投资、战略投资等多个方面助力隐私计算企业发展。

2016-2022年Q1中国隐私计算行业投融资事件数



中国隐私计算行业投资机构参与者

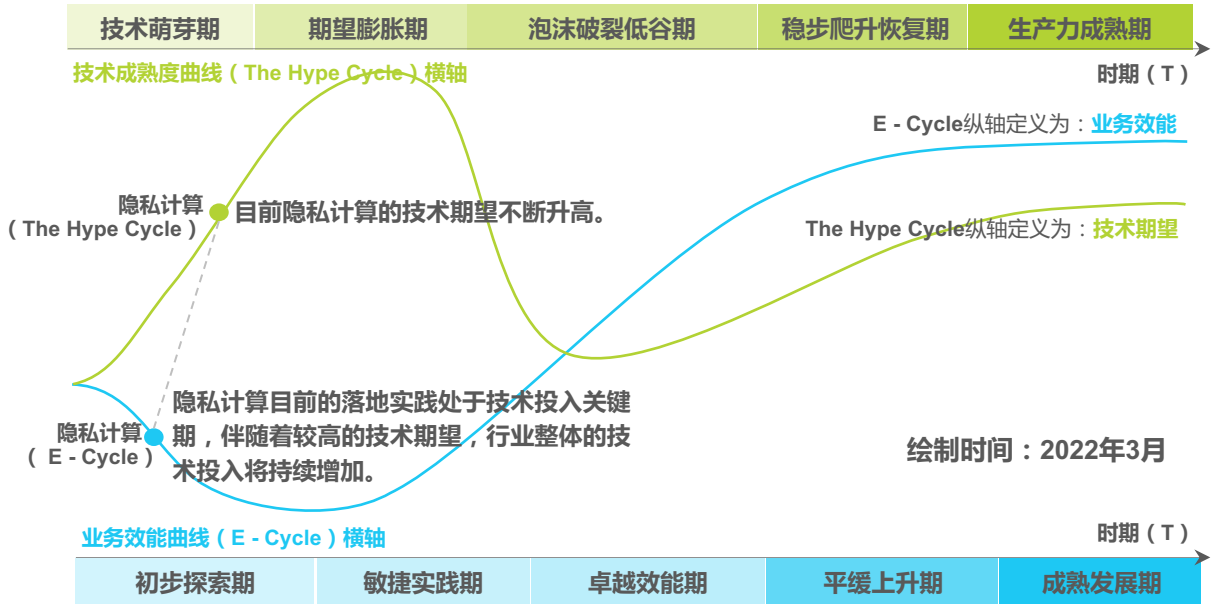
注释：1、2022年Q1的投融资事件数统计截至2022年3月9日；2、部分企业的投融资信息未进行对外公开的情况，不在上述统计范畴内。
来源：企查查等行业公开信息、厂商调研、艾瑞咨询研究院自主研究及绘制。

隐私计算所处的技术发展阶段

理性的技术期望、正确的技术理解有助于推动隐私计算的正向高效发展，最大程度规避“应用泡沫[1]”及“资本泡沫”

- 目前隐私计算处于技术期望的持续上升阶段、商用实践的初期。值得肯定的是，隐私计算的落地实践未出现较大的应用泡沫，这得益于隐私计算拥有强烈的市场需求和更为明确的政策指导方向。但隐私计算的落地实践仍需要继续攻克技术难题，加强对行业用户的技术认知教育，在技术实践和数据运营等多个方面持续探索。
- 此外，资本是技术发展初期的关键推动力之一，目前资本热度也在伴随隐私计算技术期望的提升而逐渐升温。对目前的投资机构来说，在深度考察厂商产品力及市场力的同时，应该对厂商“战略愿景的实现能力”进行着重评估。

iResearch：隐私计算发展周期洞察矩阵（对现状的研究，中国市场）



来源：隐私计算的案例实证研究、数理实证研究、艾瑞咨询研究院自主研究及绘制。

关于“矩阵”的概述说明

The Hype Cycle反映了技术由萌芽至成熟的发展周期。E – Cycle反映的是技术落地实践的业务效能发展周期。二者的融合从多视角反映了技术的发展。

技术期望的“双刃剑”属性

从多项技术的发展经验来看，非理性的技术期望会带来资本泡沫或是应用泡沫。理性的技术期望可以加速资本、产业界（技术应用者）对技术发展的推动。

注释 1：“应用泡沫”主要指技术偏离正确的价值实践方向而走向泡沫化，如缺乏价值锚定的数字货币就是一种典型“应用泡沫”。

艾瑞的“业务效能曲线”和“技术效能曲线”是技术落地的周期性研究工具，可有效判断一项技术是否存在应用泡沫，具体介绍见报告第三章或咨询艾瑞集团。

隐私计算的技术实现思路

隐私计算的三种技术实现思路：以密码学为核心、融合隐私保护技术的联合建模、依托可信硬件

隐私计算主要的技术实现思路分为三种：以密码学为核心的技术实现、融合隐私保护技术的联合建模、依托可信硬件的技术实现。

1 以密码学为核心

以密码学为核心的技术实现包含了多方安全计算、同态加密等多种密码学。目前行业的技术厂商通常将多方安全计算作为主要技术方案，而同态加密等密码学算法也同样被较多地应用于业务实践中，或是与联邦学习、可信执行环境等技术方案展开融合应用。

2 融合隐私保护技术的联合建模

融合隐私保护技术的联合建模，是将联邦学习与各类隐私保护技术相融合的技术实现方式。基于数据在各参与方分布情况的差异，联邦学习可以分为横向联邦学习、纵向联邦学习、联邦迁移学习。

3 依托可信硬件

以基于硬件的信任根，对隐私数据的计算环境进行隔离和度量。数据和算法被加密输入可行执行环境，仅对外输出最终的计算结果，原始数据和过程数据被就地销毁，从而实现数据的“可用不可见”。

隐私计算的三种技术实现思路

三个用例圆的交集，表示三类技术实现方式在实际业务应用中是可以相互融合的。

来源：艾瑞咨询研究院自主研究及绘制。

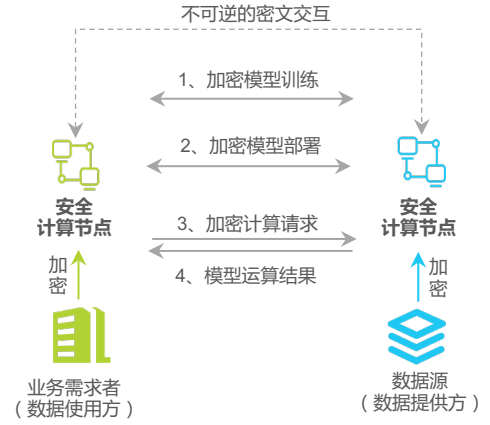
隐私计算的关键技术方案

三种技术实现思路下的主要技术方案：多方安全计算、可信联邦学习、可信执行环境

隐私计算三种技术实现思路下的主要技术方案

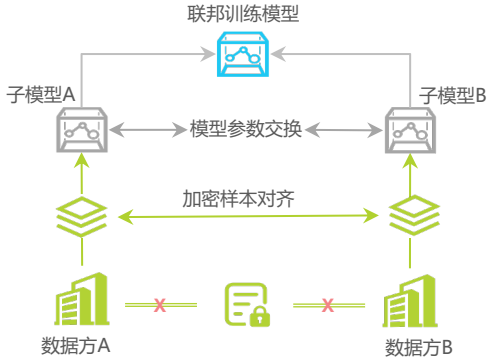
多方安全计算（MPC）
以密码学为核心

- **提出者：**安全多方计算（MPC）由姚期智院士于1982年提出。
- **定义：**安全多方计算（MPC）可以保障多个参与方进行协同计算并输出计算结果的同时，使各个参与方除了计算结果之外无法获取任何其他信息，从技术层面实现数据的可用不可见。



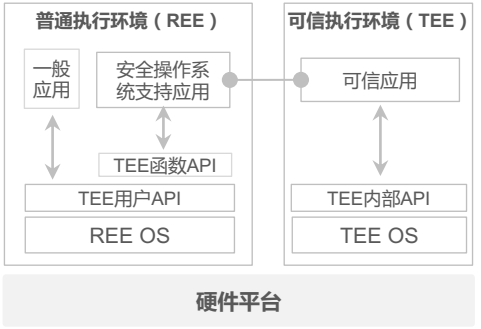
可信联邦学习（TFL）
融合隐私保护技术的联合建模

- **提出者：**联邦学习由Google于2016年提出。
- **定义：**联邦学习（FL）旨在建立一个基于分布数据集的联邦学习模型，是一种在原始数据不出库的情况下，协同完成机器学习任务的学习模式。在联邦学习实践中还需要融合各类隐私保护技术对传输信息实现进一步的保护，来构建可信联邦学习（TFL）能力。



可信执行环境（TEE）
依托可信硬件

- **定义：**可信执行环境（TEE）其方法是通过可信、抗篡改的软硬件构建一个可信的安全环境：在硬件中为敏感数据单独分配一块隔离的内存，所有敏感数据均在这块内存中展开计算，并且除了经过授权的接口外，硬件中的其他部分不能访问这块隔离内存中的信息；数据在该环境中由可信程序进行处理。以此来保护程序代码或者数据不被操作系统或者其他应用程序窃取或篡改。



来源：艾瑞咨询研究院自主研究及绘制。

01 隐私计算的技术实现思路及主要方案

02 隐私计算的技术要点分析

要点1：产品与技术选型（1/2）

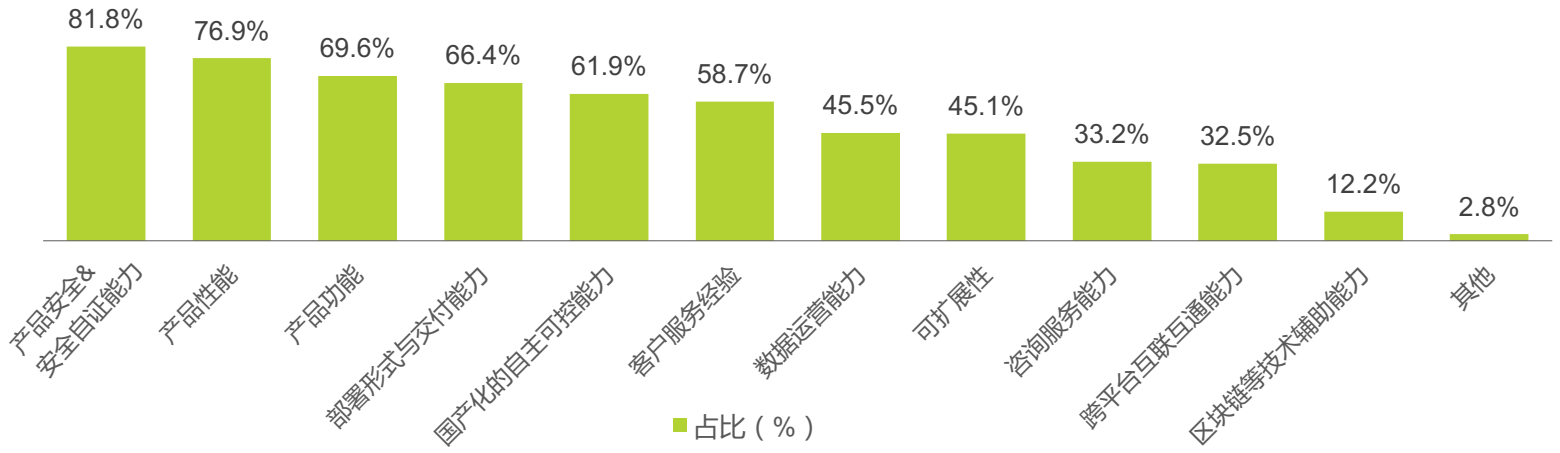
行业用户视角下的隐私计算产品与服务能力关注点

面对隐私计算的多样化技术路线以及多维度的技术指标，行业用户如何展开产品与技术选型是一个关键的问题。目前正值隐私计算的基础设施建设期，对如何能结合企业自身需求展开最优产品与技术方案选型，是后续高效开展数据应用实践的关键。基于此，我们首先要明确，在隐私计算的选型中，含有哪些关键指标，以结合目前技术应用者的实践经验来看，各项指标的重要性。对此，研究团队展开了如下调研。

行业用户所关注的隐私计算技术服务商能力

（2022年3月调研，中国市场）

- 本次累次调研了286位隐私计算实践者，其中金融领域151位、政务领域135位；受访者包括技术岗位从业者、业务岗位从业者，两类受访者分别站在不同角度，针对目前阶段的能力关注点发表了看法。
- 在报告第三章关于金融、政务领域的解读中，我们对本组数据进行了拆分，分别公布了金融、政务领域行业用户所关注的隐私计算技术服务商能力的调研数据。



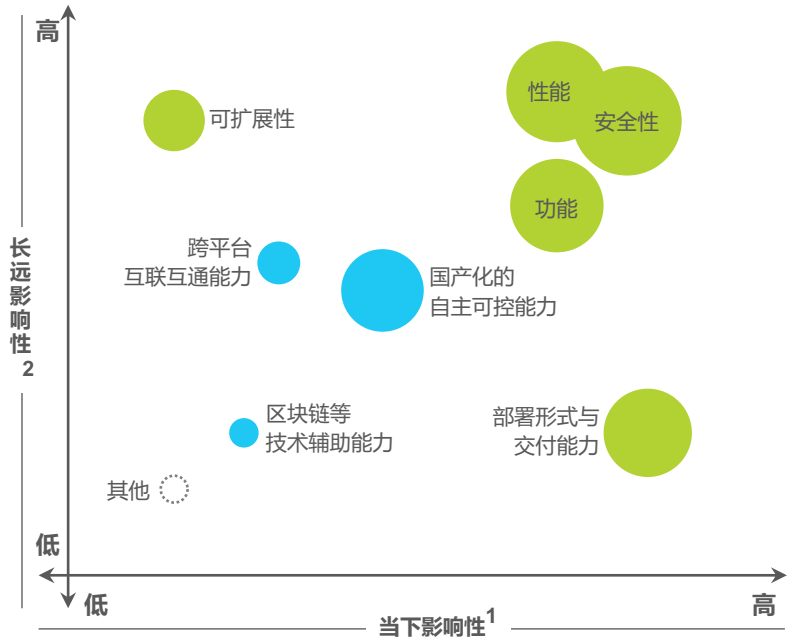
注释：1、N=286；2、研究团队首先征集了相关技术应用者主要关注的能力方向，分析师对此进行归纳整理，并设计了选项；3、在调研过程中，每一位受访者最多选择六个选项。
来源：艾瑞咨询研究院自主研究及绘制。

要点1：产品与技术选型（2/2）

隐私计算应用者应结合实际需求，设置动态敏捷的需求模型，进而展开产品与技术选型。MPC、FL、TEE等各类技术方案均具优劣势，融合应用可以形成优势互补。

隐私计算产品与技术选型象限

绘制时间：2022年3月



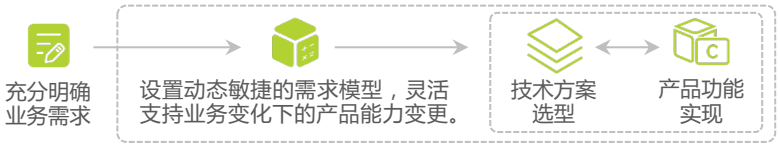
用例圆越大，表示行业用户在当下对该指标的关注度[3]越高

建议所有行业用户都去关注的指标　行业用户可根据需求而关注的指标

注：1、当下影响性：某一考量指标对当下技术实践成效的影响；2、长远影响性：某一考量指标对长远技术实践成效的影响；3、行业用户对指标的关注度，结合报告上文“行业用户所关注的隐私计算技术服务商能力”的调研数据所得。

来源：技术应用者调研、行业专家访谈、艾瑞咨询研究院自主研究及绘制。

隐私计算产品与技术选型的策略框架



- 关于产品基础功能考查的关键指标，可以参照左侧“象限”的相关内容。
- 目前隐私计算应用层的算法实践，多数需结合客户需求进行定制化实施。
- 技术方案选型将对性能、安全性等重要指标产生影响，不同技术方案各具优势，技术应用者应该重点考查隐私计算产品支持哪些技术方案，以及对应技术方案的能力实现情况。

隐私计算技术方案选型的考量

Step 1：明确产品支持MPC、FL、TEE等解决方案中的哪几类。

***Step 2：*明确各类技术方案的优劣势&选型要点**

- **多方安全计算（MPC）：**高安全性是其显著特点。理论上的通用性较高，但由于加解密过程复杂导致性能较差，局限了场景实践。因此多方安全计算通常会与其他技术方案融合，或是通过算力加速突破性能局限。产品选型应关注其支持的计算种类（<加、乘、比较>/<除法、逻辑运算>/<机器学习>）、所支持的安全假设模型等相关内容。
- **联邦学习（FL）**：以多方联合建模场景为主，相比于安全多方计算拥有更好的性能，但存在通过梯度数据反推出原始数据的风险，通常会与隐私保护技术展开融合实践。产品选型应关注其所融入的隐私保护技术能力（MPC、HE等）、(工程级)算法支持程度等相关内容。
- **可信执行环境（TEE）**：可以用于性能要求高、数据量大、计算逻辑复杂的业务场景，但需要实现对硬件厂商的信任。TEE通过与MPC、FL以及HE等密码学算法的联合实践可以各取所长，发挥更好的实践成效。产品选型应关注可信硬件国产化情况、OS和可信硬件的兼容性、是否支持一体机交付、方案标准化程度等相关内容。

要点2：安全性问题（1/3）

技术应用者对隐私计算安全性问题的关注度大幅提升

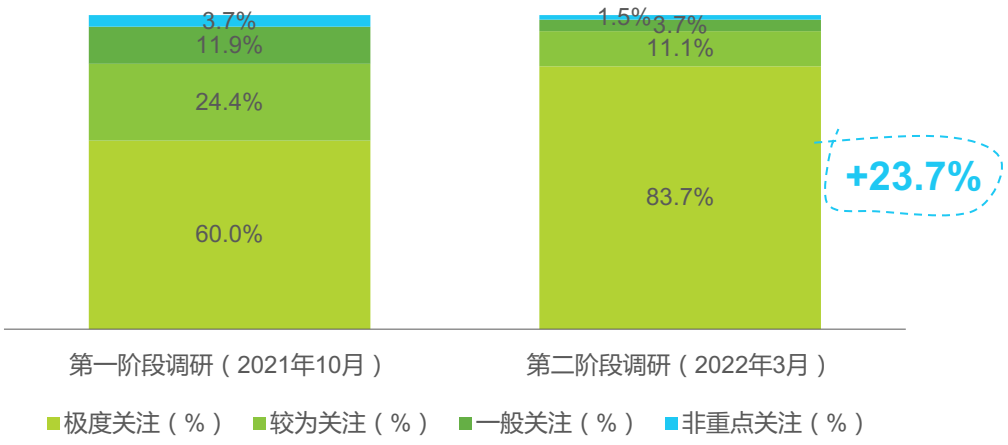
隐私计算安全性问题向技术应用者提出信任挑战，技术应用者对安全性问题持更加谨慎的态度

两次调研数据中可以看出，随着隐私计算安全性问题的出现，技术应用者对安全性的关注度实现大幅度提升。技术应用者在技术选型和产品抉择上也出现了更加谨慎的态度，部分技术应用者更加倾向于参考同业的成功实践案例。同时，接受调研的技术应用者反馈：谨慎的实践态度并不会影响整体的隐私计算投入规划，但将对厂商的安全性能力展开更深入的考察。

技术应用者目前缺乏对隐私计算安全性的有效判断力，技术认知有待加强

隐私计算产品内核涉及较多隐私保护技术和加密算法。在基于数学、密码学和硬件技术等综合形成的保障机制内的交互与计算呈现多样性和复杂性的特点，基于安全仿真用例的POC测试也难以完全检验产品安全性问题。此外，用户目前也需要具备行业共识的隐私计算安全评价体系和安全等级标准，来实现对各类隐私计算技术方案的安全能力等级界定。

行业用户对隐私计算安全性问题的关注度调研



分析师对90位技术领导者展开了访谈，根据受访者反馈意见，对安全性问题的四类关注度定义如下：

关注度	解释说明
极为关注	将安全性作为对隐私计算产品能力考察的首要维度，在具备权威机构安全性测评和认证基础上，会基于安全仿真用例进行深度POC测试，且需要产品通过形式化验证工具提供安全自证。
较为关注	将安全性作为对隐私计算产品能力考察的关键维度，在具备权威机构安全性测评和认证基础上，会基于安全仿真用例进行全面POC测试。
一般关注	将安全性作为重点关注指标之一，会基于安全仿真用例进行POC测试。
非重点关注	对合作厂商的信任度较高，认为安全性风险较低，但是也会进行相应的安全性测试。

注释：随着技术应用的持续深入，研究团队分别在不同的时期内，对同样的90位技术领导者展开了相同问题的调研。
来源：市场调研、艾瑞咨询研究院自主研究及绘制。

要点2：安全性问题（2/3）

隐私计算的安全性问题分析

隐私计算的行业用户应该正视安全性问题

- 各类技术算法、系统均存在被攻击的风险，隐私计算同样如此。诸如信道攻击、系统攻击等隐私计算所面临的安全性问题同样也常见于其他技术应用中。从另一个角度来看，技术安全性问题的发现与修复也是技术综合能力迭代的过程，而未被发现安全性问题的产品或者技术方案，并不代表一定具备更高的安全性。往往在技术实践初期对安全性问题的提早发现，也可避免技术规模化应用后再发现安全性问题而带来更大的业务损失。
- 对于隐私计算的安全性挑战，应该从“优化技术方案、增加产品安全自证能力、融入安全监测及安全防御能力”等方式，来综合提升技术实践中的安全性。

隐私计算安全性挑战的主要体现

	问题类型	问题解释	涉及风险因素
01	安全假设风险	• 所谓的安全假设是指在算法设计和实现过程中，需要基于一定的安全假定前提（如：假设多个参与方之间均遵守指定规则及协议流程且不存在同谋等），安全性假设模型之外的情况发生均会在不同程度上产生相应风险，因此需要通过博弈论、容错协议和现实约束等方式来加强安全。	• 安全假设风险 • 恶意参与者风险 • 节点攻击风险
02	算法可解释性难度	• 隐私计算拥有多元且复杂的算法以及多样化的计算与交互逻辑，增加了技术的可解释性难度。这将让隐私计算的实践过程中的多方参与者难以一致评估、理解算法模型，难以确定相关算法出现问题时应在何种程度上实现成功检测。	• 算法自身安全性 • 算法可解释性的难度
03	平台及系统安全	• 系统及平台自身设计的安全性：隐私计算产品设计模式、系统所涉及的技术方案等方面的自身安全性风险。 • 外部攻击：业务实践过程中所面临的系统外部攻击风险、网络通信攻击风险。 • 引入三方机构降低技术信任完整性，增加安全假设风险系数。	• 平台及系统自身的安全性 • 外部攻击风险 • 三方机构介入带来的潜在风险
04	可信硬件的安全风险	• 需要基于对硬件厂商的信任前提下实现（“问题类型01”范畴）。 • 可信硬件方案存在侧信道攻击（边信道攻击）风险（“问题类型03”范畴）。	• 厂商信任风险 • 外部攻击风险

来源：行业专家访谈、艾瑞咨询研究院自主研究及绘制。

要点2：安全性问题（3/3）

卓越安全隐私计算实践：最优安全设计 + 有效安全证明

- **最优安全设计**：隐私计算面临来自安全假设、算法可解释性、平台系统以及可信硬件的多方面安全挑战。行业用户可以通过“最优安全设计”原则展开技术实践。所谓“最优安全设计”并非单纯追求安全最大化，而是结合具体业务需求，平衡性能、安全性、通用性等多维因素，从技术方案设计和产品选型层面，寻找安全最优解。
- **有效安全证明**：厂商如何证明所提供产品的安全性，是目前行业用户所关心，以及厂商迫切需要解决的问题。有效安全证明是指在产品使用前、中、后通过各类方式对产品安全性、业务实践安全性进行证明。此外，在有效安全证明的基础上，还需要在产品使用中融合安全防御能力，并可以在发现安全问题后，即时中止计算执行，做到风险隔离。

卓越安全隐私计算实践思路

最优安全设计

从产品技术方案设计维度寻找安全最优解

iResearch：隐私计算产品“最优安全设计”的核心性原则

- **原则 1**：合理、充分地融合多元技术能力展开安全最优设计。
- **原则 2**：平衡业务需求的前提下，选择最优的安全假设模型。
- **原则 3**：以技术手段+管理手段，降低安全假设的风险影响。
- **原则 4**：数据安全分级下的差异化安全级别方案的精准匹配。
- **原则 5**：充分考虑系统、通信等方面的安全设计。

实证分析 **满足“最优安全设计”原则的典型实证案例：蚂蚁链摩斯**

- 摩斯通用产品和一体机分别集成了蚂蚁自研的国密认证的软密模块和密码卡，摩斯一体机还采用了基于TPM的可信度量、安全容器等技术，从硬件、系统等层面增强安全性，同时融合了差分隐私、脱敏、匿名化等隐私保护技术，全方面保障数据隐私。
- 摩斯可以在用户体验一致情况下，提供不同安全和性能级别的方案。
- 摩斯不依赖可信中心方，提供抗共谋攻击的方案，并采用零知识证明等技术手段达到恶意安全模型。
- 摩斯还从系统安全、通信安全等方面保障数据隐私。

有效安全证明

围绕产品应用的全流程进行安全性证明

产品使用前（要点列举）	产品使用中（要点列举）	产品使用后（要点列举）
• 权威机构测评证明。 • 源代码层面的安全自证。 • 安全假设模型的合理性验证。 • 通过安全仿真用例，展开深度的POC测试，主动性检验平台安全性。	• 通过形式化验证工具进行安全自证。如通过流量监测、数据抓包、代码校验等方式，来确保系统运行符合安全要求、确保计算按照预先设定的算法步骤进行执行。 • 融入安全防御能力应对恶意攻击，在风险发生时及时切断计算运行，保证数据安全。	• 通过“日志审计功能+区块链可信存证”，让数据流转过程等内容实现可追溯，进而展开产品使用后的安全审计工作。

产品POC、使用中、使用后：基于区块链不可篡改的存证，监管机构和协作方可以对算法安全性、授权体系的完备性进行检验，进一步强化安全自证的可信度。

来源：艾瑞咨询研究院自主研究及绘制。

要点3：性能问题（1/2）

隐私计算的性能问题分析

隐私计算的规模化落地实践需要满足业务需求的性能支持，而性能的影响因素来自于多个方面。

Section 1
加密算法对性能的影响

加密算法在计算过程中存在较多的加密、解密步骤，让计算量以几何级增长，相比明文计算，密文计算需要更大的存储、计算资源和通信负载，导致性能损失。

Section 2
资源因素的影响

在加密算法的计算和通信过程中，网络通信环境、数据预处理情况、算力、运行环境等因素也会对隐私计算的性能产生相应的影响。

Section 3
多方协同的“木桶效应”

多方计算模式下，需要多个参与方同步计算、实时通信，在性能上体现出了“木桶效应”，即：性能最弱的参与方或者计算节点将成为整个网络的计算瓶颈。

行业用户需要在产品测试环节中综合考量各类性能影响因素

28.9%的应用者反馈：产品在真实业务环境中的性能表现和POC测试环节中的性能表现存在差异。

为了寻找原因，我们对这部分受访者展开了访谈，来确定在产品测试环节和真实业务环境中，究竟是哪些性能影响因素存在差异而导致了上述情况的发生。其中典型原因反馈为（选取占比最高的三类情况）：

- 38.5%应用者反馈：**真实业务环境中的多方协同计算场景要远复杂于测试环境。**
- 33.3%应用者反馈：**是由于产品测试环节中的加密轮次低于真实业务环境中的要求所形成的差异。**
- 25.6%应用者反馈：**是由于数据预处理情况不同所导致的性能差异。**

目前是隐私计算商用实践的初期阶段，**关于隐私计算性能问题，行业用户需要强化技术认知，**在POC测试环节中，充分考虑“加密轮次、数据预处理情况、算力、运行环境、计算方式”等影响因素，**尤其是加密轮次是否为安全最优解，**避免在产品在正式投产后无法达到预期实践效果。

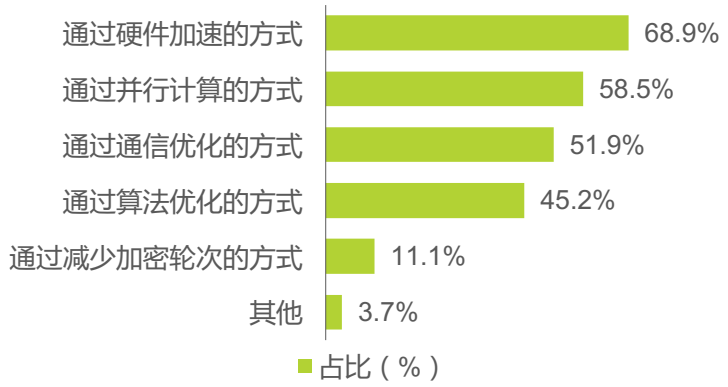
注释：1、调研样本来自银行、保险、政务、运营商、医疗等领域的隐私计算技术应用者（含IT/科技部门应用者、业务部门技术应用者）；2、调研中，每位受访者可以选择多个选项。
来源：隐私计算应用者调研（N=135），艾瑞咨询研究院自主研究及绘制。

要点3：性能问题（2/2）

隐私计算可以从硬件、算法、通信、计算方式等多个维度来提升性能，不能以牺牲安全性的方式来提升性能

- 基于GPU、FPGA、或是将算力加速能力固化至ASIC中的硬件加速方式是隐私计算应用者选择度较高的性能解决方案。此外，将特定隐私敏感处理环节通过TEE进行保护，可以有效弥补密文计算的性能损失，也为性能提升提供了新思路。比如通过TEE与联邦学习结合，将联邦学习各参与方之间的互相认证与模型训练跨组织传输逻辑移植进TEE，极大地提升了联合建模性能。
- 除了硬件加速的方式外，强化并行计算能力、算法优化（降低模块耦合度、算法流程优化等）、通信优化（节点通信优化、通信环境优化等）等也是目前行业中常见的性能优化方式，各类方式均有特点。
- 不建议采用“减少加密环节/轮次”的方式，这种安全换性能的策略将为数据安全带来隐患。

隐私计算应用者对性能解决方案的接受度调研



注释：1、调研样本来自银行、保险、政务、运营商、医疗等领域的隐私计算技术应用者（含IT/科技部门应用者、业务部门技术应用者）；2、每位受访者可以选择多个选项，因此各选项综合大于100%。
来源：隐私计算应用者调研（N=135），艾瑞咨询研究院自主研究及绘制。

隐私计算应用者对性能解决方案的选择考量

在性能优化方案的选择中（多选题设置）：

83.7%的应用者：**将安全性的影响作为「首要」考量因素**

66.7%的应用者：**将投入成本作为「关键」考量因素**

在选择“速硬件方式”的应用者中（单选题设置）：

16.1%的应用者：**在最初实践时便考虑硬件加速产品的采购**

83.9%的应用者：**在实践中遇到性能问题后，进行硬件加速产品的购买与使用。**

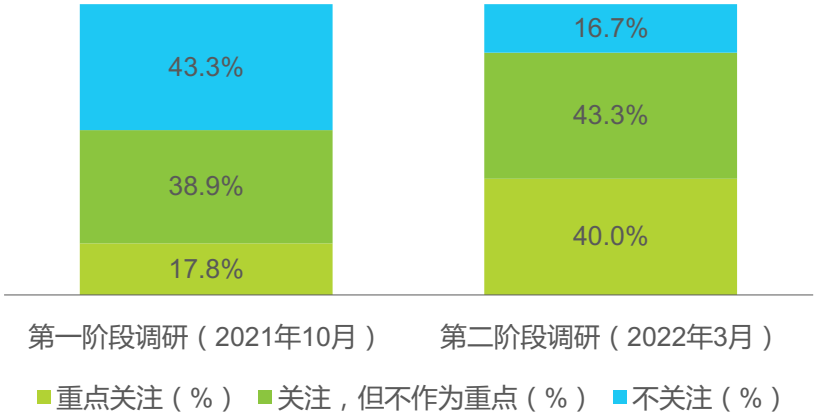
注释：访谈样本来自银行、保险、政务、运营商、医疗等领域的隐私计算技术应用者（含IT/科技部门应用者、业务部门技术应用者）。
来源：隐私计算应用者访谈（N=135），艾瑞咨询研究院自主研究及绘制。

要点4：软硬件结合

行业用户正在加深对隐私计算软硬件结合技术方案的关注

- **隐私计算软硬件结合的技术方案可以兼顾性能和安全性的保障：**在我们近期所展开的一项市场调研中发现，越来越多的行业用户开始关注软硬件结合的解决方案。从市场客户的隐私计算历史采购经验来看，大部分客户主要偏向于软件层面的技术方案，但是随着密文计算所带来的性能瓶颈越来越明显，软件层面所面临的各类安全性风险也逐渐被用户所关注。软硬件结合的技术方案可以通过加速卡、可信硬件等多维技术方式，兼顾性能和安全性的保障。
- **越来越多的市场玩家在软硬结合技术方案上展开布局：**除了多年技术能力沉淀的蚂蚁链摩斯、以信创国产化战略为基底打造软硬件一体机的冲量在线、面向数据密态计算场景提供高性能软硬件算力加速服务的星云Clustar外，还有提供面向政务金融的高性能软硬结合信创产品的洞见科技、以国产化为核心而推出软硬协同隐私计算产品的数牍科技等厂商也在积极加强软硬件结合的技术能力。越来越多参与者的入局也说明了隐私计算软硬结合技术方案的正向发展趋势。

行业用户对隐私计算软硬件结合技术方案的关注度调研



注释：随着技术应用的持续深入，研究团队分别在不同的时期内，对同样的90位技术负责人进行了相同的调研。
来源：市场调研、艾瑞咨询研究院自主研究及绘制。

隐私计算软硬件结合典型案例解读：蚂蚁链摩斯一体机

Section 1 软、硬件技术能力方面

对于软硬件结合方案的产品（或技术）选型，除了对软硬件的性能、安全性等重要指标的考查外、软硬件适配性也同样重要。我们发现摩斯一体机具备如下优势：

- **性能方面：**通过自研蚂蚁加速卡，可以实现对半同态、同态、椭圆曲线算法的百倍加速。此外，同样可以支持GPU等硬件加速设备。
- **安全性方面：**通过“国密认证密码卡、具备可信度量功能的自研TPM可信根芯片、加密硬盘”等增强数据计算和存储的安全性。
- **软硬件适配性：**自主研发隐私计算平台MORSE，实现与硬件的深度适配。

可信硬件需要依赖于对厂商及其供应链伙伴的信任，摩斯一体机具备如下优势：

- **增强用户对硬件的信任：**产品核心软硬件国产化（如蚂蚁研发的自主可控TEE方案）、无供应链和后门忧虑。

Section 2 用户体验方面

用户产品选型视角下，在Section1中对关键能力考查的基础上，如何提供卓越用户体验，是产品提供方应该重点考量的问题。摩斯一体机在这方面具备如下优势：

- **高效的集成与交付：**支持灵活的账号体系适配和日志对接、数据对接等功能，实现业务系统低成本快速集成。
- **高效的应用与运维：**摩斯一体机支持开箱即用、可视化运维等能力。

来源：艾瑞咨询研究院自主研究及绘制。

要点5：国产化

基于数据安全和技术自主可控的需求，行业用户更加青睐基于国产化可信硬件的隐私计算产品

在研究团队近期所展开的调研[1]中，在国产化与非国产化产品之间，93.6%的技术领导者会优先采购国产化隐私计算产品。报告以TEE为例展开分析：TEE需要基于预置集成了可信执行控制单元的CPU计算芯片来实现，这便需要确保芯片厂商的安全可信。虽然国外的芯片厂商相比中国厂商拥有更为成熟的产品和技术方案，但是国产芯片厂商拥有更强的自主可控性。在国产化自主可控的需求驱动下，国内芯片厂商将通过持续的研发投入来不断提升国产化可信硬件技术能力。目前国内的兆芯、海光、飞腾等芯片厂商相继推出了TEE技术方案，并与冲量在线等技术服务商联合推出软硬件一体的隐私计算产品。同时冲量在线等技术服务商也持续通过超算、金融等大规模应用场景实践，反推国产化TEE技术性能与可靠性的升级。

国内外的可信执行环境（TEE）技术方案对比

技术方案	国外			国内		
	Intel SGX	TrustZone	AMD SEV	海光CSV	飞腾TrustZone	兆芯TCT
发布时间	2015	2005	2016	2020	2019	2017
指令集架构	X86_64	ARM	X86_64	X86_64	ARM	X86_64
是否支持任意代码运行	是	是	是	是	是	是
硬件安全密钥	有	无	有	有	无	有
完整性认证与封存	支持	不支持	支持	支持	不支持	支持
内存加密	是	否	是	是	否	否
内存完整性保证	支持	不支持	不支持	支持	不支持	支持
TEE安全I/O	不支持	支持	支持	支持	支持	支持
可用内存空间	≤1T	系统内存	系统内存	系统内存	系统内存	系统内存
TCB	硬件：CPU Package 软件：Enclave内的代码实现	硬件：安全虚拟核 软件：安全世界OS和TA	硬件：AMD secure processor 软件：虚拟机镜像	硬件：海光SME 软件：虚拟机镜像	硬件：安全虚拟核 软件：安全世界OS和TA	硬件：CPU&TPCM

1、N=203，受访者主要是企业/机构内的IT/科技部门负责人，被调研企业主要是数字力领先的组织（国有商业银行、股份制银行、部分数字化程度领先的城市商业银行、头部保险机构、地方大数据局、通信运营商集团）。

来源：艾瑞咨询研究院自主研究及绘制。

要点6：隐私计算跨平台互联互通(1/3)

iResearch 艾瑞咨询

隐私计算跨平台的互联互通将打破“计算孤岛”制约，促进产业化的全域数据流通

Section 1 计算孤岛的形成

- 在应用实践中，数据使用方通常需要和不同的数据源合作，而不同的数据源也往往部署着不同的隐私计算平台。因为多数隐私计算厂商平台主要采取闭源形式，加之技术路线多样化、各平台间系统架构不同、功能实现方式差异等问题，导致不同平台之间无法实现数据的可信流通，出现了“计算孤岛”问题。
- 针对这个问题，如果数据使用方分别部署不同隐私计算平台，则会产生系统重复建设和运营成本增加的问题，同时也会降低数据使用方的业务效率。

Section 2 计算孤岛的破局之道：跨平台互联互通

- **隐私计算跨平台互联互通**：让不同隐私计算平台通过标准化协议、规范化接口进行连接，实现管理系统、算法协议等各层面的交互协同，进而让不同隐私计算平台共同完成同一项计算任务，打破计算孤岛限制。
- **隐私计算跨平台互联互通的三类模式**：**黑盒模式**（基于独立的闭源算法）、**白盒模式**（基于开源算法源码）、**灰盒模式**（基于算法逻辑）。
- **隐私计算跨平台互联互通由易到难逐次分为**：管理系统的互联互通、算法协议的互联互通、计算原语的互联互通。
- **隐私计算跨平台互联互通的意义**：互联互通的有效实现是数据要素全面流通的基础，也是产业全域数据可信流通的关键。

隐私计算跨平台互联互通的总体架构

应用层	实现系统应用层面的互联互通：主要包括节点管理、任务编排、任务执行、监控管理等内容。
协议层	实现各类协议层面的互联互通：主要包括算法协议、资源协议、节点交互协议三方面的内容。
通信层	实现通信层面的互联互通：主要包括加密传输机制、通信框架与接口、数据传输格式等内容。

来源：隐私计算跨平台互联互通的总体架构参考中国通信标准化协会《隐私计算 跨平台互联互通》标准：第1部分 总体框架、行业专家访谈、艾瑞咨询研究院自主研究及绘制。

要点6：隐私计算跨平台互联互通(2/3)

行业用户需求、厂商实践探索、行业标准制定与实施将在不同层面上推动隐私计算跨平台互联互通的发展

Section 1 发展现状：隐私计算跨平台互联互通处于初期探索阶段

- **标准方面**：目前行业标准正在持续完善中，如中国通信标准化协会《隐私计算 跨平台互联互通》系列标准目前已发布“第1部分：总体框架”，整体内容还在持续制定。
- **实践方面**：**一类是厂商自发的跨平台互联互通实践**，目前互相合作的实践者主要实现了“管理系统层、算法协议层”的互联互通，但是较多还未基于算法插件展开具体业务的应用实践，目前原语层的互联互通均在探索阶段。此外，也有部分厂商仅签订了合作协议而尚未展开具体实践。**另一类是来自行业客户的跨平台互联互通建设需求**，现阶段此类项目需求有限（如招商银行发起了跨平台互联互通建设项目），随着行业客户对多样化数据源接入需求的不断提出，互联互通建设的项目需求也会随之涌现，进而推动互联互通的产业生态发展。

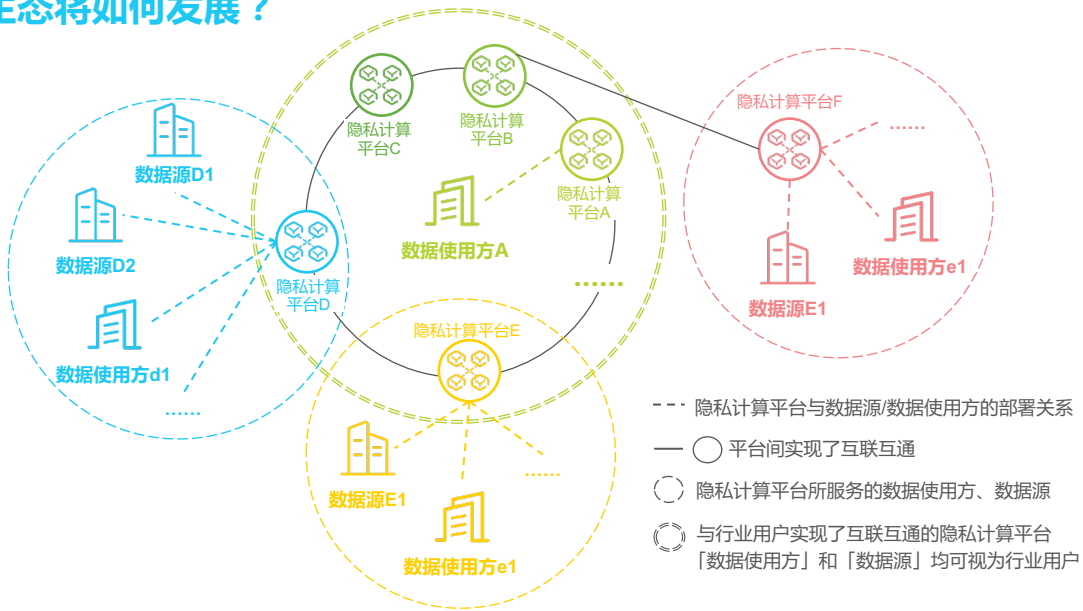
Section 2 隐私计算跨平台互联互通生态将如何发展？

互联互通将演变成为“横纵交织”的生态网路

- **横向**：隐私计算平台之间的主动实践；
- **纵向**：行业用户需求推动的互联互通实践。

除了厂商之间自主的跨平台互联互通实践外，随着行业客户在场景实践中对多样化数据源接入需求的不断涌现，**基于客户发起的跨平台互联互通建设项目，将成为互联互通发展的有效催化剂。**在两类不同方式推动的下，隐私计算跨平台互联互通将形成横纵交织的生态网路。

同时，在隐私计算实践中，**通过构建兼容性强、开放度高的互联互通技术底座**，可以支持算法组件以即插即用的方式接入，**让跨平台的应用实践更加敏捷高效。**



来源：艾瑞咨询研究院自主研究及绘制。

要点6：隐私计算跨平台互联互通(3/3)

隐私计算跨平台互联互通的典型实践案例

Case 1 基于行业客户发起的项目需求：招商银行五方异构隐私计算平台的互联互通

招商银行作为数据使用方，需要接入部署着不同隐私计算平台的数据源。为了避免多平台部署的重复建设及监管难度，招商银行“慧点”隐私计算平台通过“可插拔式平台框架+算法组件架构”的方案，与洞见科技、富数科技、平安科技、同盾科技四家企业实现了异构隐私计算平台的互联互通。

该方案的整体实现需要分为两个步骤

Step 1：管理系统互联互通

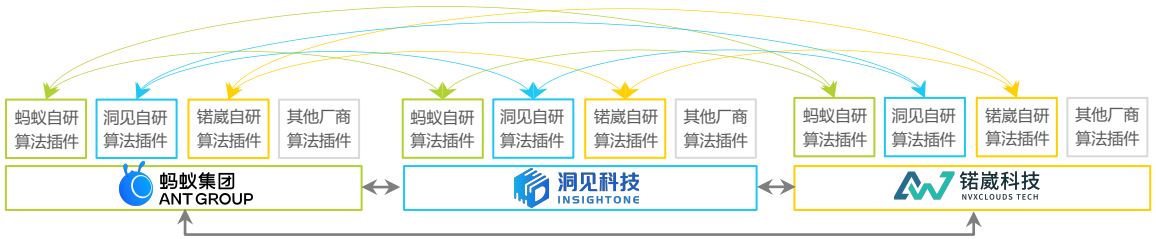
各方搭建可插拔式平台支持算法组件的即插即用，并在平台层面使用同一套协议规范进行互联互通。

Step 2：算法组件互联互通

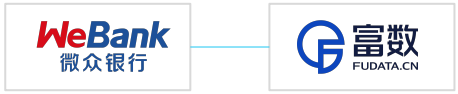
以“白盒模式（针对公开算法）+黑盒模式（针对自研算法）”的方式实现算法组建的互联互通。

Case 2 基于厂商自主发起的实践：多方异构隐私计算平台之间对等算法协议互通

该项目由蚂蚁集团共享智能部、洞见科技、锘崴科技三个厂商为探索隐私计算跨平台互联互通实践而自主发起。项目实现了“管理系统、算法协议”层的互联互通，目前正在探索“计算原语”层的互联互通。



Case 3 基于厂商自主发起的实践：异构联邦学习平台的互联互通



该案例是由微众银行的AI团队和富数科技对异构联邦学习平台互联互通探索，基于联邦学习分层协议，划分节点互联层、数据资源层、算法迁移层、计算互操作层，抽象出了“节点、数据、算法、计算任务、安全认证”等对象模型。以此为基础，践行三个战略步骤。

步骤 1：节点互相发现及数据资源共享。

步骤 2：算法组件按照统一标准实现跨平台迁移部署。

步骤 3：联邦学习任务的跨平台执行。

来源：相关厂商调研与求证、艾瑞咨询研究院自主研究及绘制。

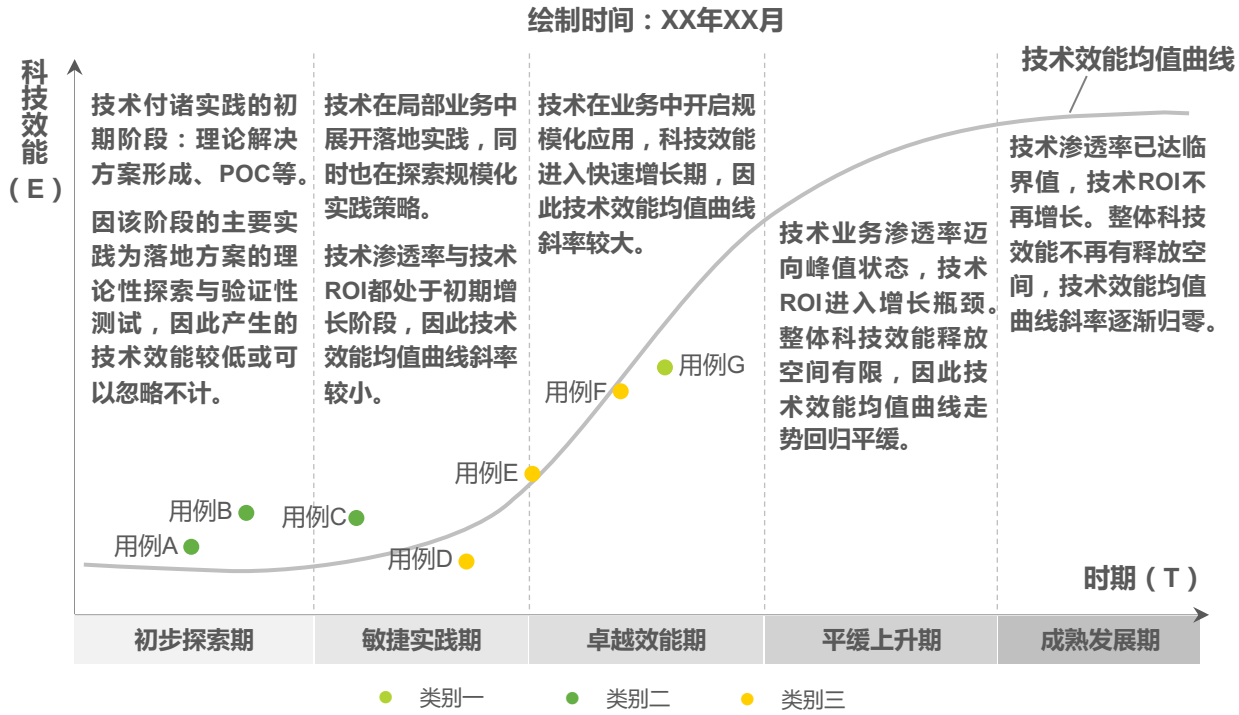
一级（核心）研究工具（1/2）

iResearch：技术效能发展象限

基于艾瑞对技术宏观面的研究，我们对“iResearch：技术（科技）效能发展象限”这一研究工具展开了进一步的细化设计与定义。

- **在一个完整的科技效能周期内，技术效能均值曲线的走势（斜率）将伴随所处时期的不同而发生变化。**
- **下述周期规律不仅适用于单项技术的落地实践研究，同样适用于一类技术（多元技术融合）的实践研究。**

iResearch：（研究周期）技术效能发展象限



来源：艾瑞咨询研究院自主研究及绘制。

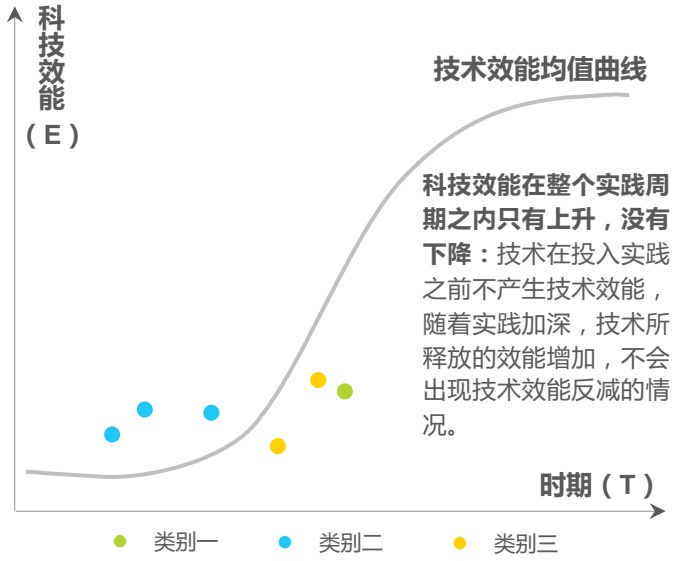
一级（核心）研究工具（2/2）

定义两种效能曲线：技术效能均值曲线 & 业务效能曲线

在艾瑞的技术宏观面研究中，我们将“技术”与“业务”作为两个主要的观测锚定点。下述两类曲线的标准制定中，艾瑞参考了大量来自金融、政务、制造业、运营商等诸多行业中多项技术实践的案例实证与数理实证。

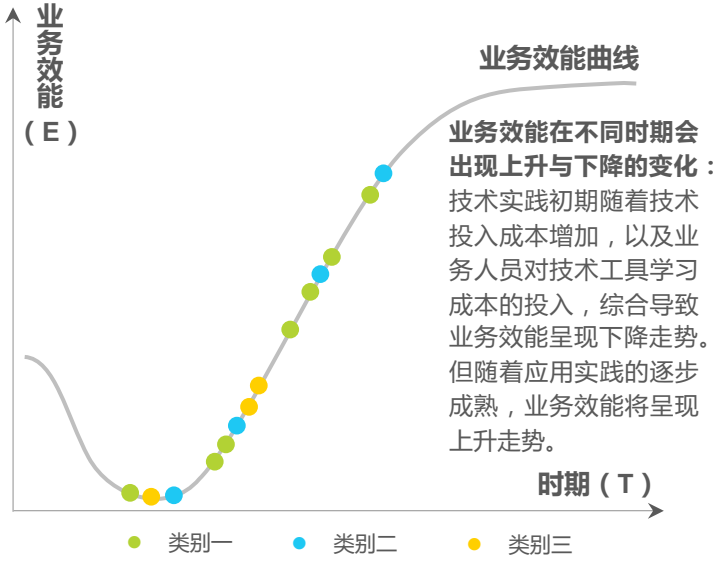
- **定义1 - 技术效能均值曲线：反映技术在一个行业/领域中实践的完整周期里，技术效能的变化规律。**
- **定义2 - 业务效能曲线：反映技术在一个行业/领域中实践的完整周期里，业务效能的变化规律。**
- 技术效能均值曲线是用例参考曲线，业务效能均值曲线是用例定位曲线。

Model 1：iResearch - 科技效能发展象限



@iResearch：科技效能发展象限

Model 2：iResearch - 业务效能发展象限

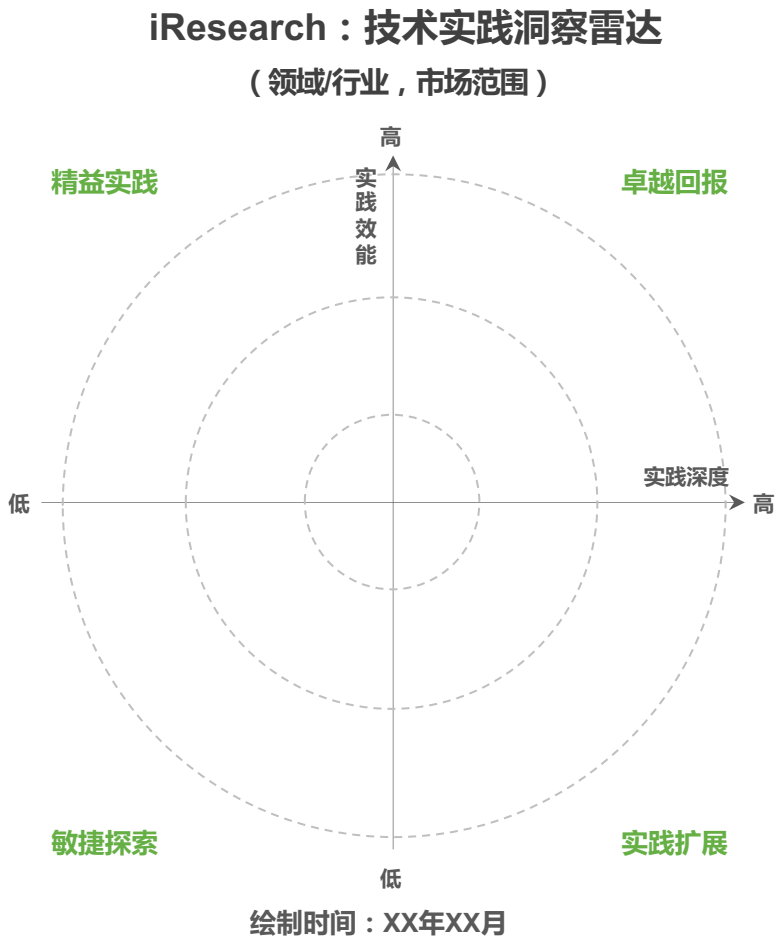


@ iResearch：业务效能发展象限

来源：艾瑞咨询研究院自主研究及绘制。

二级（辅助）研究工具

iResearch：数字实践洞察雷达



对技术应用实践情况的研究，“iResearch：技术实践洞察雷达”将设置相应评估指标（在“实践深度”与“实践效能”这两个维度下设置多个细化指标，不同类别的技术通常需要差异化设置细分指标）。以此为基础，分析师将结合案例实证研究及数理实证研究，输出研究成果。

来源：艾瑞咨询研究院自主研究及绘制。

01 研究工具说明

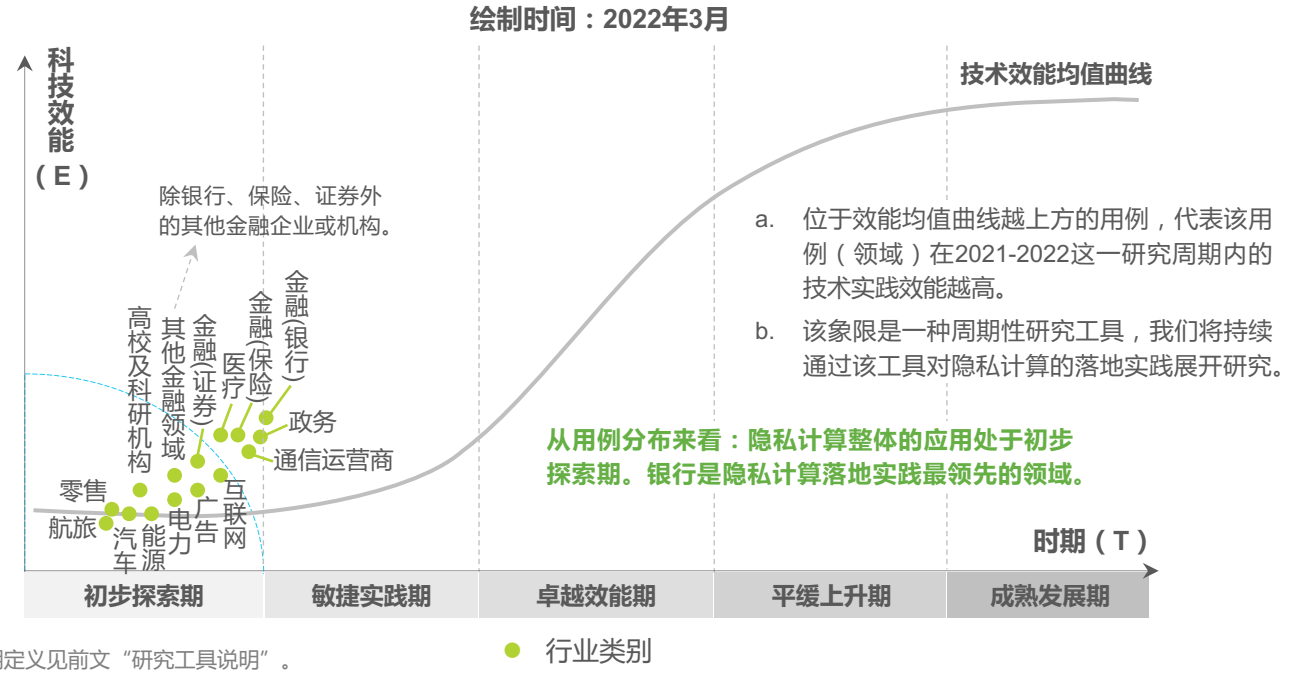
02 研究成果输出

隐私计算效能发展象限

隐私计算目前处于落地初期阶段，金融、政务、通信运营商领域的商用实践相对领先；医疗领域拥有较高的技术实践契合度，部分厂商对此寄予良好的市场发展愿景

目前行业处于“基建期”，隐私计算在企业与机构中的商业实践也主要处于POC或者通过POC的初步应用阶段。根据对行业用户技术实践规划的调研，金融、政务、通信运营商、医疗等领域在1～3年内将展开加速投入，率先推进“行业基建”的同时展开相应场景实践，逐步由初步探索期[1]迈向敏捷实践期[2]。

iResearch：2021-2022年中国隐私计算效能发展象限



注释：1&2：各发展时期定义见前文“研究工具说明”。
来源：艾瑞咨询研究院自主研究及绘制。

象限解读说明

@ iResearch：2021-2022年中国隐私计算效能发展象限

象限解读：依托象限背后所支撑的案例实证、数理实证、市场调研信息，对隐私计算商用实践中的关键问题展开分析。

象限解读分为两个部分：象限整体解读、象限关键用例解读。

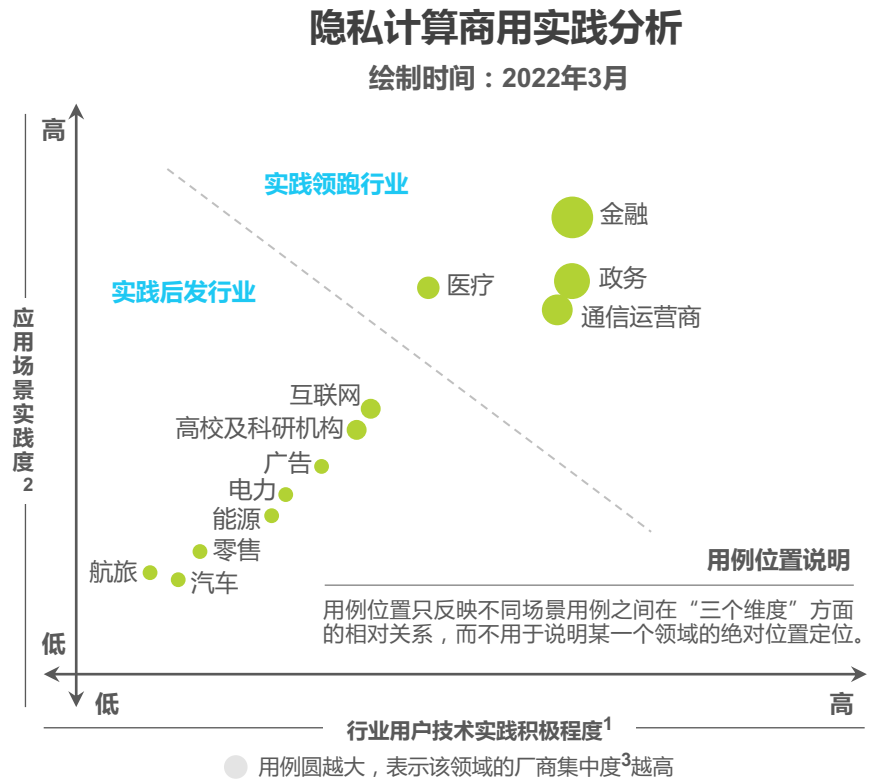
欲对象限进行更为深入的了解与研究，请联系艾瑞咨询。

来源：艾瑞咨询研究院自主研究及绘制。

象限整体解读

隐私计算的商用实践分析

在“iResearch：2021-2022年中国隐私计算效能发展象限”的研究基础上，我们围绕“应用场景实践度、行业用户技术实践积极程度、厂商领域集中度”三个维度进行解读。



注：1、行业用户技术实践积极程度：通过行业用户数、招投标次数、采购金额等维度综合反映。2、应用场景实践度：通过应用场景数量、实践深度、业务应用深度等维度综合反映。3、厂商集中度：将某一领域作为关键市场发展方向的厂商数量。

来源：艾瑞咨询研究院自主研究及绘制。

Section 1：整体商用实践

- **实践领跑行业**：金融、政务、通信运营商是招投标次数和企业采购金额较多的领域。医疗行业市场份额虽然相对少于上述三个领域，但拥有较高的技术实践契合度，市场发展空间被看好。
- **实践后发行业**：如航旅、能源、电力、汽车等领域，现阶段的招投标次数和企业采购金额相对较少。

Section 2：细分领域商用实践

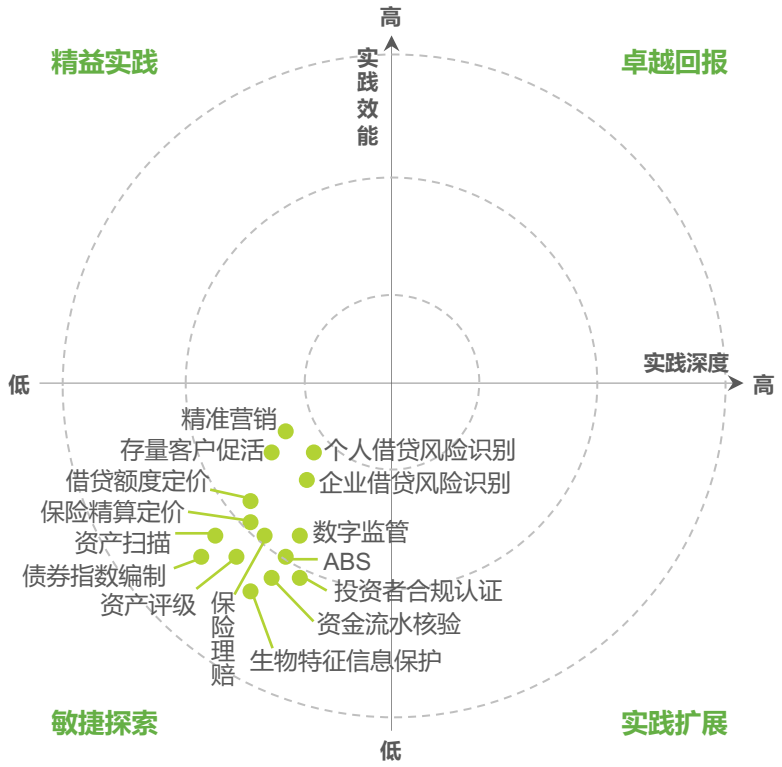
- **实践领跑行业（金融）**：金融领域客户数量庞大、数字化程度领先，成为兵家必争之地。目前银行的商用实践领先，保险、证券也在逐步跟进实践进程，这也是一项技术在金融领域落地的一贯规律。对于厂商来说：头部金融机构数量较少，与其合作更重要的意义在于树立典型实践案例。中尾部金融机构的数量庞大，对这部分目标客户的渗透率将成为决定厂商在金融领域市场占有率的关键影响因素之一。
- **实践领跑行业（政务）**：相比于金融领域，政务领域的客户数量有限，但是客单价相对较高（结合2021年客单价来看）。政务领域的数据开放将为数据运营市场带来巨大的发展机会。
- **实践领跑行业（医疗）**：医疗行业是隐私计算实践认可度较高的领域，但同时也对厂商提出了更高的专业能力要求（能力要求见后文对“医疗”用例的解读）。虽然医疗领域目前的厂商集中度不高，但部分厂商正在将医疗列为市场边界拓展的核心方向。
- **实践领跑行业（通信运营商）**：作为数据提供者的角色，运营商将基于隐私计算平台能力的建设，让数据开放走向合规化，同时也将加深数据开放的广度与深度。
- **实践后发行业**：能源、电力、航旅等领域虽然在现阶段不是隐私计算商用实践的主阵地。但是因为各领域间存在不同程度的数据流通需求，因此“实践领跑者”将在一定程度上带动“实践后发者”的隐私计算应用实践。

象限关键用例解读：金融（1/2）

技术实践分析

iResearch：隐私计算实践洞察雷达

（金融领域，中国市场）



绘制时间：2022年3月

Section 1：发展现状分析

- **基础设施建设的发展现状：** 2021年金融机构用户主要以技术基础设置建设为主。国有大行、股份制银行是展开隐私计算平台建设的主力军，部分保险公司、证券公司、少部分城商行等也有参与实践。市场调研发现，2021年第四季度的POC数量出现大幅增加，这也为2022年的金融机构隐私计算平台建设的高速增长打下基础。
- **应用层场景实践和数据调用需求：** 部分客户会在平台建设的同时提出数据源接入需求，进而为后续的应用层场景实践做准备。对于应用层的场景实践来说，风控类、营销类的场景实践案例较多，定价、评级、ABS、监管等场景也在逐步落地，部分厂商基于场景模型的定制化方案中，在逐步探索标准化数据智能产品。此外，基于银行等机构对跨平台数据调用的需求，还有行业客户（如招商银行）还发起了互联互通建设的项目需求，进而为多方数据调用和应用层场景实践做好技术铺垫。

Section 2：未来发展预估

a. 调研显示，**预计2022年展开隐私计算投入的金融机构数量约是2021年的2倍或2倍以上（增量部分包括了在2021年处于POC进而在2022年正式投入应用的金融机构）。**参与隐私计算实践的金融机构数量的增加，将在一定程度上让技术实践深度、技术实践效能实现同频提升。

b. 随着平台建设的完善，应用层的场景实践将陆续展开，拥有优秀数据运营能力的厂商将具备竞争优势。

c. 分析师认为**风控、营销大类场景中至少分别会有1～3个细分场景用例进入“实践扩展”象限，这些细分场景将在技术性能允许的范围内，扩大业务实践范围。**

d. 隐私计算将进一步与区块链技术融合，推进金融可信基础设施建设，强化数字监管能力，并逐渐融入监管沙盒体系。

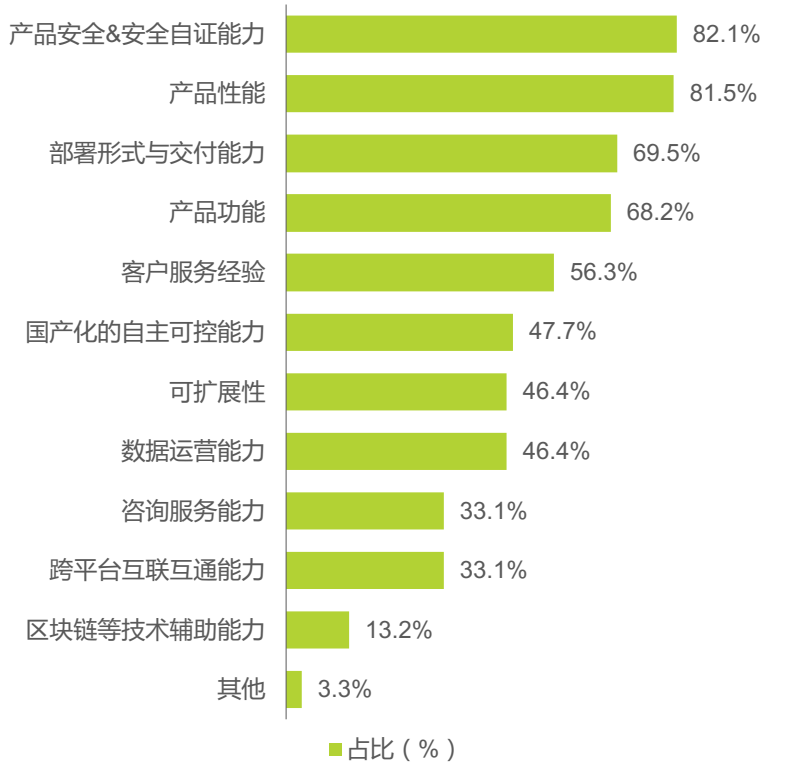
注释：1、隐私计算处于落地实践初期，且较多案例处于POC阶段，因此各类业务场景主要集中于“敏捷探索”象限；2、在当下隐私计算的落地阶段，雷达图主要用于反映隐私计算在各领域中的整体落地状态，现阶段行业中的高价值案例实证与数理实证有限，且技术实践中的变量因素较多，雷达图用例分布状态在短期内极有可能发生较大位置变化。
来源：艾瑞咨询研究院自主研究及绘制。

象限关键用例解读：金融（2/2）

行业用户调研

金融机构用户所关注的隐私计算技术服务商能力

（2022年3月调研，中国市场）



注释：1、N=151，受访者涵盖金融机构中的IT/技术部、各金融业务部门等技术应用者；2、研究团队首先征集了相关技术应用者主要关注的能力方向，分析师对此进行归纳整理，并设计了选项；3、在调研过程中，每一位受访者最多选择六个选项。
来源：金融机构调研、艾瑞咨询研究院自主研究及绘制。

行业用户的技术战略实践视角下：
隐私计算应用的重要关注点

该部分内容由分析师对金融机构用户进行访谈而综合整理得出，下述所列是受访者关注度较高的内容。这些内容从数字战略角度反映了行业用户对隐私计算的价值定位与实践考量。

约75.5%的金融机构技术实践者关注：

隐私计算对开放金融战略的影响

金融机构将自身服务能力对外开放时，需要多维度的数据对目标用户需求展开精准判断，以此加深金融服务质量与深度。在这个问题上隐私计算将发挥卓越价值。

约67.5%的金融机构技术实践者认为：

隐私计算将推动金融全域数字化建设进程

根据艾瑞持续对金融机构数字战略的关注，全域数字化的发展一直被定义为数字金融发展的关键底层能力。银行、保险领域对全域数字化建设的需求更为迫切，隐私计算以数据可信流通为基础，将协同多元化的可信技术能力，构建全域数字化建设的闭环。

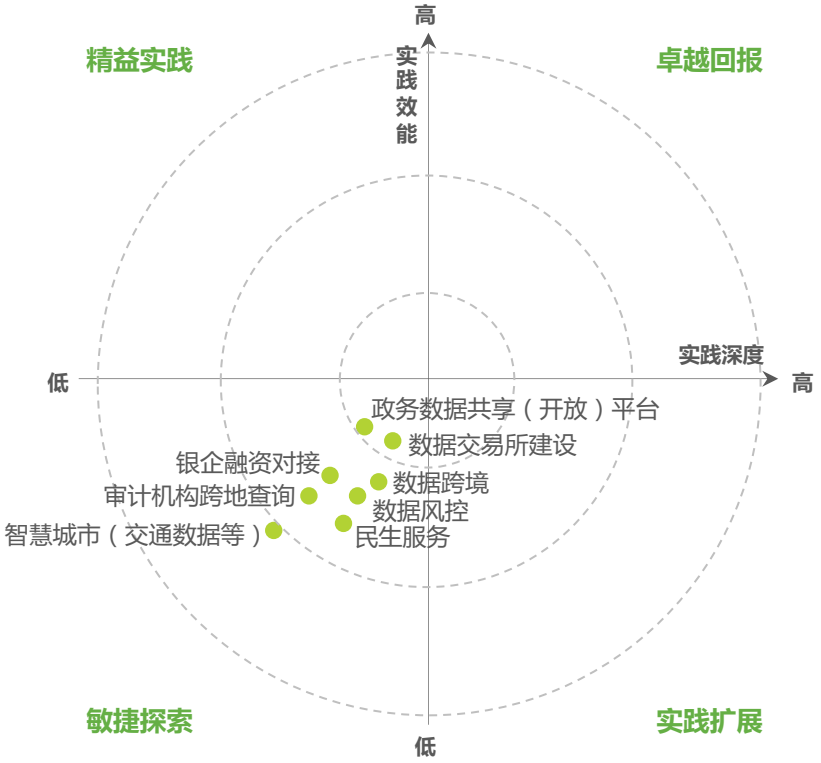
注释：N=151，受访者涵盖金融机构中的IT/技术部、各金融业务部门等技术应用者。
来源：金融机构调研、艾瑞咨询研究院自主研究及绘制。

象限关键用例解读：政务（1/2）

技术实践分析

iResearch：隐私计算实践洞察雷达

（政务领域，中国市场）



绘制时间：2022年3月

Section 1：发展现状分析

- **政务机构的隐私计算整体实践分析：**2021年，随着《数据安全法》《个人信息保护法》的相继出台与实行，以及相关政策的支持与鼓励下，政务机构开始逐步进行隐私计算平台建设的投入。地方大数据局、数据资源管理局等相关单位是现阶段的主要技术采购方。因目前隐私计算在政务领域的实践主要处于基础设施建设阶段，**应用层的场景实践主要以探索为主，所以雷达图暂不进行细化场景的用例展示。**
- **政务机构的隐私计算应用，可以从“横向”和“纵向”两个维度来分析。从“横向”角度来看，**政务机构在数据跨境、民生服务等方面展开了积极探索，在数据隐私保护的前提下，一定程度上降低了不同组织间数据协作的审核成本；**从“横向”角度来看，政务机构需要践行数据开放战略。**政府部门汇集了交通、教育、税务等多维度、高量级、高价值的数据，隐私计算的应用让传统模式下无法开放的政务数据可以实现安全可控的流通，因此除了隐私计算平台的建设外，政务机构还需要具备数据运营能力的服务商，让数据以“产品化”的形式对外开放。

Section 2：未来发展预估

a. 结合市场调研，预计2022年展开隐私计算投入的政务机构数量约是2021年的1.5～2倍（增量部分包括了在2021年处于POC进而在2022年正式投入应用的用户）。

b. 基础设施建设将依然是政务机构在2022年的主要投入，部分应用层场景实践也会随着基础设施建设的实现而同频展开。

c. 在促进数据要素流通的背景下，政务机构将逐渐开放自身数据能力赋能各行各业。**政务机构将与技术服务商有望以BOT的模式展开合作。**

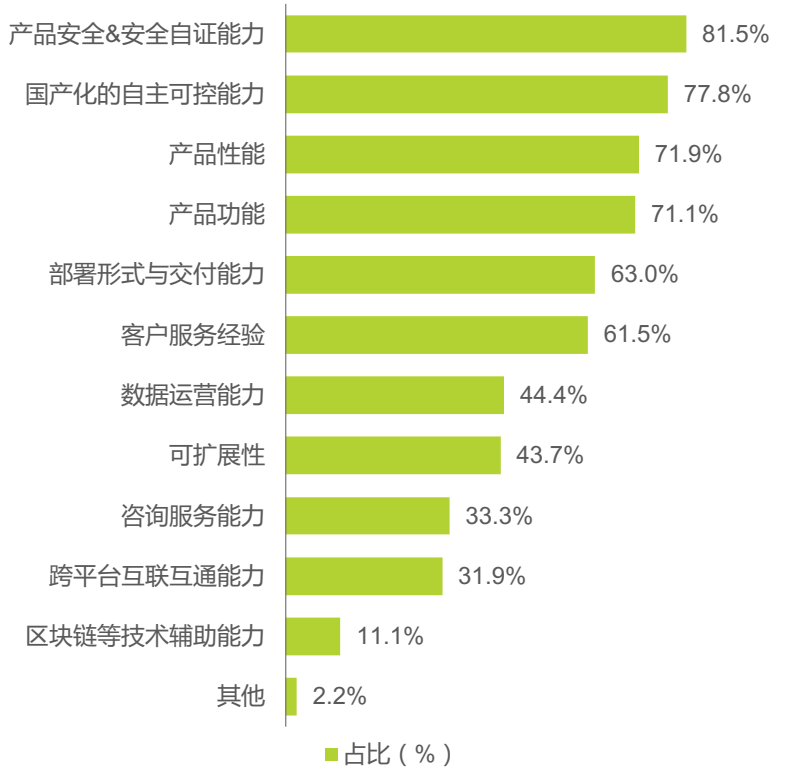
注释：1、隐私计算处于落地实践初期，且较多案例处于POC阶段，因此各类业务场景主要集中于“敏捷探索”象限；2、在当下隐私计算的落地阶段，雷达图主要用于反映隐私计算在各领域中的整体落地状态，现阶段行业中的高价值案例实证与数理实证有限，且技术实践中的变量因素较多，雷达图用例分布状态在短期内极有可能发生较大位置变化。
来源：艾瑞咨询研究院自主研究及绘制。

象限关键用例解读：政务（2/2）

行业用户调研

政务机构用户所关注的隐私计算技术服务商能力

（2022年3月调研，中国市场）



注释：1、N=135；2、研究团队首先征集了相关技术应用者主要关注的能力方向，分析师对此进行归纳整理，并设计了选项；3、在调研过程中，每一位受访者最多选择六个选项。
来源：政务机构调研、艾瑞咨询研究院自主研究及绘制。

行业用户的技术战略实践视角下：隐私计算应用的重要关注点

该部分内容由分析师对政务机构用户进行访谈而综合整理得出，下述所列是受访者关注度较高的内容。这些内容从数字战略角度反映了行业用户对隐私计算的价值定位与实践考量。

约87.1%的政务机构技术实践者关注：

隐私计算在“政务数据开放共享，促进数据要素市场化配置”方面的实践价值

政务领域的技术应用者积极响应政策，在通过隐私计算所构建的可信数据流通基础设施上，将积极践行数据开放战略。受访者反馈，除了基础设施的建设外，未来政务机构的数据开放需要与具备良好数据运营能力的厂商进行合作。

约71.0%的金融机构技术实践者关注：

隐私计算对“跨部门/单位的数据流通效率提升”方面的实践价值

受访者较为关注隐私计算对打破数据孤岛的实践价值，改变以往不同单位/部门之间数据流转效率低的问题，提升机构内部的工作效率以及面向群众的公共服务效能。

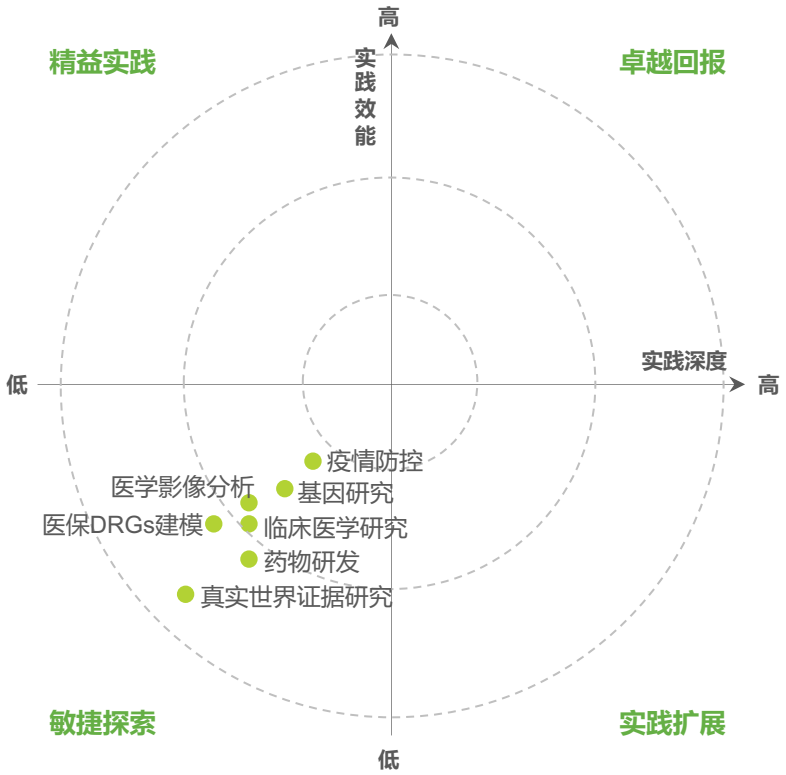
注释：N=135。
来源：政务机构调研、艾瑞咨询研究院自主研究及绘制。

象限关键用例解读：医疗

技术实践分析

iResearch：隐私计算实践洞察雷达

（医疗领域，中国市场）



绘制时间：2022年3月

Section 1：隐私计算+医疗的应用实践特点

- **医疗领域的数据类型更为多元化、且复杂度高**：医疗领域中，除HIS系统中的结构化数据外，还拥有如病例、医嘱等大量非结构化数据，以及CT医学影像信息、基因等多类型的数据信息。相比其他领域的数据类型更多，复杂度更高。
- **数据处理与分析方法更为多元化**：非医疗领域通常以逻辑回归、树模型等方法可以实现征信、风控、营销等多数场景的应用需求。医疗领域除了常用的数据分析模型外，还需要基因数据对齐、全基因关联组分析、影像勾划、病灶识别、非结构化数据的关键信息提取等关于统计学分析、生成率分析等数据处理与分析的方法。
- **医疗领域的联合计算参与方数量更多**：例如科研合作、新药研发等应用场景通常需要十几家甚至几十家医院的联合参与，因此对多节点并发计算的能力要求更高。
- **安全性要求更高**：医疗领域多数场景的联合计算数据结果与患者生命安全相关。在隐私计算的实践中需要更为安全的恶意模型假设，在计算过程中发生恶意篡改时，可以实现即时阻止。
- **计算结果精度要求更高**：医学领域的数据计算结果需要实现零误差或者将误差控制在极低的范围内，否则将会在新药获批、临床辅助诊断结果等方面产生影响，因此需要可以保证精准计算结果的隐私计算解决方案。

Section 2：未来发展预估

a. 医院之间存在医疗信息互联互通的考核，卫健委正在加速制定医疗领域的数据安全指南及相关标准方案，在《数据安全法》等相关法律出台后，医学专家需要通过数据不出院的方式展开联合科研，这些因素都将加速医疗机构的隐私计算投入。

b. 结合医疗机构调研及卫健委相关政策的实施，预计在2022年底或者2023年初，医疗领域的隐私计算采购将实现一定程度的增长。并在2023～2025年，医疗领域进入隐私计算投入的增速期。

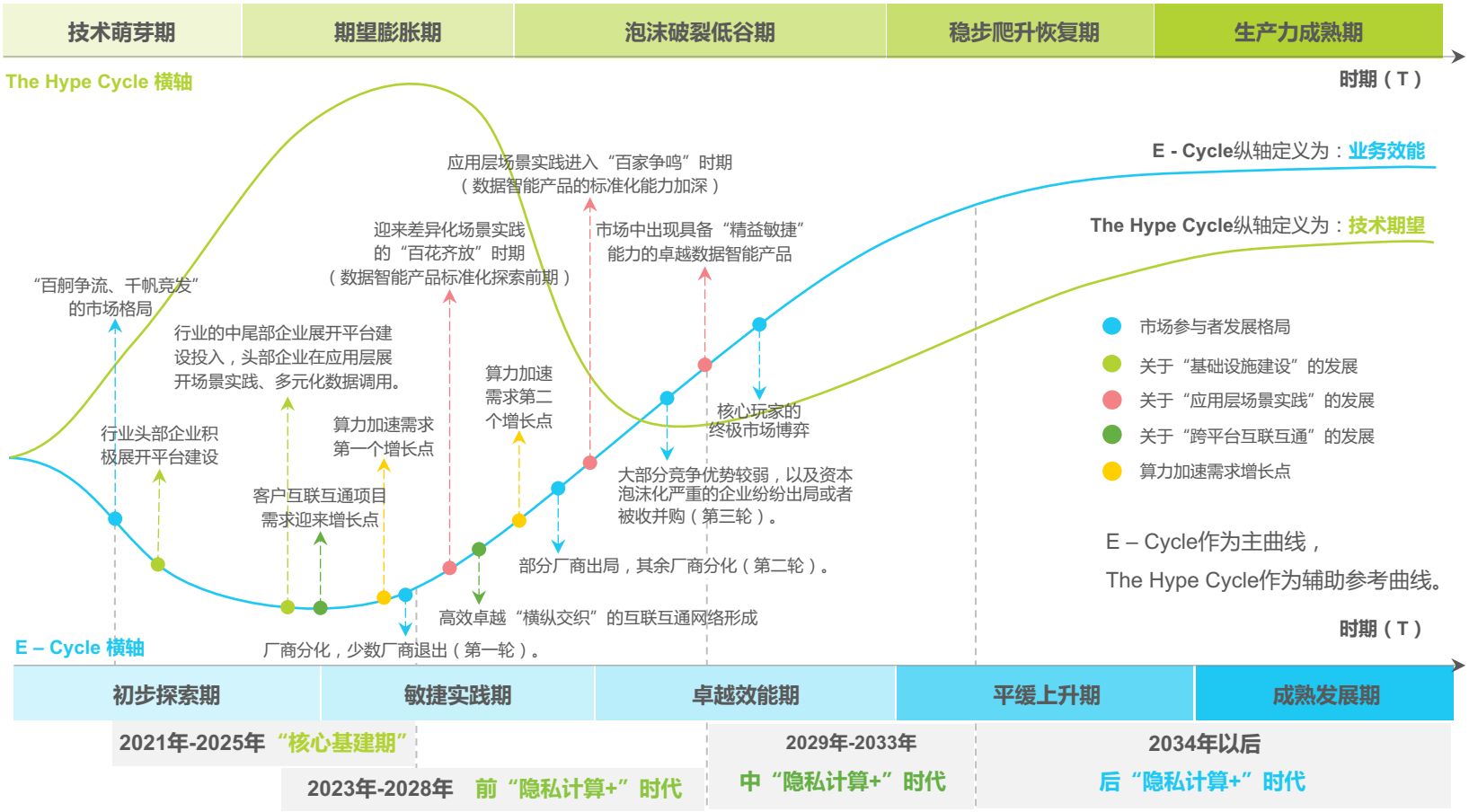
注释：1、隐私计算处于落地实践初期，且较多案例处于POC阶段，因此各类业务场景主要集中于“敏捷探索”象限；2、在当下隐私计算的落地阶段，雷达图主要用于反映隐私计算在各领域中的整体落地状态，现阶段行业中的高价值案例实证与数理实证有限，且技术实践中的变量因素较多，雷达图用例分布状态在短期内极有可能发生较大位置变化。

来源：艾瑞咨询研究院自主研究及绘制。

隐私计算发展周期洞察矩阵

iResearch：隐私计算发展周期洞察矩阵（对趋势的研究，中国市场）

绘制时间：2022年3月



注释：“矩阵”通过被验证的方法论，基于大量案例实证、数理实证、市场调研信息、顶级专家观点、技术领导者意见等内容的研究而综合绘制。
来源：隐私计算的案例实证研究、数理实证研究、行业用户调研、隐私计算厂商调研、艾瑞咨询研究院自主研究及绘制。

矩阵解读说明

@ iResearch：隐私计算发展周期洞察矩阵

矩阵融合了“技术成熟度曲线（诞生于硅谷）和业务效能曲线[1]（一种被验证过的研究方法[2]，由艾瑞可信科技研究团队设计）”两种研究工具，从技术能力、业务实践等多个视角反映了技术的发展周期。

矩阵解读：依托矩阵背后所支撑的案例实证、数理实证、市场调研信息、顶级专家观点、技术领导者意见，对隐私计算的发展趋势进行解读分析。

欲对矩阵进行更为深入的了解与研究，请联系艾瑞咨询。

说明： 1、关于业务效能曲线的介绍，见本报告第三章“研究工具介绍”。
2、业务效能曲线（E - Cycle）被应用在诸多的咨询项目、行业研究、案例实证研究中，其合理性和实用性均接受过完备校验。

来源：艾瑞咨询研究院自主研究及绘制。

矩阵解读（1/3）

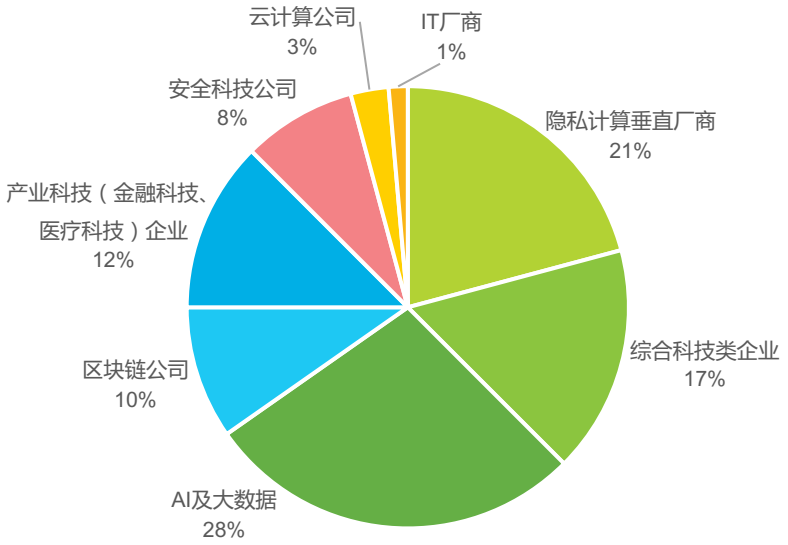
iResearch 艾瑞咨询

市场参与者发展格局

Insight 1 在目前“千帆竞发”的市场格局下，中国隐私计算市场将经历多次的“大浪淘沙”

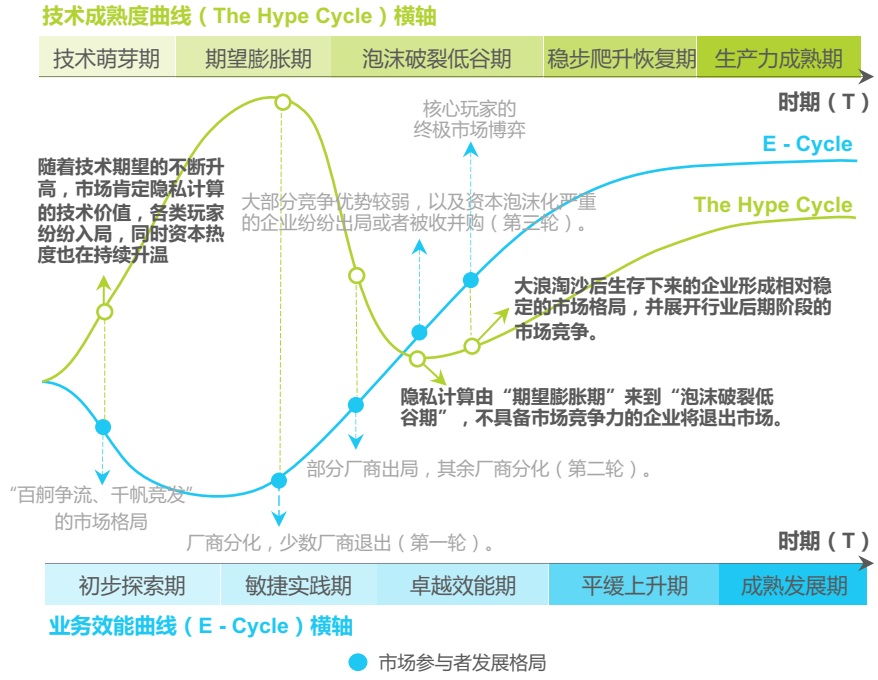
目前隐私计算的市场参与者类型众多，不同厂商的能力优势、发展策略也存在差异。在行业的早期阶段，市场营收和融资能力将同时影响公司的生存发展。但是随着技术由期望膨胀期走向泡沫破裂低谷期，资本热度将逐渐退去，没有“造血能力”的市场玩家将逐渐退出市场或者被收并购。在“核心基建期”，具备卓越产品力（技术优势）、市场力（市场开拓能力和资源优势）的厂商通常会获得更多的行业用户，这些厂商通过行业用户的积累将在“隐私计算+”时代占据一定的基础优势。而在“隐私计算+”时代，能够打造卓越数据智能产品、拥有差异化优质数据源、能提供精益敏捷服务的厂商将更具发展优势。

中国不同类型的隐私计算市场参与者占比



注释：1、“中国不同类型的隐私计算市场参与者占比”统计范畴为通过了“中国信通院、国家金融科技测评中心（银行卡检测中心）、中国金融认证中心（CFCA）隐私计算产品测评”的科技企业（金融机构、运营商等非技术企业不在统计范畴内）；2、统计时间截至2022年2月。
来源：艾瑞咨询研究院自主研究及绘制。

隐私计算市场格局变化分析



来源：艾瑞咨询研究院自主研究及绘制。

©2022.3 iResearch Inc. www.iresearch.com.cn

矩阵解读（2/3）

iResearch 艾瑞咨询

● **关于“基础设施建设”的发展**

Insight 2 2022年~2025年是中国隐私计算基础设施建设的关键时期

“矩阵”所定义的「核心基建期」是指到2025年，关键领域的头部企业和具备领先数字实践力的中尾部企业将会完成核心的技术基础设施建设，将2025年作为隐私计算基础设施建设的一个节点，主要源于如下实证判断：

1. **基于行业用户的调研：**在金融（针对数字实践力领先的机构）、政务、运营商领域的技术领导者调研[1]中，80%+的技术领导者计划在2022~2025年期间陆续展开并完成隐私计算的基础平台建设，随之进行应用层的场景实践。
2. **相关发展政策的推动：**2025年是《“十四五”大数据产业发展规划》、《金融科技发展规划（2022-2025年）》等相关发展规划的收官之年，其发展规划中均有提及利好隐私计算基础设施建设的相关内容。

● **关于“应用层场景实践”的发展**

Insight 3 中国隐私计算行业终将进入“隐私计算+”时代，打造“精益敏捷”的卓越数据智能产品将成为核心竞争力

「“隐私计算+”时代」是在完善隐私计算基础设施建设的前提下，行业用户展开应用层差异化场景实践的时期。商用实践的聚焦点由“基础产品服务”转向“数据运营服务”。**数据运营方需要通过数据运营能力来持续创造价值，**如数据字段变更、数据分布密度变化、算法模型变化等都可能需要对数据产品进行敏捷调整，面对数据「使用者」的差异化需求，还需要提供多元化的数据接入能力。因此，打造卓越数据智能产品，以及丰富高质量数据源生态的建设变得尤为重要。然而，数据提供者往往也更愿意与用户认可度高的数据智能产品合作，因此打造卓越数据智能产品将成为核心竞争力。

打造卓越数据智能产品

精益化的产品服务	多样化变动下的敏捷应对
以用户需求为核心，设计最好用的产品	构建敏捷能力应对多元变化，持续创造价值
• 通过构建丰富多元的模型库满足用户差异化场景实践需求。 • 通过差异化用户需求的精益洞察，打造用户体验最优产品。	面对差异化用户需求、算法模型变化、数据字段变更、数据分布密度变化等，可通过“分层设计”等策略实现敏捷应对。

封装通用模型组件，设计可参数化调整的功能模组，最大程度上展开标准化数据智能产品的设计。

1、N=203，受访者主要是企业/机构内的IT/科技部门负责人，被调研企业主要是数字实践力领先的组织（国有商业银行、股份制银行、部分数字化程度领先的城市商业银行、头部保险机构、地方大数据局、通信运营商集团）。

来源：艾瑞咨询研究院自主研究及绘制。

矩阵解读（3/3）

● **关于“跨平台互联互通”的发展**

Insight 4 行业客户需求将成为隐私计算跨平台互联互通发展的强力催化剂

相比于厂商自主的隐私计算跨平台互联互通实践，基于行业用户所发起的互联互通建设项目更加具备业务实践的针对性。这也会有效打破厂商之间因为竞争隔阂而引起的互联互通阻碍。“矩阵”预测了跨平台互联互通的两个关键节点：

- **在「核心基建期」内的互联互通项目需求增长点：**主要是由隐私计算实践力领先的企业发起，在「核心基建期」中后期阶段，实际上已经进入了「前“隐私计算+”时代」，这个时间节点中，实践力领先的企业在应用层的场景实践方面已经展开了相应的投入，对跨平台数据调用的需求也在不断增多。
- **在「前“隐私计算+”时代」的中期阶段：**跨平台互联互通建设是深入展开应用层场景实践的基础，在企业应用层场景实践对多方数据调研需求的驱动下，将推动高效卓越“横纵交织”的互联互通网络的建成，这将为差异化应用场景实践的顺利开展提供基础保障，同时也为进入「中“隐私计算+”时代」打下基础。

● **算力加速需求增长点**

Insight 5 随着隐私计算场景实践的逐渐深入和计算量的增加，算力加速需求也将不断涌现

隐私计算场景实践的加深将会在不同程度上同频带动算力加速需求的增加。从“矩阵”的洞察结论也可以发现：在隐私计算跨平台互联互通推动下的场景应用实践的加深，以及差异化场景实践“百花齐放”时期的到来，算力加速需求都迎来了同频增长。结合“矩阵”研究过程中，对具备领先实践力的技术领导者调研，艾瑞研究团队与其最终的共识为：

- 未来3～5年，**30%+**开展隐私计算应用场景实践的企业将为算力加速展开投入或者已经在应用具备算力加速能力的产品。
- 未来5～10年，**70%+**开展隐私计算应用场景实践的企业将为算力加速展开投入或者已经在应用具备算力加速能力的产品。

来源：艾瑞咨询研究院自主研究及绘制。

“隐私计算 卓越者”介绍（1/2）

报告研究过程中，分析师团队累计调研了39家企业。

其中包括：隐私计算垂直厂商、大型科技企业/集团、人工智能公司、云计算企业、大数据服务公司、金融科技公司等多类企业。

每家企业均经过了1～3轮的调研，形式包括调研表填报、企业高管及业务人员访谈、面向技术应用者的验证性访谈。

在所调研的39家企业中，有17家入围卓越者。

研究团队重点征询了53位来自金融、政务、通信运营商、医疗等领域的产业专家意见，确定“隐私计算卓越者”的入围企业。

来源：艾瑞咨询研究院自主研究及绘制。

“隐私计算 卓越者”介绍（2/2）

如何确定入围者？

“隐私计算 卓越者”的评选由内外两部分评审团组成：内部评审团的评审权重为*20%*、外部评审团的评审权重为*80%*。

步骤1 卓越者提名

由“隐私计算 卓越者”的内、外部评审团队，共同进行隐私计算企业提名（本次共计提名企业45家，展开调研企业39家）。

步骤 2 内部评审

由“隐私计算 卓越者”的内部评审团队对提名企业进行评选，输出评选结果。

步骤 3 外部评审

由“隐私计算 卓越者”的外部评审团队对提名企业进行评选，输出评选结果。

步骤 4 结果的审核校验

对评审结果进行校验审核，保证结果的准确公正性，确定最终入围者名单（本次最终入围企业17家）。

入围者的评估指标有哪些？

根据企业类型的不同，我们将“隐私计算 卓越者”分为“前瞻推动者、核心攻坚者、精益融合者”三个类别。每个类别企业均有相应的入围基准（在入围者名单公布的内容中有介绍），在此基础上，我们将对企业从下述维度展开能力评估。

综合得分 = 产品力×0.35 + 产品实践力×0.3 + 市场力×0.35

产品力

1、产品安全性（20%）
2、产品性能（20%）
3、产品功能（20%）
4、集成与交付能力（15%）
5、服务能力（15%）
6、其他能力（10%）

说明：“其他能力”中包含了各类技术路线的实现能力、互联互通能力、国产化能力、区块链辅助隐私计算能力等多维指标。

技术实践力（实践案例评估）

1、案例实证评估（50%）
- 如实践背景、实践模式、定性价值等。

2、数理实证评估（50%）
- 从定量角度对厂商技术实践力的评估。

市场力

1、覆盖行业数量（35%）
2、客户数量（65%）
3、商业营收（辅助参考项）

注释：评选指标括号内的百分数代表指标的评审权重。
来源：艾瑞咨询研究院自主研究及绘制。

卓越者入围说明

Qualification Statement for Outstanding Enterprises

@ iResearch：“隐私计算 卓越者”艾瑞咨询研究团队 & 产业专家团队

1. 所有的入围者，均为接受过研究团队调研的企业，其在综合能力或者关键能力方面获得了研究团队及产业专家团的一致肯定。
2. “隐私计算 卓越者”的选定，艾瑞咨询研究团队征询了来自金融、政务、通信运营商等领域的专家意见，外部专家团站在技术应用者的角度提出了相应的观点和看法。
3. “隐私计算 卓越者”由艾瑞咨询研究团队及产业专家团共同提名（共计提名企业45家），研究团队也在最大程度上实现了对厂商的触达（实际调研企业39家）。对未展开调研或者未接受调研的企业，艾瑞咨询不对其发表任何评判观点。
4. “隐私计算 卓越者”不代表企业排名，也不能说明未入围者完全不具备产品力或市场力的优势。
5. 本次调研仅为对企业的当下能力判断，不代表对企业的长期判断。

联系研究团队

来源：艾瑞咨询研究院自主研究及绘制。

“隐私计算 卓越者”入围企业

iResearch 艾瑞咨询

前瞻推动者

按企业汉语名称音序排列

蚂蚁集团 ANT GROUP　WeBank 微众银行

大型科技企业/大型机构对隐私计算的前瞻性布局，有效地推动了行业的发展。“前瞻推动者”要求企业拥有顶尖的科研团队、3年以上的隐私计算投入与研发、具备隐私计算技术的前瞻性探索经验、卓越的产品技术创新能力、优秀的技术落地实践能力。

核心攻坚者

按企业汉语名称音序排列

冲量在线 IMPULSEONLINE　洞见科技 INSIGHTONE　富数 FUDATA.CN　華控清交 HUA KONG TSINGJIAO　金智塔 数智引领未来

蓝象智联　锘崴科技 NVXCLOUDS TECH　数牍 sudo　CLUSTAR 星云

“核心攻坚者”是推动隐私计算技术发展、商用落地的核心力量。“核心攻坚者”的入围企业是在综合能力或者某一项重要能力方面具备卓越优势，并受到研究团队和产业专家一致认可的隐私计算垂直厂商（目前公司自身定位是隐私计算厂商的企业）。

精益融合者

按企业汉语名称音序排列

4Paradigm 第四范式　趣链科技 HYPERCHAIN　RealAI 瑞莱智慧　天冕　TRANSWARP 星环科技　UCLOUD 优刻得

产业专家及艾瑞研究团队一致认为：隐私计算将与多元科技实现深度融合，而非“孤立式”的应用。“精益融合者”主要为非垂直于隐私计算领域的科技公司，包括区块链公司、人工智能公司、云计算公司、大数据服务公司、金融科技公司等。这类企业在隐私计算与多元技术融合的探索中发挥了高效的推动价值。

来源：艾瑞咨询研究院自主研究及绘制。

蚂蚁链摩斯：中国隐私计算行业的领先布局者和卓越推动者

- **蚂蚁链摩斯是隐私计算行业的领先布局者：**早在2017年，蚂蚁集团启动了MPC项目，并于2018年正式发布蚂蚁链摩斯品牌。蚂蚁链摩斯通过多年来的产品和技术能力沉淀，打造了行业领先的隐私计算产品。
- **多样化的产品服务、多维度的技术能力：**蚂蚁链摩斯可以为用户提供开源、软件、一体机多个产品版本，且拥有世界领先的核心算法能力、低耗能高精度MPC、自研TPM芯片、自研蚂蚁卡等多维度领先的技术能力。进而形成了蚂蚁链摩斯在“产品安全、产品性能、产品功能、版本选择、用户体验、用户服务”等方面的卓越产品优势。
- **部分发展成果：**截至2022年2月，蚂蚁链摩斯已服务150余家行业客户，拥有200余项自主研发专利。曾获得国际隐私计算顶级赛事idash2019MPC大赛、idash2021同态加密和联邦学习大赛世界冠军。

蚂蚁链摩斯（MORSE）：产品能力及优势

安全合规
- **全生命周期安全保障：**计算前分级授权，计算中算法+规则双重保护，计算后日志审计。
- **多项权威认证，**信通院、金标委、国密等。
- **双安全引擎：**MPC、TEE。

功能完善
- **覆盖场景丰富：**隐私计算+可信协作。
- **权限管理：**跨机构多层次权限体系。
- **系统对接：**账号、数据、日志、消息。

多版本可选
- **开源：**安全模型
- **软件：**基础版和专业版
- **一体机：**密码卡、TEE卡、GPU加速。
- **API组件**

性能超群
- **在线服务支持千万级QPS，**性能为同类产品5-60倍。
- **大数据分布式框架，**支持10亿级数据计算。
- **低耗能：**比传统MPC协议CPU占用低80%，带宽减少50%。
- **多次获得国际大奖：**国际idash大赛MPC、同态加密、联邦学习冠军。

体验无忧
- **图形化+IDE：**满足不同数据角色产品使用需求。
- **数据对接：**文件/文件服务器/数据库/接口等。
- **自主运维：**健康检查、任务看板。

服务保障
- 专人支持交付
- 专人支持销售
- 丰富数据和媒体资源对接

来源：艾瑞咨询研究院自主研究及绘制。

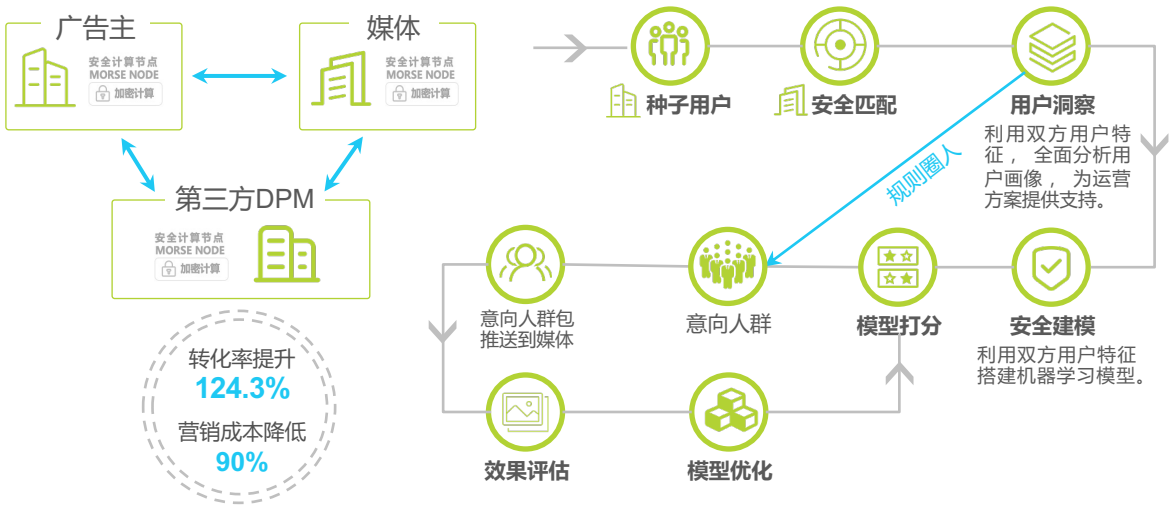
蚂蚁链摩斯：典型应用场景及实践案例解读

- **典型应用场景**：蚂蚁链摩斯通过多年来隐私计算实践积累，目前在联合营销、数据开放、联合风控、联合科研等领域拥有大量成功的实践案例。
- **实践案例解读**：本报告以联合营销场景为例，阐述蚂蚁链摩斯为某公司提供的精准营销解决方案。在该实践案例中，蚂蚁隐私计算平台可以在保护数据安全和个人隐私的前提下，针对客户和场景平台进行精准圈人，精准营销，有效提升营销转化率，降低营销成本。

蚂蚁链摩斯典型应用场景

联合营销	**客群**：有营销需求的商家，客群广泛。 **场景**：帮助广告商基于多方数据进行联合安全建模、部署、预测、精准刻画用户需求，提高广告设施投放转化率。
数据开放	**客群**：政务/民生/运营商/金融等机构等。 **场景**：提供数据开放服务，避免数据泄露，安全查询保护查询方用户隐私。
联合风控	**客群**：金融机构等。 **场景**：帮助金融机构之间提供风控数据分析、模型训练和风险决策，实现风控模型精细化和个性化，提升风险识别能力。
联合科研	**客群**：高校、科研机构等。 **场景**：帮助科研单位进行数据价值流通，联合研究，如疾病研究等。

蚂蚁链摩斯“某公司精准营销解决方案”案例解读



多方ID安全碰撞，保证ID安全。多方标签数据安全联合圈人/画像，精准触达，提升转化率。

多方数据安全建模，客群自动排序，进一步人群优化。

效果数据安全统计，可进行渠道转化分析，成本分析，轻 松完成营销活动ROI测算。

来源：艾瑞咨询研究院自主研究及绘制。

微众银行 WeBank 微众银行

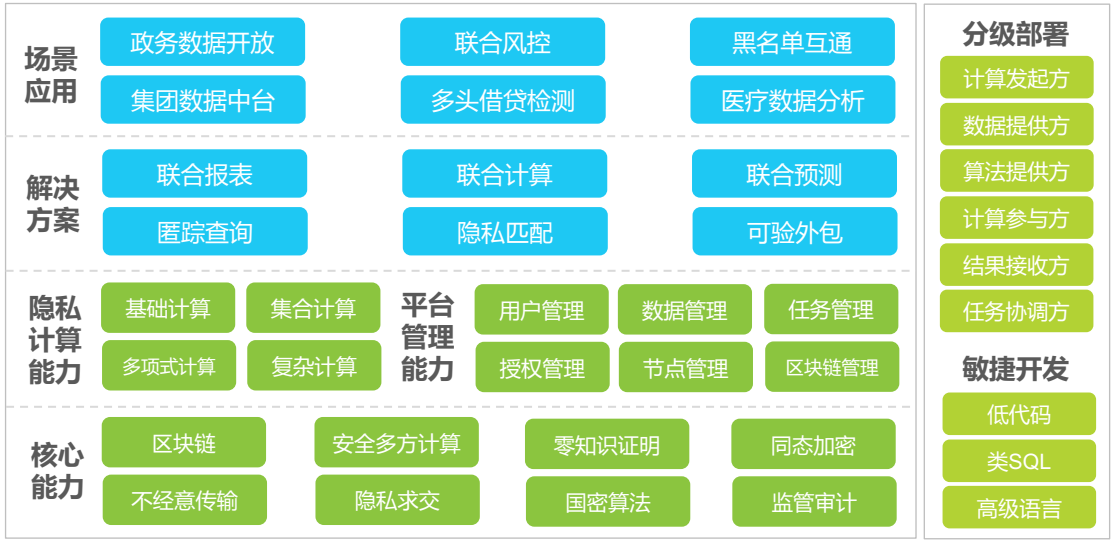
iResearch 艾瑞咨询

倡导技术开放，推动中国隐私计算行业高效发展

微众银行是中国隐私计算技术的领先布局者，以区块链、安全多方计算等关键技术，构建隐私计算核心能力，已形成丰富成果：正式发布的区块链开源项目超10个，生态圈汇聚超3000家企业机构、70000余名个人成员共建共治共享，成功支持政务、金融、社会治理等领域落地200余个标杆应用；针对隐私保护典型场景，提供场景式隐私保护解决方案WeDPR，并结合区块链和安全多方计算的优势，推出多方大数据隐私计算平台WeDPR-PPC。WeDPR-PPC首批通过中国信息通信研究院“区块链辅助的隐私计算产品”权威评测，并创行业之先，面向全行业开放核心功能体验，助力各界伙伴在可快速迭代的实验环境中，探索隐私计算的实际效果和能力边界。

微众银行：隐私计算技术能力介绍（以WeDPR-PPC为例 ）

WeDPR-PPC的主要功能



WeDPR-PPC全面满足国家级测试标准

全面隐私
- 明文数据不出库
- 全程密文计算
- 全程不解密
- 中间结果无法反推原始数据

性能优异
- 十万样本毫秒级匿踪查询
- 两方千万样本秒级跨表统计
- 两方亿级样本分钟级隐私求交

多方对等
- 支持多个机构参与计算
- 各参与机构地位对等
- 无需可信第三方

安全合规
- 全面支持国密
- 全项通过权威机构认证
- 全程基于区块链可信数据治理

功能齐全
- 支持通用计算，不限于建模、预测、查询、统计、比较
- 支持用户自定义计算逻辑

灵活易用
- 支持代理、直连等多种部署模式
- 无需特殊硬件
- 无需绑定特定平台
- 支持SQL及Python敏捷开发，可自定义业务逻辑。

来源：艾瑞咨询研究院自主研究及绘制。

微众银行 WeBank 微众银行

iResearch 艾瑞咨询

隐私计算应用场景探索

微众银行是中国率先投入隐私计算技术研发的企业之一，积极应用隐私计算解决金融、政务、公共健康、数字权益等领域的数据可信流通难题。同时，微众银行所践行的开放理念，大幅降低了应用隐私计算的门槛，有效拉近隐私计算技术和行业应用的距离。本报告以联合风控评分的场景为例，解读隐私计算的应用逻辑和成效。

微众银行“隐私计算+联合风控评分”应用场景解读

Part 1 面临问题

数据方在进行风控、定价、营销时，缺乏相应模型来分析、评估用户各维度数据，而模型方，则希望能持续使用外部数据来检验并更新自身风控模型，以提升模型质量。双方诉求的满足，需数据方与模型方协作进行联合预测。**然而，各机构的数据对于本机构来说属于核心资产，数据、模型直接互通牵涉利益和合规风险，实际场景中，各机构数据往往不能出库，难以实现跨机构的数据互通。**

Part 2 解决方案

数据方与模型方优势互补，开展协作预测，可基于安全多方计算（MPC），在密文形式下进行数据、模型参数的传输与计算。

数据方

具有用户各维度数据

ID	Age	Balance	loan
P1	23	5万	1万
P2	45	20万	18万
P5	17	1万	0

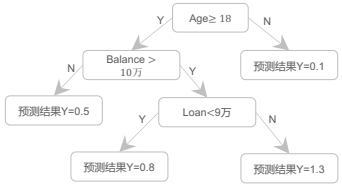
本地将己方数据计算为密文分片 ⟷ 交互密文分片 ⟷ 本地将己方模型参数计算为密文分片

获得预测结果的密文分片 ⟷ 密文下交互计算预测结果 ⟷ 获得预测结果的密文分片

结果密文分片 → 汇总、解密得到评分结果

模型方

具有风控模型



隐私计算方案流程：

步骤 1：数据方与模型方分别在本地加密私密数据与模型参数。

步骤 2：数据方与模型方交互数据密文与模型密文。

步骤 3：数据方与模型方根据自身密文及收到的密文，本地进行密文下的计算、比较、判断。

步骤 4：经过步骤3，双方均获得最终风控模型预测结果的一个密文分片，可指定数据方将其密文分片发送给模型方，由模型方汇总解密得到最终预测结果。

Part 3 项目优势及实践成效

- **业务提效**：汇集多数据源与模型源，实现优势互补的数据协作，提升风控评估质量；
- **功能完善**：支持多种主流的模型预测算法，包括逻辑回归、神经网络、决策树等；
- **性能优异**：可支撑大规模数据下的金融风控预测；
- **安全合规**：数据与模型参数的原文均不出库，保护数据安全与模型安全，满足合规要求；
- **灵活易用**：支持多种部署及调用方式，模型方可直接载入现有模型，实现对模型的高效调用。

来源：艾瑞咨询研究院自主研究及绘制。

数牍科技

数牍 sudo

iResearch 艾瑞咨询

发挥系统性工程能力优势，打造数据要素安全流通基础设施

数牍科技以数据全生命周期为视角，基于系统化、工程化且产品驱动的模式推动业务设计，研发了国产自主可控的软硬一体隐私保护计算平台以及多种贯穿数据全生命周期的工具链。

2020年，数牍科技率先落地了行业TB级隐私计算商用标杆项目，两年内，数牍科技与三大运营商、银联、工商银行、北京银行等多家国央企、金融机构、头部互联网公司及其对应各行业数据协作生态企业达成合作，覆盖金融、营销、风控、医疗等场景，积累了近百个数据协作产品和模型。2021年，数牍科技还陆续成为北京、上海、深圳、重庆、合肥等多地数据交易所首批数商及交易平台建设方。

数牍科技：隐私计算平台Tusita能力及优势介绍

在数据协作过程中，实现完整的数据应用支撑。

平台运营方不触碰数据，保证数据的可用不可见。

用法用量可监管，协调节点实现对任务和数据传输的完整实时监管。

完全自主研发，安全中立

计算分布式架构，用法用量可监管；平台不参与计算，不触碰数据，不运营数据；平台从授权管理、算法实现、结果输出等多个层面保护用户ID、特征、标签等核心数据。

完整的数据科学应用

可实现大规模无代码化规则标签能力、支持算法标签全流程可视化搭建，提高建模效率，灵活易用；平台具有良好的可集成性，充分考 虑了同数据中台、AI中台、区块链等平台的对接，极大降低隐私计算同现有技术环境的融合成本。

工业级落地能力

平台具备高可扩展性，支持快速实施部署和平台迭代；支持亿级数据联邦学习建模能力，支持亿级数据隐私求交；数据应用通信成本低，具备高并发、高实时性，毫秒级响应能力，满足多场景业务需求。

来源：艾瑞咨询研究院自主研究及绘制。

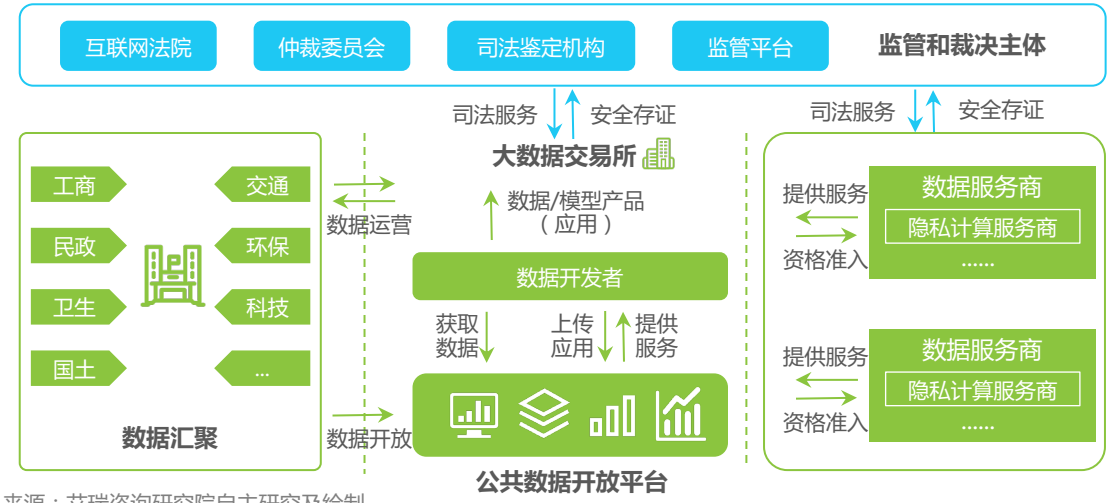
数牍科技：隐私计算实践案例解读

数牍科技金融、政务、通信等领域取得了卓越的实践成效。例如，信贷风控方面：2021年，数牍科技与某国有银行、数据合作伙伴共同完成了“基于隐私计算的普惠信贷风控服务”，其中，数牍科技提供隐私计算平台和建模服务，实现了双方双向信息隐蔽下的用户特征探查和模型特征选择，对目前信贷风控模型进行了补充和完善，最终联邦模型相比于银行单边模型，AUC值得到了数个百分比的提升；在已参与数百比贷款的贷前审批中，目前放款小微企业尚无出现重大风险企业（出现M3+逾期）；预计可年降低小微企业不良贷款损失数千万元。**又如，保险存量客户价值挖掘方面：**数牍科技调用了隐私计算产品赋予保险公司与合作运营商基于双向隐私保护的数据协作能力，在不交换原始数据前提下，实现数据价值交叉挖掘。让既有人群评估评分前 50%的人群购险率提升至原先1.8倍。|**报告重点以数牍科技的“数据交易所数商及交易平台建设方案”展开详细介绍。**

数牍科技：数据交易所数商及交易平台建设方案

方案概述

数牍科技发挥隐私工程能力优势，帮助多个大规模数据安全协作工程建设隐私技术底座，并通过“数商”身份，推动数据要素流通与交易的标准化。目前，数牍科技已成为北京、上海、深圳、重庆、合肥等多地数据交易所首批数商及交易平台建设方。



来源：艾瑞咨询研究院自主研究及绘制。

方案实践方式及亮点

Part 1 完善交易监管机制及数据贡献度指标体系

在符合监管要求的前提下，一方面，数牍科技协助交易所完善交易和管控机制（包括数据合规、数据产品上架和定价建议，以及数据承销，数据资产化，基于智能合约的数据确权和智能管控等服务）。目前，数牍科技已经形成了四个大类，共数十个指标的数据贡献度量化指标体系，基于该指标体系，可以分别为数据供需双方建立数据定价建议模型，从而帮助供需双方形成更优的成交价均衡。

Part 2 多层次产品体系优化市场接入体验

面向数据应用主体，通过构建包括数据产品、模型产品等在内的多层次产品体系（提供包括数据及交易合规辅助工具，数据贡献度评估等配套服务，提供灵活、安全的隐私计算可视化建模能力），优化市场接入体验，并积极引入、撮合更多的数据开放主体，从而更好的满足数据应用主体需求。

洞见科技

洞见科技 INSIGHTONE

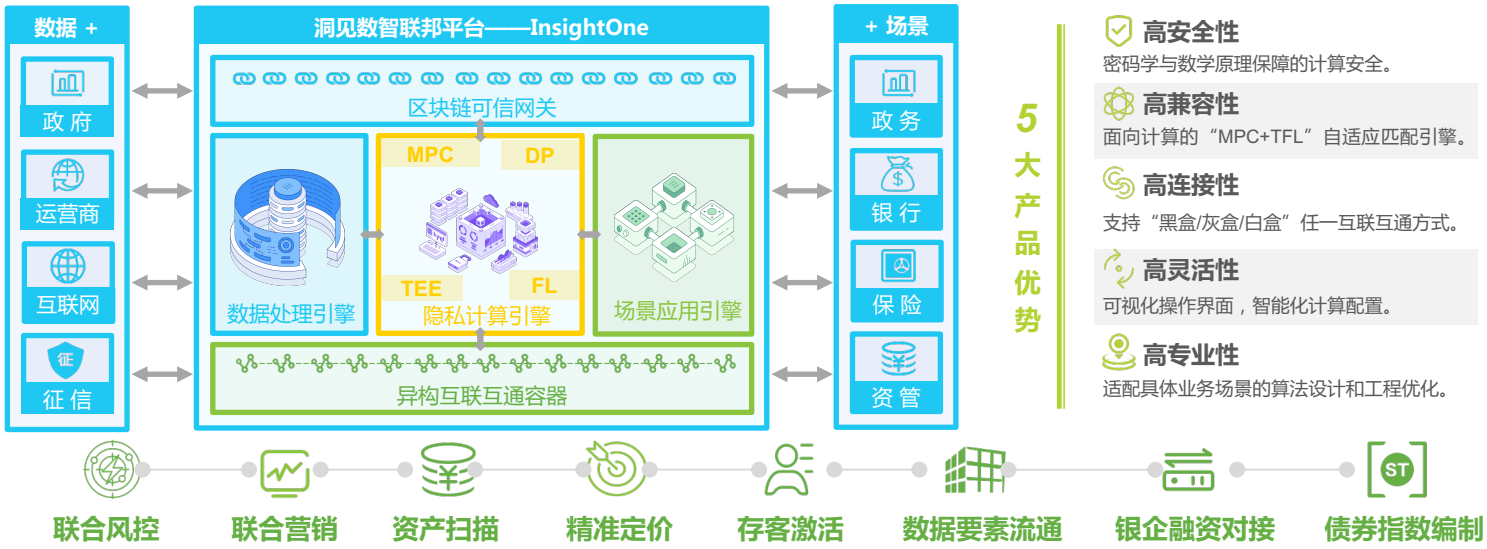
iResearch 艾瑞咨询

安全可信的数据要素“连接器”和金融业务“增效器”

洞见科技是由**信用产业集团“中诚信”孵化、网信事业国家队“中电科”投资**的领先的隐私计算技术服务商，公司创始团队是中国大数据征信和智能风控行业的推动者和领军人物，核心成员来自中诚信征信、大型银行、保险公司以及人工智能企业，具备丰富的行业知识和服务经验。凭借过硬的技术与业务实力，洞见科技已在政务、金融、运营商等领域落地了包括山东省大数据中心、聊城市大数据局、中国银行、中国建设银行、招商银行、北京银行、中国人寿、三大运营商等大量隐私计算合作案例，并与北京、山东、重庆、海南、合肥等数交所开展合作，赋能数据要素安全开放流通。

InsightOne是洞见科技自主研发的金融级隐私计算平台，**首创面向场景的“MPC+TFL”融合引擎架构**，是国内唯一通过工信部中国信通院多方安全计算和联邦学习功能、性能、安全、辅助工具，以及央行国家金融科技测评中心多方安全计算和联邦学习金融应用等隐私计算全系列评测的产品，并适配主流国产信创芯片、服务器及操作系统。

洞见科技：隐私计算平台InsightOne及典型应用场景



来源：艾瑞咨询研究院自主研究及绘制。

洞见科技

洞见科技 INSIGHTONE

iResearch 艾瑞咨询

洞见科技：隐私计算实践案例解读

凭借领先的产品能力和精益化客户服务经验，洞见科技率先在各领域落地了大量行业里程碑案例，包括：基于隐私计算的省级政务数据开放平台、大型商业银行隐私计算互联互通平台、大型保险公司隐私计算技术服务平台、大型运营商联邦学习平台等。本报告以“基于隐私计算的省级政务数据开放平台”案例为例，展开解读。

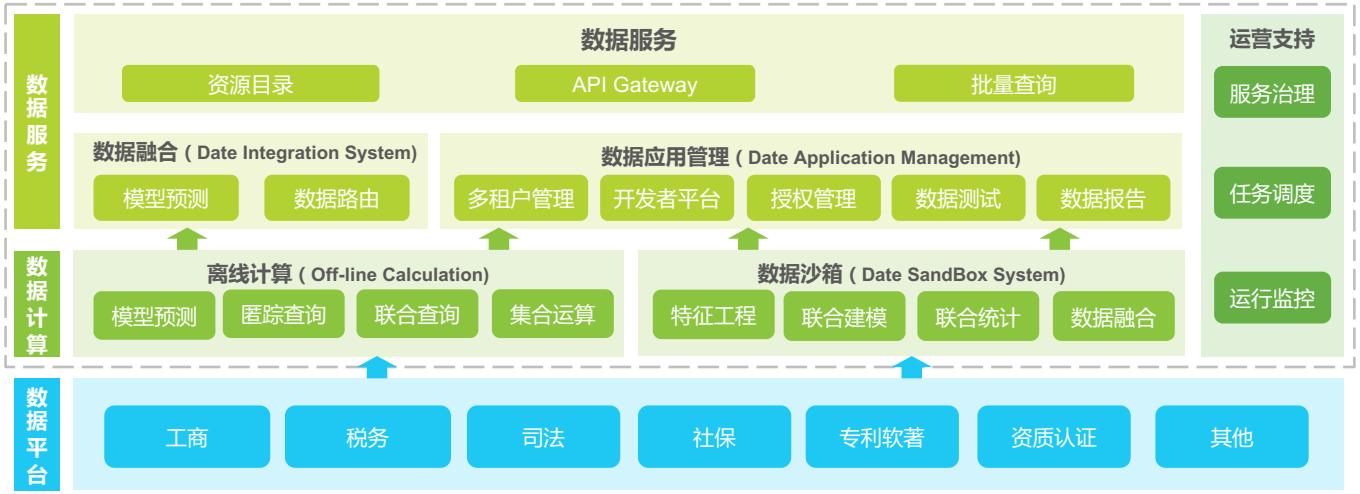
洞见科技“基于隐私计算的省级政务数据开放平台”实践案例解读

Part 1 项目背景与目标

为贯彻国务院《要素市场化配置综合改革试点总体方案》及山东省人民政府颁发的《山东省公共数据开放办法》，更好地解决政务数据开放和隐私保护之间难以两全的问题，提升政务数据存储、计算、应用、通用支撑和服务管理能力，提高社会治理能力和公共服务水平，洞见科技联合智慧齐鲁公司为山东省大数据中心建设了国内首个基于隐私计算的省级政务数据开放平台，为政务数据开放、流通与应用提供技术基础设施，推动数字经济发展。

Part 2 解决方案

基于洞见科技InsightOne隐私计算平台成熟框架开发，支持多方安全计算和联邦学习融合应用模式，为数据隐私保护与安全应用之间的矛盾提供了“技术最优解”，在数据要素流通过程中实现“数据可用不可见”。



来源：艾瑞咨询研究院自主研究及绘制。

Part 3 实践成效

- 国内典型的省级政务数据隐私计算平台，行业标杆意义突出。
- 以差异化的综合性信用评价能力，助力该省的中小微企业融资对接。
- 有利于建立健全涉企数据信息共享机制并在其他省市进行复制。
- 提升产业链各环节、各节点数据采集能力，加强上下游信用服务。

冲量在线

冲量在线 IMPULSEONLINE

iResearch 艾瑞咨询

融合多元科技能力，打造数据智能数据流通解决方案

冲量在线致力于促进数据生产要素在社会间的互联互通，构建可信、安全、隐私、公平、高效的“数据互链网”。冲量在线的团队技术人员占比超过80%，主要来自百度、字节跳动、阿里巴巴、腾讯、华为等头部科技公司，多位核心骨干是人工智能、大数据、区块链、隐私计算等多个国际和国内相关标准组织核心成员，并主导或参与撰写了数十个行业标准。冲量在线先后获得了IDG资本、苏州元禾原点领投等机构的投资。

冲量在线：隐私计算产品能力介绍

冲量平台基础服务

- 区块链基础设施管理
- 联盟组织管理
- 日志审计中心
- 消息与审批中心
- 授权管理

冲量数据交易平台

- 数据交易管理
- 数据价值分析
- 数据交易监管
- 数据资产登记
- 数据血缘图谱
- 数据确权公证

冲量数据互联平台

- 可信计算
- 可信建模
- 可信查询
- 数据源管理
- 计算节点管理
- 隐私算法管理

冲量机密计算平台

- 密钥托管
- 证书托管
- 密钥派生
- 签名管理
- 密钥轮转

数据平台生态

- 关系型数据库
- 图数据库
- 文件数据库
- 大数据平台

可信硬件生态

- 兆芯
- 海光
- 飞腾
- 鲲鹏
- 申威
- 龙芯
- Intel SGX
- ARM TrustZone

算法中心

- 通用TEE算法
- 联邦学习算法
- 算法开发工具：C++、Python、Golang、Rust

冲量数据互联平台：数据流通与隐私计算平台，用于管理和执行多方数据协作任务，在数据协作计算的过程中保障隐私信息的安全，实现数据“可用不可见”。冲量数据互联平台向上支撑各类大数据业务应用，向下对接不同的数据源平台。

冲量数据交易平台：数据交换与共享平台，助力数据生产要素的市场化交易。支持数据所有方更好地管理数据资产、需求方更便捷对接和获取数据价值。冲量数据交易平台与冲量数据互联平台结合使用，可以实现数据资产价值交易而所有权不丢失。

冲量机密计算平台：机密信息托管与使用平台，用于密钥、证书、签名等敏感信息的全生命周期保护，提供一站式机密数据管理、数据加密存储等能力。冲量机密计算平台可无缝集成到已有的业务系统中，对业务系统使用的密钥、证书提供简单、可靠、安全、合规的保护能力。

来源：艾瑞咨询研究院自主研究及绘制。

国产化隐私计算一体机产品

隐私计算一体机是冲量在线推出的一款致力于数据安全流通的全国产化一体机产品，支持兆芯、飞腾、海光、鲲鹏等国产化隐私计算芯片，提供软硬件一体的一站式数据流通解决方案，助力政务、金融、运营商等行业机构打造自己的国产化数据流通网络。

4大产品优势

开箱即用

1、集群化部署；*2*、多个节点可组成数据互联网络。

国产化

1、飞腾/海光的可信执行环境；*2*、支持国产化X86架构和ARM架构；*3*、可保证在安全区域内部加载的代码；*4*、数据在机密性和完整性方面得到芯片级保护。

芯片算法优化

1、支持十亿级别数据量的业务应用能力，支持金融/政务/医疗场景下的10+个隐私机器学习算法能力；2、支持国密，同态，椭圆曲线，MPC，联邦学习等安全技术；3、综合性能提升20-30倍以上。

安全流通

1、全套冲量在线软件能力；*2*、结合区块链、联邦学习、多方安全计算、 TEE可信执行环境等多维度方案，提供数据流通能力。

冲量在线：隐私计算实践案例解读

冲量在线是业界率先推出端到端国产化芯片级隐私计算解决方案的企业，并在金融，政务，运营商，saas，区块链领域具有数十个实践落地案例。

以运营商的实践案例为例：2021年4月，冲量在线受邀参加中国电信集团“融通创新”主题日，并签约成为融通创新合作伙伴中重要的隐私计算厂商，与电信研究院创新业务部门合作建设电信集团的数据融合与对外输出平台，打造“数信链网”产品，促进电信省分公司与集团子公司之间的数据互联互通，实现电信数据对外输出运营。

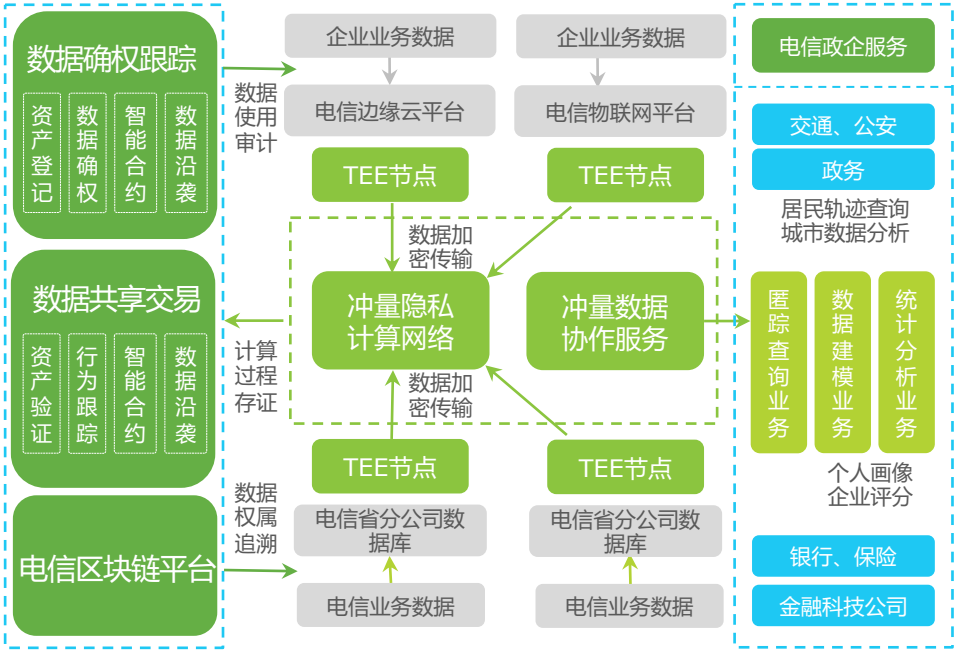
冲量在线“中国电信数信链网”实践案例解读

Part 1 项目概况

2021年9月，中国电信研究院联合隐私计算和可控硬件领域的领先企业冲量在线、中科可控联合研发的最新成果：“数信链网”—基于数算云网的区块链可信数据共享平台落地实践。“数信链网”对于数据要素产业相关技术进行了持续关注和深入研究，专注于解决数据要素流通链条中的一系列核心问题，包括：数据资产确权、数据隐私和安全、数据定价和交易、数据价值深度挖掘、基础设施自主可控等。三方以电信“数算云网”一体化框架为基础，共同推进数据确权流通和隐私计算平台的建设。

Part 2 实践方案与成效

在技术栈层面，“数信链网”融合了区块链与隐私计算两大新兴技术，创新性地实现了区块链的分布式互信特性与隐私计算的机密性协作能力融合互补，充分满足了数据要素流通中可信、安全的需求。在交付模式方面，“数信链网”采用了业界领先的一体机架构，解决了区块链和隐私计算技术实施难度大的问题，可在各类场景中快速交付、无缝扩展，真正在生产场景中实现大规模应用。此外，“数信链网”还实现了从芯片、到操作系统、到加密算法、到应用软件的全面国产化，是业内率先实现端到端自主可控性的同类型解决方案。平台在芯片层面深度优化了隐私算法的性能，极大程度解决了安全性与性能不可兼得的难题。



来源：艾瑞咨询研究院自主研究及绘制。

金智塔

金智塔 数智引领未来

iResearch 艾瑞咨询

依托浙江大学背景，致力打造卓越隐私计算产品

金智塔是由浙江大学人工智能研究所和浙江大学金融科技研究院联合孵化的隐私计算服务商，获得国家重点研发项目支持，并入选杭州市海外高层次人才创业计划。金智塔不断突破隐私计算领域核心技术，拥有三十余项专利和软著，并通过CMMI3、ISO9001、ISO27001、华为鲲鹏技术、中国信通院隐私计算评测等资质认证，参编数据要素流通与隐私计算相关标准17项。

金智塔隐私计算平台基于多方安全计算、联邦学习、同态加密、差分隐私及数据脱敏技术，实现数据可用不可见，为数据提供方、使用方、授权方、监管方提供安全合规可信的数据共享和流通平台，并提供数据鉴权、追溯、审计等能力，保护数据隐私，打通数据壁垒，实现数据流通，激活数据价值，为金融机构、政府、大型企业的数字化转型提供支撑，助推数字经济发展。

金智塔：隐私计算产品能力介绍

来源：艾瑞咨询研究院自主研究及绘制。

丰富的产品功能

产品支持数据分类分级、隐私求交、隐匿查询、联合查询、联合建模、安全存证等核心功能。通过可视化的操作界面，屏蔽复杂的密码学技术，简单易用，支持自动调参等功能以及一键式训练达到最佳效果。系统支撑方面，平台可对多节点硬件负载合理调配，实现多任务、大数据、高并发场景下的稳定运行。系统集成方面，平台算子独立、功能解耦，可支持算法模块独立部署，并支持接口调用、文件写入等形式的输出方式。

自主研发性能高

平台采用分层设计理念，自底向上包含了安全原语层，安全算子层，以及安全算法层。平台研发过程中融合了联邦学习、秘密分享、混淆电路、差分隐私、同态加密等多种技术，针对不同的业务场景及环境设置，进行深入的定制化优化，从而达到安全性、可用性、效率的最优平衡。

全链路安全防护

在使用数据进行计算前，针对不同安全等级的数据，匹配不同的技术方案。在数据的使用过程中，使用多方安全计算和安全联邦学习保护数据安全，同时对使用的全过程进行存证并上链。在数据使用之后，平台支持多维度的存证检索，实现数据使用的可回溯、可追责。

金智塔：隐私计算实践案例解读

金智塔隐私计算平台经过多年来的技术实践沉淀，目前在“智慧金融、智慧政府、智慧企业”三大领域均有丰富的客户服务经验并受到客户的认可。**金融智能领域：**基于金智塔隐私计算所展开的联合智能授信、联合智能营销等方案已推广到**10余家农商行、城商行和股份制银行**，取得了良好的社会效益和经济效益。**智慧政务领域：**金智塔通过与省市数据管理部门和业务管理部门合作，在政务部门内部数据共享、数据交换、数据校验等方面提供隐私保护技术支持，同时为政务数据的社会开放提供解决方案。**智慧产业领域：**金智塔隐私计算平台依托其技术优势，积极赋能传统产业转型升级，近年来在零售企业智慧选址、销售预测、智能营销推荐等领域积累丰富经验，助力企业数据资产建设，赋能企业数字化转型。

报告以金智塔科技的“某商业银行：小微科创数贷”隐私计算实践案例为例展开解读。

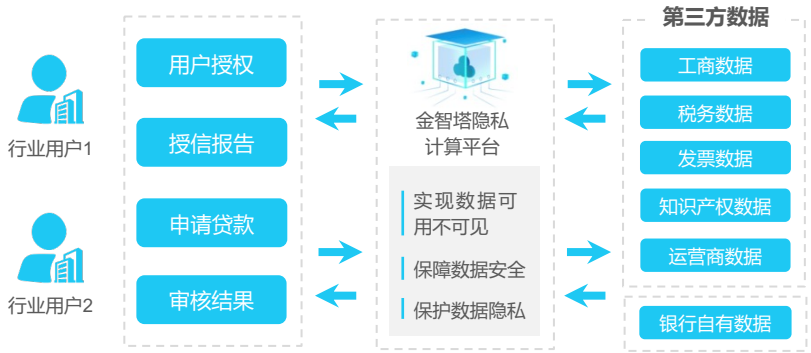
金智塔“某商业银行小微科创数贷”实践案例解读

Part 1 项目简介

基于“金智塔隐私计算平台”，融合政府部门开放数据、行内数据、第三方商业数据，通过联邦学习与多方安全计算解决数据孤岛和用户隐私保护难题，实现面向全域小微、科创企业的在线智能授信。

Part 2 具体方案

基于“金智塔隐私计算平台”的联合智能授信方案设立准入评估、成长力评估、风险评估、授信额度估算等各类模型。



a) 小规模纳税人授信模型以企业实际应税销售额、实有净资产和纳税额为基础，结合行业特点，充分考虑企业发展需求，合理配置参数，实现对小规模纳税人的在线智能授信。

b) 一般纳税人授信模型则以企业实际应税销售额、实有净资产和纳税额为基础，结合企业流动资产周转率、资产负债率等指标，合理配置参数，实现对一般纳税人企业的在线智能授信。

c) 考虑到科创企业重智少资特点，金智塔自主研发企业生命周期、企业成长力、知识产权估价为核心的授信模型，实现数据驱动的科创企业智能授信。

Part 3 实践成效

（1）小微企业信贷申请**审批周期从天为单位压缩到分钟为单位**；（2）有效解决某区**12.8万**家小微企业的在线智能授信问题；（3）获得省担保集团认可，**授信50亿**；（4）帮助企业**降低50%以上融资成本**，助力政府扶持小微和科创企业，服务实体经济。

来源：艾瑞咨询研究院自主研究及绘制。

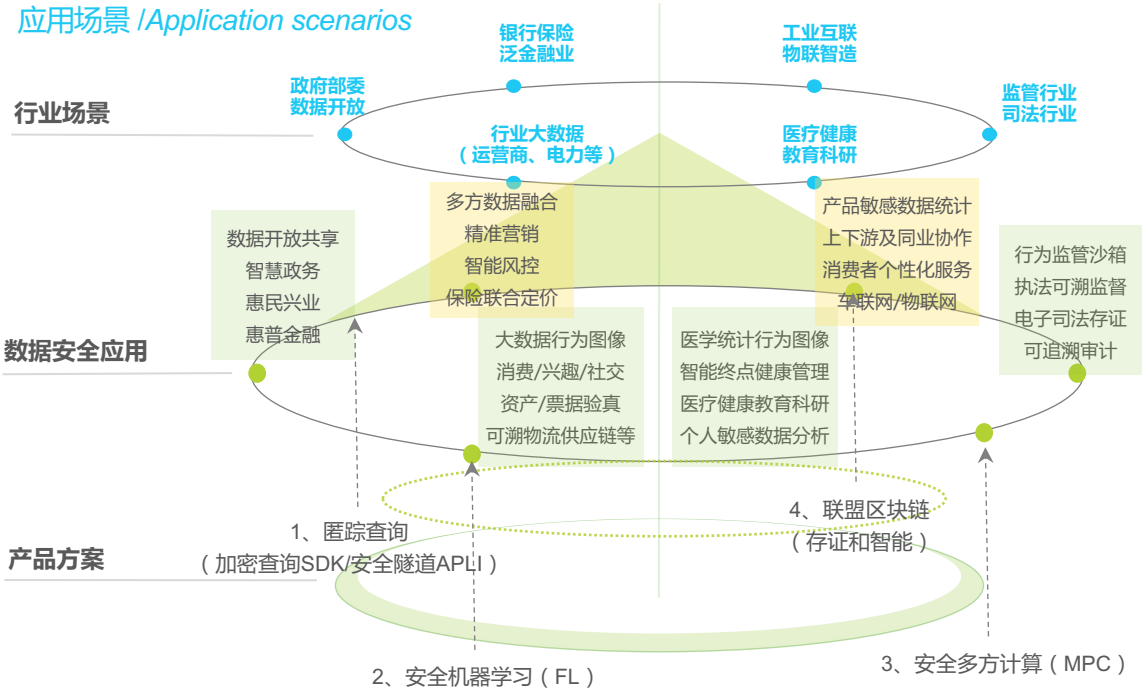
富数科技 富数 FUDATA.CN

iResearch 艾瑞咨询

构建安全桥梁，释放数据价值

上海富数科技有限公司（简称“富数科技”）是国内隐私安全计算的领跑者，专注于联邦学习、多方安全计算、匿踪查询等加密计算领域，依托安全计算和机器学习等AI技术，致力于「构建数据安全和隐私保护的数字安全底座」，是隐私计算互联互通国家标准的牵头单位，深度参与信安标委、金标委、工信部等标准的制定，亦是上海市商用密码行业协会会员单位。2021年富数科技完成数亿元C轮融资，入选福布斯中国企业科技50强，自研产品隐私计算产品Avatar是首批获得银行卡检测中心、中国信通院、中国公安部的权威认证产品，落地场景覆盖金融、政务、运营商、电力等各个数据相关领域。

富数科技：Avatar 安全计算平台及典型应用场景



- 富数科技自主研发的一站式企业级多方安全计算平台Avatar（阿凡达），集成隐私集合求交（PSI）、多方安全计算（MPC）、联邦学习（FL）、隐私信息检索（PIR）等核心安全计算技术，提供企业级的数据安全匹配，安全联合计算、安全联合建模、安全查询等跨机构间可信数据协作能力。
- Avatar安全计算平台支持有/无第三方，产品成熟度行业领先，具有支持一键部署、托拉拽图形化界面、算法组件化等特点。性能比行业快 3-5 倍，支持异构体互联互通，释放数据价值，助力业务创新与增长。
- 目前已经广泛部署于政务、运营商、银行、电力、保险、券商等多个领域超过**60**家合作伙伴。

来源：艾瑞咨询研究院自主研究及绘制。

富数科技

富数科技：隐私计算实践案例解读

富数科技在金融、政务、运营商等领域具备丰富实践经验，我们以“基于多方安全图计算中小微企业普惠金融服务”为例进行解读。

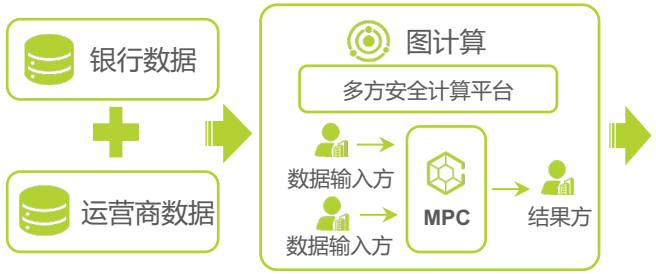
富数科技“基于多方安全图计算中小微企业普惠金融服务”实践案例解读

Part 1 项目概况

近年来，中小微企业融资中的金融欺诈问题日益严重，随着时间演化、发展和反欺诈技术的进步，金融欺诈团伙呈现有组织欺诈趋势，金融风控压力持续提升，导致融资成本难以下降，进一步导致融资难、融资贵，不利于普惠金融业务发展，市场急需新技术来对传统反欺诈技术进行补充。

Part 2 解决方案

基于富数AVATAR多方安全计算系统平台，可确保银行和运营商在数据不出库前提下联合建模，并应用于小微企业普惠金融业务中，进而精准防范和打击伪冒审贷等扰乱金融秩序的行为，为进一步降低中小企业融资成本，安全高效的服务实体经济提供助力，如图所示：



反洗钱
可疑交易
疑似洗钱

信用风险
团伙欺诈
逾期风险
多头借贷

金融犯罪
洗钱欺诈
可疑账户

- 通过数据融合应用，充分发挥移动运营商数据价值，结合风控平台结果，为客户鉴权、增信，实现 银行风控模型精准化，提升普惠金融服务的安全性、易得性；
- 运用在线金融工具打造线上线下一体化“交银e办事”服务，实现身份核验手段多元化、线上融资服务差异化、普惠金融生态健康化，提升银行普惠金融的时效性、便捷性。
- 图计算技术与多方安全计算技术结合，通过多方安全图计算等技术作为开户真实性意愿审核的辅助手段，达到身份核验手段多元化效果，并将客户移动网络信息与申贷信息进行交叉比对分析和联合建模，精准防范和打击伪冒申贷等扰乱金融秩序的行为，助力银行中小微企业精准贷款投放和集群风险管控，提升金融机构风险防控能力及客户贷款体验，营造健康的普惠金融生态。

Part 3 实践成效

该案例入选上海市金融科技创新监管试点首批创新应用，由上海富数科技有限公司、交通银行股份有限公司、中移(上海)信息通信科技有限公司、上海理想信息产业(集团)有限公司和联合申请，是国内金融领域率先对外公开运行的多方安全计算应用。

来源：艾瑞咨询研究院自主研究及绘制。

趋链科技

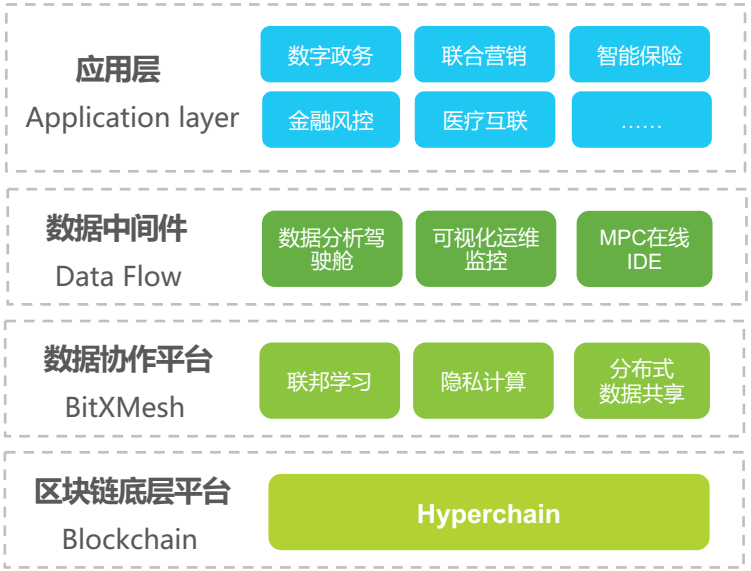
趋链科技 HYPERCHAIN

iResearch 艾瑞咨询

通过“隐私计算+区块链”打造数据要素流通新基建

BitXMesh是趋链科技自主研发的链原生数据协作平台，是率先将区块链与多方安全计算技术结合，并支持链上链下协同的数据共享平台。融合多方安全计算（MPC）、可信执行环境（TEE）等软硬件技术，**首创提出**跨网闸数据交换等适配各类复杂工业场景的通信协议，及零知识黑名单共享算法等具有高度应用价值和社会牵引力的高性能应用算法，**可支撑上千机构间数据的安全共享和隐私计算；专用算法延时低至毫秒级别，可支撑亿级以上数据量的应用场景。**BitXMesh首批参加且全项通过中国信通院的《隐私计算性能专项评测》、《区块链辅助的隐私计算工具专项评测》等行业技术评测，且在功能、性能评测的多项指标均达到行业顶尖水平，是构建数据要素市场的可信基础设施。

趋链科技：隐私计算能力介绍



业务发展情况

BitXMesh团队自2018年底成立至今，专注于隐私计算研究和落地实践，已积累了金融、政务、农业、能源、营销等多领域的客户，并结合用户实际业务场景总结出十余种行业解决方案，用隐私计算技术为客户解决实际问题。

所获奖项/成绩

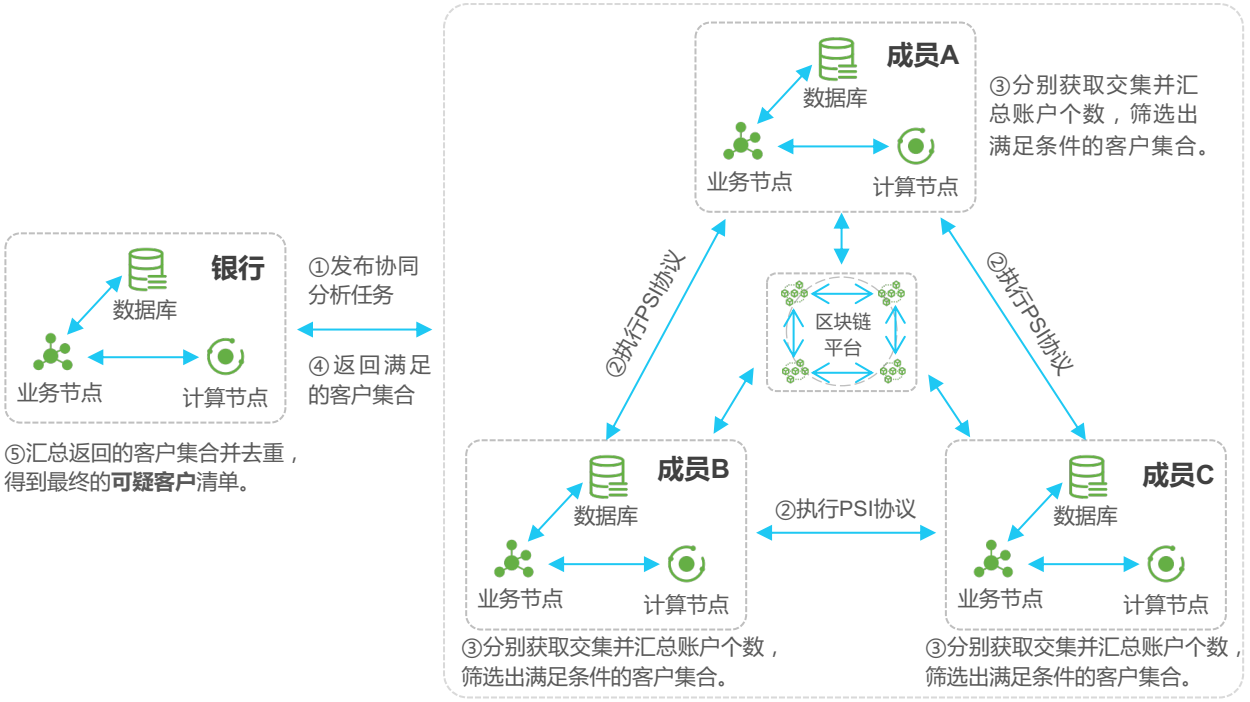
- 参与制定《区块链辅助的隐私计算工具标准》，参加首届《区块链辅助的隐私计算性能评测》并全项通过；
- 参加信通院《多方安全计算性能评测》，全项通过且各项算法性能指标均远超行业平均水平；
- BitXMesh应用《基于MPC的链原生联邦金融风控与反欺诈应用建设》荣获信通院2021年度星河隐私计算年度优秀案例；
- 发布首个融合区块链、大数据、隐私计算、人工智能技术，以构建数据要素流通市场为目标的《数据要素可信流通》白皮书。

来源：艾瑞咨询研究院自主研究及绘制。

趣链科技：隐私计算实践案例解读

趣链科技联合西南地区金融科技企业，由央行牵头，联合20多家银行机构形成风险信息数据的共享联盟，实现市域范围内金融机构间风险“联防联控”利器。结合多方安全计算等前沿技术，将金融和非金融机构链接起来建立风险共治联盟，在**“一人多企”、“一人多户”、“频繁开户”等场景**中进行广泛应用。平台遵循“数据可用不可见”的严格隐私保护标准，实现安全可靠的风险信息共享协同分析及穿透式监管等核心业务功能。

趣链科技“省级金融风险数据协同分析平台”实践案例解读



应用场景1：电信诈骗

通过信盟链共享在账户开立、交易监测、风险筛查过程中发现的存在异常开户或异常交易行为、涉嫌买卖账户或账户用于电信网络诈骗等违法犯罪的可疑个人或企业信息，**有效提升电信反欺诈能力。**

应用场景2：信用卡审批

通过信盟链共享各机构日常业务中积累的欺诈授信黑名单、信用卡审批拒绝名单、信用卡套现名单等风险信息，**有效提升信用卡业务反欺诈能力。**

应用场景3：欺诈骗保

某客户在一个多月时间内向40余家寿险公司购买了大量短期意健险，累计身故保险金超过4000万。通过信盟链共享客户投保信息，在“数据互不可见”下进行协同分析，可有效识别该风险，**从而避免骗保案例出现。**

来源：艾瑞咨询研究院自主研究及绘制。

UCloud优刻得

以云服务为支点，UCloud在隐私计算领域发挥独特优势

- **UCloud介绍：**作为国内第一家云计算科创板上市公司，UCloud推出公有云、私有云、混合云、边缘云等全线云产品，自主研发IaaS、PaaS、 AI、安全屋隐私计算平台等100+产品。截至2022年1月，UCloud已服务50000+家客户，其中上市企业客户达400+家。
- **UCloud相较于其他隐私计算厂商有着独特优势：**1）云计算企业在长期服务用户的过程中，更了解用户的数据使用场景，进而更好地结合场景开发产品；2）隐私计算的应用实践与云计算公司本身具有的计算、大数据、人工智能等技术具有很高的契合度；3）云平台本身对安全能力的要求很高，隐私计算可以保障数据的安全流通。
- **安全屋隐私计算平台介绍：**UCloud于2017年率先推出数据安全流通平台 – 安全屋，运用数据沙箱、安全多方计算、区块链、数据加密等技术，创新提出数据“所有权”和“使用权”分离的理念，解决数据要素流通困境，确保数据在流通过程中“可用不可见”、“可用不可拿”。推出至今，安全屋已发展出可信数据沙箱平台、安全多方计算平台、联邦学习平台这三大产品矩阵，广泛应用于政府、金融、医疗等多个领域。

安全屋隐私计算平台三大产品线及优势

01 可信数据沙箱平台

- 基于可信芯片技术。
- 解决安全边界、信任可见问题。
- 与人脸识别技术、视频监控体系结合。

02 安全多方计算平台

- 基于密码学
- 同态加密
- 差分隐私
- 易于使用、强可扩展性分布式高性能、监管友好。

03 联邦学习平台

- 完整机器学习框架。
- 将分布式特征提取和联邦模型计算进行合理的规划，形成共有模型。

平台先进

- 单一平台支持：MPC、联邦学习 、隐私查询等数据安全技术，秘密 分享、混淆电路、可信计算等计算引擎。
- 支持横向扩展和数据并行，TB级数据处理。
- 支持细粒度并行计算。

技术安全

- 具有完备的数学/密码学证明
- 安全假设明确而且容易实现和审计
- 数据授权管理
- 系统实现安全：SSL、CA认证等
- 核心密码协议设计简单而且开放
- 同时兼容国际开源和中国商密体系
- 存证审计功能

开发便利

- 支持 SQL、Python 等高层语言
- 集成开发/调试环境
- 常用数学计算函数库
- 密文机器学习算法库
- 特定行业算法库
- 方便的应用开发-授权-发布全流程方案

部署可靠

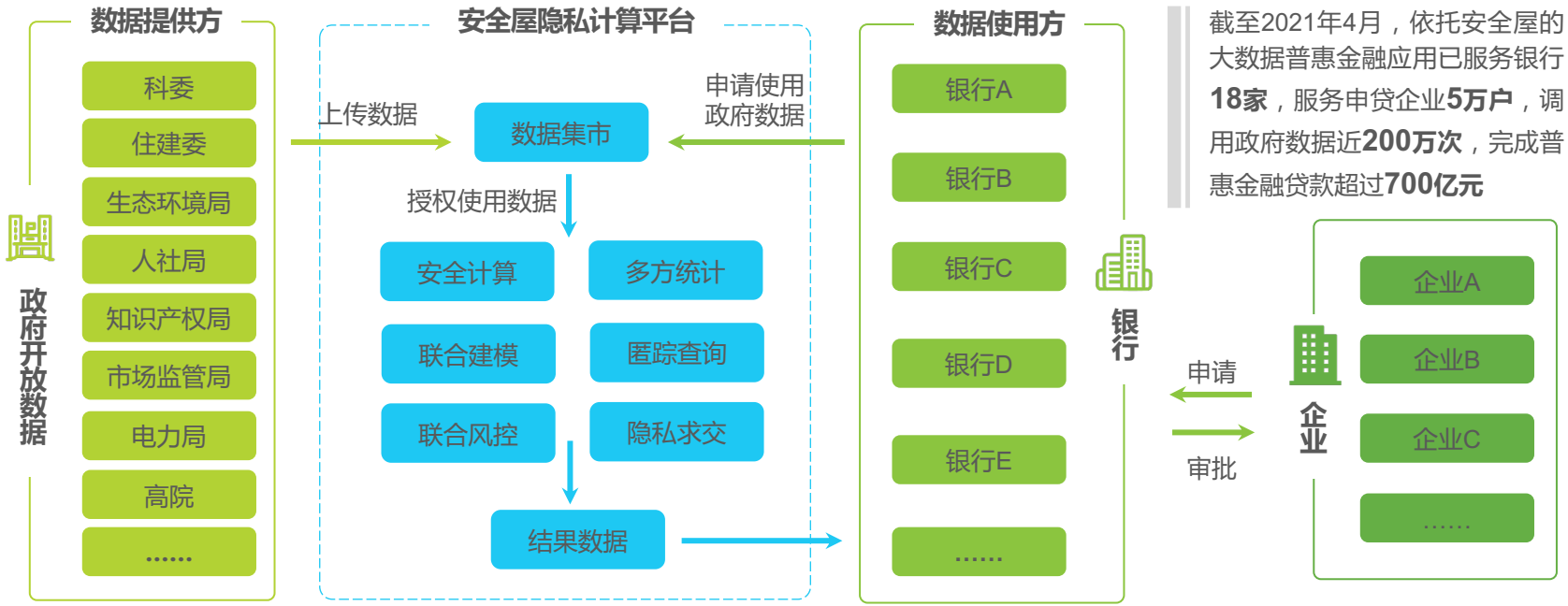
- 云+端部署
- 服务安全/健康监控
- 各组件/各层级的高可用
- 各种VM或物理机的部署
- 多种CPU架构

来源：艾瑞咨询研究院自主研究及绘制。

UCloud优刻得：隐私计算实践案例解读

凭借UCloud多年来的隐私计算能力积累以及企业自身丰富的客户服务经验，安全屋隐私计算平台已经为多领域的行业用户提供了产品与解决方案服务。例如：在政务领域，UCloud安全屋帮助厦门市政府建立了全国首个大数据安全开放平台，参与市级部门达37个，开放数据目录881个，开放数据994万条；在医疗领域，UCloud安全屋帮助上海市第九人民医院打造了一套安全、可控、开放的血管外科数据隐私计算平台，实现数据安全地跨院流动，加速科研创新成果转化。报告着重以“上海大数据中心普惠金融项目”项目展开介绍。

安全屋隐私计算平台金融实践案例：上海大数据中心普惠金融项目



来源：艾瑞咨询研究院自主研究及绘制。

第四范式 4Paradigm

iResearch 艾瑞咨询

提供“平台+场景+数据+连接”的隐私计算平台服务

作为企业级人工智能领域的行业先驱者与创新者，第四范式为企业提供以平台为中心的人工智能解决方案，并运用核心技术开发了端到端的企业级人工智能产品，同时构建了“平台+场景+数据+连接”的隐私计算全栈解决方案。第四范式隐私计算产品可帮助企业机构在保护数据资产权益的同时，充分发挥数据的商业价值，提高组织间和组织内部协作效率。通过AutoML+隐私计算的方式尽量减少人员参与程度，进一步保证数据的安全隐私。

第四范式目前拥有金融、零售、制造、能源电力、电信及医疗等多行业的客户服务与实践经验，为第四范式隐私计算产品的市场发展打下坚实基础。

第四范式：隐私计算平台服务能力

提供不暴露原始数据的多方联合计算能力：包括联邦学习、多方安全计算和可信计算环境在内的全流程、多场景安全多方计算框架。保护数据资产权益，安全发挥商业价值。

联邦学习FL

- **安全性**：数据不出域，基于差分隐私和同态加密等技术。
- **高性能**：自研FL框架，软硬一体深度性能优化，支持FPGA、GPU加速。
- **全自动模型训练**：AutoML建模，支持丰富机器学习算法，安全性高，易上手。

多方安全计算MPC

- **安全性**：国密标准，加密协议保证计算安全。
- **高性能**：自研密码库优化技术，支持超大规模数据高性能计算，支持FPGA、GPU加速。
- **场景多样性**：支持多种场景，包括匿踪查询、比较、排序、四则运算等。

可信计算环境TEE

- **安全性**：通过芯片硬件技术保护模型算法和计算过程中的代码及数据。
- **多架构**：支持海光CSV、Intel SGX、华为Trustzone等多种TEE技术方案。
- **快速部署**：无需二次开发，快速部署于公有云、私有或线下环境。

平台 *Platform*

基于MPC、TEE、FL等技术，提供端到端、全自动、高性能、自主可控的多方联合隐私计算平台。

场景 *Scenes*

依靠丰富的行业场景落地经验，基于隐私计算产品，帮助客户构建联合风控、联合营销、联合分析等场景模型，保证业务效果达到预期。

数据 *Data*

自带海量优质数据协作方，一站式赋能基于隐私计算的数据生产要素遴选和联合创新。通过高价值商业洞察，帮助企业降本增效、管控风险以及实现业务创新。

连接 *Connect*

聚合金融、零售、制造、能源电力、电信及医疗等客户，建设可持续的数据生态，提供业务连接机会，实现共赢。

来源：艾瑞咨询研究院自主研究及绘制。

第四范式：隐私计算实践案例解读

第四范式凭借其多年打磨而形成的卓越隐私计算产品能力为行业客户提供了风控、营销等多维场景的解决方案。第四范式支持“两方去中心化部署、多方中心化部署”的部署方式，提供可视化交互界面，保证技术应用实践的高效性。
银行作为隐私计算的重要落地领域，第四范式在银行业务的风控场景、营销场景均具备良好的实践能力。以隐私计算+营销为例，第四范式通过联邦学习技术协助银行打通本行及跨行消费数据，实现本行优质高潜客户挖掘。

第四范式“隐私计算+营销”实践案例解读

来源：艾瑞咨询研究院自主研究及绘制。

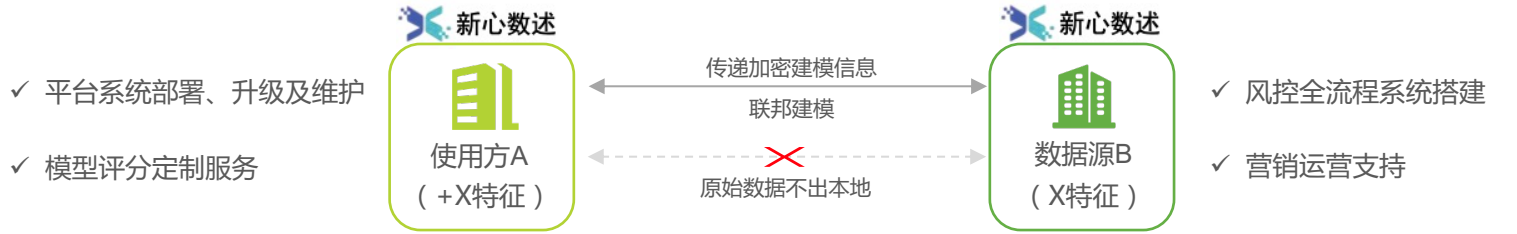
新心数科

新心数科

基于丰富的金融实战经验推进“隐私计算+金融”战略实践

新心数科是一家市场领先的金融科技服务商，基于二十多年国内零售金融实战经验，在信用卡、消费金融、小微金融等领域，为银行等金融机构提供多元化解决方案。公司基于多年技术沉淀与经验积累而推出的联邦学习+AI平台，在技术安全可信前提下，让数据价值得到深度释放，为金融科技创新提供技术支持。目前新心数科已在“联邦学习平台、OCR、AI信审、AI营销、风控、反欺诈、可解释模型”等金融科技解决方案与技术能力上进行了深度实践与布局。新心数科目前累计服务C端客户**数百万**，协助银行等金融机构发放**数百亿**信用贷款，并取得了“信贷风险不良率长期在**1%**左右（**风险表现优异**）”的实践成效。

新心数科的隐私计算能力与相关技术认证



丰富的金融实践经验

a. 融合多年的行业风控经验
b. 基于业务场景的解决方案
c. 技术与金融业务深度融合

灵活的技术架构

a. 支持多种主流数据源
b. 支持单机与集群部署
c. 对接大数据生态

极致安全保障

a. 多方安全计算, RSA+同态加密
b. TLS加密信道，保证信道安全
c. 安全看板，模型训练与预测监控

高效多方联合建模

a. 去中心化联邦建模
b. 高性能隐私求交
c. 组件化配置建模流程

新心数科获得的国家级认证

来源：艾瑞咨询研究院自主研究及绘制。

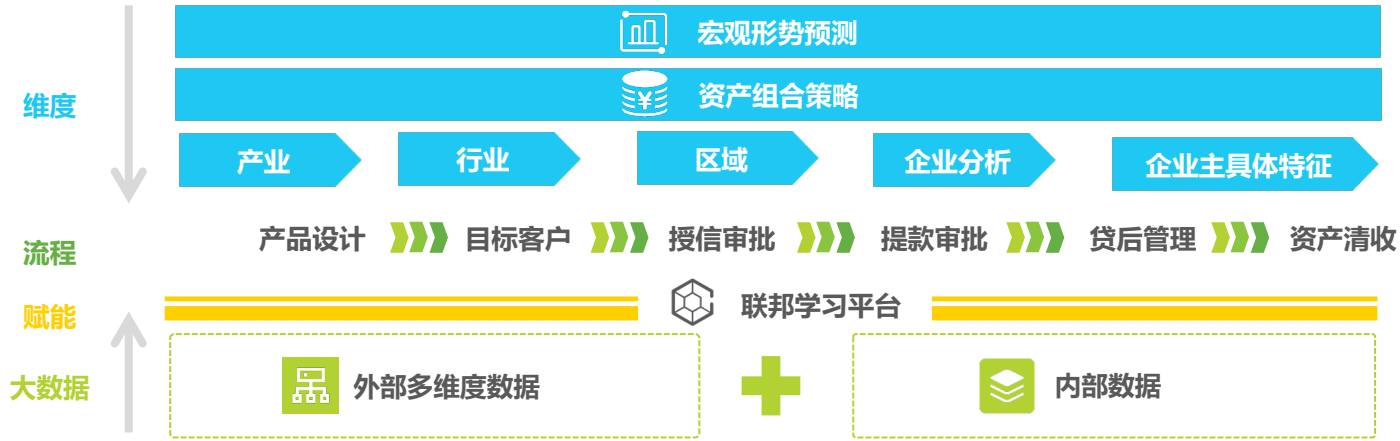
新心数科在不断强化技术能力的同时，积极丰富数据生态，助力隐私计算的应用实践

新心数科拥有基于开源框架开发的联邦学习平台和基于自研框架的多方安全计算平台。同时，新心数科积极践行互联互通战略，目前已经建立了多维类型的数据生态，并在精准营销、风险管理等场景中开始了隐私计算的落地探索与解决方案实践。

新心数科的隐私计算实践案例 – 风险管理场景

模型实践目的：新心数科通过联邦学习技术以及多元类型的数据进行联合风控作业建模，进而更好地识别风险客户，提升贷前风险管理效能。

模型实践效果： ✓ 风控场景下模型区分能力可提升 25%+ ✓ 联邦建模对比传统建模效果差异小于0.5%



来源：艾瑞咨询研究院自主研究及绘制。

天冕科技

一站式金融科技服务商

天冕科技是WeLab汇立集团旗下一站式金融科技服务商，依托集团多年来金融科技的输出与积累，以大数据分析、人工智能、机器学习等核心技术为基础，自主研发了涵盖智能信贷风控服务、系统平台服务、数据中台以及联邦学习平台等在内的产品，助力合作机构降低运营成本，提升服务效率。

天冕联邦学习平台-打破数据孤岛 助力企业多场景挖掘数据价值

天冕科技自主研发的联邦学习平台是利用隐私计算技术打造的高效、安全数据合作解决方案；在充分保护各方用户数据安全、非共享数据的前提下打破数据孤岛，实现跨数据、跨行业的合作；支持私有化或云服务，操作简单，数据安全性强。目前，天冕联邦学习平台已经服务于多家合作企业。

天冕联邦学习平台产品优势与建模流程

产品优势

开箱即用
部署时间短，部署完成即可使用。

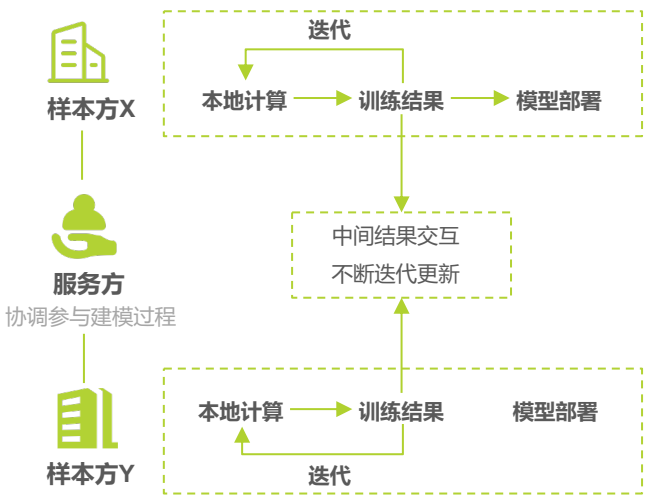
数据价值社区
展示企业与数据价值，创造合作共赢机会。

算法多样
提供多种算法，算法间可灵活替换。

操作简易
可视化建模流程，拖拉拽式建模。

安全稳定
采用同态加密算法和多方安全计算的方式，通过信通院安全认证。

部署灵活
采用容器化部署方式，支持私有化、云端化以及安全一体机。



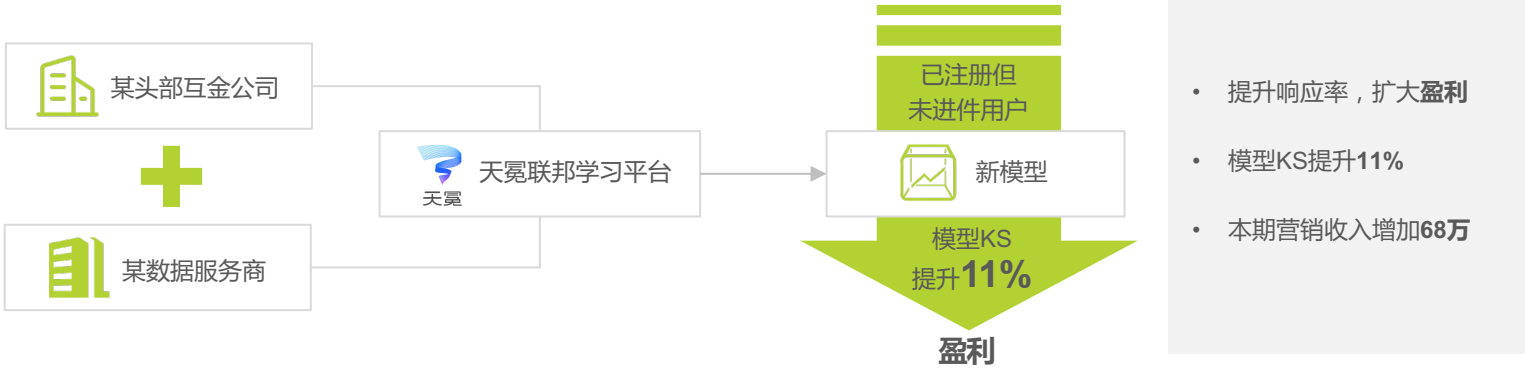
建模流程

来源：艾瑞咨询研究院自主研究及绘制。

天冕联邦学习平台落地案例：某头部互金公司通过画像补充提升营销效果

- 该互金平台依托天冕联邦学习平台进行联合建模之后，将用户特征维度扩大至上千维度，然后抽取样本中70%的沉默用户作为训练模型，并用该训练模型对剩余30%沉默用户进行评分预测。
- 结果显示，分值越高的用户，进件概率越大，在训练模型中分值排名前5%的样本用户里，预测的进件准确率能达到3%（较以往单独建模预测进件准确率为1%）左右，这说明了该训练模型对于有贷款需求的用户具有较高的预测性。
- 与此同时，天冕科技对比了该头部互金公司单方建模和多方联合建模的模型效果，从模型角度和最终预判的贷款需求用户数量来看，**联合建模比单方建模在AUC、KS等指标上具有更好的区分度和排序性，在对前10%评分高的用户营销后，模型KS提升11%。通过使用天冕联邦学习平台建模后，该头部互金公司本期营销收入增加了68万。**
- 截至目前，**天冕联邦学习平台已经与数十家金融及传统机构建立了合作**，合作的内容主要是联合数据提供方，在各方数据不出私域的前提下，进行联合风控和联合营销模型训练。

天冕联邦学习平台在金融领域中的落地案例



来源：艾瑞咨询研究院自主研究及绘制。

艾瑞新经济产业研究解决方案

iResearch 艾瑞咨询

行业咨询

• 市场进入	为企业提供市场进入机会扫描，可行性分析及路径规划
• 竞争策略	为企业提供竞争策略制定，帮助企业构建长期竞争壁垒

投资研究

• IPO行业顾问	为企业提供上市招股书编撰及相关工作流程中的行业顾问服务
• 募投	为企业提供融资、上市中的募投报告撰写及咨询服务
• 商业尽职调查	为投资机构提供拟投标的所在行业的基本面研究、标的项目的机会收益风险等方面的深度调查
• 投后战略咨询	为投资机构提供投后项目的跟踪评估，包括盈利能力、风险情况、行业竞对表现、未来战略等方向。协助投资机构为投后项目公司的长期经营增长提供咨询服务

关于艾瑞

艾瑞咨询是中国新经济与产业数字化洞察研究咨询服务领域的领导品牌，为客户提供专业的行业分析、数据洞察、市场研究、战略咨询及数字化解决方案，助力客户提升认知水平、盈利能力和综合竞争力。

自2002年成立至今，累计发布超过3000份行业研究报告，在互联网、新经济领域的研究覆盖能力处于行业领先水平。

如今，艾瑞咨询一直致力于通过科技与数据手段，并结合外部数据、客户反馈数据、内部运营数据等全域数据的收集与分析，提升客户的商业决策效率。并通过系统的数字产业、产业数据化研究及全面的供应商选择，帮助客户制定数字化战略以及落地数字化解决方案，提升客户运营效率。

未来，艾瑞咨询将持续深耕商业决策服务领域，致力于成为解决商业决策问题的顶级服务机构。

联系我们 Contact Us

400 - 026 - 2099

ask@iresearch.com.cn

企 业 微 信

微信公众号

法律声明

版权声明

免责条款

本报告中行业数据及相关市场预测主要为公司研究员采用桌面研究、行业访谈、市场调查及其他研究方法，部分文字和数据采集于公开信息，并且结合艾瑞监测产品数据，通过艾瑞统计预测模型估算获得；企业数据主要为访谈获得，艾瑞咨询对该等信息的准确性、完整性或可靠性作尽最大努力的追求，但不作任何保证。在任何情况下，本报告中的信息或所表述的观点均不构成任何建议。

本报告中发布的调研数据采用样本调研方法，其数据结果受到样本的影响。由于调研方法及样本的限制，调查资料收集范围的限制，该数据仅代表调研时间和人群的基本状况，仅服务于当前的调研目的，为市场和客户提供基本参考。受研究方法和数据获取资源的限制，本报告只提供给用户作为市场参考资料，本公司对该报告的数据和观点不承担法律责任。

为商业决策赋能

EMPOWER BUSINESS DECISIONS