WeBank 微众银行 | 金融科技 微洞察

KPMG 毕马威

2021

深潜数据蓝海
隐私计算行业研究报告

2021/04/06

序言

Preface

作为数字经济时代的新型生产要素，数据的重要意义已被社会各界充分认可，聚合多维海量数据、充分挖掘和利用其内在价值，成为各个产业机构的战略重点。同时，以欧盟GDPR和我国《个人信息保护法》（草案）等为代表的数据治理法律法规，又对数据安全和用户隐私保护提出了一系列严格的要求，各个机构对向外分享己方所拥有的数据也顾虑重重。为克服数据不易流通共享的障碍，打破数据价值释放的壁垒，隐私计算（privacy-preserving computation）成为关键的技术解决之道，有助于实现多方数据“可用不可见”。

隐私计算融合了人工智能、密码学、区块链以及计算芯片等一系列软硬件技术，在近年来在金融、医疗、政务等多个场景应用落地，取得了良好效果。从业机构也因此受到了资本的不断热捧，成为近期的一个热门投资赛道。不过，市场上的现有研究偏重于技术比较和从业机构介绍，缺少对行业发展的整体解析。为此，本报告将全面分析隐私计算领域的发展现状和趋势，在介绍政策、技术流派和应用场景案例基础上，重点研究产业市场空间和格局、商业模式及战略打法，展望行业的未来走向。

本报告的主要发现和观点如下：

（一）隐私计算受到大数据融合应用和隐私保护的双重需求驱动，也是目前国内外政策法规的必然要求。国内市场规模将快速发展，三年后技术服务营收有望触达100-200亿人民币的空间，甚至将撬动千亿级的数据平台运营收入空间。

（二）要达到这个规模，突破商业化的规模瓶颈，需克服四个难点：1）技术和解决方案还不够完全成熟；2）技术的安全性有待提高，缺乏可靠的技术标准认定；3）市场需求尚未充分展现，缺乏明确的拉动性政策和标杆性示范项目；4）较难搭建产业推广的多方协同合作模式。

（三）国内的隐私计算玩家各有差异，有来自于大型互联网公司，也有独立创业公司，还有来自于垂直行业

的机构。各家的资源生态、技术路线和行业布局均有不同，由此产生了不同的战略打法。互联网大厂体系玩家的主要优势是丰富的数据生态和应用组件；产业背景公司的主要优势是垂直行业的专注积淀和应用能力；创业公司的主要优势是中立性和贴近客户的服务能力。决定的关键是能否为客户带来足够的、特有的数据源，提供完整解决方案的能力。

（四）在商业模式上，通过搭建平台和运营来实现分润是更被看好的营收方式。由于行业之间的壁垒差异较大，隐私计算的应用平台很可能局限在一个个具体的垂直行业之内，但技术平台有望跨行业打通。不同类

别的玩家在平台构建上有各自差异化的优势。此外，隐私计算在未来有望形成服务订阅的收入模式，部署在云端——尽管目前以私有化部署为主。

（五）隐私计算市场未来可能形成若干家主流技术框架“寡头竞争”的局面，其中开源框架有突出的竞争力。另外，因为区块链与隐私计算是互补的技术体系，具备区块链能力也将有助于隐私计算技术服务商脱颖而出。

报告最后提出三条政策建议：

1）健全完善数据流通和分享的政策监管体系，奠定隐私计算产业的合法性框架。

2）逐步建立隐私计算技术和应用标准和产品认证体系，促进行业规范发展。

3）通过一系列高标准示范应用项目，为市场形成示范。

目录

Contents

1.风起于青萍之末：隐私计算迎来大时代

1.1.数据融合和隐私保护的双重需求驱动

随着移动互联网、云计算、物联网、大规模存储、高性能计算和芯片等信息技术蓬勃发展，世界进入数据爆炸的“大数据时代”。据估计，目前每年产生的数据总量达40ZB，若将这些数据储存在DVD里，将所有DVD叠加起来可绕地球50圈[1]。与传统的资本、土地、劳动、技术等一样，数据已是重要生产要素之一，与算力、算法组合，作为一种新型社会生产力，在人们的生产生活中发挥显著作用。越来越多的业务场景需要多方数据的流通和共享。在金融领域，银行保险机构借助内外部数据进行联合建模，实现数字营销、精准获客、差异化定价、智慧风控、智能反欺诈等。在医疗领域，医药企业、医疗机构和保险公司通过病例数据共享，形成联合AI模型进一步提高精准度。在政务、能源、交通、环保、工业和电信等具备大量数据基础的领域，数据共享和利用已经成为规划和落地应用中必不可少的部分。

社会各界高度认同数据生产要素的重要意义，合理挖掘、释放和使用数据要素所蕴含的巨大价值，已成为商业、技术和政策的一个热点主题。为此，人们需要促进数据的共享流通，或创造不同来源数据之间的协同效应。但横亘在人们面前的，是两个亟待解决的重要问题。

[1] IDC. Data Age 2025.

第一，如何打通融合多方数据，创造整合多维数据、释放更大价值的机会？

数据要素具有几个突出而矛盾的特性。一是分散性，数据持续不断地从各个途径产生，来源非常分散，缺乏数据授权、获取、存储、传输、验证及共享等交互标准；二是数据复制成本极低。这两个特性决定了很多情况下，各个数据所有方不愿意、不能够共享数据，不仅因为一旦分享出去就失去了对数据的控制权，也因为数据互联互通的成本较高，于是一个个“数据孤岛”出现。而且，即使数据能联通，它们的可信程度也存有疑问。三是价值聚合性，即单一数据源的价值有限，多维数据、海量数据的联合应用的价值更高。这些特性构成一对尖锐的矛盾——一方面数据需要聚合才能有价值，但另一方面数据却分散成一个个“孤岛”。因此如果能打破现实世界中数据高度分散的状况，以适当方式集成多方数据资源，并保证数据的可靠性，就有可能产生可观的协同效应。

第二，如何做好隐私保护，实现合法合规的数据应用？蕴藏着巨大价值的数据能够以极低的成本复制和无限使用，这种“野蛮掘金”的诱惑导致了各种各样数据泄露、盗用、滥用等问题案件频频发生，给人们带来了不少困扰。这造成了社会各界对于数据安全和隐私保护的担忧。为此，近三年来，欧盟GDPR、美国加利福尼亚州CCPA和我国的《数据安全法》（草案）、《个人信息保护法》（草案）等代表性法律法规出台，严格要求在数据使用过程中做好隐私保护，例如不允许数据离开本地、不允许未经授权使用个人数据等等。对于数据安全和隐私保护的担忧及相关法律法规的出台，在一定程度上给多方数据的融合应用设置了或硬或软的要求，迫切要求数据应用者找到可靠的方法，合法合规地实现数据的共享流通。

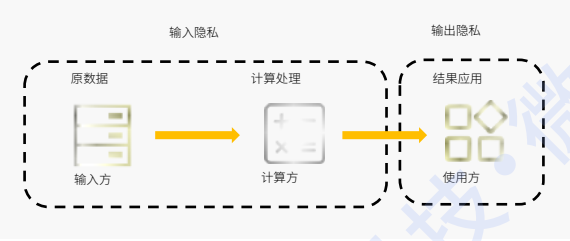
为克服这两大难题，隐私计算应运而生。隐私计算是“隐私保护计算”（privacy-preserving computation）的中文简称，根据“大数据联合国全球工作组”（Bigdata UN Global Working Group）的定义，这是一类技术方案，**在处理和分析计算数据的过程中能保持数据不透明、不泄露、无法被计算方以及其他非授权方获取**[2]。与之基本同义的一个概念是“隐私增强计算”（privacy-enhancing computation），通常可换用。

[2] Bigdata UN Global Working Group . UN-Handbook of Privacy Preserving Techniques.

本报告下文统一用“隐私计算”来称呼。

根据数据的分析处理全生命周期，隐私计算参与方可分为数据输入方、计算方、结果方三部分。根据保护目标不同，隐私计算方法可分为“输入隐私”（input privacy）和“输出隐私”（output privacy），输入隐私是参与方不能在非授权状态下获取或解析原始输入数据及其中间计算结果，输出隐私是指参与方不能从输出结果反推出敏感信息。下图1描述了两类方法和三类参与方之间的关系。

图1｜隐私计算参与方和目标



来源：Bigdata UN Global Working Group, 金融科技微洞察&KPMG

隐私计算技术出现后，能有效解决建构数字经济的上述两大难题。拥有独特数据的各个参与方能够以数据不出本地的新颖形式分享出去——分享“价值”、“知识”、“信息”而不是原始数据，做到数据“可用不可见”，从而既让潜在的数据价值被挖掘释放，又不损害数据所有者的权益和隐私权。由此，各方才有动力和能力通过数据流通协作来进行深度合作，用户也才能最大程度减少将个人数据放在各种互联网平台上的隐私泄露忧虑，有助于促进数字经济深度发展演化。

隐私计算技术解决的是让数据分享流通过程中的隐私保护问题，**然而需要注意的是，使用隐私计算的前提是数据源机构和使用方机构都必须征得用户同意。**机构应在自己的隐私政策中明确告知用户，会对其收集的信息在标识化后用于研究、统计、分析，并为第三方合作伙伴的商业决策提供支持。否则，机构无权将数据用于联合计算。这是从业机构要注意的一个基本前提。

1.2.隐私计算典型应用场景

（一）金融领域

金融行业是最早应用信息技术的产业之一，从上世纪80年代的ATM机到近年的开放银行，金融行业已经收集、产生、积累了大量的数据。同时，金融行业也是能够最大化利用数据价值的行业之一，从个人征信到公司估值，从价值投资到技术分析，金融行业想提供高效服务、获取用户价值，离不开对数据的合理使用。

当今，金融行业在使用数据时面临数据孤岛和数据隐私保护两大问题。这两个问题的解决方案在传统的技术方案中看似是相互矛盾的，但通过隐私计算技术，金融行业可以做到在保护数据安全和个人隐私的前提下，解决数据孤岛问题，充分发挥数据价值。

以银行业为例，反洗钱是银行业在风险控制时的一个重要任务。传统做法是使用规则和模型，利用银行自身的数据，来判断交易是否为洗钱活动。

但这些传统方法效率较低，覆盖范围小。

银行可以在互相之间或与其他数据源（例如互联网公司）联合，通过交换加密参数，联合计算建模，解决反洗钱样本少，数据质量低的问题，形成一个稳健、特征丰富的智能模型。调用联合建立的模型，不用集合各方数据，银行的反洗钱能力大大增强。

此外，通过打破数据孤岛，聚合各方数据，隐私计算还可以在发现多头借贷、信贷风控、保险定价、精准营销等多个金融行业的细分领域发挥重要价值。

（二）医疗领域

近年来，随着医疗流程线上化、病例电子化、医院信息化程度的不断加深，基于大数据的智能医疗逐渐成为可能，如果能够对医疗数据加以妥善利用，不仅可以提升医学研究水平，而且可以提升公共卫生服务水平，弥补基层诊疗能力短板。

但是医疗数据具有隐私性极强的特点，医疗数据的安全常常关乎人们的生命财产安全。目前，海量的医疗数据分散在各个孤立的医疗机构中，传统的方法下，数据安全和隐私保护的要求使得这些数据无法聚合起来，而单个医疗机构的数据样本量又不足以支撑大规模的模型训练，难以实现数据价值。

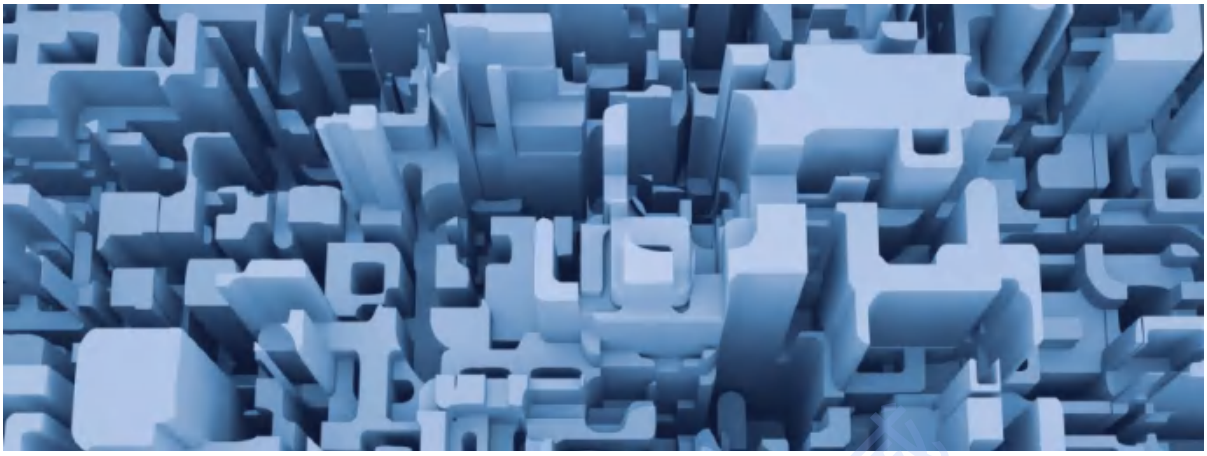
利用隐私计算技术，则可以使得各个医疗机构的数据在不出库的前提下实现联合建模。例如，患者确诊前常常会进行一些标准化的化验，检验结果受到操作人员影响较小，可以依靠设备及标准流程进行规范化，从而获得标准化的医疗数据。引入隐私计算技术，能够进一步实现不同医疗机构的化验检查数据联合建模，通过联合建模、共享模型，即使是病例量较小的医院，也能获得效果较好的模型。模型可用于辅助医生诊断，在减轻医生工作负担的同时，帮助医生提高诊断准确率。

隐私计算技术在医疗领域的应用，将以极低的成本促进优质医疗资源下沉，提升医疗资源稀缺地区和基层医疗机构的医疗服务能力和水平。

（三）政务领域

隐私计算技术不仅在企业、机构间大放异彩，而且在政务领域逐渐得到了充分应用。一方面，隐私计算的应用有利于实现政府各部门数据的互联互通，促进政府跨部门协同。另一方面，政府和企业都积累了海量数据，隐私计算提供了政企数据共享利用的解决方案，有利于充分释放政企数据蕴含的巨大价值。

以智慧城市这一应用场景为例，智慧城市涉及安防、交通、环保、文旅等各个行业，其业务生态虽然纷繁复杂，但功能本质上都是通过对数据的不同处理形式来实现的。通过交通出行数据、物联网数据、公安数据、水电燃气数据、互联网数据等的融合利用，智慧城市可以提高一个城市的公共管理、公共服务、公共安全水平，而各类数据的融合利用则离不开安全的数据共享。隐私计算技术为隐私保护、数据安全前提下的数据共享提供了解决方案。



2.各领风骚：隐私计算关键技术路线

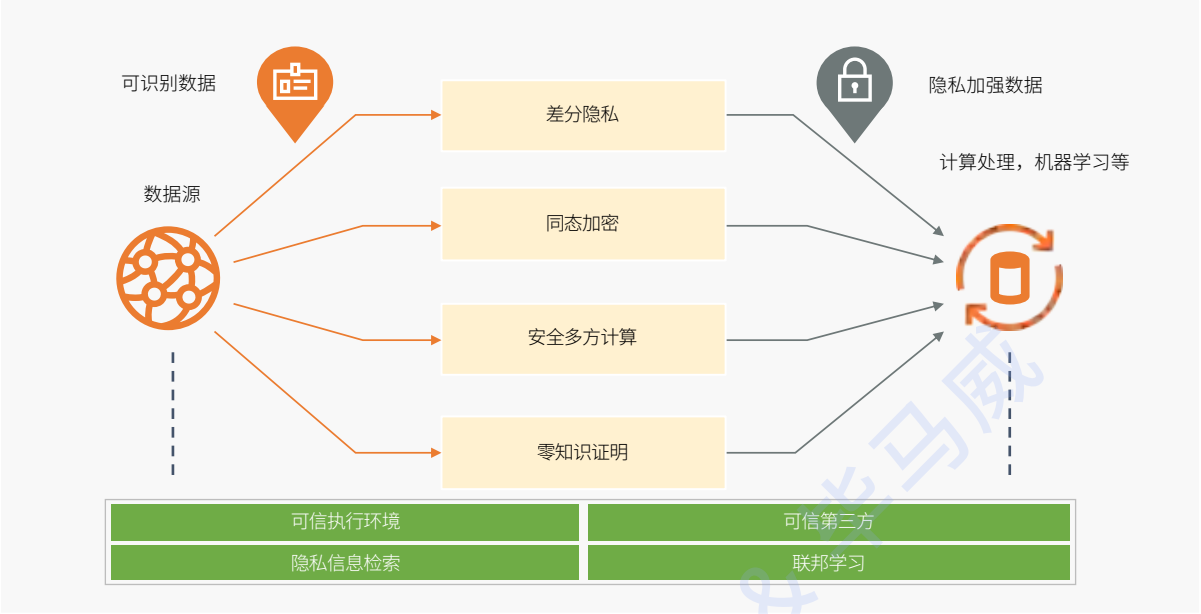
考虑到本报告核心目的是进行产业分析，因此本章只对隐私技术的技术体系和关键技术路线进行概述和简要分析，来方便读者了解隐私计算技术的全貌，对隐私计算的关键技术形成清晰的认识，从而易于理解隐私计算产业的产业图景。

2.1.技术分类

数据的分析处理全生命周期可分为数据输入、计算、结果三个环节，当下市面上的隐私计算技术体系普遍依据这一原则进行构建。如图3所示，隐私计算技术体系包括差分隐私、同态加密、多方安全计算、零知识证明、可信执行环境、联邦学习等技术。Gartner公司认为，按照实现的功能，这些技术进一步可分为以下三类：

- **提供可信的环境来执行处理或分析；**
- **在处理或分析之前转换数据和/或算法；**
- **在不公开数据的情况下执行数据本地处理或分析。**

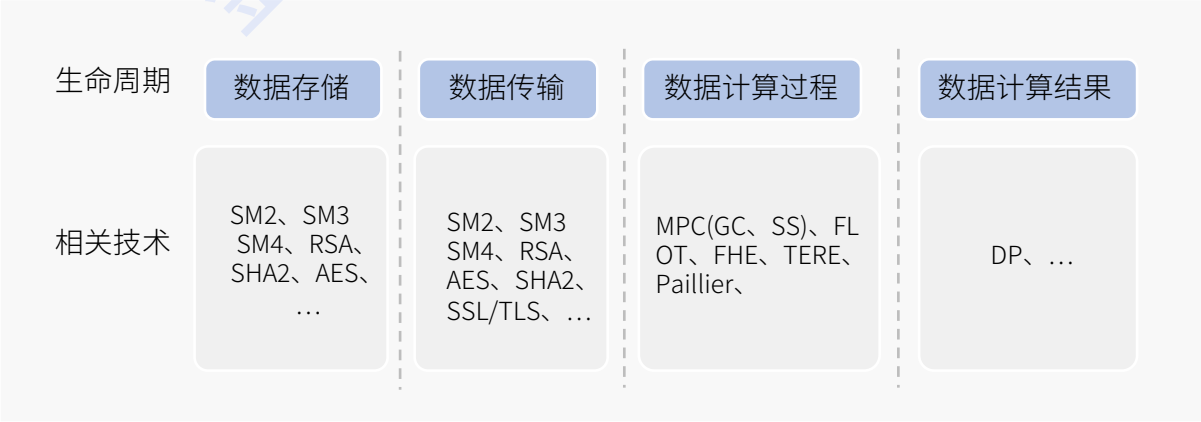
图2 | 隐私保护技术体系



来源：Gartner，金融科技微洞察&KPMG

与此类似，中国信通院同样根据数据的生命周期，提出了隐私计算技术体系（见图4）。信通院将数据的生命周期分为数据存储、数据传输、数据计算过程、数据计算结果四个环节，每一个方面都涉及不同的技术类型。在该技术体系中，除了包括了Gartner体系中涵盖的技术之外，还包括了加密算法和安全技术如SM2算法、RSA算法、SSL技术（安全套接层，security socket layer）等。

图3 | 根据数据生命周期划分的隐私计算技术



来源：中国信通院

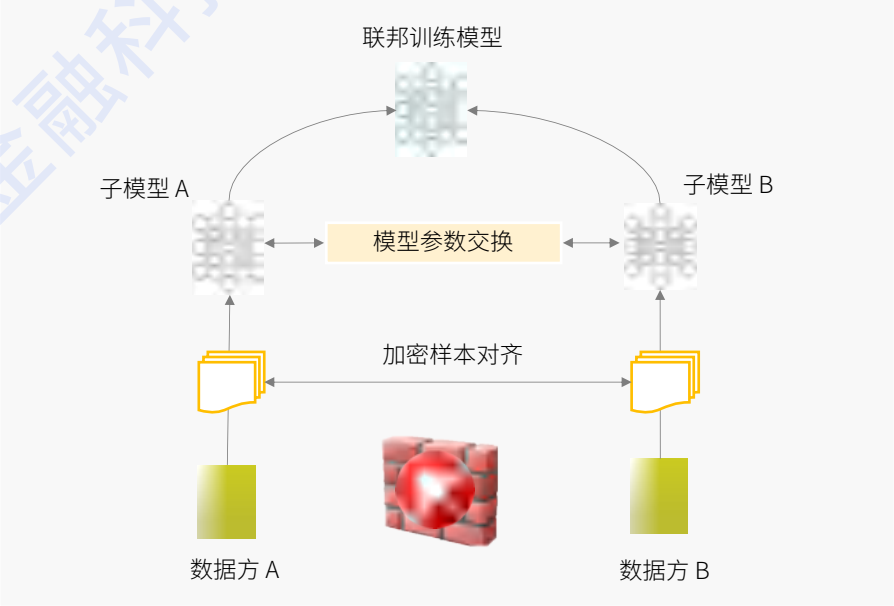
值得一提的是，其中算法和技术——如SM2、SM3、SM4、RSA、SHA2、SSL/TLS等——经过长期发展和完善，目前已相对成熟，未来进一步优化和发展的潜力相对有限，已经不属于隐私计算产业关注的热点。然而，还有一些技术则在近年来取得了关键的突破，并将对未来隐私计算产业的发展有重要的影响，如联邦学习、多方安全计算等，下文将对这些关键的技术进行介绍和分析，来方便读者对隐私计算技术的未来发展方向和趋势有一个宏观的认识和把握。

2.2.联邦学习

联邦学习(Federated Learning, FL)，又名联合学习，联盟学习，通常可以理解为是由两个或以上参与方共同参与，在保证各数据方的原始数据不出库的前提下，协作构建并使用机器学习模型的人工智能技术。联邦学习能有效帮助多个机构在满足用户隐私保护、数据安全和政府法规的要求下，进行数据使用和机器学习建模。联邦学习实际上是一个综合性的技术组合，底层融合了多种机器学习算法和隐私保护的算子，如安全多方计算的多种协议和差分隐私，都可以被用于联邦学习。

联邦学习的原理是通过构建一个计算网络，使客户可以在自己的终端通过使用本地数据对模型进行训练，并将模型的更新内容进行上传汇总，将不同终端的模型更新进行融合，以此优化预测模型，客户终端再将更新后的模型下载到本地，并不断重复这一过程。在整个过程中，终端数据始终存储在本地，来避免数据泄露的风险。

图4 | 联邦学习架构



来源：微众银行《联邦学习白皮书》，金融科技微洞察&KPMG

根据训练数据在不同数据方之间的特征空间和样本空间的分布情况，联邦学习可分为横向联邦学习（horizontal FL）、纵向联邦学习(vertical FL)和联邦迁移学习（federated transfer learning），对于每个具体分类的详细解释，不在这里赘述[1]。

[1]有兴趣的读者可以参考——杨强，刘洋，程勇等. 2020. 联邦学习. 电子工业出版社.

联邦学习的优势在于原始数据不出本地，从而实现共享数据最小化，来保护数据隐私。然而，由于各参与节点计算能力不一致、网络连接状态不稳定、数据通常非独立同分布等现实因素，联邦学习的通信效率极易成为联邦学习应用的瓶颈之一。另外，联邦学习还面临着梯度带来的隐私泄露的风险。因此，如何突破效率瓶颈，达到实用性、安全性的平衡，并进一步提升安全性，是联邦学习技术未来发展面临的主要问题。

2.3.安全多方计算

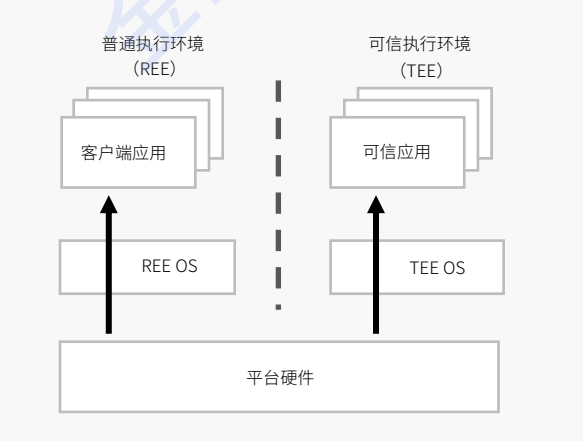
安全多方计算（secure multi-party computation，MPC）顾名思义，是在保证多个参与方获得正确计算结果的同时，无法获得计算结果之外的任何信息，从而保证各方数据的安全和私密。安全多方计算技术包括秘密共享（secret sharing）、不经意传输（oblivious transfer）、混淆电路（garbled circuit）、隐私集合求交（private set intersection），隐私信息检索（privacy information retrieval）等关键计算协议。

MPC的优势在于，各个参与方对其所拥有的数据拥有绝对的控制权，保证基本数据和信息不会泄露。然而，目前MPC技术包含复杂的密码学操作，计算开销较大，需要付出很大的性能代价。此外，针对特定问题和场景，还需要设计专用协议。另外，该技术的落地还受到网络带宽、延迟等因素制约。因此，提升计算效率，降低实施方案设计复杂度，与此同时拓展技术落地场景，将是未来MPC在产业应用的优化和发展方向。

2.4.可信执行环境

可信执行环境(trusted execution environment, TEE)是在基于硬件防护能力的隔离执行环境中计算,来实现数据安全和隐私保护功能。TEE的原理是将系统的硬件和软件资源划分为两个执行环境——可信执行环境和普通执行环境(rich execution environment, REE),TEE的操作系统比REE的操作系统的安全级别更高,为密钥和代码运行提供了一个安全隔离环境,有独立的内部数据通路和计算所需存储空间。普通环境的应用程序无法访问TEE。当不安全的用户模式需要获取安全环境内的服务时,或一个应用程序想要进入安全环境中,操作系统需要检查其安全性,只有通过检验的程序才能进入,从而为代码和数据提供机密性和完整性保护,免受破坏。即使在TEE内部,多个应用的运行也互相独立,不能在未授权的情况下互相访问。

图5 | TEE基本原理



来源:《信息网络安全》期刊

TEE技术的核心在于硬件技术,实现该方案的前提在于必须要相信可信执行环境厂商是可信的。然而这带来了几个问题。首先,目前硬件技术被掌握在英特尔、高通、ARM等少数外国核心供应商中,国内相关技术和产业尚不成熟,因此从安全可控层面考虑,国内隐私计算产业尚无法大规模应用该项技术,从国外购买指定的硬件会显著提高该技术使用成本,不利于该技术的大规模推广。其次,硬件的可信度是中心化的,也就是说,用户必须相信硬件厂商和平台服务商的信誉,那么谁来作为这个可信第三方?再次,TEE硬件设备被质疑有安全缺陷,相关缺陷陆续曝光,需要不断改进升级硬件,不过相比于软件升级,硬件升级更换的成本较高。因此,该技术未来的产业发展方向在于打造自主可控、安全可靠的国产TEE 芯片等安全相关产品,实现自主替代,从而为该技术的大规模应用铺平道路。

2.5.其他常见隐私保护技术

(一)差分隐私

差分隐私技术(differential privacy)基于严格的数学理论,通过在计算结果中添加噪声的方法,保证攻击者无法根据输出差异推测个体的敏感信息,从而在不损害个人隐私的前提下,实现数据资源的最大利用。此外,差分隐私对隐私保护进行了严格的定义并提供了量化评估方法,对隐私保护水平进行了科学严谨的证明。

差分隐私通过噪声添加实现隐私保护，会对模型数据的可用性和准确率造成一定程度的影响。如果数据添加的噪声过大，数据统计时的可用性和准确度则会严重受损。因此，对于对准确度要求较高的场景如人脸识别、金融风险计量，目前无法大规模应用该项技术。如何降低噪音对准确率的影响，更好地平衡隐私性和可用性，从而提升该技术的应用广度和深度，是当下差分隐私计算技术发展的重点。

（二）同态加密

同态加密（homomorphic encryption）是一种允许在加密之后的密文上直接进行计算，且计算结果解密后正好与明文的计算结果是一致的加密算法。按照支持的功能划分，目前的同态加密方案可以分为”部分同态加密”（somewhat homomorphic Encryption）和"全同态加密”（fully homomorphic encryption)两类。

目前同态加密的发展瓶颈在于计算开销大，加密效率低，运算速度慢。因此，该技术还不能适用于大规模业务。未来，如何突破性能和效率的瓶颈，将是同态加密技术的产业应用和发展的重点。

（三）零知识证明

零知识证明(zero—knowledge proof)，指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的计算技术。零知识证明的原理在于构建一个多方协议，即参与的多方需要完成一项任务所需采取的一系列步骤，通过完成这些步骤，证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。

在使用零知识证明时，不会降低安全性，并且可以保证信息的完整隐秘性。然而，生成零知识证明需要大量的算力和较长的时间，效率瓶颈限制了该技术的大规模应用。因此，优化算法、提升计算效率将是未来零知识证明产业应用的一个重要方向。

通过归纳总结，我们不难看出，当下隐私计算技术体系中的关键技术有联邦学习、安全多方计算、TEE、差分隐私等，都有一定的应用优势，也能在一定程度上保护隐私。不过，虽然它们在隐私安全性、发展方向和应用场景等方面相差较大，在大规模产业落地时，这些技术普遍面临着计算效率低和应用场景有限的两个主要瓶颈，这是隐私计算产业需要突破的技术难点。

3.大势浩荡：政策现状和市场空间

3.1.隐私计算是政策趋势所向

数据要素的流通和共享已经成为实现数据价值的必然选择，但如何兼顾数据的流通性和隐私安全保护，让海量数据流动的同时又能保护数据隐私安全、防止敏感信息泄露，成为业界关注焦点。隐私计算相关技术可以很好地解决数据流通难题，为释放数据价值打下基础，具有良好的发展前景。政策引导和扶持是隐私计算技术和产业发展的重要推动因素，成为相关从业者的关注重点。这些政策可分为三大类。

第一类是大数据产业政策，为隐私计算奠定了发展环境，供给了计算的“燃料”。从国家发展规划到各个有关部委文件都在积极推动数据要素市场建设，由此促进数据融合应用以及相关技术应用。最具有标志性的事件是2020年4月党中央、国务院颁布《关于构建更加完善的要素市场化配置体制机制的意见》，将数据列为一种新型生产要素，与土地、劳动力、资本、技术等传统要素并列为要素之一，指出要推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护、引导培育大数据交易市场，加速各种智能场景的应用。该文件表明了数据正在成为现阶段最为核心的生产要素，表达了国家对数据价值的高度重视以及对数据安全的严格要求。2020年10月，十九届五中全会通过“十四五”规划建议，更明确地指出，新时代的数据不再是传统意义上的数据，要明确数据作为核心生产要素的重要性。只有正确认识数据的生产价值与重要性，有计划地安排、使用好数据，才能为科技创新提供更多可能。2020年末，国家发改委等四部委联合发布《关于加快构建全国一体化大数据中心协同创新体系的指导意见》，提出数据是国家基础战略性资源和重要生产要素，要强化数据中心、数据资源的顶层统筹和要素流通，加速数据流通融合，推动核心技术突破及

应用，强化大数据安全保障。中国人民银行在2019年9月颁布的《金融科技(FinTech)发展规划(2019-2021年)》也提出，在切实保障个人隐私、商业秘密与敏感数据前提下，强化金融与司法、社保、工商、税务、海关、电力、电信等行业的数据资源融合应用，加快推进服务系统互联互通，建立健全跨地区、跨部门、跨层级的数据融合应用机制，实现数据资源有机整合与深度利用。

第二类是数据安全和隐私保护政策，为隐私计算创造了需求，使之成为数据使用机构的“刚需”。2018年欧盟发布的《通用数据保护条例》(GDPR)是目前最全面、应用最广泛的隐私保护法规之一。GDPR规定了违反数据隐私法规的严厉制裁，对于违反某些重要规定的罚款最高可达2000万欧元或全球年营业额的4%。我国的法律法规在数据安全和隐私保护方面也明显趋严。2016年，我国发布了第一部网络安全和数据保护相关的法律《网络安全法》，规定“未经被收集者同意，网络运营者不得向他人提供个人信息”，并要求互联网企业不得泄露或篡改收集得到的用户个人信息。《信息安全技术-个人信息安全规范》从标准角度明确了各条款的要求。2020年10月，中国人大网公布了《个人信息保护法(草案)》全文，规定侵害个人信息权益的违法行为若情节严重，将没收违法所得，并处5000万元以下或者上一年度营业额5%以下罚款。2020年最新发布的《民法典》也明确了个人信息受法律保护。

第三类明确提出鼓励应用隐私计算，目前主要有工信部的两个大数据产业政策。工业和信息化部早在2016年底发布的《大数据产业发展规划(2016-2020年)》中，就提出要支持企业加强多方安全计算等数据流通的关键技术攻关和测试验证。工信部《工业大数据发展指导意见(征求意见稿)》提出，在工业领域积极推广多方安全计算技术，促进工业数据安全流通。

一系列政策的出台和布局落地，不仅从法律层面明确了数据安全和个人隐私保护的必要性，也从国家层面为隐私计算技术和应用的关键领域奠定了良好基础，有力促进各行各业在数据的采集、使用、交易和流通等各环节中加强数据保护，为隐私计算产业带来重大利好。

图6 | 我国隐私计算相关政策文件

文件名	文件类别	发布时间	发布机构	相关核心内容
网络安全法	法律	2016年11月	全国人大	第一部网络安全和数据保护相关的法律
民法典	法律	2020年6月	全国人大	明确了个人信息受法律保护
个人信息保护法（草案）	法律	2020年10月	全国人大	第一部保护个人信息的法律
大数据产业发展规划（2016-2020年）	发展规划	2016年12月	工信部	提出要支持企业加强多方安全计算等数据流通的关键技术攻关和测试验证
金融科技(FinTech)发展规划(2019-2021年)	发展规划	2019年9月	中国人民银行	强化金融与司法、社保、工商、税务、海关、电力、电信等行业的数据资源融合应用
工业大数据发展指导意见（征求意见稿）	发展规划	2019年9月	工信部	在工业领域积极推广多方安全计算技术
关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议	发展规划	2020年10月	中共中央	明确数据作为核心生产要素的重要性
个人信息安全规范	技术标准	2017年12月	全国信标委	明确了个人信息保存和处理的具体要求
个人金融信息保护技术规范	技术标准	2020年2月	中国人民银行	对个人金融信息保护提出了具体明确的要求
关于构建更加完善的要素市场化配置体制机制的意见	规范性文件	2020年4月	中共中央，国务院	将数据列为一种新型生产要素
关于加快构建全国一体化大数据中心协同创新体系的指导意见	规范性文件	2020年12月	发改委，网信办，工信部，能源局	指出要加快构建全国一体化大数据中心，加速数据流通融合，强化大数据安全保障

来源：中国信通院

3.2.隐私计算将撬动千亿级规模市场

隐私计算的从业机构以技术服务商为主，为客户提供软硬件系统解决方案。尽管遥望远期，隐私计算系统能部署于边缘侧甚至终端设备——例如以SDK嵌入手机App，服务于小B和C端客户的日常隐私保护需求，但这种应用场景由于技术、通讯等原因还非常遥远，目前主流应用聚焦在政府和企事业单位的业务场景，所以本报告聚焦于主流应用，估计隐私计算的国内市场空间。

隐私计算机构的营业收入主要分为两大类（详见下文4.1节），一是传统的软件销售和服务收入，二是通过隐私计算平台上的业务运营产生利润分成。后者是很多投资人非常看重的一点[1]，认为隐私计算会在平台分润上形成很有想象力的空间。下文分别讨论这两种收入的空间。

[1] 参见36氪报道https://www.36kr.com/p/801141060510982

[2] IDC将软件市场细分为16个子市场

[3] IDC. 中国人工智能软件及应用跟踪（2019年下半年），见https://www.idc.com/getdoc.jsp?containerId=prCHC46625720

（一）软件销售和服务收入在三年后的潜在规模可达100-200亿元

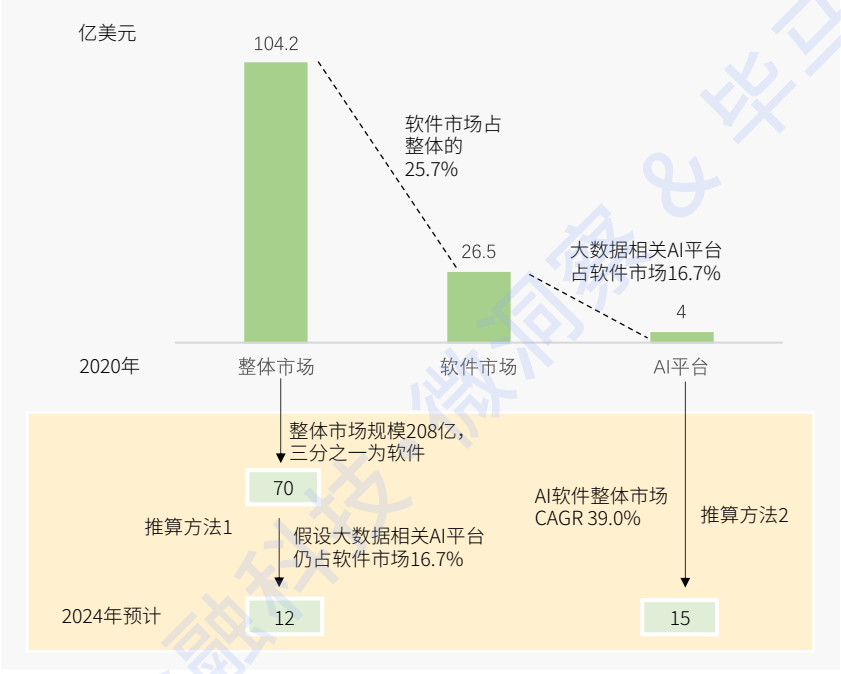
因为隐私计算产业刚刚兴起，几乎找不到直接相关的销售数据和统计，所以本报告会从两个角度来粗略估计和佐证。

第一个角度是自上而下，从国内大数据软件市场观察，因为隐私计算服务于数据市场，软件系统可归类于大数据相关软件体系之内。这里先不考虑基于可信执行环境（trusted execution environment, TEE）技术路线所带来的硬件市场（见本报告第3章）。我们统一采用国际知名调查和资讯机构IDC的报告以保持数据源一致，增强可信度。根据IDC在2020年中发布的《全球大数据和分析支出指南》（Worldwide Big Data and Analytics Spending Guide 2020），中国大数据相关市场的规模在104.2亿美元，其中25.4%是大数据软件，约为26.5亿美元。在大数据软件领域，预计50%的份额由最大的三个细分子市场组成，分别是终端用户查询汇报分析工具（end-user query, reporting, and analysis tools）、人工智能软件平台以及关系型数据仓库[2]。假设前述3个细分市场规模相近，那么AI软件平台占到整个大数据软件市场的16.7%，约为4亿美元。

下面我们用两种方法来推算五年后的市场（见图7）。第一个数据源仍然是该报告，报告预测到了2024年，中国大数据相关整个市场将达到208亿美元规模，其中硬件、服务、软件将各占三分之一，那么软件市场大概为70亿美元。若AI软件平台仍然占其中16.7%，则规模为12亿美元。换一个数据源，IDC在另一份报告中指出，中国整个AI软件市场在2018-2024年的复合增长率达39.0%[3]。假设大数据相关AI软件平台也是同一个增长率，那么从2019年的4亿美元增长到2024年，国内市场规模约为15亿

美元。可以看到，两个方法得出的结果相近，较好地交叉检验了对AI软件的推算。因为现在隐私计算与人工智能通常紧密结合，即在人工智能软件中增加隐私计算模块，**那么我们粗略地用AI软件平台的规模来近似隐私计算软件规模，作为隐私计算规模的上界。**由此可见，2024年我国隐私计算软件平台的市场规模上界约在12-15亿美元，若再考虑到TEE技术路线带来的芯片硬件支出，规模总和可突破百亿人民币。

图7｜2024年国内隐私计算软件市场规模推算



来源：IDC，金融科技微洞察&KPMG

第二个角度是分行业自下而上来推算，考察每个行业的IT支出。因为隐私计算系统支出是客户IT支出的一部分，客户IT预算高低决定了隐私计算市场的上限。我国隐私计算主要服务于金融、医疗和政务三大客群。

金融行业的应用较为成熟。在金融业中，目前银行是隐私计算的主要客户，证券和保险公司很少。而且根据金融科技微洞察的早年研究[1]，银行业的IT投入占到金融行业的80%，所以根据“二八原理”，我们只估计银

[1] 徐磊，李思琪. 2019. 产业互联网的核心模式（下）：金融SaaS之市场规模、赛道和竞争要点. 见https://mp.weixin.qq.com/s/dnKhshuL-TizS7UA6XGhbLw.

行。目前隐私计算在银行业内的应用场景以风险管理和反欺诈为主，和反欺诈为主，还有部分用于商业分析等，所以主要是用于智能风控。根据亿欧智库和智研咨询的研究，我国智能风控在2020年已达到78亿元市场规模，2024年预计达到203亿元，其中反欺诈约为81亿、信贷风控约为91亿[1]。由于随着未来金融业数据合规和隐私保护的要求越来越严格，隐私计算将成为智能风控必不可少的基础，成为主要技术模块，因此隐私计算在金融业的潜在市场空间可达170亿。

医疗和政务的隐私计算应用场景较为分散，在医保控费、病历质检、医疗研究、政务信息平台搭建等等多个场景都能得到应用。这意味着估计隐私计算的支出就变得非常困难。仅以医保控费技术服务为例，这个市场的潜在规模就在100-300亿[2]，但很难估计隐私计算在其中能分到多少份额。

到2024年，仅我国金融业的风控需求就能提供将近200亿的潜在应用市场空间，再加上医疗和政务场景支出，隐私计算撬动的市场规模潜力能突破200亿人民币。

综合以上两个角度，**我国隐私计算系统的销售和服务收入规模在三年之内有希望触达100-200亿的市场空间。**

（二）平台运营分润的潜在市场空间极大，仅消费金融业务就能撬动千亿规模市场

如果通过所运营的平台来分润，这部分营收的上限就非常高，但是很难估计，因为业务场景太广，不同场景的营收和分成方式大相径庭。本报告只能管窥知豹，从一个主要场景来看隐私计算市场空间的想象力。

[1] 智研咨询 https://www.chyxx.com/industry/202010/903862.html，亿欧智库https://www.cebnet.com.cn/20181130/102536930.html

[2] 见36氪在2016年所做的估测，https://36kr.com/p/1721016696833。另外，可参见卫宁软件在2014年的公告估计，https://finance.qq.com/a/20140306/007091.htm

本报告仅以隐私计算目前主要落地场景之一——个人短期消费金融业务为例估计，包括车贷、小额消费贷、现金贷、信用卡分期等。金融机构风控需要基于多方数据进行联合建模，隐私计算就是刚需，信贷业务就发生在隐私计算的平台上。国内个人短期消费金融的市场在2019年已达到9.92万亿元，假设以10%的低复合增长率增长[1]，那么到2024年能达到16万亿元。

[1] 事实上我国短期信贷消费余额在2015-2019年的年复合增速达24.72%。

隐私计算技术通过搭建平台，帮助平台运营商分享这个巨大市场的收益。我们来计算平台能分得多少红利。不妨参照某金融科技服务商M公司招股书所披露的消费信贷营收规模做粗略估计，它提供了较高的一个分润比例。该公司在消费信贷科技平台上收取的业务收入与其促成的贷款规模余额之比约在2%，即按照贷款余额的2%作为平台技术服务费。再看业内另一个J公司的招股说明书，它的企业小微贷款技术平台约收取贷款余额的1%作为技术服务费。那么**即使2024年消费信贷平台的分润比率只有1%，分润规模也能达1600亿！**

要注意的是，这个规模是隐私计算技术能撬动的平台市场想象空间，单纯的技术服务商能从平台运营收入中分得的实际收益需打折扣，其原因有两点：首先，上述两家公司能获得1%-2%的分润比例，最重要的依赖于它们的流量议价能力，而不是技术服务能力，隐私计算技术和数据源重要，但如果客户流量在别人手中，那分得的市场有限。其次，此处假设个人短期消费信贷都依赖于隐私计算平台，但实际上隐私计算平台在短期消费贷市场上的渗透率一定会有折扣。

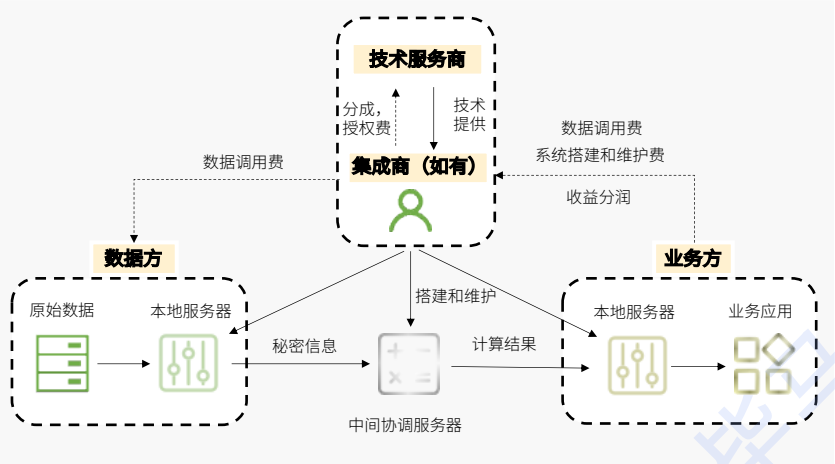
4.一时多少豪杰：隐私计算的产业图景

4.1.主要商业模式

一个典型的隐私计算业务场景会包含三类参与方（见图7）：（1）使用数据的业务方，如金融机构、政府机构等要应用数据服务于自身业务，它是隐私计算服务的客户；（2）作为数据源的数据方，如各地的大数据局、征信公司、拥有用户数据的互联网公司等，原始数据不出本地，将经过处理后的秘密信息（例如加密数据、模型梯度、参数...）发到中间方服务器上计算；（3）隐私计算技术服务商本身，为客户搭建整个计算系统，包括在业务方、数据方以及可信第三方部署服务节点，提供计算服务。在某些情况下，技术服务商本身不直接面向客户，而是将技术模块放入一个大的集成方案里，由集成商面向客户。

通常情况下，三个角色是分离的。不过在有些场景里，一个机构可能身兼两种角色。比如企业集团在内部应用隐私计算来调用各个子公司数据，又比如金融机构自己有部分数据和业务需求，它们既是业务方，也是数据方；有些互联网公司自身既有数据、也有计算技术，希望将技术和数据价值输出给客户，它就既是技术服务商，也是数据方；还有金融机构有技术，也有金融计算场景，但缺乏足够数据，希望联合外部数据源一起做，它就兼有技术服务商和业务方的角色。

图8｜隐私计算产业一般商业模式示意（本地部署）



来源：金融科技微洞察&KPMG

由于隐私计算应用基于数据而存在，所以一般情况下，**技术服务商不仅为业务方搭建技术系统，同时要为客户找到数据源，**数据方也接入到系统。**目前绝大多数部署方式是在客户和数据方进行本地部署，**极少场景下是通过云端为客户提供SaaS服务——但在未来有可能云端部署会越来越多[1]。基于目前的主流部署和合作模式，技术服务商对业务方有4种基本营收方式：

[1] 比如某厂商的科研工作者客户需要将本地的科研数据和外部公共数据融合计算，就通过软件订阅来获取

销售模式——收取一次性技术系统搭建费，这是最经典的软件系统销售模式，费用按照系统所消耗的计算存储资源、布置节点数目测量，每单从数十万到数百万不等，差异较大。

服务模式——收取年度系统维护和服务费用，这不仅是因为一般软件系统都有日常维护需求，还因为隐私计算的算法本身和应用场景中的模型更新较快，可能需要重新调整算法和模型。

调用模式——收取数据使用费，这部分费用主要归属于数据方，技术服务商只是作为收费通道代数据方向客户收取，也有时候会赚取数据使用的差价或撮合费用。收费标准根据数据种类和价值而定，按照数据调用次数收取，单次调用费从几分到几角不等。有时候，数据价值无法

在使用前确定，需要经过一段时间试用，客户才能根据实际效果确定付费标准。

分润模式——根据业务运行效果，获取收益分成。在这种模式下，客户早期往往并不需要承担大笔技术系统搭建费，相当于技术服务商与客户联合运营业务。基于系统接入数据源，原有业务改善或新业务开展之后，双方根据业务实际效果分润。

实际商务场景中，这几种模式会混合搭配。对于早期起步的创业团队，销售系统和收取服务费固然是最快和最主要的营收模式，能快速获得经营性现金流。而且，在很多项目中，隐私计算只是作为更大解决方案的一个模块，从解决方案整体销售中获取分成。但是从长远看，由于开发和部署系统需要做不少定制化工作，系统销售所收取的费用是一次性、低毛利的，技术服务商并不能从中获得稳定、较高的利润，就希望结合分润模式，从实际运营中获得长期可持续的收入。比如为银行客户搭建基于隐私计算的新型风险控制系统，接入新数据之后改善了风控模型、降低了违约率，技术服务商就有机会分享银行增长的利润。双方联合运营隐私计算平台，通过深度运营获取分润，很有可能成为未来的主要模式。下文将进一步详细讨论这个问题。

4.2.国内代表性玩家

随着近几年隐私计算的重要性愈发凸显，市场上已经出现了多个入局者，根据自己的技术和商业资源进行市场定位，制定战略决策。本报告从资源生态、技术路线和行业布局三个维度来介绍国内的一些代表性玩家。这三个维度都是支撑企业战略制定的重要依据，不同的特征决定了企业的市场定位和发展路线。

- **资源生态，指企业发展所依托的资本和关系网络，**在很大程度上影响了企业的市场定位、品牌形象、资本储备、客户来源、伙伴关系等，成为企业战略打法的基本参照轴。最典型的资源生态就是股东和创始人资源等，由此区分出大型互联网公司、政府背景公司、产业背景公司（例如金融机构、金融数据公司）、隐私计算起家的创业公司等不同派系的企业。互联网公司和产业背景公司有自身的数据积累和应用场景，创业公司较为中立，各有优势。

- **技术路线，指企业主要产品所采纳的底层技术选项，**在较大程度上影响了产品的适用场景、功能和性能表现，从而影响到客户和落地应用选择。隐私计算的联邦学习、多方安全计算（MPC）、TEE、同态加密等都是典型技术路线，此外有些厂商还会结合区块链技术，将区块链技术和隐私计算紧密结合来推出解决方案。在技术路线维度上，还有一个选项是技术框架是否开源。开源已经越来越多地成为IT企业的选择，产生了以Linux、Android、Kubernates、TensorFlow、MySQL等为代表的高市占率产品，由此推动了背后公司的成功。

- **行业布局，指企业获客和商业化落地的主要行业，**非常显著地体现了每个企业在隐私计算产业中的差异化定位，决定了企业的具体战略战术，如资源投放的广度和力度、产品和解决方案的设计。受到企业资源生态和技术路线的较大影响。隐私计算目前的主要应用场景会落地在金融、医疗、政务和智慧城市、电商等行业，有些公司主打某一个行业，做得垂直深入，先树立一个行业内的稳固地位；而另一些公司则多覆盖几个行业，追求收入来源的多样化。

图9根据这些维度列举了国内的一些代表性玩家，主要包括以腾讯、百度、蚂蚁、字节跳动为代表的互联网大厂、金融机构代表微众银行以及光之树、翼方健数等创业公司。其中，不少玩家选择将底层技术框架开源，成为一个重要的战略选项（后文将继续讨论这个问题）。在落地行业上，绝大多数公司选择以金融为主，但也有翼方健数这样几乎专注于医疗行业应用的企业。

图9 | 国内隐私计算产业代表性玩家

公司	资源生态	核心产品	主要技术路线	开源与否	应用行业
微众银行	金融机构	FATE，WeDPR	联邦学习，区块链	是	金融为主
腾讯	互联网公司	腾讯安全联邦学习、神盾联邦学习平台，底层框架Angel PowerFL	联邦学习	底层框架开源	金融，政务
蚂蚁	阿里生态，互联网公司	蚂蚁摩斯	MPC+TEE，区块链	否	金融
百度	互联网公司	点石, MesaTEE，PaddleFL	联邦学习，MPC+TEE	逐步开源	政务，舆情
字节跳动	互联网公司	Fedlearner	联邦学习	是	电商、金融、教育
光之树	创业公司	天机可信计算框架，云间联邦学习平台	联邦学习，MPC+TEE	否	金融为主
翼方健数	创业公司	翼数坊	MPC等多种技术	否	医疗为主
富数科技	创业公司	Avatar, FMPC安全计算产品	联邦学习，MPC	否	金融，医疗
矩阵元	创业公司	Rosetta, PlatONE	区块链，MPC	是	金融
同盾科技	金融垂直行业公司	智邦iBond平台	MPC，联邦学习	否	金融

来源：金融科技微洞察&KPMG

4.3.隐私计算商业化的影响因素

从技术研究、产品开发、实际应用落地到最后商业化，隐私计算产业在走向成长的过程中面临着一系列问题和影响因素，制约了大范围推广和商业化进程。这些因素既有技术和产品方面的问题，也有政策和标准方面的缺失，还有产业本身固有的商业模式本质问题。具体来说，我们归纳了成功商业化的4方面难点。

技术和解决方案还不够完全成熟，与客户的需求有一定差距。

- **隐私计算的技术效率还有待进一步提升。**例如MPC和联邦学习技术都受制于网络传输的带宽、通信速率和网络稳定性，计算和建模效率尚不够令人满意；同态加密的计算有严重的性能瓶颈[1]。

- 由于计算效率和安全性等问题，**现有系统产品还比较复杂，工程化程度还不够完善，**会产生一定维护成本，但客户对复杂系统的维护费用支付意愿较弱，可是单纯售卖系统的毛利较低甚至不

[1] 中国信通院，阿里，数牍科技. 隐私保护计算技术研究报告.

足以覆盖成本。

- **现有的产品和技术还不足以支撑客户对一个完整解决方案的需求。**客户在实际业务场景中，往往需要的是一个业务问题的整体解决方案，如客户需要拉新促活的完整营销技术，而不仅仅是在隐私保护前提下带来新的数据。隐私计算可以作为方案中的一个模块，但要满足客户端到端的整体需求则有一定难度，因为有些需求并不是现有隐私计算技术能满足的，有些需求依赖于其他合作伙伴来共同满足——这又意味着复杂的协调合作问题。

- **隐私计算的模型可解释性还需提高，**但在金融风控和营销等领域，模型的可解释性、规则简单性是监管机构非常关注的问题，在AI业界也是一个发展重点，这就会给技术的应用带来较大障碍。

技术的安全可靠性有待提高，且目前缺乏可靠的技术标准认定，导致客户对采纳技术有疑虑。客观而言，隐私计算的技术效果和安全性仍然不够让人信服。TEE技术因为中心化可信程度和硬件的安全性、依赖性、内存容量等问题而饱受质疑[1]；联邦学习需要模型梯度传递，但梯度也有可能泄露一些信息；差分隐私的计算结果准确度有较大不确定性[2]。在这种情况下，国家缺乏明确的监管文件和技术标准认可隐私计算的安全可靠性。所以，很多客户都对如何证明技术的安全合理性有疑虑，只能在小范围内测试和监管沙箱内应用。去年央行出台了第一份隐私计算的金融行业标准——《多方安全计算金融应用技术规范》，还需要更多标准出台。

市场需求尚未充分展现，还缺乏明确的拉动性政策和标杆性示范项目。此外，很多行业的数字化程度低，制约了数据价值挖掘的需求。隐私计算是服务于数据的技术，为满足数据分享流通的需求而生也为解决该需求与隐私保护等监管规制的矛盾而生。但在前几年，技术的扩散主要依靠厂商自行推动，宏观环境上缺乏打开市场需求的助力。欧盟出台

[1] 参见https://zhuanlan.zhihu.com/p/149287280

[2] Wood, Alexandra, Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, et al. 2018. Differential Privacy: A Primer for a Non-Technical Audience. Vanderbilt Journal of Entertainment & Technology Law 21 (1): 209.

GDPR和国内的《个人信息安全规范》为这个市场揭幕，2020年国家出台《关于构建更加完善的要素市场化配置体制机制的意见》、《网络安全法》以及《个人信息安全法》（草案），才真正让产业界认识到数据的价值和隐私保护的必要性。但是，这些文件只是确认了隐私保护和数据安全的重要性，奠定了产业发展的大背景环境，尚缺乏政策、监管文件来明确鼓励采用或肯定技术的安全可靠性。除了政策缺乏，行业中虽然有已经落地的应用项目，但项目的示范意义尚不够放大，还缺乏非常具有代表性、能塑造行业认知的标杆性项目。由于很多客户是国有企业、商业银行、政府，有显著的风险规避性，在没有明确的政策拉动和示范项目引导下，技术的推广落地就有难度。不过，2020年以来越来越多的落地项目得到了关注和认同，有望改善这一现象。另外，诸多产业的数字化程度较低，数据管理不够成熟。除了金融、电信、电商等行业，我国许多产业的数字化程度较低，数据管理方式较为粗放，尚未建立成熟的数据管理体系，甚至连业务数据化都没做到。这些也制约了市场需求。

产业推广需要搭建多方协同的合作模式，这样的模式建立并不容易。与一般技术不同，隐私计算的商业模式天然需要多方协同，是一个基于数据生态、搭建基础设施的商业。技术服务商需要搭建起数据方和业务方联通的平台，有时候数据源甚至有多家，此时促成各方之间的合作，不论从技术还是商务上就变得很不容易。尤其对于资源不足的创业公司而言，这样的搭台合作更为困难。与之相似，作为隐私保护重要组成技术的区块链在商业化过程中也面临着同样的难点。这个特点决定了隐私计算的商业化是一个相对较为漫长的过程。

在这4个难点中，技术的安全可靠和效率是最根本的，有赖于技术服务商持续不断提升自己的技术和产品。只有这样，产业才能在政策窗口机会期打开的时候更好地起飞。技术和产品完善，有明确的政策引导，合作模式的搭建就可能会更加顺利。

5.百花齐放：隐私计算的应用案例

5.1.腾讯助力佛山顺德搭建普惠金融平台

2020年新冠疫情袭击之下，中小微企业遭遇现金流冲击。作为连续八年综合实力百强区，佛山市顺德区积极响应政府的号召，向市场发出英雄令，旨在寻找一个好的企业融资和贴息平台，能够打通政府、金融机构数据，为中小微企业提供平稳、合理的授信。顺德政府提到政务数据开放是大趋势，但核心的痛点是传统的联合建模方式无法满足数据安全的需求，金融机构和各委办局数据均存在壁垒，怎么发挥数据价值是头等难题。

腾讯作为中国领先的科技公司，一直在隐私计算领域进行深耕。为此，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。

顺德区政府普惠项目业务逻辑如图10所示，其中不同角色的任务分为：

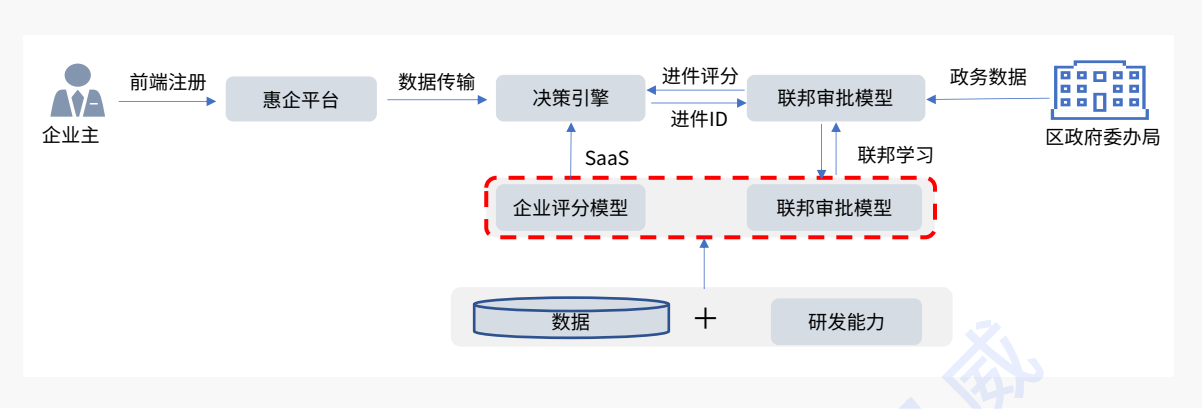
1)腾讯侧：提供联邦学习平台，融合顺德区的政务数据、申请企业数据、银行业务数据，建立实时进件分析和风险控制模型。

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。

在这个项目中，由腾讯提供的“腾讯安全联邦学习平台”起到了核心的建模作用，融合了顺德区政府各委办局的政务数据服务，帮助政府建立进件审核模型并输出。

图10 | 顺德普惠金融项目业务逻辑图



来源：腾讯云

截至2020年12月，顺德地区已经有7家金融机构通过该普惠金融平台发放小微企业贷款，共计433笔，总金额3.4亿，初步解决了顺德区中小微企业融资难题。

5.2.光之树助力大型卡机构赋能金融机构客户

某全国性银行卡清算机构主要负责建设和运营全国统一的银行卡跨行信息交换网络、提供银行卡跨行信息交换相关的专业化服务，拥有海量、丰富的优质银行业支付数据，数据维度多且粒度细。但是，在数据用途无法明确和监管的情况下，它难以开放数据，也缺乏安全输出数据的技术平台，导致它很难利用数据为金融机构做增值服务。

为此，光之树综合了“天机可信计算框架”和“云间联邦学习平台”两个产品，基于区块链架构，在卡机构和银行、证券、保险等各类金融机构之间搭建了隐私计算平台，帮助卡机构实现数据使用权变现和数据要素创新。

以银行客户营销场景为例，银行机构的数据维度较少，无法综合判断现有客户的资产价值，不利于挖掘高潜力客户，实施进一步精准营销。为此，该平台以联邦学习技术协助银行打通本行数据和卡机构能触达的丰富跨行消费数据，从而实现本行优质高潜力客户挖掘。本行数据包括客户在本行的资产、消费行为、平均投资额度、平均交易额度等，而卡机构能为它补充客户跨行消费行为、资金流动性数据等。双方通过联邦学习建模，得到了更优质高净值客户的画像。

图11 | 大型卡机构客户价值挖掘项目

来源：光之树

5.3.微众银行建立小微企业信贷风控模型

近年来，随着国家政策的支持，小微企业贷款越来越受到重视，已成为衡量银行发展潜力和能力的重要指标。由于风险过高，许多银行不愿给小微企业贷款，因此如何规避风险，降低微型企业贷款的不良率显得尤为重要。

目前，大多数银行都将白名单机制用于小微企业贷款的风险管理，而白名单是通过筛选规则和风险模型来实现的。不管是规则和风险模型，都需要依赖于对小微企业及其控制人的相关数据了解。对于风险管理来说，相关数据包括央行征信报告，税收，声誉，财务，无形资产以及企业交易数据等，维度丰富，但一家金融机构所能获取的数据往往有限。

为了解决小微企业贷款风控数据不足的问题，微众银行联合多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习系统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。

在进行纵向联邦建模之前，首先需要用隐私保护集合求交（PSI）技术找到微众银行与票据公司之间的公共用户，例如双方共同的纳税人识别号。使用基于RSA加密技术的PSI，票据公司可以通过传输加密的中间结果（而不是原始用户数据）来找

到双方的交集用户。然后双方进行建模，使用的联邦训练模型为纵向逻辑回归（Hetero-LR）。微众银行和发票信息服务公司利用各自的数据一起训练模型，使用加密的中间结果进行交互，并且各自维护属于自身的模型。当需要预测的时候，再结合两边的模型共同预测。整个模型训练的过程保证了数据和模型的安全性。

与只使用传统模型来训练标签Y相比，联合了发票数据的纵向逻辑回归模型AUC增加了12%。随着模型效果的改善，贷款不良率明显下降。

5.4.翼方健数提升厦门智慧分级诊疗能力

我国医疗资源总量不足，优质资源匮乏，分布也不够合理，分级诊疗是重要的解决方案。自分级诊疗推行已来，国家做了很多提高基层社区医生诊疗水平的举措，比如请三甲医院的医生下基层医院坐诊，到边远地区支边，让基层医院医生到厦门附属医院进修，起到了一定的效果。但是这些举措都有一个共同的局限——社区医院的医生无法得到长期地、持续性地指导。为此，基层医生们需要一套系统，将三甲医院医生积累的丰富临床经验转化为智能化的知识输出，辅助诊断。但是，医疗人工智能依赖高数量和高质量的医疗数据，由于医疗行业对于数据安全、医学伦理和个人隐私方面的担心，数据获取、数据治理和数据合理应用一直是医疗AI行业的一个痛点。

图12 | 病历结构化应用开发流程

来源：翼方健数

为了解决隐私保护问题，翼方健数基于隐私安全计算技术平台“翼数坊”（XDP），在厦门市卫健委的主导下，汇聚厦门市各医疗机构的健康医疗数据，并引入第三方服务机构来处理和挖掘原始数据，提供应用服务。该平台首先在全市基层社区医院儿科诊疗过程中落地应用，通过学习海量的儿科电子病历（如图11），开发了病历结构化、辅助诊断、辅助用药，辅助检查推荐等一系列深度学习模型，通过打通智能模型、电子病历EMR与其他信息系统，形成了一套智能临床辅助决策系统和知识库体系，辅助基层医生全面观察患者的症状和体征，完成高质量的病历书写，并在此基础上为基层医院的医生提供检验检查、疾病诊断、用药等推荐。系统还可以实现通过模型智能识别危重病和传染病风险，提示基层医生通过厦门市卫健委主导的双向转诊平台对于患者进行转诊，为转诊病患给予相对高的优先级，保证社区医院的潜在风险病人能够得到及时的医治。

系统于2019年3月开始在厦门市思明区的中华、莲前社区医院2家试点，于2019年5月中下旬在思明区的9家社区医院正式上线，并于2020年3月在厦门全市39个社区全面上线。该产品作为厦门市儿科智能分级诊疗系统的AI应用，在产品上线后，使用率快速增长，屡获殊荣，联合厦门市第一医院，获得国家卫健委的医疗健康人工智能应用落地优秀案例大奖。

6.路在何方：未来发展路径的思考

作为一个新兴细分领域，隐私计算尚处于推广初期。不少从业者认为，直到刚刚过去的2020年，这个领域才真正在数据要素政策确立的大背景下开始启动。在这行业萌兴的时刻，各个玩家都在“摸着石头过河”，在市场的洪流中摸索正确的方向和策略打法。不论是关于市场格局、战略打法还是技术路线，每一个问题都可能有两个可能的答案。究竟哪一种答案才是有说服力的，哪一条道路才是正确的，只有留待时间来揭晓。本报告只能提出问题，竖起靶子，呈现当下人们的猜想及其理由。

6.1.市场格局

(一)什么类型的玩家更可能领先?

如上文所述，隐私计算领域内既有创业公司玩家，也有不少互联网大厂和金融机构下场。那么，什么类型的玩家更有可能领先甚至胜出?为分析这个事情，离不开一个重要问题——在这个行业里，什么是重要甚至核心的竞争力?

在底层算法原理公开甚至有现成开源框架参考的情况下，技术的壁垒并不高，每一家主要的技术服务商都有一定的技术实力和特色。对于玩家——尤其是创业公司而言，一定不能仅仅凭借单点的技术优势来竞争，否则在技术快速进步和产业竞争环境的快速变化下，很可能被上下游所挤压整合。决定竞争关键的因素，更可能是两点。一是完备的产品工程化能力，即做出易用、功能完善、可靠的产品。但这一点是

任何行业都需要的核心能力，**真正跟隐私计算领域关系密切的能力是第二点——为客户提供完整解决方案的能力，而解决方案的核心就在于找到合适的数据源。**

因为隐私计算本质上是属于大数据领域的生意，为了解决客户的数据需求而生。**对于客户而言，技术服务商能否提供合适的数据，从而解决客户的业务问题，在一定程度上要比提供合适的产品和技术更为重要。**所以，如果技术服务商有丰富的、特有的数据资源，能为不同客户带来所需的数据，就会有较强的市场竞争力。由此来分析，市场上各类玩家的各自竞争优势就较为明显。

互联网大厂体系玩家的主要优势是丰富的数据生态和应用组件。来自于腾讯、阿里、百度、字节跳动等互联网公司的玩家天然就有渠道调用公司生态中丰富的数据，并具有多样化应用场景的组件，有助于为客户组装一套完整的解决方案。例如腾讯云联邦学习团队不仅能凭借自有的黑产数据，为客户提供更强的反欺诈能力，还能将隐私计算产品与其他产品打包成一个完整的解决方案，更好地满足客户端到端的业务需求。百度“点石”大数据平台能开放自身丰富的舆情数据及在舆情分析方面积累的深厚能力，为政府、媒体、企业等客户带来价值。

但是，值得注意的是，大厂玩家所固有的数据优势也并非绝对优势。随着隐私保护相关法律法规出台和广大用户对于个人数据保护的认知逐渐树立，有些积累的数据并不能被任意使用，拥有数据并不一定必然会转化为拥有胜势。必须首先满足数据的合规性，才能进一步使用数据。

产业背景公司的主要优势是垂直行业的专注积淀和应用能力。来自于垂直行业的玩家相比于互联网大厂更为聚焦，具有本行业领域内的丰富数据、对客户业务的深入理解、扎实的应用服务能力积淀。既有数据、又有技术能力、还懂业务，能为客户提供从售前咨询、体系架构到产品供给和运营辅助的端到端解决方案。这些构筑了公司的竞争优势。

隐私计算创业公司的主要优势是中立性和贴近客户的服务能力。虽然创业公司自身没有天然的数据生态优势和完善的应用组件，但具备2个特别的优势。

- **中立性。**来自于互联网大厂的团队不可避免地会被客户打上公司烙印，有些客户就对此有介意。例如有一些国有企业就较为介意大厂团队为它们搭建隐私计算系统，担心大厂是否会拿走它们的客户数据；有些公司更不可能采用竞争对手资本派系团队的产品。这时候创业公司凭借中

立性就更容易得到客户的信任。

- **贴近客户的服务能力。**现阶段为客户提供隐私计算服务，需要根据实际问题场景做较多定制化的解决方案，且伴有不少维护和驻场工作。互联网公司的人力成本较高，不适合提供较多人力服务。创业公司在这方面的包袱较轻，能为客户提供更全面的服务。

除了以上两个特别优势之外，有些创业公司凭借创始团队的资源，也可以像产业背景公司一样，通过专注于某一垂直行业来获得竞争优势。

由以上分析可见，每一种玩家都有独特的优势，重要的是根据自身的优势，制定合适的战略打法，扬长避短，就有可能在某些垂直行业、某些特定场景上实现领先。

更重要的是，**目前的发展阶段是做大蛋糕、争取存量的时候，各方之间的合作大于竞争，**需要领先玩家来教育市场、争取政策制定者认可、推动标准和相关政策制定，才是整个行业的福音。

6.2.战略打法

(二)主打行业是否要聚焦？

隐私计算目前主要应用于金融、政务、医疗等行业。有些玩家会侧重在某一行业，例如翼方健数以医疗为主打行业；而另一些玩家的范围更广，如富数科技、字节跳动涉及多个行业。对于资源有限的非大厂出身公司而言，一个重要的问题就是是否要聚焦于某些主打行业。

在资源有限的情况下，先聚焦于某一垂直行业，稳扎稳打，可能是一个更好的选项。第一，正如3.3节所述，在每一个垂直行业内，链接多方数据源、打通数据提供方和业务方，并不是一件容易的事，往往要依赖于创始团队或企业本身所拥有的资源来攒局。攒好一个行业的局就需要耗费相当大的功夫。第二，一个垂直行业的做深做透，同样需要持续不断的积淀，形成满足该行业内多样化场景的解决方案，形成可靠的工程化产品。然后才能有标准化的产品复制，从而降低边际成本，增加销售毛利，形成可持续的商业模式。由此可见，在资源有限的情况下，铺张资源到多个行业，既无必要，也不现实。

(三)隐私计算会走出什么样的平台商业模式？

4.1节介绍了目前隐私计算的四种营收模式。在销售系统的营收毛利较低的情况下，基于运营效果的分润模式更受到从业机构的看好。运营分润模式的基础既可能是单一客户的一套解决方案，例如为某保险公司提供基于隐私计算的产品定价方案；也可能是一个由多客户、多数据源构成的平台。平台模式，正是不少从业机构及背后投资方看好隐私计算赛道的一个重要理由，被认为是隐私计算

的终极商业模式[1]。为此，我们需要渐进地讨论几个问题：这个行业是否可能跑通平台模式？会涌现出什么样的平台？谁更可能做出这样平台？

隐私计算领域的应用有可能形成平台模式。作为一种商业模式，平台形成的基本条件是：(1) 某一资源的供需两端有分散的、多样化的参与者，(2) 这些参与者之间直接联系的成本较高——不论是初次联系成本还是持续联系成本。这样平台才会有联系两端的、可持续的存在价值[2]。

- 关于条件 (1)：隐私计算领域的资源是数据，在任何一个场景里，一头连接着分散的各种各样数据提供方，另一头是应用数据的业务方。尽管目前很多项目里，业务方是个单一机构，例如为某银行搭建风控系统，为保险公司和医院搭建病例数据系统，但理论上只要市场上存在着许多相同需求的业务方——例如风控场景是众多金融机构的刚需，将项目扩大成一个数据流通网络，就完全有可能。

- 关于条件 (2)：业务方和数据方之间的初次联系成本较高，需要隐私计算服务商为业务方找到合适的数据，为数据方找到有用的客户。除了初次联系，隐私保护法律法规的限制天然地给供需两端的持续联系树立了屏障，必须要通过隐私计算技术解决数据应用问题，持续联系成本较高。

隐私计算的应用平台很可能扎根于垂直行业，但技术平台有可能跨行业。隐私计算很有可能在应用层上走通平台商业模式。除了应用平台，技术平台也是一种可能性。区别在于应用平台扎根于垂直行业，技术平台可能有通用性。

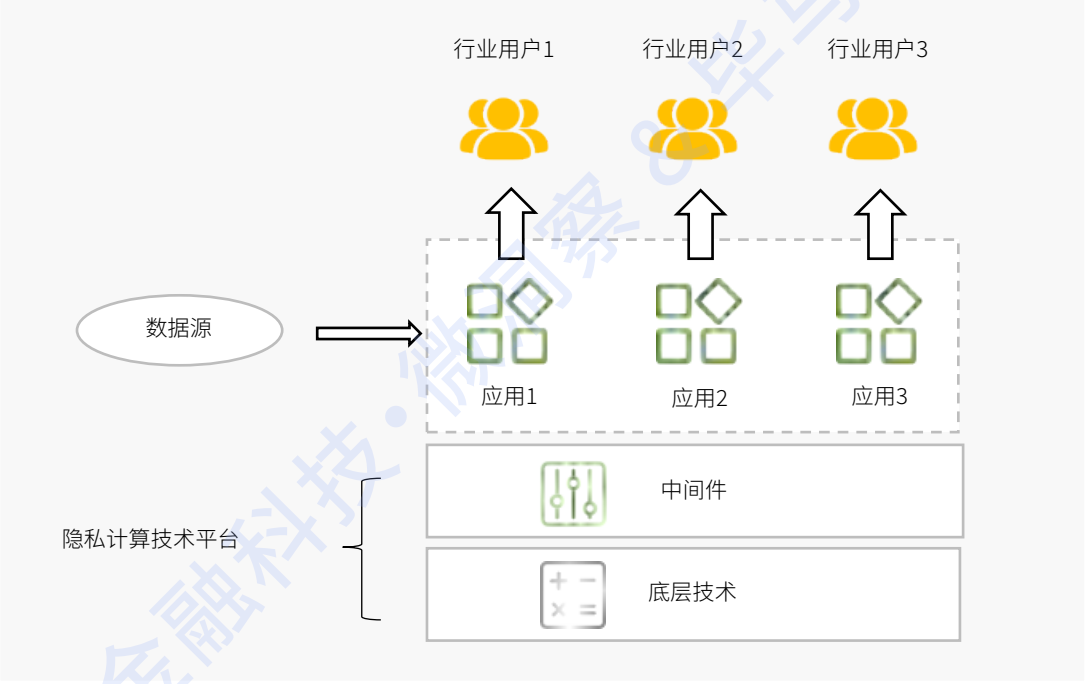
- **应用平台将基于垂直行业。**不论是金融、医疗、政务还是电商等，每个行业、每个场景所需要的数据大相径庭，客户特点和需求也相差很大。一旦跨行业，平台资源需求很难呈现标准化的形式，技术服务商的应用层产品不大可能跨行业通用，就很难在单一平台上以低边际成本去高效匹配资源供需。而且，不同行业的数据差异大，导致很难在一个应用平台实现跨行业、大一统的数据集。

[1] 见36氪报道 https://www.36kr.com/p/801141060510982

[2] 陈威如. 2013. 平台战略. 中信出版社. 另见《财经》杂志对美团高级副总裁张川的专访 https://news.caijingmobile.com/article/detail/402650?source_id=40&share_from=moments&from=timeline&isappinstalled=0

- **技术平台有可能呈现跨行业的通用性。**与应用层要面临各个行业的复杂需求不同，但在隐私计算的底层技术上具有一定通用性，不论是联邦学习、机器学习、统计算法，还是秘密共享、不经意传输、差分隐私等算子，都有可能成为一套隐私计算技术平台的标配。在中间件层面上，技术服务商再搭配起完备的数据管理、任务调度管理、身份权限管理、可视化界面、集群管理等组件，将这些能力开放出去给众多应用开发者，从而服务不同行业终端客户需求（见图12）。此时，如上文所述，由于各个行业的数据大不一样，只能让垂直行业应用开发商去接入数据，那么平台本身供给的交易资源不再是数据，而是技术。

图12｜技术平台架构设想



来源：金融科技微洞察&KPMG

不过，**走技术平台的难点在于，如何吸引应用开发商和客户？**在行业中，各个玩家还是习惯于自己搭建从底层技术到上层应用的整套体系，掌握了数据和客户才是真正具有主导权。如果只定位于技术平台，这样的商业模式是否能真正走通、或空间多大，仍须存疑。

大厂玩家和创业公司做应用平台的优势各不一样。打个比方，这是围棋中“金角”和“草肚皮”的区别。大厂玩家的优势还是在于天然地占据了一类场景和相关的丰富数据源，是“金角”，好处是启动成本较低，

护城河深，跟外面合作谈判的筹码也较多，甚至自身就可以满足平台所需的相当多数据需求和应用能力。与之相比，创业公司的中立性优势再一次在搭建应用平台时得以显现。搭建平台的一个重要基础是融合多方数据，对接多方客户。大厂占据了一方场景，也意味着丢掉了数据融合和场景扩展的中立性，这给占据“草肚皮”的创业公司带来了机会。虽然它们合纵连横的成本较高，守天下也难，但延展性大。事实上，不少学术研究也表明，在组建平台时，中立方的难度要小于产业中的既有大玩家[1]。

[1] Kretschmer, Tobias, Melissa Schilling, Aija Leiponen, and Gurneeta Vasudeva. 2020. “Platform Ecosystems as Metaorganizations.” Strategic Management Journal.

(四)隐私计算能否走通订阅服务模式?

上一节商业模式的讨论前提是销售模式毛利较低、标准化程度还不够，所以才需要平台运营模式来支持隐私计算技术服务商的长期收益。但事实上也存在着另一种可能，即隐私计算变成一种标准化的、订阅制计算服务，通过公有云端提供SaaS或PaaS性质的服务，或集成到应用开发商的解决方案里。那么这种情况是否可能，会存在什么样的困难?

目前的障碍一是标准化程度太低，二是客户不愿意系统部署在公有云上。前一个问题随着产业的发展应该能消除，后一个问题是我国云计算和大数据产业的系统性状况，也不是隐私计算服务商能独立解决的。不过，如果这两个障碍不存在，等到技术和场景需求标准化到了一定程度后，隐私计算技术服务商可以将自身技术嵌入到应用集成商或SaaS服务商的解决方案里，或者自己做SaaS形式的标准应用放到公有云上。不过，下一个问题在于，如何跟公有云和集成商协调利益问题，尤其是公有云服务商?

这个问题对于互联网大厂背景的技术服务商并不存在，但对于非云服务商背景的中立从业机构而言，放在公有云上提供服务的最大担忧是利益冲突，因为大型的云服务商如阿里云、腾讯云、AWS等通常有自己的隐私计算产品。不过，至少在中短期内，这样的担忧并不大可能转化为事实，原因有两点：

第一，中立技术服务商是公有云服务商的重要渠道生态伙伴和客户。单个公有云服务商的能力有限，只要它想服务更多行业、更多场景的客户，就需要接入更多数据、集成行业内的应用能力，那么它就需要在垂直行业内做得较好的创业公司，来吸收更多的终端用户。而且，此时中立技术服务商本身也是公有云的客户，使用云上的PaaS和IaaS服务。

第二，中立性便于客户采用云上的隐私计算应用，加快行业发展。首先，它最大程度减少了客户将系统部署在云上的不信任感，有助于未来隐私计算系统部署上云。其次，很多客户本身就采用了多云基础架构，那么数据跨云在一个中立性隐私计算平台上运行，相对而言会更方便，互联互通性更佳。

事实上，去年美国数据仓库供应商Snowflake被业界看好的原因也在于此，尽管AWS和微软等云厂商都有自己的数据仓库，但Snowflake凭借它的中立性、跨云功能，仍然得到了客户和投资者的认可。隐私计算就是一种类似于Snowflake的“数据即服务”（Data-as-a-Service）的特殊服务。由此可见，只要行业需求的成熟度、数据和产品的标准化程度得以提高，以政府和大型企业为代表的客户逐渐愿意接受系统上公有云而非本地部署，那么隐私计算应用部署在云端，以订阅服务模式收费，是很有可能性的。

6.3.技术发展

(五)开源底层技术框架是否会成为主导？

技术是产品的根本，底层技术的好坏在很大程度上影响了产品性能和功能。当前隐私计算行业内，大部分玩家采用了闭源的底层技术框架，但也有少部分玩家如微众银行、腾讯、字节跳动开源了底层框架，贡献了如FATE这样业内领先的工业级联邦学习框架。那么，在探讨企业的发展时，技术层面就有一个重要问题：底层技术框架是否要开源，开源框架是不是可能成为主导的框架？这个问题可以分解为两个小问题：第一，未来是不是会有主导框架？第二，对于企业而言，底层框架开源的意义是什么？

未来很难有1-2个垄断的技术框架，但主流框架数量也不会多，更像是“寡头竞争”的局面。

- 新兴行业的技术路线通常会经历从百花齐放到逐步收敛的过程，技术框架也有一类类似过程。比如云原生主流框架收敛到K8S，TensorFlow成为深度学习的主导框架。在隐私计算行业，技术路线和底层框架也会有收敛的过程。

- 但是，由于客户的迁移成本较高，平台框架的收敛程度有限。首先，在许多服务B端的科技行业，底层技术框架很难像C端产品一样容易迁移，因为系统麻烦、B端客户决策流程冗长。所以在行业发展初期，市场群雄割据，接入客户合作之后，由于更换技术平台的成本高，客户通常不愿意换。更重要的是，隐私计算本质上一个比拼数据生态的行业，技术和产品只是载体，所以技术平台搭建不是孤立的产品售卖，实际上

附带着数据合作，换了系统就意味着要更换数据。这更增加了迁移成本。因为这两条迁移成本，市场经过一段时间的跑马圈地和技术收敛演化之后，会形成若干家寡头竞争式的主流框架，但很难进一步收敛出1-2个主导垄断的框架。

尽管开源框架不会成为主导框架，但很可能成为行业内的主流框架，有助于玩家在市场上领先。在开源软件席卷IT界的今天，除了有助于技术的持续迭代，人们已经充分认识到开源技术框架还有着重要的商业意义：

- 以透明、安全、可控的特性教育市场，增加市场对于隐私计算产品的接受度。在数据成为重要资产的今天，各个机构都高度重视数据资产的保护。尽管隐私计算声称能保护数据，“可用不可见”，但涉及到数据机密，参与各方若要完全信任计算系统，代码开源是最好的获得信任的方法。开源框架为基础的产品更容易被各方接受。特别是在安全可控成为我国当前信息技术创新主旋律的背景下，代码透明的信任更加重要。

- 推广技术，让更多的人开发出更好的框架和产品，从而做大整个产业。成熟的开源框架会被业界广泛接受，让更多从业者用来开发产品或改善框架，从而产生更多更好的隐私计算产品，利好整个产业。在此过程中，开源框架的话语权和地位就会越来越强，自然有利于以此为基础的产品。

当然，各家公司有自己的财务情况和策略打法，并不一定都需要自研或采用开源框架。闭源仍然是IT界的主流商业模式，毕竟开源产品的盈利难度更大一些。如果没有同一公司内其他产品的交叉补贴，单纯依靠开源产品来盈利的周期会更长。

(六)隐私计算与区块链、边缘计算等其他技术的结合点是什么？

将区块链技术与隐私计算相结合，共同作为数据要素流通分享的新型基础设施，已经成为隐私计算业内玩家的共识。在区块链实际应用中，交易、存证等业务流程也必须基于隐私保护的前提，相关厂商必须保证区块链产品中有足够的隐私保护能力。微众银行、蚂蚁、光之树等都将区块链纳入

隐私计算解决方案之中，作为重要的产品模块。目前业内也正在制定多项区块链和隐私计算结合的行业和团体标准[1]。可以预见，区块链技术能力将有助于玩家领先，形成更完备的解决方案，原因在于：

区块链和隐私计算的商业模式组织是同构的，都体现了分布式体系的商业模式理念[2]。隐私计算需要三类参与方，每一类参与方还可能包含多个实体机构，所以是一个多方参与的网络组织。区块链则是为多方协同生产而存在，完全有能力作为隐私计算业务的基础IT架构，让各方都作为节点接入。

在这样的分布式架构之上，区块链提供了新的功能，与经典隐私计算形成互补的技术体系。之所以需要利用区块链来提供基础IT架构，是因为区块链提供了一系列经典隐私计算技术所没有的功能。隐私计算解决的是计算过程可信的问题，但不能确保数据本身是可信的，也不能记录历史上的数据调用和计算结果。区块链根据账本的不可篡改性解决了数据来源可信、计算结果追溯和验证问题，数据调用和计算结果的记录还有助于根据数据价值进行报酬分配，有助于建立隐私计算的良好激励机制。

隐私计算与边缘计算在中长期内也有较大的结合应用空间。目前隐私计算的数据来自于机构服务器，模型训练和推理应用发生在服务器上。但事实上，基于边缘端、终端设备的数据进行联合建模应用，也有很大市场。比如在装备制造业、安防等行业，人们可利用联邦学习训练分散的数据，形成计算机视觉模型，用来检测行人、设备、火焰烟雾等。微众银行探索过一个智慧安防案例。不同工厂的监控数据分散在不同本地设备上，要使用视频智能监控工人是否吸烟、是否戴安全帽等，但数据不能流出本地或本工厂，而且工人面孔和行为是个人隐私，因此要将联邦学习与边缘计算结合，在工厂边缘端训练模型[3]。未来随着手机芯片、5G通信等技术的改进，降低计算和通信成本，隐私计算SDK可能被集成在App里，让个人手机也能分享自己的数据，参与隐私计算。

[1] 如“中国区块链技术和产业发展论坛”的团体标准《区块链隐私计算服务指南》

[2] 马智涛 等. 2020. 分布式商业. 北京: 中信出版社.

7.政策建议

作为解决数据价值流通分享问题的重要技术，隐私计算正处于产业快速导入期，形势大好，但也面临着一系列产业发展环境的制约。为了解决制约问题，需要监管机构和各个政府部门从数据法规、技术标准、示范项目等方面入手，完善相关政策。业界应不断推进政策的完善和升级，促进隐私计算技术与实体经济深度融合，加快培育数据要素市场，落实国家大数据产业发展规划中的关键任务。

第一，健全完善数据流通和分享的政策监管体系，奠定隐私计算产业的合法性框架。当前国内已经出台或正在制定个人信息安全、网络安全等方面的法律，金融等行业也颁布了本行业的数据保护监管规则和标准，为隐私计算建立了必要性基础。但目前还缺乏进一步支持数据规范流通和隐私计算应用的政策，在较大程度上阻碍了较为保守的大型客户贡献分享数据贡献，从而影响了技术的推广。建议未来进一步出台鼓励数据流通分享和支持隐私计算行业发展的相关政策，明确该类技术在大数据行业内的意义和作用，鼓励使用隐私计算技术。

第二，逐步建立隐私计算技术和应用标准和产品认证体系，促进行业规范发展。目前除了央行发布的金融业安全多方计算规范和工信部下属若干研究院牵头团体所发布的团体标准外，隐私计算的技术和应用标准还有大片空白，都有很多问题需要明确。在产品认证工作上，国内也缺乏较为权威规范的认证机构，只有个别市场机构开展了一定认证业务，但权威性和收费合理性都有待商榷。标准制定和认证体系能为行业树立技术发展和应用的标尺，也有助于客户选择合适的技术服务商，最大程度减少客户采纳隐私计算的忧虑。

第三，通过一系列高标准示范应用项目，为市场形成示范，更好地认识到隐私计算的作用，理解

隐私计算与区块链等其他技术融合的效果，也有助于发现实际问题。示范推广对于新技术发展具有非常重要的意义，往往是新技术能否成功越过导入期、步入快速发展期的关键。目前市场上还缺乏标杆性、能塑造行业和市场认知的重要应用项目。建议政府选择一批数据信息流通分享有关的重要数字新基建、智能金融、智慧城市和医疗健康等项目——例如跨境信息共享、信贷联合风控等，推动隐私计算技术及区块链技术在这些项目中的应用，总结和宣传使用效果和经验教训，为技术的下一步大规模推广打好坚实基础。

金融科技·微洞察

“金融科技·微洞察”是微众银行运营的金融科技研究品牌，聚焦国内外金融科技领域的技术发展、标准制定及产业应用，把握当下金融科技热点话题与政策动向，洞察未来领先的金融形态和商业模式。

微众银行作为国内首家互联网银行，自2014年成立之初即将“科技、普惠、连接”作为银行的三大发展愿景，将积极运用科技创新探索普惠金融新模式、新业态作为银行重要的发展方向，致力于为普罗大众、微小企业提供差异化、有特色、优质便捷的金融服务。自立行至今，微众银行在金融科技“ABCD”（人工智能、区块链、云计算、大数据）等四大领域积极探索，2017年即已成为国内首家获评“国家级高新技术企业”的商业银行，截至2020年末共申请国家及国际专利数超过2300余件，拥有自身所有重要业务和技术系统的知识产权，有效实现了银行业信息化安全可控的战略目标。

毕马威

毕马威是一个由独立的专业成员所组成的全球性组织。成员所遍布全球146个国家及地区，在2020财年拥有接近227,000名专业人员，提供审计、税务和咨询等专业服务。毕马威中国在二十五个城市设有二十八家办事机构，合伙人及员工约12,000名。在IDC 2019年“亚太区数字转型咨询和系统集成服务供应商”评估报告 中，毕马威被评价为数字转型咨询和系统集成服务的领导者。毕马威深耕中国金融业多年，非常幸运地参与中 国银行业变革和里程碑事件，与业内同仁在每一次的变革浪潮中共同奋楫前行。毕马威认为，未来银行是银行 业把握科技变革对商业社会重塑的奇点性机遇，以此重新认知和构建银行的生态和企业价值链，重塑银行与社 会和客户的链接。毕马威面向银行业客户，提供数字化银行、开放银行战略，金融科技生态与智慧风控、智慧财 务、智能租赁、智能合规等未来银行的全方位解决方案。将会携手银行共同把握未来银行的机遇，通过客户洞察、产品与服务、渠道交互、运营流程等进行智能化改造，从而实现对未来银行的全方位赋能。

免责声明

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，本报告所载的资料、工具、意见及推测只作参考之用，并非作为或被视为出售或购买证券或其他投资标的邀请或向人作出邀请。在任何情况下，报告的编著机构不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

所载资料仅供一般参考用，并非针对任何个人或团体的个别情况而提供。虽然我们已致力提供准确和及时的资料，但我们不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

联合出品

WeBank 微众银行 | 金融科技 微洞察

KPMG 毕马威

报告出品人

姚辉亚　赫荣科　陈天健

报告作者

徐 磊　魏思远　葛 娴　马千里

鸣谢

范 涛　郝玉琨　黄 勇　李 文　刘站奇　田 娜　魏 征　武姗姗　张莺耀

（以上人士按姓氏拼音排序）

美术编辑

邓少雁

联络邮箱

weinsights@webank.com

金融科技·微洞察

毕马威KPMG