计算机

2021 年 08 月 09 日

隐私计算，千亿蓝海市场加速开启

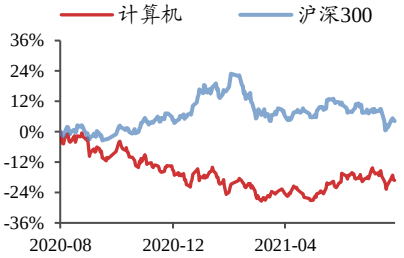
——行业深度报告

陈宝健（分析师）
chenbaojian@kysec.cn
证书编号：S0790520080001

刘逍遥（分析师）
liuxiaoyao@kysec.cn
证书编号：S0790520090001

投资评级：看好（维持）

行业走势图



数据来源：贝格数据

相关研究报告

《行业周报-周观点：全民健身计划发布，关注教育信息化投资机会》-2021.8.8

《行业周报-周观点：解决“卡脖子”难题，高度重视工业软件产业趋势》-2021.8.1

《行业周报-周观点：教育“双减”新政落地，高度利好教育信息化产业》-2021.7.25

● 高度看好隐私计算蓝海市场，重点推荐安恒信息、奇安信等

伴随着数据要素市场改革加速，隐私计算技术成为数据价值安全释放的关键突破口，有望在金融、政务、医疗等行业实现快速应用，其千亿蓝海市场有望开启。重点推荐在隐私计算/数据安全领域有前瞻布局的公司安恒信息、奇安信、深信服、绿盟科技、美亚柏科、启明星辰，其他受益标的包括卫士通等。

● 数据要素市场改革加速，催生广阔的隐私计算新兴市场

一方面，2020 年出台的《关于构建更加完善的要素市场化配置体制机制的意见》，为推进数据要素市场化改革指明了方向，此后，深圳、北京、广东等地相继发文，规划设立交易场所进行大数据交易。另一方面，《数据安全法》将于 2021 年 9 月 1 日正式实施，《数据安全法》将与《网络安全法》及正在立法进程中的《个人信息保护法》一起，为保护数据资源安全提供了法律依据。隐私计算技术是解决数据开放安全问题的重要突破口，在隐私计算框架下，参与方的数据不出本地，在保护数据安全的同时实现多源数据跨域合作，可以破解数据保护与融合应用难题。根据 Gartner 数据，到 2024 年，隐私驱动的数据保护和合规技术支出将在全球突破 150 亿美元以上，即达到千亿人民币以上。

● 隐私计算三大技术路径：联邦学习、安全多方计算、可信计算

常见的实现隐私计算的技术路径包括联邦学习、安全多方计算、可信计算等，此外区块链也是隐私计算的重要补充。由于技术路径的不同，各类隐私计算技术均有其更加适用的场景：多方安全计算技术不依赖硬件且具备较高的安全性，但是仅支持一些相对简单的运算逻辑；可信执行环境技术具备更好的性能和算法适用性，但是对硬件有一定依赖；联邦学习技术则可以解决复杂的算法建模问题，但是性能存在一定瓶颈。

● 行业应用快速推广，创新企业不断涌入，隐私计算进入蓬勃发展阶段

隐私计算的技术和产品成熟度迅速提升，同时在我国加快培育发展数据要素市场、数据安全流通需求快速迸发的推动下，隐私计算技术有望在金融、政务、医疗等行业实现快速应用。

参与方：目前蚂蚁金服、腾讯云、百度、京东等互联网企业推出了各自的产品，同时微众银行、安恒信息等行业性公司也开始布局，此外，华控清交、富数科技、矩阵元、数牍科技、锘崴科技、光之树科技、零知识科技等一批专注于隐私计算产品化的初创企业也不断涌现。

商业模式：隐私计算的商业模式尚处于探索过程中，我们预计在发展早期主要以系统销售模式和服务模式为主，未来调用模式和分润模式将打开更大的市场空间。KPMG 预测，隐私计算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，甚至撬动千亿级的数据平台运营收入空间。

● 风险提示： 市场竞争加剧风险；技术变革风险；人员流失风险。

目 录

图表目录

1、 隐私计算技术将成数据价值安全释放的关键突破口

数据要素市场改革正在加速。2015 年开始，大数据上升为国家发展战略，全国各地相继成立大数据交易所，各个大数据交易平台网站也陆续上线，但由于缺乏相关的行业规范和安全保障，这些数据交易平台并没有发挥最大效用。2020 年出台的《关于构建更加完善的要素市场化配置体制机制的意见》，为推进数据要素市场化改革指明了方向。此后，深圳、北京、广东等地相继发文，规划设立交易场所进行大数据交易。

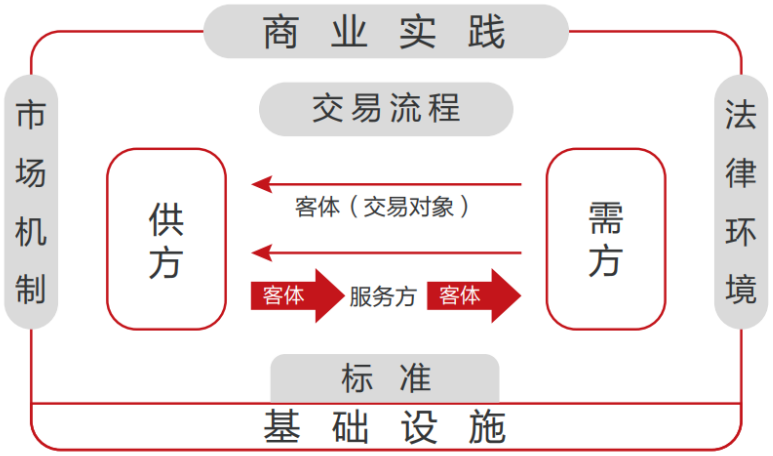
表1：深圳、北京、广东等地相继发文，规划设立交易场所进行大数据交易

时间	文件	内容
2020 年 8 月	-	北部湾大数据交易中心在南宁揭牌成立，**北部湾大数据交易中心将积极探索政务数据交易模式和跨境数据流通机制，构建安全、开放、共赢的数据生态，建成数据产品交易额、交易量、交易品类中国-东盟区域领先、7×24 小时永不休市的数据产品交易服务机构**
2020 年 9 月	《北京国际大数据交易所设立工作实施方案》	北数所具备五大功能定位：一是权威的数据信息登记平台；二是受到市场广泛认可的数据交易平台；三是覆盖全链条的数据运营管理服务平台；四是以数据为核心的金融创新服务平台；五是新技术驱动的数据金融科技平台
2020 年 10 月	《深圳建设中国特色社会主义先行示范区综合改革试点实施方案（2020－2025 年）》	率先完善数据产权制度，探索数据产权保护和利用新机制，建立数据隐私保护制度。试点推进政府数据开放共享。**支持建设粤港澳大湾区数据平台，研究论证设立数据交易市场或依托现有交易场所开展数据交易，开展数据生产要素统计核算试点**
2021 年 7 月	《广东省数据要素市场化配置改革行动方案》	广东将加快数据交易场所及配套机构建设，推动建设省数据交易场所，搭建数据交易平台，提供数据交易、结算、交付、安全保障等综合配套服务

资料来源：各政府网站、开源证券研究所

数据要素市场改革推动了数据产业的商业模式创新。据《数据交易的商业模式》研究报告，数据交易商业模式的框架主要由“3+4+1”要素构成。其中，3 表示“数据交易的环境”、“数据交易的基础设施”、“法律环境和市场机制”，4 表示“主体”、“客体”、“流程”和“标准”，1 表示“数据交易的商业实践”。经过多年探索和实践，当前市场存在直接交易模式、授权转移模式、数据市场模式、一般数据平台模式、具备授权和问责制数据平台模式、数据银行模式和数据信托模式 7 种数据交易商业模式。

图1：数据交易商业模式的框架主要由“3+4+1”要素构成



资料来源：《数据交易的商业模式》

数据产业商业模式创新对数据安全提出新需求。要进行数据交易要着力破解制约要素市场化的主要矛盾，如数据开放共享和安全保护、数据确权、隐私安全等瓶颈制约，隐私计算技术是解决数据开放安全问题的重要突破口。**隐私计算能够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。在隐私计算框架下，参与方的数据不出本地，在保护数据安全的同时实现多源数据跨域合作，可以破解数据保护与融合应用难题。**

图2：隐私计算解决数据开放安全问题的重要突破口

资料来源：KPMG

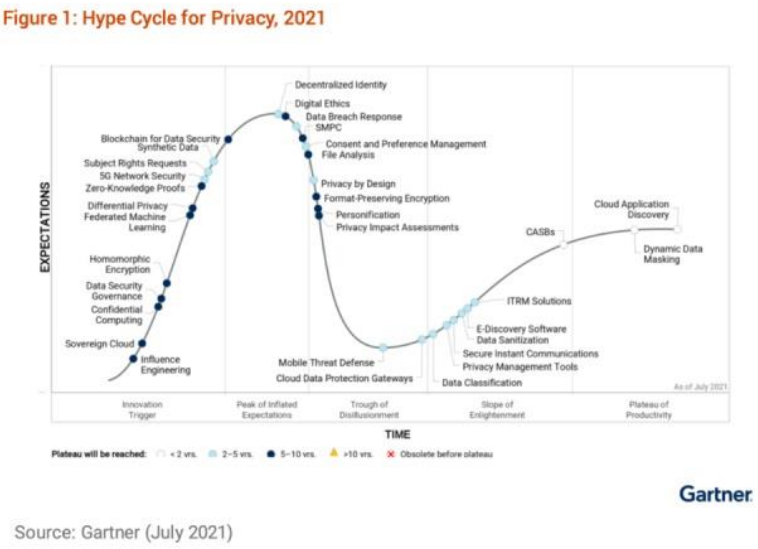
2020 年 11 月，Gartner 发布了企业机构在 2021 年需要深挖的重要战略科技趋势，其中就包括隐私增强计算。并提出：随着全球数据保护法规的成熟，各地区首席信息官所面临的隐私和违规风险超过了以往任何时候。不同于常见的静态数据安全控制，隐私增强计算可在确保保密性或隐私的同时，保护正在使用的数据。

图3：Gartner 发布了企业机构在 2021 年需要深挖的重要战略科技趋势

资料来源：Gartner

2021 年 7 月，Gartner 发布隐私计算的技术成熟度曲线-2021 版本。Gartner 指出：在 2023 年底之前，全球 80%以上的公司将面临至少一项以隐私为重点的数据保护法规。到 2024 年，隐私驱动的数据保护和合规技术支出将在全球突破 150 亿美元以上，即达到千亿人民币以上。到 2025 年，60%的大型组织将在分析、商业智能或云计算中使用一种或多种隐私增强的计算技术。

图4：Gartner 预计 2024 年隐私驱动的数据保护和合规技术支出将达近千亿人民币



资料来源：Gartner

2、 隐私计算三大技术路径：联邦学习、安全多方计算、可信计算

常见的实现隐私计算的技术路径包括联邦学习、安全多方计算、可信计算等，此外区块链也是隐私计算的重要补充。

- **联邦学习**

联邦学习是一种分布式机器学习技术和系统，包括两个或多个参与方，这些参与方通过安全的算法协议进行联合机器学习，可以在各方数据不出本地的情况下联合多方数据源建模和提供模型推理与预测服务。在联邦学习框架下，各参与方只交换密文形式的中间计算结果或转化结果，不交换数据，保证各方数据不露出。联邦学习可以通过同态加密、差分隐私、秘密分享等提高数据协作过程中的安全性。联邦学习首先由谷歌公司于 2016 年提出，2018 年由微众银行引入国内，恰好遇到隐私保护、信息安全监管趋严，该技术很快就得到各大互联网公司、科技巨头、人工智能公司重视。

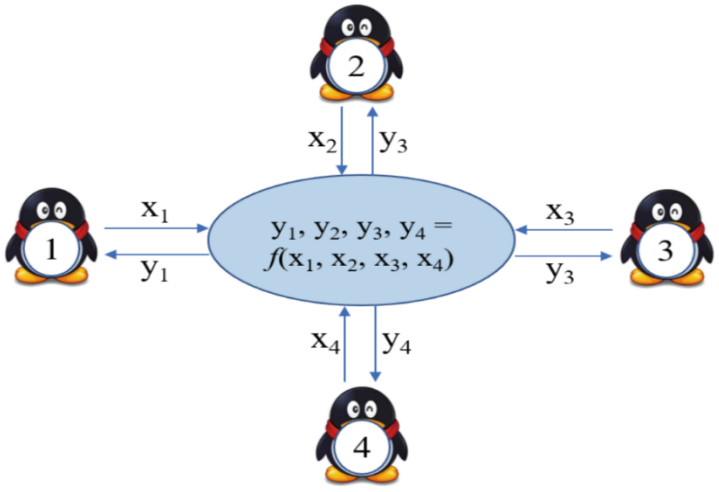
图5：联邦学习是一种加密的分布式机器学习技术

资料来源：深鉴科技

- **安全多方计算**

安全多方计算是一种在参与方不共享各自数据且没有可信第三方的情况下安全地计算约定函数的技术和系统。通过安全的算法和协议，参与方将明文形式的数据加密后或转化后再提供给其他方，任一参与方都无法接触到其他方的明文形式的数据，从而保证各方数据的安全。安全多方计算的基本安全算子包括同态加密、秘密分享、混淆电路、不经意传输、零知识证明、同态承诺等。解决特定应用问题的安全多方计算协议包括隐私集合求交、隐私信息检索及隐私统计分析等。由于安全多方计算需要消耗大量的计算和通信资源，目前应用更加适用于小规模数据量，并且应用主要是聚焦相对简单的统计、查询等类型的计算，而基于安全多方计算的联合建模框架只能支持相对简单的机器学习模型，如逻辑回归模型等。

图6：安全多方计算提供更加安全的联合数据分析能力



资料来源：腾讯

- **可信计算**

可信计算指借助硬件 CPU 芯片实现可信执行环境（TEE），从而构建一个受保

护的“飞地”（Enclave），对于应用程序来说，它的 Enclave 是一个安全的内容容器，用于存放应用程序的敏感数据与代码，并保证它们的机密性与完整性。可信计算（TEE）是基于硬件和密码学原理的隐私计算方案，相比于纯软件解决方案，具有较高的通用性、易用性和较优的性能。其缺点是需要引入可信方，即信任芯片厂商。此外由于 CPU 相关实现属于 TCB，侧信道攻击也成为不可忽视的攻击向量，需要关注相关漏洞和研究进展。

由于技术路径的不同，各类隐私计算技术均有其更加适用的场景：多方安全计算技术不依赖硬件且具备较高的安全性，但是仅支持一些相对简单的运算逻辑；可信执行环境技术具备更好的性能和算法适用性，但是对硬件有一定依赖；联邦学习技术则可以解决复杂的算法建模问题，但是性能存在一定瓶颈。

表2：由于技术路径的不同，各类隐私计算技术均有其更加适用的场景

技术	多方安全计算	可信执行环境	联邦学习
安全机制	基于密码学原理对数据加密	引入可信硬件	数据不动、模型动
性能	低-中	高	高
通用性	高	中	低
高效性	中	中	低
准确性	高	高	中-高
可控性	高	中	高
保密性	高	中-高	中
可信方	不需要	需要	不需要
整体描述	开发难度大、性能提升迅速	易开发、性能佳、但需信任芯片厂商（Intel\ARM）	综合运用各类密码学方法、主要针对机器学习

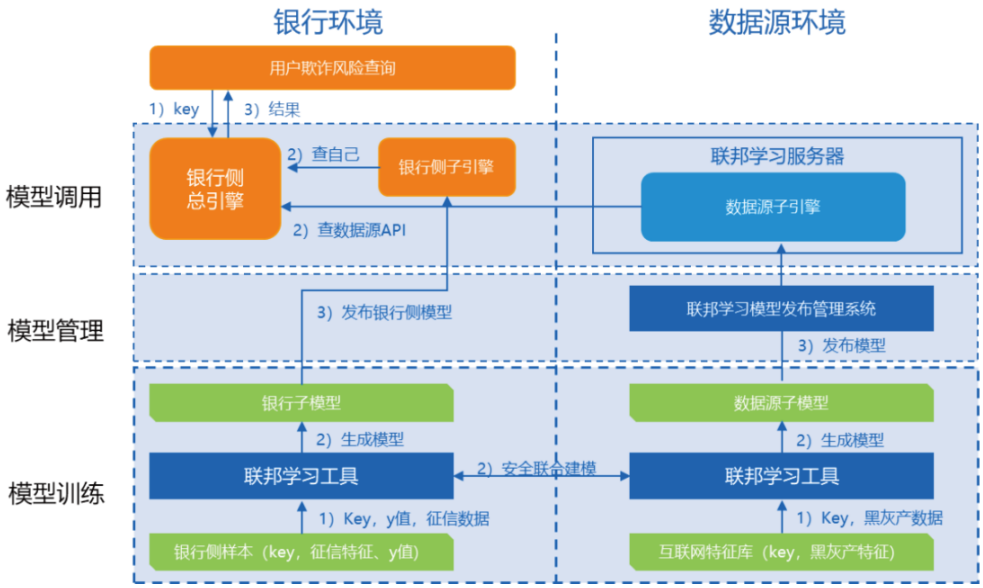
资料来源：中国信息通信研究院、开源证券研究所

3、 隐私计算在金融、政务、医疗等行业有望获得快速应用发展

自 2018 年开始，隐私计算的技术和产品成熟度迅速提升，在我国加快培育发展数据要素市场、数据安全流通需求快速迸发的推动下，隐私计算技术的应用场景越来越多。

在金融领域，隐私保护计算为金融机构间甚至跨行业的数据合作、共享提供可能。PSI 技术可以解决数据对齐时造成客户名单泄露的问题，联邦学习可以保证各方数据不出本地的情况下实现联合建模、预测等。国内隐私计算在金融场景应用方面，以营销、风控端（反欺诈、反洗钱等）等为主要落地场景。

图7：隐私计算可在金融反欺诈场景实现良好应用

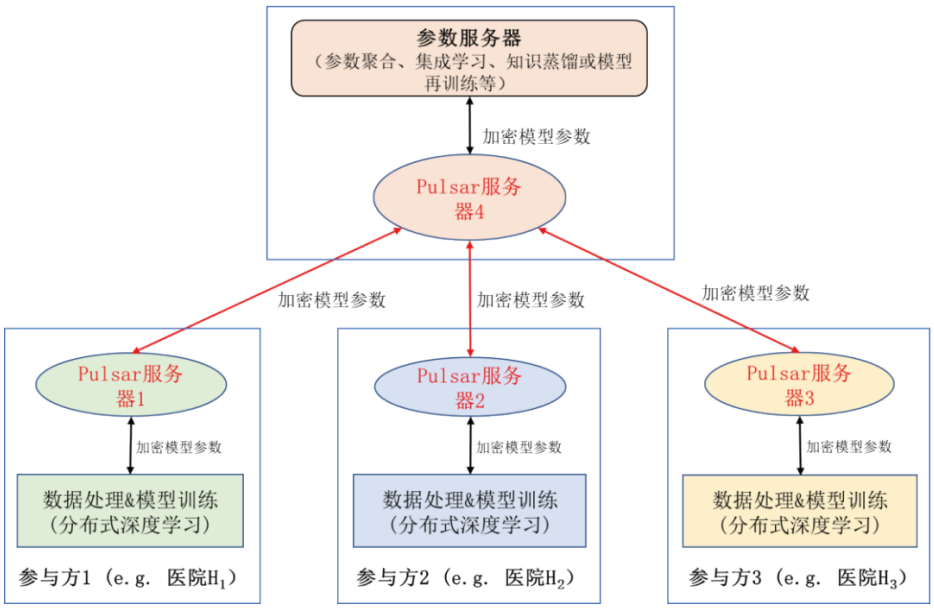


资料来源：腾讯

在政务领域，通过隐私保护计算和其他技术的结合，可以有效保护各政府部门的数据，在一定程度上解决政务数据孤岛问题，提高政府治理能力。

在医疗领域，医疗机构想要使用人工智能对某一疾病进行早期发现或临床诊断，一方面需要收集不同维度的数据包括临床数据、基因数据、化验数据等，另一方面也需要收集来自不同群体、不同地区的样本数据，单个医疗机构无法积累足够的数据来进行模型训练。通过隐私保护计算，可以对不同的数据源进行横向和纵向的联合建模，保证各方医疗数据安全。另外，对于 DNA 测试，用户可以通过 PSI 等技术将某段 DNA 序列和数据库进行匹配，实现遗传疾病诊断。

图8：隐私计算有效助力医学影像识别、疾病筛查



资料来源：腾讯

4、 蚂蚁、腾讯纷纷入局，初创企业不断涌现

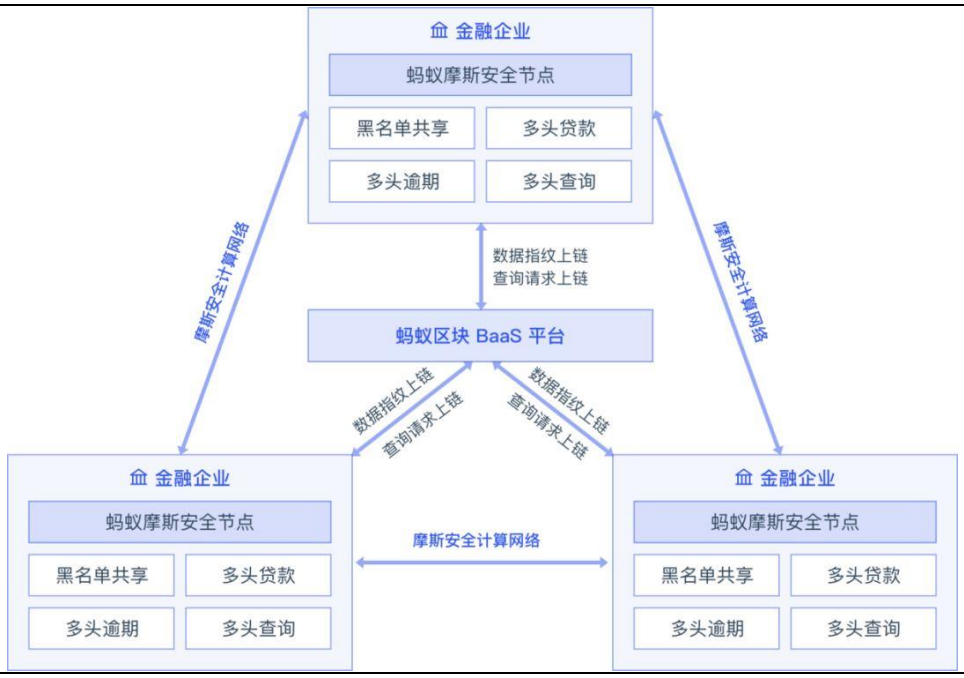
目前，蚂蚁金服、腾讯云、百度、京东等互联网企业推出了各自的产品，同时以微众银行、安恒信息等行业性公司也开始布局，此外，华控清交、富数科技、矩阵元、数牍科技、锘崴科技、光之树科技、零知识科技等一批专注于隐私计算产品化的初创企业也不断涌现。

（1）蚂蚁金服

蚂蚁链摩斯多方安全计算平台：大规模多方安全计算商用平台，基于多方安全计算、隐私保护、区块链等技术，实现数据可用不可见，解决企业数据协同计算过程中的数据安全和隐私保护问题，助力机构安全高效地完成联合风控、联合营销、联合科研等跨机构数据合作任务，驱动业务增长。

蚂蚁链摩斯多方安全计算平台获得 70 多项相关专利（全国第一），性能超业内算法 3~100 倍，iDASH2019 隐私计算比赛全球冠军，率先在金融、电信、汽车等 10 多个行业中完成商用，支持上百家企业线上系统运行，能够支撑实际生产环境下的复杂数据安全计算任务。蚂蚁链摩斯多方安全计算平台是全球首个可信联合计算商业联盟创始成员，致力于技术、产品、生态等资源和能力共享。

图9：蚂蚁链摩斯多方安全计算平台是基于安全多方计算、密码学、隐私保护技术以及区块链技术所打造的一个用于安全共享数据的基础设施



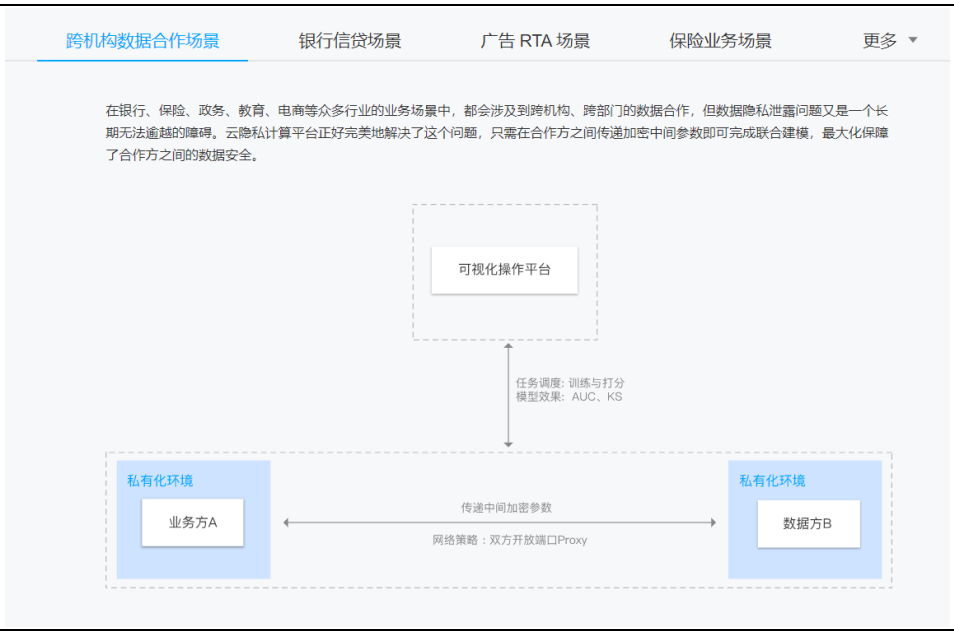
资料来源：蚂蚁集团

（2）腾讯云

腾讯云安全隐私计算（CSPC）是腾讯云推出的以联邦学习（FL）、安全多方计算（MPC）、可信执行环境（TEE）等隐私数据保护技术为基础的隐私计算平台，产品针对机器学习算法进行定制化的隐私保护改造，保证原始数据不出本地即可完成联合建模，同时支持安全多方 PSI（隐私保护集合求交技术）、安全隐私查询、安全统计分析，提供基于硬件的 TEE 可信执行环境。通过腾讯云安全隐私计算，各合作机构既能保障数据安全，又能发挥数据最大价值，很好地解决了业界数据孤岛的难

题。

图10：腾讯云安全隐私计算应用场景多样



资料来源：蚂蚁集团

（3）微众银行

联邦学习方面，早在 2019 年 2 月，微众银行便将自主研发的全球首个工业级联邦学习框架 FATE 予以正式发布，提供基于数据隐私保护的分布式安全计算框架，为机器学习、深度学习、迁移学习算法提供高性能的安全计算支持。目前，FATE 已在信贷风控、客户权益定价、智慧零售、智慧医疗、监管科技等领域推动应用落地。

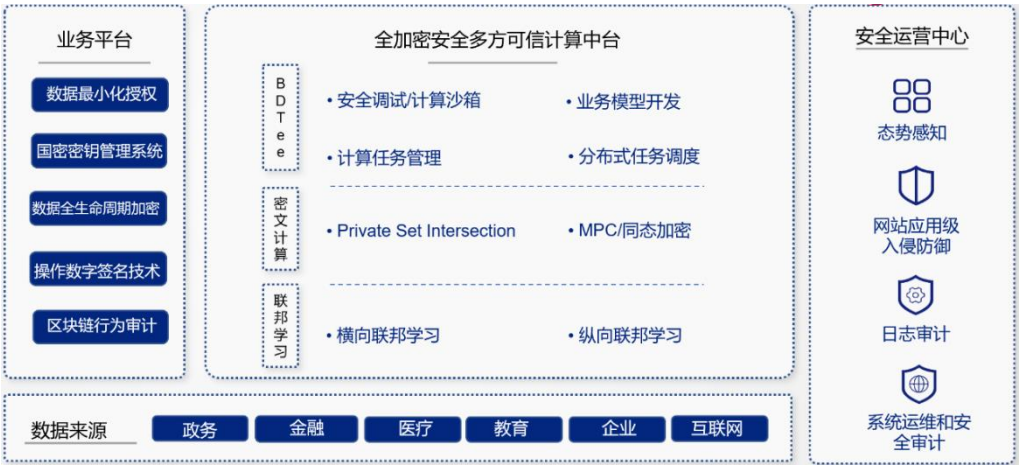
安全多方计算方面，微众银行给出了场景式隐私保护解决方案 WeDPR。该方案组合多种隐私保护策略，融合安全多方计算、同态加密、零知识证明、选择性披露等算法，满足多变业务流程，并围绕开放数据平台、敏感黑名单互通、联合风控、匿名投票、安全支付、隐秘竞拍等典型场景，陆续开源其中的核心算法实现。

区块链方面，微众银行在多年技术沉淀的基础上，发布的区块链核心项目已超过 10 个，构建了涵括底层、中间件和应用组件在内的全栈技术体系。其中，由微众银行牵头研发的国产安全可控区块链底层平台 FISCO BCOS，成为国家信息中心顶层设计的区块链服务网络 BSN 中首个国产联盟链底层框架。且自 2017 年向全球开源以来，已汇聚了 2 千多家企业机构、逾 4 万名社区成员，建成最大最活跃国产开源联盟链生态圈。开源社区内数百个应用基于 FISCO BCOS 研发，其中已有超过 120 个应用投入使用，覆盖政务、跨境数据流通、金融、公益、医疗、教育等多个领域。

（4）安恒信息

AiLand 数据安全岛平台是一个专注于保障数据安全流通，致力于解决数据共享过程中的安全、信任和隐私保护问题的隐私计算平台。综合应用安全计算沙箱，联邦学习，MPC 等多种前沿技术，配合关键行为数字验签和区块链审计技术，实现共享数据的所有权和使用权分离，确保原始数据的“可用不可见”、“可用不可取”，保障多方数据联合计算过程的可靠、可控和可溯。

图11：AiLand 数据安全岛平台致力于解决数据共享过程中的安全、信任和隐私保护问题



资料来源：安恒信息

（5）翼方健数

翼方健数成立于 2016 年，被业界称为国内“隐私计算四小龙”，其核心团队成员来自软银愿景基金合伙人、阿里巴巴美国数据科学研究院、阿里巴巴软件平台架构部门、百度人工智能板块以及医疗、医药、保险等多行业的管理者和资深技术人才。2021 年 7 月底，公司宣布完成 3 亿元 B+轮融资。

公司自主研发的隐私计算平台——XDP 翼数坊基于核心隐私安全计算技术为政务、医疗、医药、生信、金融、保险和营销等行业赋能，业务板块覆盖中国超 30 个城市。公司相关解决方案应用在了高校、机构和企业中，如中国科学院、健康医疗大数据国家研究院、香港科技园、国内著名三甲医院、金融机构、世界 500 强快消品企业等。

图12：XDP 翼数坊基于核心隐私安全计算技术为医疗等行业赋能

资料来源：翼方健数

5、 隐私计算未来有望形成多样化的商业模式

隐私计算往往涉及到 3 类角色：首先是使用数据的业务方，包括金融机构、政

府机构，这类机构是隐私计算服务的客户；其次是作为数据源的数据方，包括大数据局、征信公司、拥有用户数据的互联网公司等；隐私计算技术服务商，则为客户搭建整个计算系统。通常情况下，三种角色是分离，而在有些场景下，一个机构可能兼两种角色。

据 KPMG《隐私计算行业研究报告》，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）销售模式，即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。

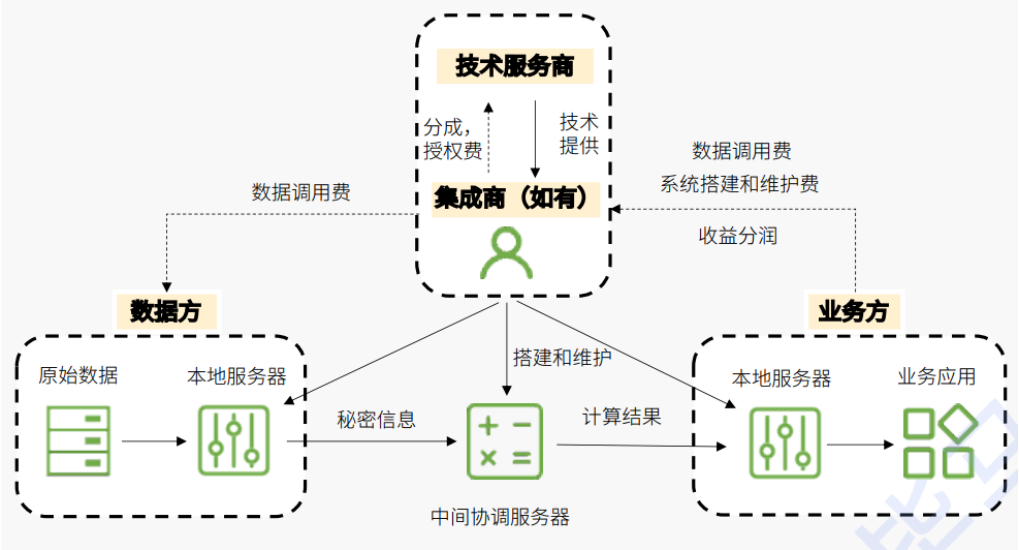
（2）服务模式，即收取年度系统维护和服务费用，这不仅是因为一般软件系统都有日常维护需求，还因为隐私计算的算法本身和应用场景中的模型更新较快，可能需要重新调整算法和模型。

（3）调用模式，即收取数据使用费，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。

（4）分润模式，即根据业务运行效果，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。

目前来看，隐私计算的商业模式尚处于探索过程中，我们预计在发展早期主要以系统销售模式和服务模式为主，未来调用模式和分润模式将打开更大的市场空间。KPMG 预测，隐私计算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，甚至撬动千亿级的数据平台运营收入空间。

图13：隐私计算产业 3 大角色：数据方、业务方与技术服务商



资料来源：KPMG

6、 投资建议

伴随着数据要素市场改革加速，隐私计算技术成为数据价值安全释放的关键突破口，有望在金融、政务、医疗等行业实现快速应用，其千亿蓝海市场有望开启。重点推荐在隐私计算/数据安全领域有前瞻布局的公司安恒信息、奇安信、深信服、绿盟科技、美亚柏科、启明星辰，其他受益标的包括卫士通等。

表3：重点推荐在隐私计算/数据安全领域有前瞻布局的公司（截止 2021.8.6 收盘）

证券代码	公司简称	当前市值（亿元）	归母净利润（亿元）			PE			PS			
			2021E	2022E	2023E	2021E	2022E	2023E	2021E	2022E	2023E	评级
688023.SH	安恒信息	222	1.69	2.36	3.2	131.4	94.1	69.4	11.4	8.0	5.8	买入
688561.SH	奇安信	635	1.66	6.72	8.62	382.5	94.5	73.7	11.0	8.1	6.0	买入
300454.SZ	深信服	1012	10.09	13.49	18.49	100.3	75.0	54.7	13.1	9.8	7.6	买入
300369.SZ	绿盟科技	182	4.19	5.58	7.47	43.4	32.6	24.4	6.8	5.3	4.2	买入
002439.SZ	启明星辰	296	10.51	13.72	16.85	28.2	21.6	17.6	6.3	5.0	4.1	买入
300188.SZ	美亚柏科	154	4.87	6.18	7.93	31.6	24.9	19.4	5.2	4.2	3.5	买入
002268.SZ	卫士通	242	2.28	2.96	3.65	106.3	81.9	66.4	7.8	6.1	5.0	-

数据来源：Wind、开源证券研究所（注：卫士通盈利预测来源于 Wind 一致预期）

7、 风险提示

市场竞争加剧风险；技术变革风险；人员流失风险

特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。
因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

分析师承诺

负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及开源证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5%～20%；
	中性（Neutral）	预计相对市场表现在－5%～＋5%之间波动；
	减持	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡	预计行业弱于整体市场表现。
备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。		

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的机构或个人客户（以下简称“客户”）使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于机密材料，只有开源证券客户才能参考或使用，如接收人并非开源证券客户，请及时退回并删除。

本报告是基于本公司认为可靠的已公开信息，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。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。在任何情况下，本公司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。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的开源证券网站以外的地址或超级链接，开源证券不对其内容负责。本报告提供这些地址或超级链接的目的纯粹是为了客户使用方便，链接网站的内容不构成本报告的任何部分，客户需自行承担浏览这些网站的费用或风险。

开源证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。开源证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

开源证券研究所

上海
地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼10层
邮编：200120
邮箱：research@kysec.cn

深圳
地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层
邮编：518000
邮箱：research@kysec.cn

北京
地址：北京市西城区西直门外大街18号金贸大厦C2座16层
邮编：100044
邮箱：research@kysec.cn

西安
地址：西安市高新区锦业路1号都市之门B座5层
邮编：710065
邮箱：research@kysec.cn