2021年中国隐私计算市场研究报告

——蓝海壮阔，扬帆起航

目录

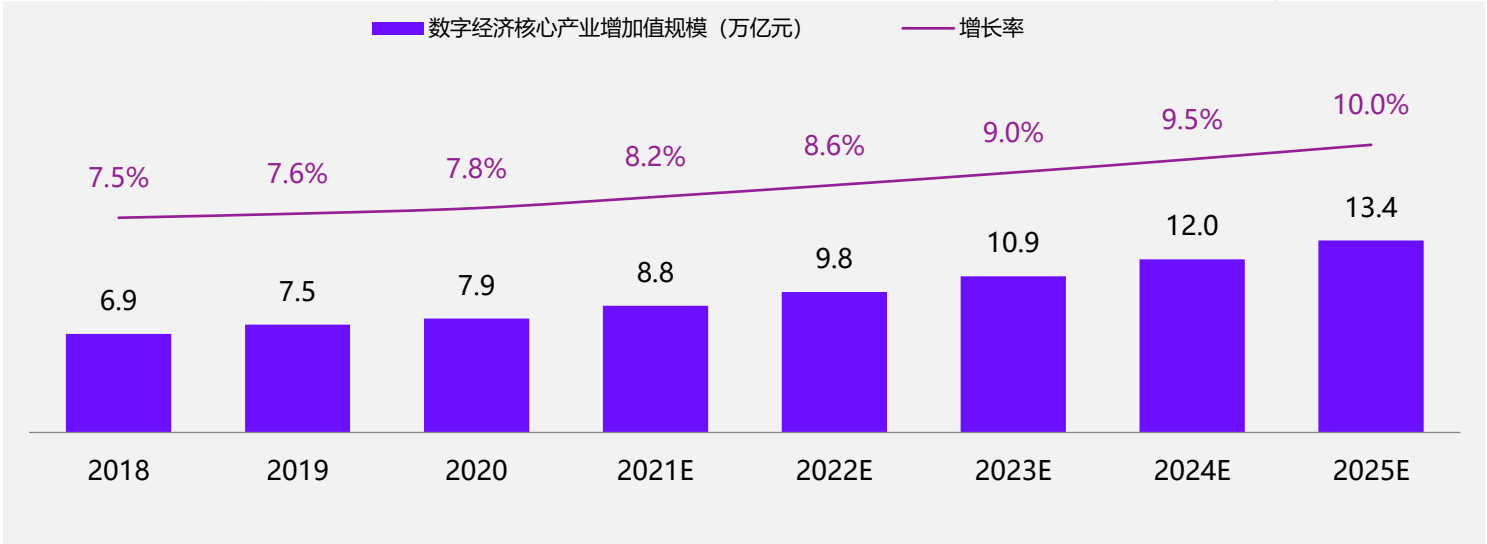
CONTENTS

- 近年来，一系列政策出台和布局落地，从法律层面明确了数据安全和个人隐私保护的重要性。隐私计算及其相关技术作为平衡数据利用和安全的重要方式，多次被政府等国家监管部门在相关政策文件中提及。

发布时间	文件名	文件类型	发布机构	核心内容
2016年11月	《网络安全法》	法律文件	第十二届全国人民代表大会常务委员会第二十四次会议	强调收集的用户信息严格保密，维护网络数据的完整性、保密性和可用性，实行网络安全等级保护制度
2016年12月	《大数据产业发展规划（2016-2020年）》	政策文件	工业和信息化部	支持企业加强多方安全计算等数据流通关键技术攻关和测试验证
2019年9月	《金融科技发展规划（2019-2021）》	政策文件	中国人民银行	提出利用多方安全计算技术提升金融服务安全
2019年9月	《工业大数据发展指导意见（征求意见稿）》	政策文件	工业和信息化部	在工业领域积极推广多方安全计算技术
2020年2月	《个人金融信息保护规范》	政策文件	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
2020年4月	《关于构建更加完善的要素市场化配置体制机制的意见》	政策文件	中共中央，国务院	将数据列为一种新型生产要素
2021年5月	《中国一体化大数据中心协同创新体系算力枢纽实施方案》	政策文件	国家发改委、中央网信办、工业和信息化部、国家能源局	提出“试验多方安全计算、区块链、隐私计算、数据沙箱等技术模式，构建数据可信流通环境，提高数据流通效率
2021年6月	《数据安全法》	法律文件	第十三届全国人民代表大会常务委员会第二十九次会议	强调数据安全与开发利用并重，确立数据分类分级管理制度，多种手段保证数据交易合法合规
2021年7月	《网络安全产业高质量发展三年行动计划（2021-2023）(征求意见稿)》	政策文件	工业和信息化部	提出推动隐私计算等数据安全技术的研究攻关和部署应用，促进数据要素安全有序流动
2021年8月	《个人信息保护法》	法律文件	第十三届全国人民代表大会常务委员会第三十次会议	强调个人信息在数据流通过程中的安全合规

- 根据甲子光年智库测算，2025年中国数字经济核心产业增加值规模将达13.4万亿。在数字经济发展背景下，深挖数据价值、保护数据全生命周期安全成为重中之重，隐私计算产业得以在这一浪潮中乘风而起。

图：2018-2025年中国数字经济市场规模



- 2020年4月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，将数据同土地、劳动力、资本、技术等传统生产要素并列，作为一种新型生产要素参与分配。伴随着数据要素市场改革推进，传统数据流通机制进一步升级，数据协同模式由一次交易向多次安全应用演进。此外，数据要素市场改革推动了数据产业的商业模式创新，从而对数据安全也提出了新出的需求。

图：数据协同模式演进

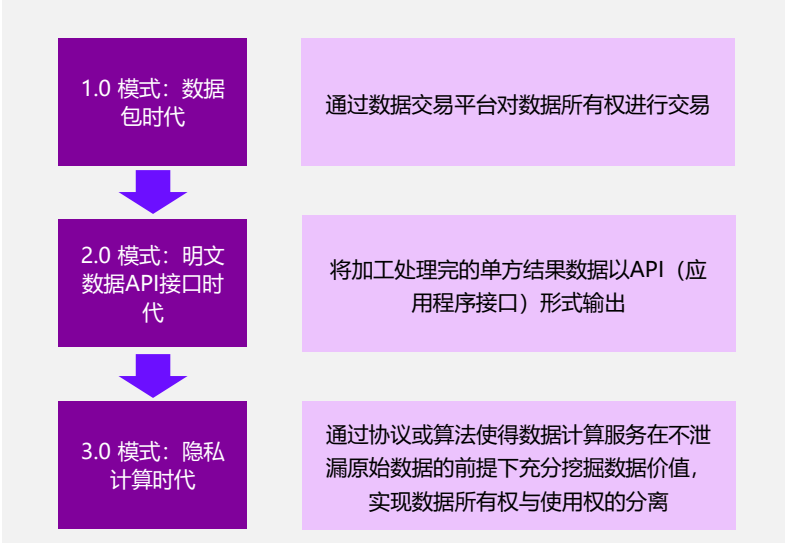
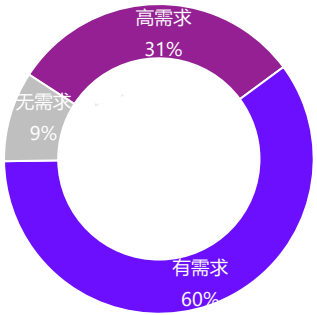


图2:七种数据交易商业模式

- 随着企业数字化转型深入渗透，企业累计数据资产增多，平均数量级达到3.2PB，海量数据资产一方面意味着存在大量价值等待挖掘，另一方面意味着对数据安全防护能力提出了更高的要求，隐私计算的应用能够帮助实现数据“可用不可见”。

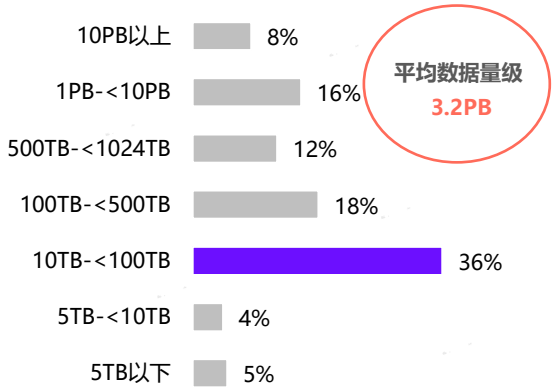
企业数字化需求高

图1：企业数字化需求度



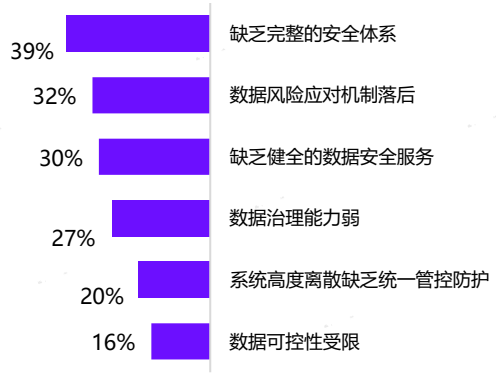
数据资产累积多

图2：企业累积数据资源分布情况



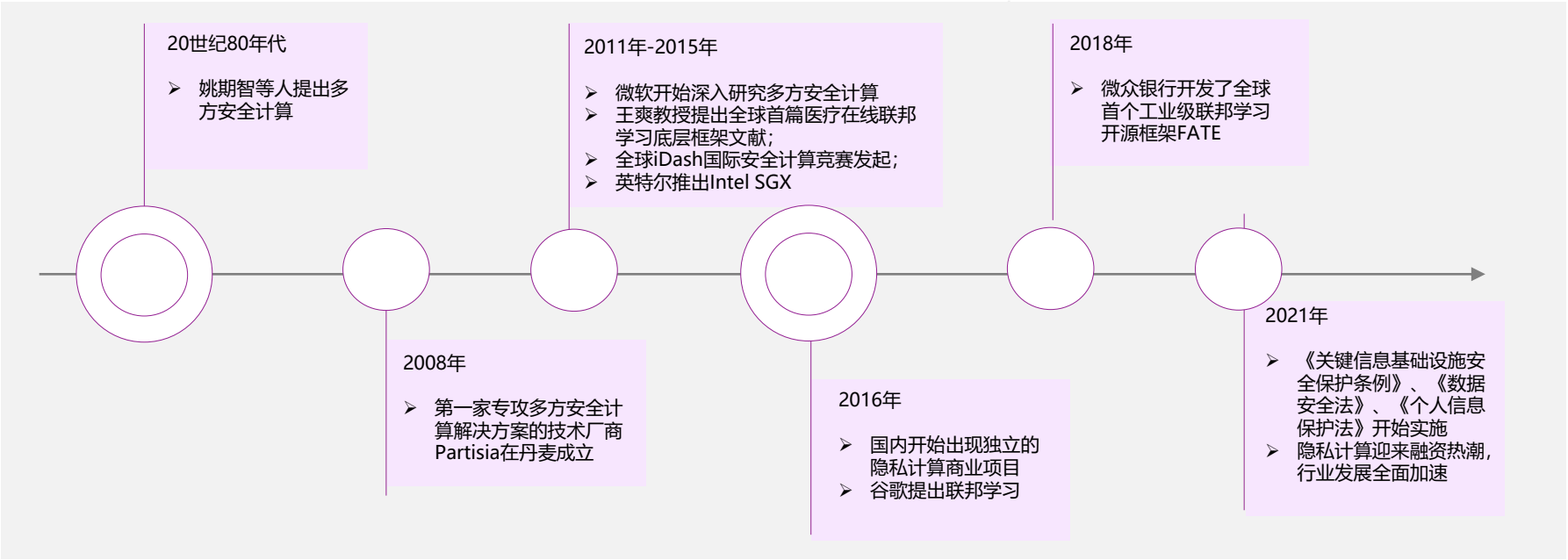
数据安全面临多重挑战

图3：企业数据安全困境



- 从20世纪80年代多方安全计算提出至今，隐私计算相关技术发展已经将近半个世纪，商业化也已经十余年。2021年以来，相关政策出台催化了行业发展进程，隐私计算行业开启加速发展模式。

图：隐私计算发展历程



- 隐私计算（Privacy Computing）是“隐私保护计算”（Privacy-Preserving Computation ）的简称，有时也被称为“隐私增强技术”（Privacy-Enhancing Computation），指的是由两方或者多方联合计算的技术或系统，参与方在不泄露各自数据的前提下通过协作对数据进行联合学习和联合分析，且计算结果可被验证。
- 数据价值挖掘对于个人、企业、政府来说具有显著意义，而如何兼顾数据应用和安全，平衡效率和风险是数据价值挖掘过程中的核心问题，隐私计算有助于破解这一难题。

个人消费者

随着《个人信息保护法》落地，提升个人数据所有权，实现授权机制下的数据使用是大势所趋。隐私计算能够降低个人隐私数据在应用过程中泄密风险。

企业

数据作为一种生产要素，越来越多的业务场景需要多方数据流通和共享，打破“数据孤岛”。隐私计算能够兼顾多方协作过程中的安全性与效率性。

政府

数据开放已成为提升政务服务的关键。隐私计算能够在保障数据安全的同时，增强全社会的数据协作，推动数据要素赋能产业升级。

- 由于正处于发展早期，隐私计算产业在走向壮大的过程中面临许多挑战。比如政策和法规落地的迟滞；技术和产品成熟度欠缺；未来商业模式走向不明晰等。

法律法规落地

2021年以来实施《数据安全法》和《个人信息保护法》，但数据分级、技术标准落地应用仍需时日。

数据源数量和质量

数据源是隐私计算的基础，获取足够多的数据源才能展开更多应用。目前，隐私计算网络上数据源节点占比较低。并且，数据源中存在数据质量不高的问题，比如数据缺失、数据错误等，均将影响计算结果。

商业模式

目前商业模式有待进一步分野，销售模式、服务模式、分润模式等商业模式仍然缺少标杆性案例。

算力

隐私计算所采用的一些密码学加密算法，对于平台的算力和通信开销很大，尤其是在面临跨行业、大规模、多模态的计算任务时，往往是以牺牲性能换安全，需要算力平台从通用型向专精型演进。

安全性

隐私计算对于数据调用的全链路安全要求提升，比如数据安全、密码安全、模型安全、协议安全等。

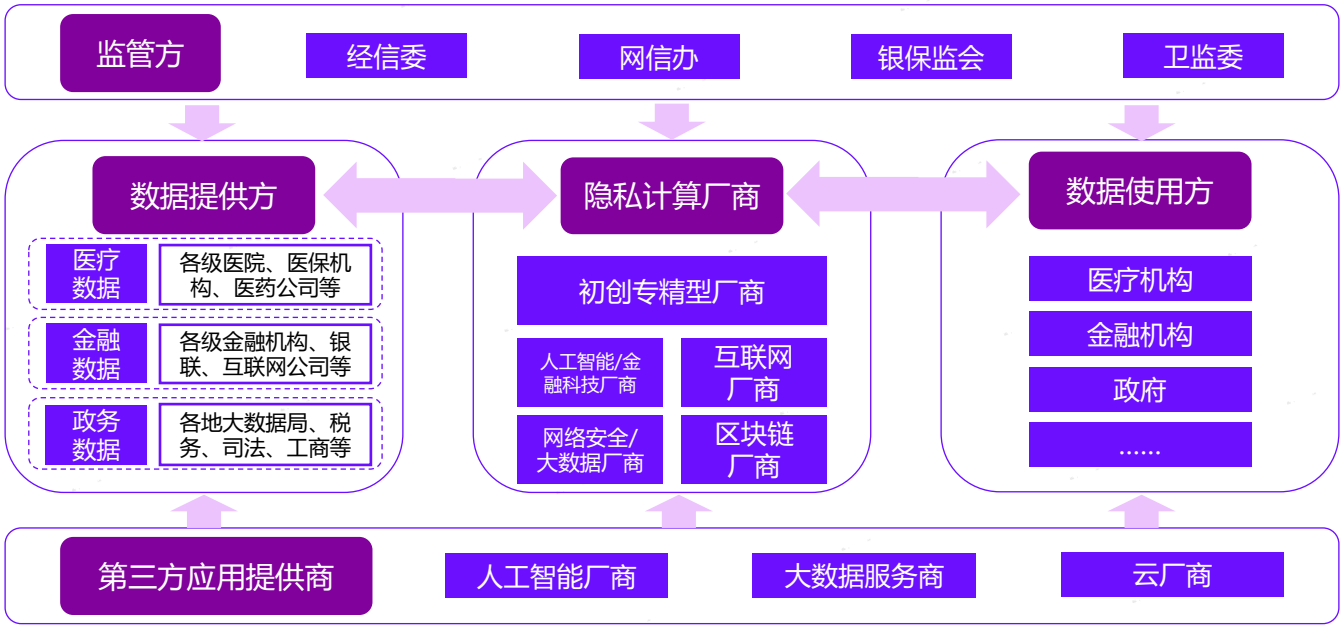
计算精度

随着对应用场景深入，隐私计算对计算精度的要求持续提升，比如同态加密技术中，如何解决复杂函数的浮点运算等。

目录

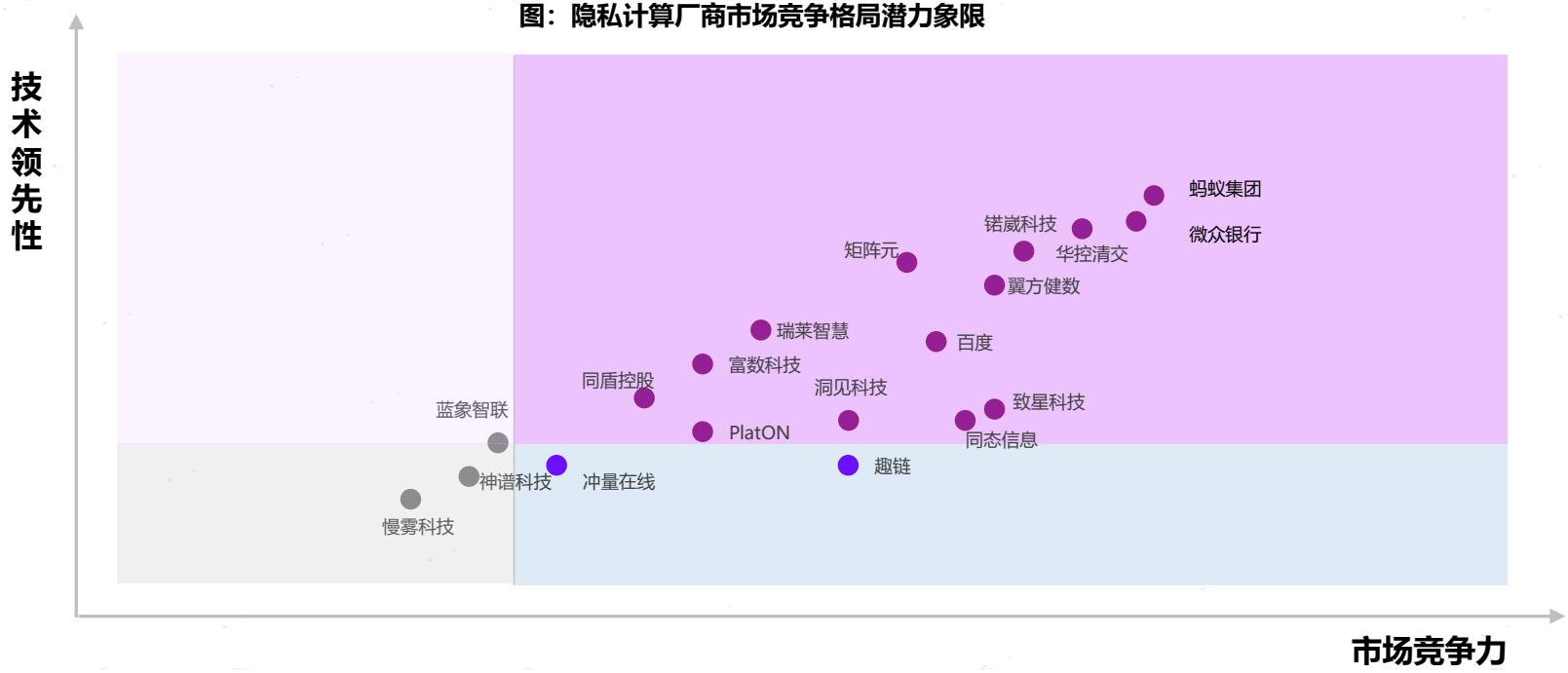
CONTENTS

- 隐私计算产业链包括数据提供方、隐私计算厂商、数据使用方、第三方应用提供商、监督方五大角色。其中，数据提供方、隐私计算厂商、数据使用方是主要角色，分别占据产业链上中下游。第三方应用将为这三大角色提供技术支持也能参与分润，监管方则对产业链各环节进行监管，有时也作为数据源存在。



- 目前，隐私计算市场正面临一片蓝海，从隐私计算总体竞争格局来看，第一象限企业包含各类型隐私计算厂商。蚂蚁集团、微众银行等大型厂商具备技术和市场积累，在竞争中具有一定先发优势，而像锘崴科技、瑞莱智慧等厂商，凭借顶尖科研团队，能够在市场竞争不充分时占领一席之地。

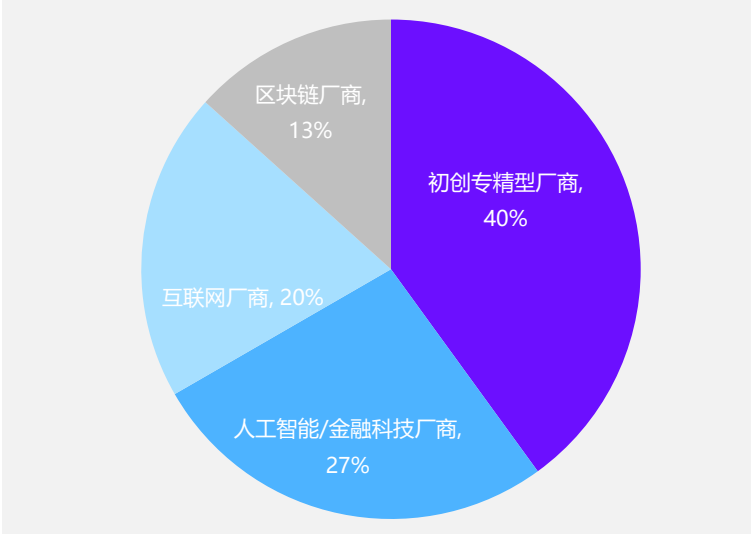
图：隐私计算厂商市场竞争格局潜力象限



- 甲子光年智库通过统计隐私计算核心技术专利数量TOP15申请人，从专利数量来看，蚂蚁集团、微众银行、平安科技等金融科技大厂占据优势；从厂商数量来看，初创专精型厂商占据半壁江山。

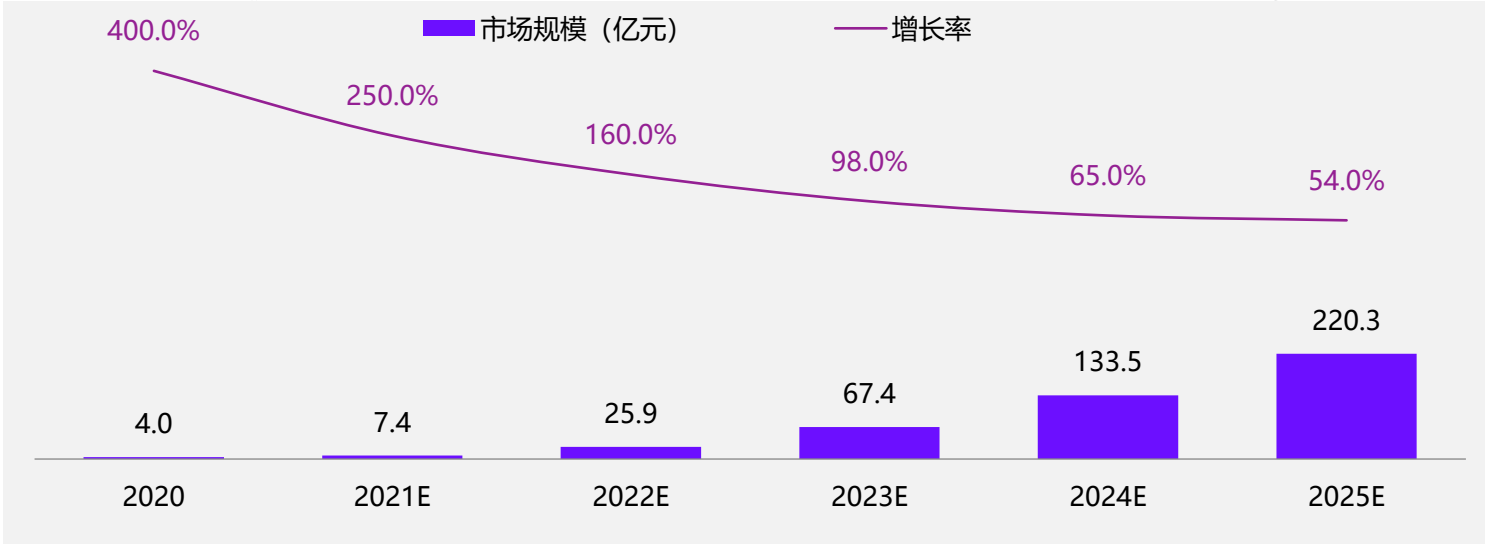
图1：隐私计算核心技术专利数TOP15企业

图2：隐私计算核心技术专利申请人TOP15各类型企业占比



- 随着中国大数据产业发展以及隐私计算技术不断实现商业化，隐私计算市场规模将持续增长。目前数据使用方支出主要为产品及服务费，根据甲子光年智库测算，到2025年该领域市场将超过200亿，2021年至2025年年均复合增长率达133.4%。

图：2020年-2025年中国隐私计算市场规模（单位：亿元）



- 根据甲子智库统计，2021年各领域隐私计算厂商中，初创专精型厂商市场规模总量最高，其次是人工智能/金融科技厂商；从聚焦行业来看，金融行业占比最高。

图1：2021年各领域隐私计算厂商市场规模占比

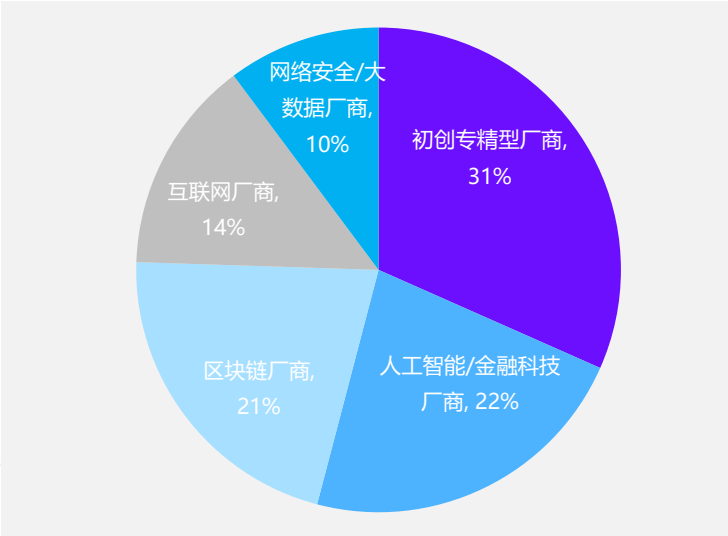
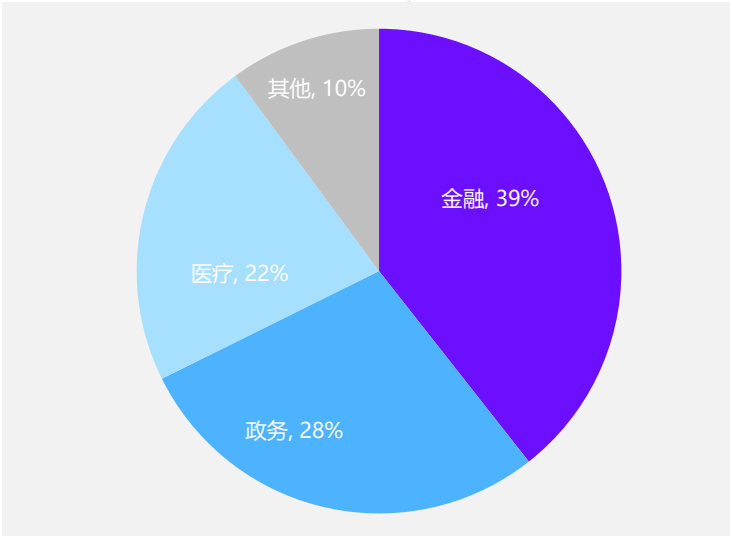


图2：2021年隐私计算各行业市场规模占比



- 甲子光年智库通过对金融、政务、医疗领域隐私计算市场规模进行测算，2021年至2025年，年均复合增长率均在130-150%左右，呈现高速增长态势。

图1：2020-2024年隐私计算金融领域市场规模（单位：亿元）

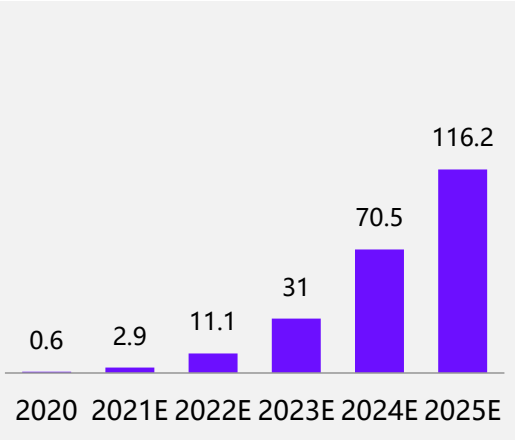


图2：2020-2024年隐私计算政务领域市场规模（单位：亿元）

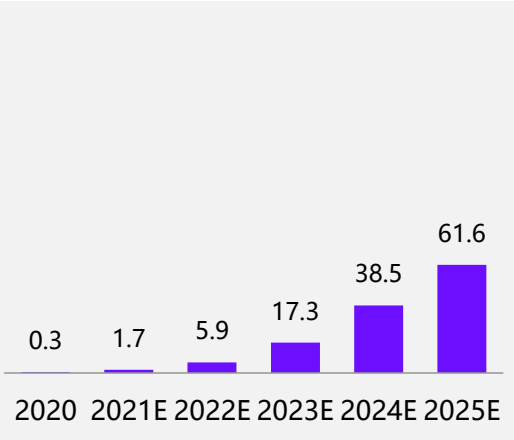
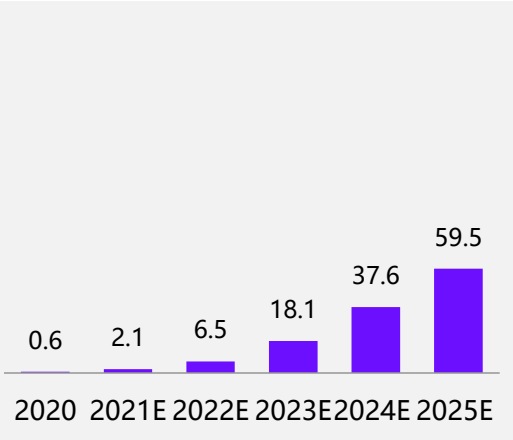


图3:2020-2024年隐私计算医疗领域市场规模（单位：亿元）

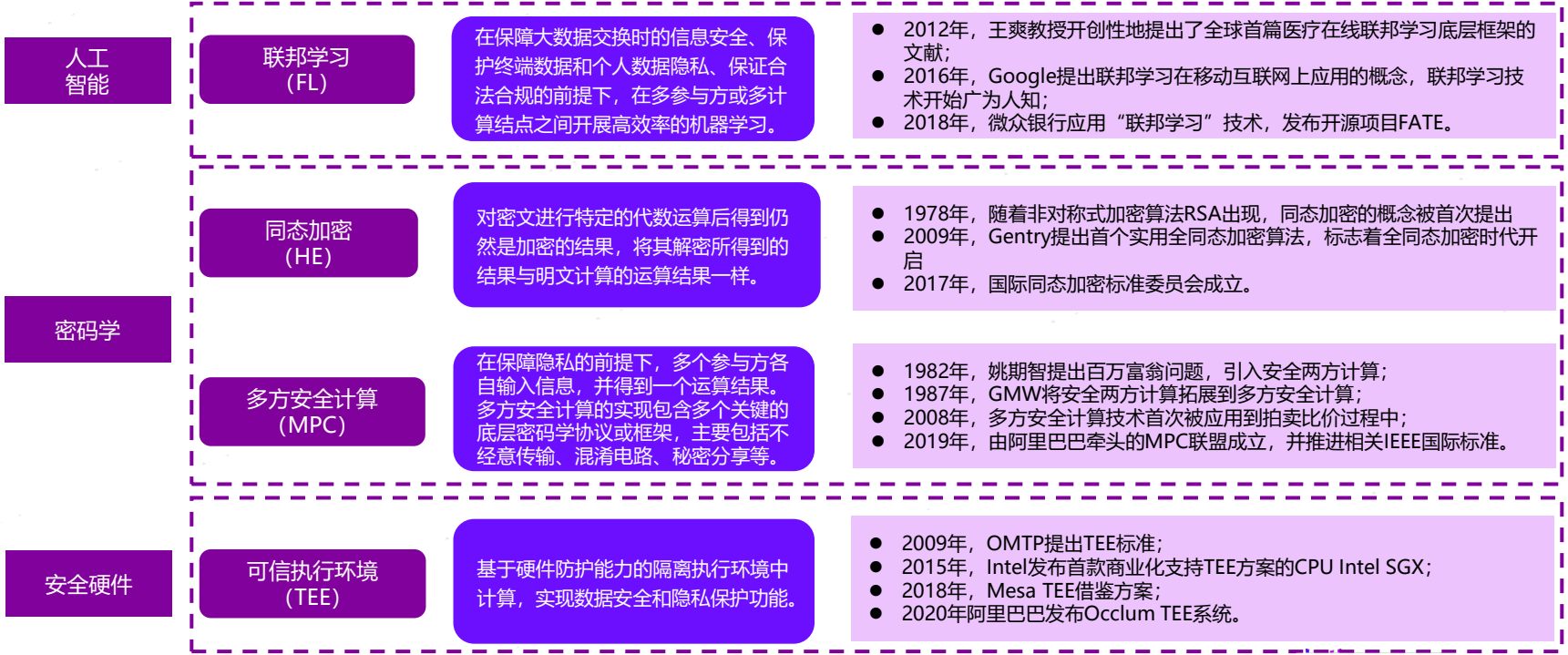


目前，隐私计算已经成为各领域企业跑马圈地的赛场，互联网厂商、人工智能/金融科技厂商以及网络安全/大数据厂商基于其原有资源生态和技术路线，切入到隐私计算领域。初创专精型厂商则专注于提供隐私计算技术和服务；区块链厂商基于原有技术积累，开始在隐私计算领域寻求第二条增长曲线。

目录

CONTENTS

- 隐私计算不是某一具体技术，其由密码学、人工智能、安全硬件等许多领域交叉融合而成。从技术原理上看，隐私计算主要分为密码学和安全硬件两大领域。密码学技术目前以多方安全计算为代表，同态加密还在研发早期；安全硬件领域主要指可信执行环境；此外，还有由人工智能和密码学衍生出的联邦学习等技术。

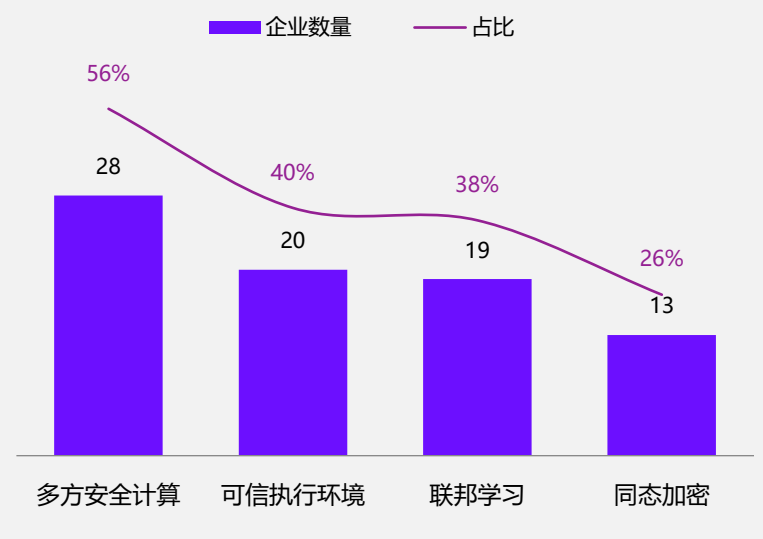


- 甲子光年智库根据对50家隐私技术服务商核心技术分析，56%的厂商应用了多方安全计算技术，其次是可信执行环境、联邦学习、同态加密。从技术成熟度来看多方安全计算已经达到成熟的预期峰值，可信执行环境和联邦学习均处于高速发展阶段，同态加密处于早期快速发展阶段。

图：隐私计算核心技术发展情况

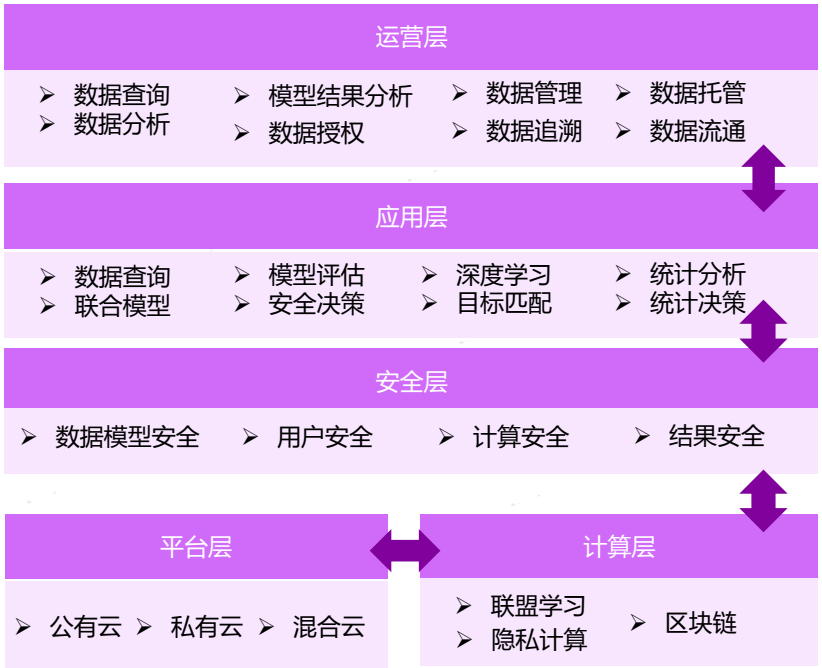
技术	可信执行环境	多方安全计算	同态加密	联邦学习
性能	高	低~中	低	高
通用性	中	高	中	低
高效性	中	中	高	低
准确性	高	高	高	中~高
保密性	中~高	高	高	中
整体描述	通用性强，性能佳，但需要信任芯片厂商（Intel、ARM）等	通用性强，安全性高，研究时间长，性能不断提升，目前应用广泛	计算开销大，通信开销小，安全性高，开发难度大，目前实用性较低	综合运用密码学各类方法，应用已进入相对成熟阶段
技术成熟度	处于技术发展快速成长期	已达到技术成熟的预期峰值	处于技术创新早期，快速发展阶段	处于技术发展快速成长期

图：隐私计算服务商技术分布及占行业整体数量比重



- 技术架构可分为平台层、计算层、安全层、应用层和运营层，平台层由云厂商组成，大多数隐私计算服务商覆盖计算层、安全层，应用层厂商则需要与金融、医疗场景深度融合，运营层则侧重于数据流通过程中的运营服务。

图：隐私计算平台技术架构体系



典型代表

蓝象智联 冲量在线 IMPULSEONLINE

锘崴科技 NVXCLOUDS TECH RealAI 瑞莱智慧

锘崴科技 NVXCLOUDS TECH 富数 FUDATA.CN

華控清交 HUA KONG TSINGJIAO 锘崴科技 NVXCLOUDS TECH CLUSTAR 星云

- 目前市场上隐私计算产品以平台类产品为主，主要包括基于多方安全计算的隐私计算平台、基于联邦学习的隐私计算平台以及可信执行环境类产品。其中，基于联邦学习的隐私计算平台在金融领域应用广泛。

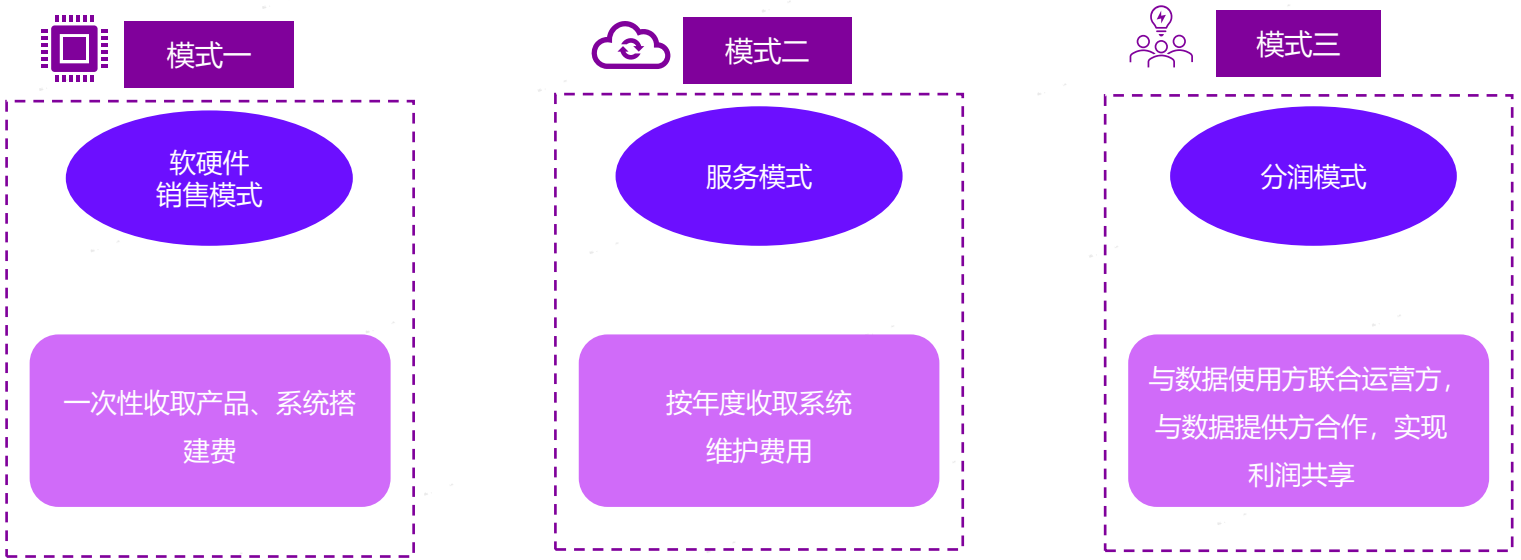
	产品类型	特点	代表厂商
平台类产品	基于多方安全计算的隐私计算平台	一种是数据流通基础设施平台，提供底层技术平台，一般不直接接触数据和提供具体应用开发服务；另一类则与业务结合紧密	诺崴科技 NVXCLOUDS TECH；BaseBit.ai 翼方健数
	基于联邦学习的隐私计算平台	主要应用于业务场景，比如智慧风控、疾病防控、新药研发等	RealAI 瑞莱智慧；CLUSTAR 星云
硬件安全产品	可信执行环境类产品	受限于对国外芯片的强依赖，国内该产品较少，但仍有部分厂商已开始开展在国产化硬件方面的合作探索	Baidu 百度；冲量在线 IMPULSEONLINE

目录

CONTENTS

- 目前，隐私计算服务商主要有三种商业模式，通常三种模式混合搭配。由于行业发展处于早期，对于大多数公司来说，软硬件以及服务是主要的营收来源。随着数据源节点不断丰富、行业生态日趋完善，隐私计算服务商与数据使用方或提供方合作，能够获得长期持续性收入。

图：隐私计算主要商业模式



图：隐私计算软硬件销售/服务模式

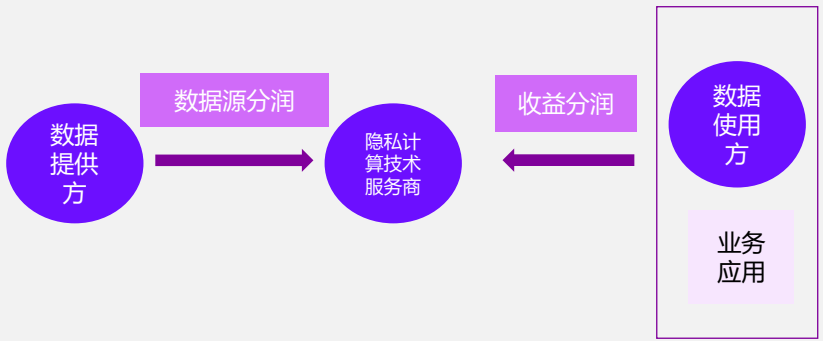
主要特点

- 产品类型：隐私计算一体机、隐私计算平台、 FPGA加速卡
- 维护和服务：算法和模型更新，按年度收取服务费
- 收费方式：根据客户需求按照系统所消耗的计算存储资源、数据源节点数量收费，每单数十万到数百万不等。

典型企业及其产品

锘崴科技 NVXCLOUDS TECH	锘崴信®隐私计算平台
RealAI 瑞莱智慧	隐私保护计算平台RealSecure
CLUSTAR 星云	星云Cluster隐私计算软硬件一体机
華控清交 HUA KONG TSINGJIAO	PrivPy多方安全计算平台

图：隐私计算分润模式



主要特点

- 收费方式：

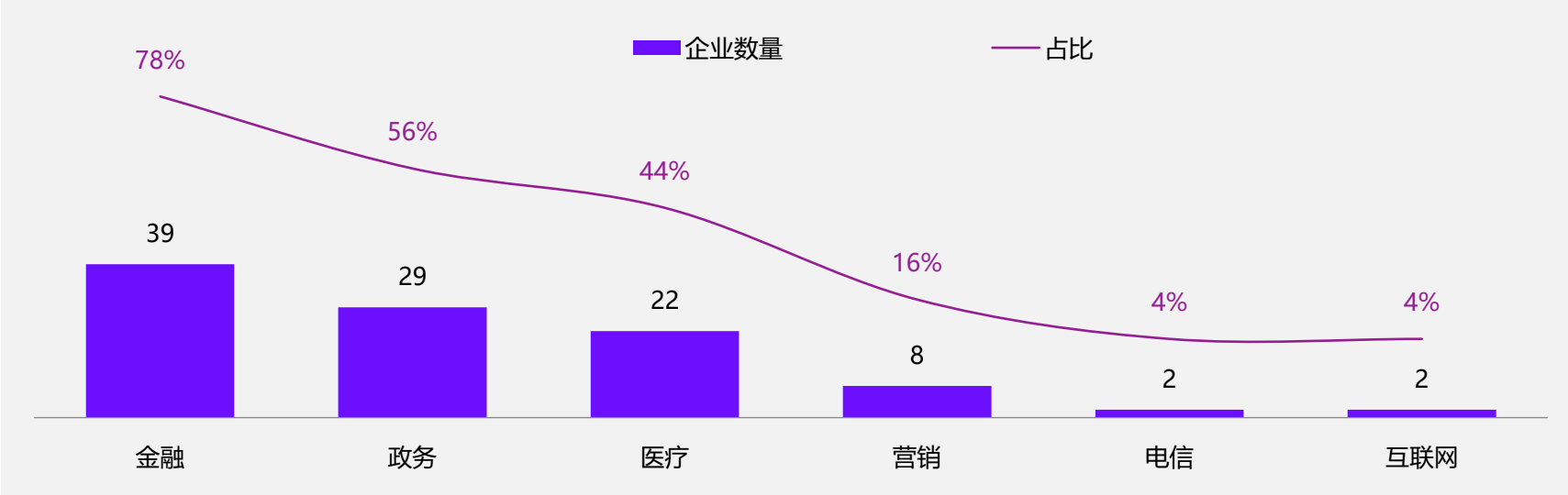
1）早期数据使用方无需承担大额平台系统搭建费用，技术服务方从数据使用方业务应用的收益中分润；

2）根据数据使用方的数据调用量，从数据源收益中分润；

3）目前该模式还在探索当中，还未被广泛使用。

- 从50家隐私计算服务商服务客户领域来看，占比较高的有金融、政务、医疗、营销等，其中金融占比较高，达39家，其次是政务、医疗。

图：隐私计算各行业应用企业数量及占整体企业数量比重



- 目前隐私计算各领域场景应用比较单一，比如金融领域多集中于风控和营销，医疗集中于疫情防控、医保风控等。未来在这些赛道还有大量场景可以挖掘。

数据能力开放、一网通管、联合安防、政企互联、智慧医疗、智慧城市、应急管理和应急响应等

CLUSTAR 星云　同盾科技 www.tongdun.cn
NVXCLOUDS TECH

联合征信、精准营销、联合风控、客户画像等

RealAI 瑞莱智慧　蚂蚁集团 ANT GROUP
華控清交 HUA KONG TSINGJIAO

新药研发、临床辅助诊断、疫情防控、基因分析、医保风控、科研、医疗AI等

NVXCLOUDS TECH　BaseBit.ai 翼方健数
蓝象智联　IMPULSEONLINE

杭州锘崴信息科技有限公司(锘崴科技)团队由联邦学习开拓学者王爽教授、前硅谷知名科学家和工程师组成。锘崴科技致力于为我国开发一整套自主、安全、可控的隐私计算基础设施平台，实现数据“可用不可见”和”数据不动价值动“的新型计算范式，赋能医疗、保险等多个行业，促进多方的数据协作和计算。

技术能力

- ✓ 联邦学习
- ✓ 可信执行环境
- ✓ 多方安全计算
- ✓ 同态加密

- 2011年开始研究隐私计算，2013年开创性地提出了全球首篇医疗在线安全联邦学习底层架构
- 隐私计算领域发表超300余篇学术论文，总引用量超2万余次

标杆客户

上海长征医院　新华医院　华西医院　浙江大学　中国移动 China Mobile

行业应用

医疗

- 生物基因联合分析
- 医学影像分析及辅助诊断
- 医疗数据匿踪查询
- 临床数据多中心研究

金融

- 多中心跨机构金融联合征信及风控
- 交易策略隐私保护及知识库
- 联合营销、供应链金融

政务

- 农村精准扶贫
- 医保核保或者医保控费
- 政务数据开放共享

- 锘崴科技以锘崴信®隐私计算平台为核心，包括医疗保险（NovaVita），金融(NovaFintech)、政务（NovaGov）等系列产品。产品具备部署灵活、强大技术平台、开发便利等特征。

代表产品

锘崴信®隐私计算平台

产品特色

部署灵活

- 容器化、云原生部署 + 端部署
- 服务安全/健康监控
- 各组件/各层级的高可用、松耦合
- 各种虚拟机或物理机的部署
- 多种CPU及国产化架构

强大技术平台

- 通用平台 - 支持自主开发应用
- 软硬件结合，联邦学习、MPC、同态加密等技术集成方案
- 面向政务、金融、医疗、安防等行业垂直应用场景解决方案
- 支持横向扩展和数据并行，TB级数据处理能力
- 支持细粒度并行计算

开发便利

- 支持多种高级开发语言
- 常用数学计算函数库
- 机器学习、深度学习算法库
- 特定行业（医疗、金融等）算法库
- 开发-授权-发布全流程方案

安全保证

- 具有完备计算及结果可以验证证明
- 支持恶意安全假设模型
- 数据应用授权管理流程
- 系统通信安全：SSL、CA认证等
- 兼容国际开源和国产密码体系
- 支持区块链存证审计功能，且可替换
- 核心协议设计简洁，支持可信第三方开放

瑞莱智慧RealAI是第三代人工智能技术基础设施和解决方案提供商，提供一站式赋能平台。其隐私保护计算平台RealSecure是一款基于安全多方计算、联邦学习、匿踪查询等核心技术打造的数据安全共享基础设施，能够帮助金融机构完成联合风控、联合营销、联合科研等跨机构数据合作任务。

技术能力

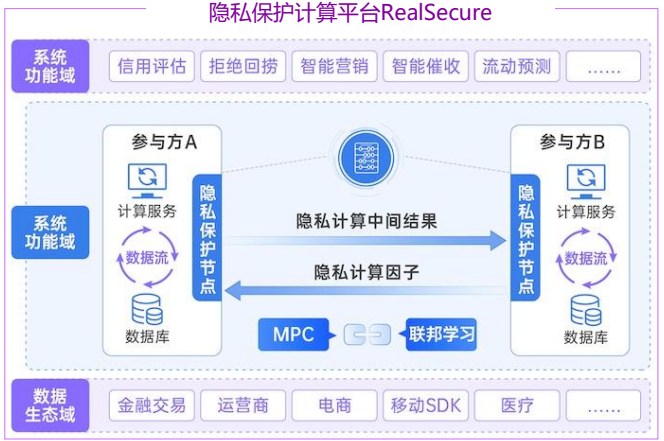
- ✓ 联邦学习
- ✓ 多方安全计算
- ✓ 匿踪查询

- 团队孵化自清华大学人工智能研究院，由张钹院士、朱军教授共同担纲首席科学家。

应用场景

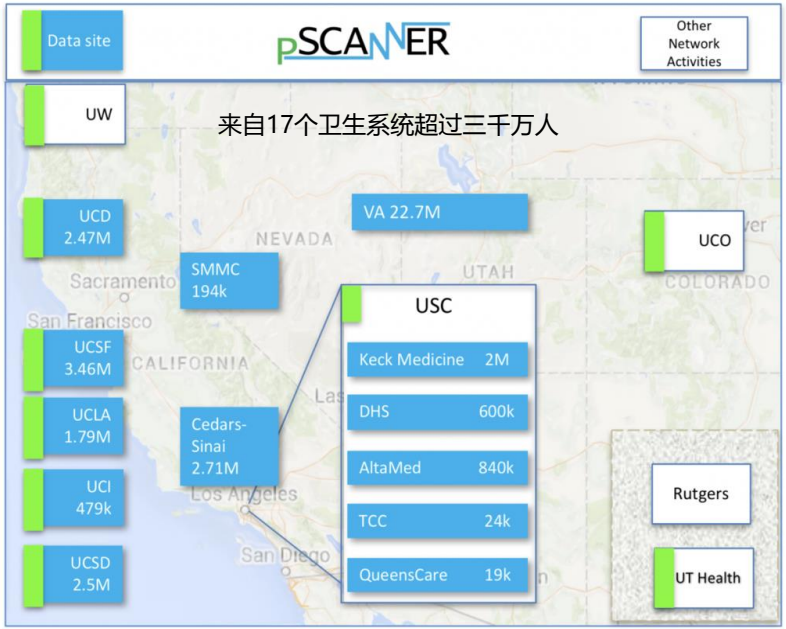
智慧风控　智能营销　联合科研

代表产品

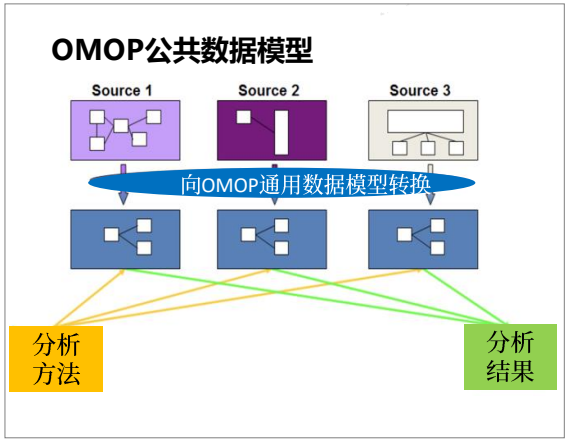


自主研发的联邦AI编译器　直观可验证的安全性

- 锘崴科技基于隐私保护的超大规模医学科研网络pSCANNER在全球属于首创，该项目始于2014年，通过创建一个大型、具有高度代表性的医疗网络来辅助临床结果研究，提高国家进行比较有效性研究（Comparative Effectiveness Research）的能力。



pSCANNER 利用联邦学习等隐私计算技术，通过“数据可用不可见”的方式，连接了17家现有医疗卫生系统的数据源，覆盖了超过 3700 万患者。



传统数据共享方法

方式一：不同的数据源的数据脱敏后，汇总进行分析

- 影响数据质量
- 影响时效性
- 影响数据的覆盖范围

方式二： 数据存在不同数据源的沙箱进行独立分析，对于分析结果通过荟萃分析的方式整合

- 基于每个数据源的独立结果的荟萃分析的精度有限，影响实验结果。

pSCANNER

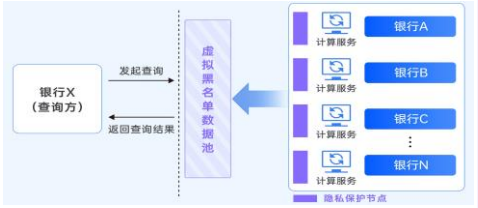
通过使用可扩展的联邦式网络基础设施以及新颖的隐私计算能够对从多中心临床数据库收集的数据进行近乎实时的比较有效性研究和前瞻性分析。

- 风控一直被视为银行的核心能力，数据是关键要素，但是银行自身能拥有与收集到的数据只是“小数据”，尤其在合规要求下，各家机构面临“不愿、不敢、不能”共享数据的困境，导致无法支撑效果优异的风控模型。瑞莱智慧通过隐私计算保护平台RealSecure，让参与方银行完成数据安全合规的互联对接。在此基础上，基于横向联邦和匿踪查询等功能分别实现了反欺诈模型共建和黑名单共享，帮助银行机构提升风控能力。

核心技术

RealSecure横向联邦交易反欺诈示意图

银行间基于匿踪查询技术查询黑名单示意图

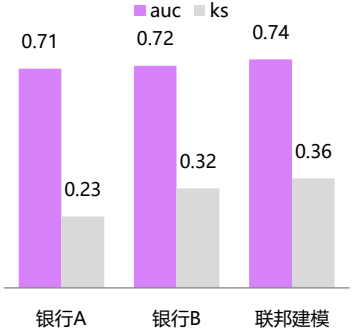


使用隐私保护计算平台，银行A和银行B可以分别准备相关反欺诈样本数据，包括标签和特征，上传至隐私保护计算节点，通过横向联邦的方式，基于双方银行准备的反欺诈样本数据进行特征对齐及建模。在双方数据可用不可见的情况下，构建一个双方可用的效果更优的反欺诈模型。

基于匿踪查询技术，银行之间可发起隐私黑名单查询服务。匿踪查询技术是在发起方不暴露查询ID的前提下，能够获得该ID在其他机构的信息。查询方可获得黑名单信息的密文结果，并解密获得和名单标签信息。

应用效果

图：应用RealSecure前后银行反欺诈效果差异



在黑名单共享匿踪查询场景中，银行拥有数万量级黑名单的情况下，匿踪黑名单服务单次查询的平均耗时为720ms，通信数据量为420M，满足了业务场景时效性的要求。

应用客户

中原银行 ZHONGYUAN BANK　　中融信托

目录

CONTENTS

- 隐私计算行业在中国发展正处于发展早期，底层技术很大程度影响产品的性能和功能，一方面多方安全计算等密码学技术将不断迭代发展；另一方面，区块链、联邦学习与密码学相关技术的融合成为未来发展趋势。此外，未来开源框架将如何推动产业发展、构建新的商业模式同样值得期待。

区块链技术

隐私计算和区块链能够形成互补的技术体系。隐私计算解决的是计算过程可信问题，但不能确保数据本身可信。引用区块链技术能够解决这一问题。数据使用方能够将得到的加密信息在区块链中进行验证，既能确保数据真实性又能确保安全性。

联邦学习

联邦学习最大的特点是能够在数据不出本地的前提下，构建共有模型，其或将成为下一代人工智能协同算法和协作网络的基础。目前，其与隐私计算重合度越来越高，尤其在金融领域应用广泛。

开源框架

中国隐私计算开源是从微众银行的FATE开始。开源一方面能够帮助产业发展，另一方面开源的企业也能从中获利。未来，开源将逐渐发展成熟的商业模式，比如以软件的运维、部署盈利，或以订阅制的方式收费。

- 隐私计算核心是为了解决数据流通和使用问题，未来3-5年内，隐私计算有望成为数据要素市场建设的关键基础设施，一批隐私计算厂商将致力于打造数据底座，并逐步按照数据流量进行收费。

“十四五”规划提到：

- **夯实产业发展基础**。适度超前部署通信、算力、融合等新型**基础设施**，提升技术攻关和市场培育能力，发挥标准引领作用，筑牢产业发展根基。

隐私计算数据底座特征

- 数据安全流通的“高速公路”，按照数据流量进行收费；
- 倾向于为其他公司提供底层技术平台，一般不直接与业务应用进行关联。

- 对隐私计算厂商融资情况分析，我们可以发现早期轮次的企业数量占比最高，其次是战略融资/股权融资以及Pre-IPO/IPO阶段企业占比较高，整体行业呈现出“两头大，中间小”的趋势。随着早期轮次企业发展，我们可以预计2022年隐私计算行业Pre-B/B/B+轮企业数量将有所增加。
- 在已经融资的企业当中，由于金融、医疗、政务三大领域具备广阔成长空间，因而备受资本青睐，短期内资本投资将在这三大领域集中。未来，伴随各行业相关规范落地、技术应用成熟，隐私计算将向其他领域渗透。

图1：隐私计算厂商最新一轮融资轮次占比

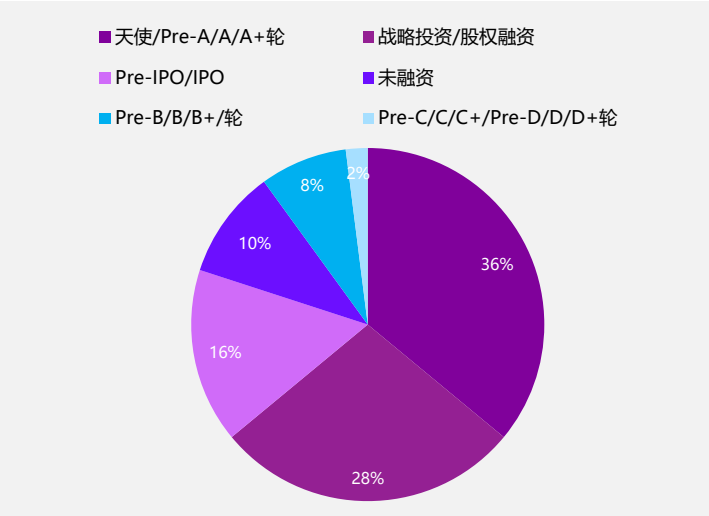
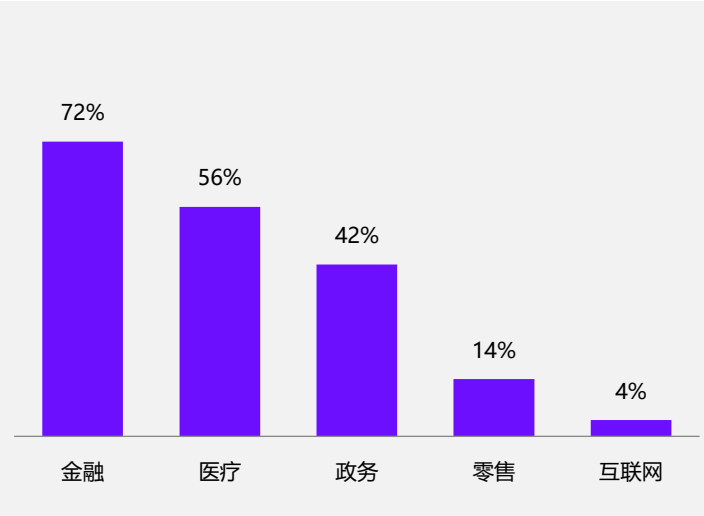


图2：已融资隐私计算厂商涉及行业占比



- 目前，隐私计算应用只窥见冰山一角，随着数字经济发展，发挥数据价值、保护数据安全对于各行业来说都是刚需。未来隐私计算行业发展一方面基于已布局行业的持续性开拓，比如医疗、金融领域还有许多应用场景可以挖掘；另一方面，伴随着应用成熟，隐私计算应用也能向其他领域拓展。根据2021年中国数字经济核心产业值增加规模，数据产品制造业占比超一半，未来将有大量的需求在制造业领域释放；除此之外，农业、教育、互联网等行业仍具备想象空间。

图1：2021年中国数字经济核心产业增加值各领域占比

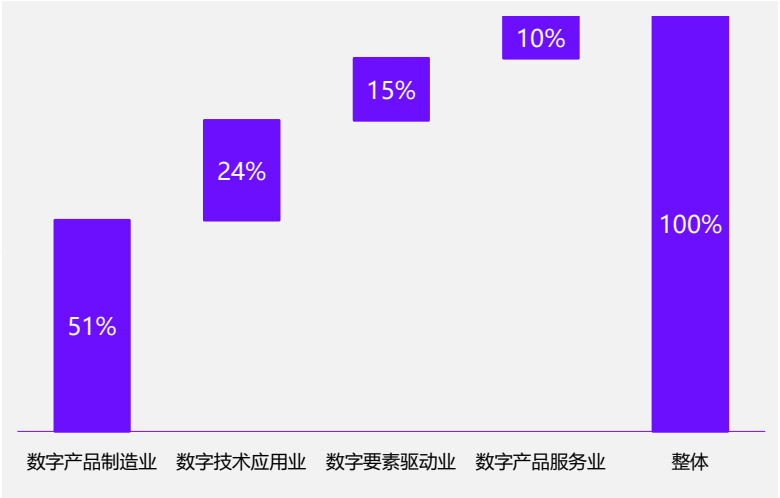


图2：隐私计算未来行业应用