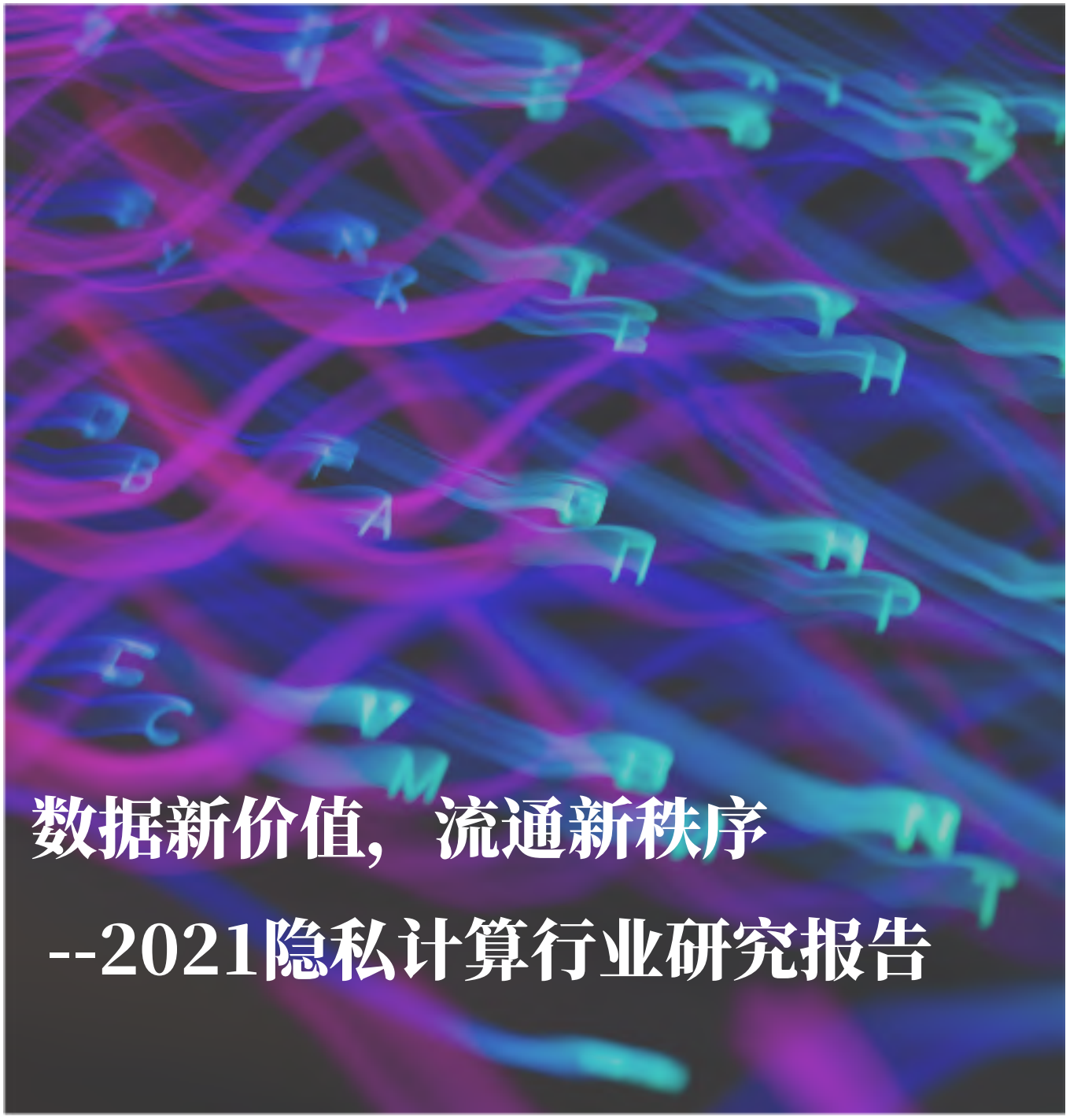


数据新价值，流通新秩序
--2021隐私计算行业研究报告

甲子光年智库团队出品

2021年8月

序

人工智能、大数据、云计算以及区块链的迅猛发展，不仅为数据应用带来升级变革的新机遇，也给数据安全和网络安全带来了新挑战。

- **挑战与机遇并存**

数据孤岛阻碍业务协同。不同行业的企业会产生大量的数据信息，同一企业下不同层级的部门也会产生各类信息，由于行业间的竞争和垄断，以及同一企业下不同系统和业务的闭塞性与阻隔性，很难实现数据信息的交流与整合。这类挑战被称为数据孤岛问题。

隐私计算打破壁垒，保障数据安全流通。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”。目前，随着市场对隐私计算相关技术和厂商的需求不断增加，各类相关企业纷纷推出了自己的隐私计算算法和系统，且积极地以开源、开放体验的形式共享，市场空间和格局初步显现。

- **关键技术初步落地**

从隐私计算核心能力来看，隐私计算体系主要涉及三个方面的关键技术支撑：区块链、联邦学习和多方安全计算。

- 区块链（Blockchain）是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链与隐私计算的技术融合能够在保护数据隐私的同时增强隐私计算过程的可验证性。
- 联邦学习（Federated Learning，FL ）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，通过交换中间数据的形式，联合建模和提供模型推理与预测服务。
- 多方安全计算（Secure Multi-party Computation，MPC）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。

序

- **市场出现典型企业**

尽管中国隐私计算产业尚处于“基建期”，但随着近几年隐私计算的重要性日益凸显，市场上已经出现了众多类型的企业。它们根据自己的技术能力、技术路径和资源生态进行市场定位，制定战略决策。从技术能力来看，隐私计算能力与区块链、联邦学习、多方安全计算这三项技术强相关。三大支撑技术的强弱成为影响企业隐私计算能力定位、战略制定的重要依据。

隐私计算典型企业及技术能力

代表企业	资源生态	核心能力	主要技术路线	典型应用行业	价值评估分析
微众银行	开源生态 金融机构	多方大数据隐私计算平台WeDPR-PPC、联邦学习平台FATE	区块链 联邦学习 多方安全计算	金融、政务、医疗等	三大核心技术构建隐私计算能力体系，以最大开源联盟链生态圈、全球首个联邦学习工业级开源框架FATE开源社区服务全行业应用场景
蚂蚁	阿里生态 金融科技	蚂蚁摩斯	TEE 多方安全计算 区块链	金融、物流仓储等	生态型平台，数据自产自销

- **效果评估体系逐步完善**

当前，隐私计算技术的可用性较之前有了较大提升，使用场景也逐渐丰富，作为新兴的技术，使用者难以综合判断隐私计算的应用效果从而选择相应的隐私计算技术，因此市场亟需建立一套隐私计算的评价规范和评估体系。

从**供应商**角度来看，共性的评估体系能够有效促进厂商之间的有序发展，建立行业的技术门槛，提升供应商的服务能力。从**用户**角度来看，共性的评估体系能够帮助用户理解技术特点与能力，便于用户选型。

综合来看，可从市场需求、收付模式、产品体验、应用效果等细分的维度来定性和定量的进行评估。

甲子光年
JAZZYEAR

目 录

Contents

01 PART 隐私计算的产业发展概况

1.1 隐私计算政策环境

近年来我国数据立法进程不断加快，尤其强调数据应用过程中的数据安全

- 《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法（草案）》逐步完善了我国数据相关立法的顶层设计，着重强调了流通过程中的数据安全和个人信息保护。

- 隐私计算是平衡数据利用和安全的重要路径。自2016年，工业和信息化部、中国人民银行、国家发改委、中央网信办、国家能源局等政府监管部门先后在相关政策文件中提到加强隐私计算相关技术的攻关和应用。

相关法律及政策文件				
	时间	文件名	发布单位	简述
法律文件	2016年11月	《中华人民共和国网络安全法》	十二届全国人民代表大会第二十四次会议	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。
	2021年4月	《中华人民共和国个人信息法（草稿）》	十三届全国人民代表大会第二十八次会议	强调个人信息在数据流通过程中的安全合规。
	2021年6月	《中华人民共和国数据安全法》	十三届全国人大常委会第二十九次会议》	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。
政策文件	2016年12月	《大数据产业发展规划（2016-2020年）》工业和信息化部	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）》	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性。
	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》	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)》	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。

资料来源：国家部委官网、公开资料，甲子光年整理

1.2.1 隐私计算市场概况-数据应用的演进

隐私计算作为数据协同使用新范式，是对传统数据流通机制的又一次重大升级。且数据协同模式逐渐由一次交易向数据多次安全应用演进

3.0 模式：隐私计算时代

3.0模式：真正实现数据所有权与使用权的分离

能够通过协议或算法使得数据计算服务在不泄漏原始数据的前提下充分挖掘数据价值。目前主流的隐私计算技术主要包括安全多方计算、联邦学习、可信硬件机密计算。

2.0 模式：明文数据API接口时代

2.0模式：将加工处理完的单方结果数据以API（应用程序接口）形式输出

通过程序对元数据进行隔离，在用户发出数据使用请求后，由程序从元数据中抽取、调用数据反馈给用户。在该模式下，按照数据分类沉淀的API接口日调用量可达到上亿次，可满足较广的服务覆盖范围；保护用户隐私信息以及降低二次利用可能性；降低数据价值融合的可行性。

1.0 模式：数据包时代

1.0模式：通过数据交易平台对数据所有权进行交易

由于数据所有权相关法律法规不明晰，该模式有较高的数据安全风险，较难保护数据所有者利益，易导致涉及用户隐私的信息暴露以及数据被使用方二次利用甚至滥用。

资料来源：国家工业信息安全发展研究中心

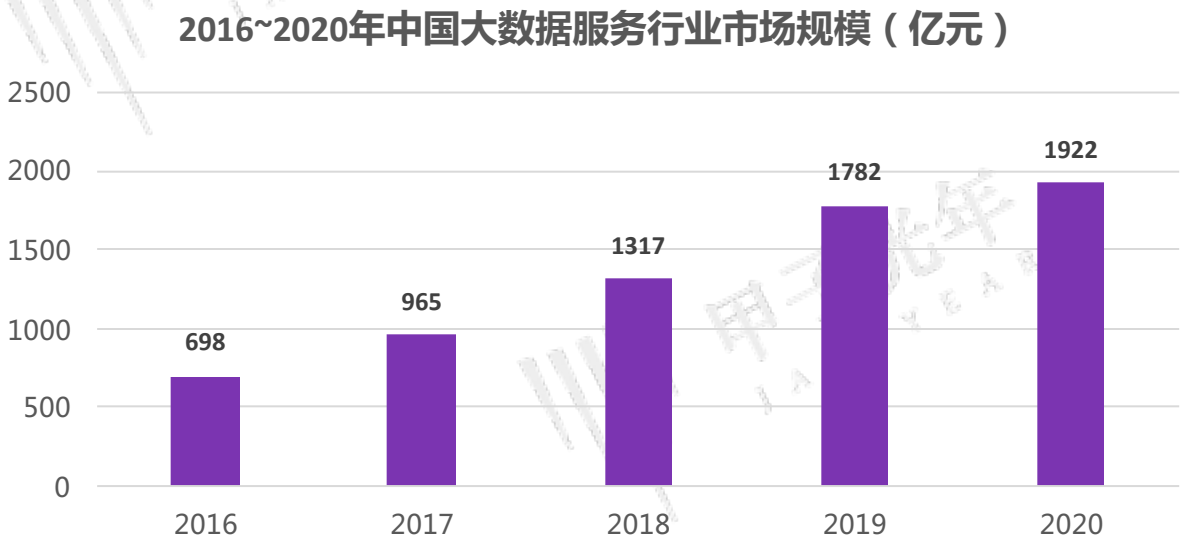
1.2.2 隐私计算市场概况-数据流通需求推动隐私计算发展

作为数字经济时代的新型生产要素，数据的价值日益被充分认可，数据安全也备受社会广泛关注，而数据泄露频发生则直接催生了对隐私计算的迫切需求

- **数据作为一种新型生产要素，是数据服务业的基础，大数据服务是数据服务行业的重要组成部分**

➢ 数据处理技术、数据应用和数据服务业兴起于20世纪90年代， 随着政府和企业的数字化转型逐步受到了社会关注和重视。

➢ 中商产业研究院数据显示，我国大数据服务市场规模由2016年的698亿元跃升至2018年的1317亿元，据预测，2020年我国大数据服务行业市场规模将达1922亿元，数据服务市场规模的持续增长。



- **数据泄露频发，隐私计算技术需求迅速增长**

➢ 一个完整的数据生命周期包括数据从产生、获取到销毁的全过程，具体可分为：采集、存储、整合、呈现与使用、分析与应用、归档和销毁几个阶段。任何一个阶段都存在一定的数据资产损失风险。

数据来源：中商产业研究院，甲子光年整理

1.2.3 隐私计算市场概况-数据流通需求推动隐私计算发展

2020年CNCERT监测隐私泄露数据

107起 未脱敏展示公民个人信息事件107起，涉及未脱敏个人信息近10万条。

203起 个人信息非法售卖事件203起，金融机构数据非法交易事件总数的40%。

- 对于日益数字化的信息社会，各种新技术新应用不断涌现，网络安全环境日趋复杂，网络安全事件所引发的业务运行中断、关键数据泄露、数字资产损失等后果，都是企业所不能承受之痛。但企业自身普遍存在专业人才不足、防护手段滞后、缺乏应急机制和技术能力等问题。
- 2020年，多项网络安全法律法规面向公众发布，我国网络安全法律法规体系日臻完善。国家互联网信息办公室等12个部门联合制定和发布《网络安全审查办法》，全国人大法工委就《数据安全法》和《个人信息保护法（草案）》征求社会公众意见，《密码法》正式施行。中共中央印发《法治社会建设实施纲要（2020-2025年）》，要求依法治理网络空间，同时，国家发改委、工业和信息化部、公安部、交通运输部、国家市场监督管理总局等多个部门陆续出台相关配套文件，不断推进我国各领域网络安全工作。
- 一方面，面对数字化社会发展的痛点，众多企业都急需一站式的网络安全解决方案来全方位助力互联网安全发展，加快保护信息安全，保障网络安全。
- 另一方面，国家大力整治网络安全问题，从上到下颁布多个网络安全相关法律法规及配套文件。隐私安全计算技术的应用伴随着社会发展的需要和政策的支持迎来空前的规模。

数据来源：国家互联网应急中心CNCERT

1.3.1 隐私计算产业配套环境-政务应用情况

在政府的公共治理过程中，隐私计算为跨机构、跨部门间的数据流转和精准施策创造条件

- 2020年10月，《中华人民共和国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纲要》发布，其中提出加快建设数字经济、数字社会、 数字政府，建设数字中国，打造数字经济新优势。

隐私计算对政务治理的影响

隐私计算助力政务数据透明化

隐私计算提高政府施策精准度

隐私计算促进数据流转与政企协作

政府与个人

数字政务涉及个人隐私数据，针对性和可用性大大减弱；政府机构及其部门之间的数据流转同样受到阻碍。

借隐私计算可以帮助政府实现隐私保护下的高质量数据协作，在不暴露数据明文的前提下，以数据密文形态进行统计和分析，既保证了数据使用安全，又降低了数据泄露风险。

政府与各司

伴随着数据开放性和流通性的提高，隐私计算有助于政府实现精准施策。

推进政务数据开放共享将有助于促进社会经济的发展和提升政府的治理和服务水平，尤其是在政策实施过程中，通过政府数据与多方数据的融合，能够实现基于数据驱动的精准施策。

政府与企业

通过隐私计算平台，可以促进政府和企业的数据协作，实现政企数据融合应用。

在基于隐私计算的数据流通背景下，政府与企业间将重构数据信任机制，形成常态化的互联互通、数据协同。
这不仅对企业具有商业价值，而对政府提高公共治理效果同样具有长远意义。因为，企业的数据通常拥有更加具象化的特点，所以它对政府数据及相关指标设计可以起到监督、修正和补充的作用。

1.3.2 隐私计算产业配套环境-行业应用环境

隐私计算产业的发展将推动并赋能相关行业数据的应用向安全性、合规性迈进

- 尽管隐私计算技术的发展方兴未艾，但已经在多个领域中发挥作用。目前基于隐私计算技术实现数据融合应用的传统产业包括（但不限于）金融、医疗、广告、电信、零售、物流和能源等。其中以金融、医疗和广告业的应用最为典型。

隐私计算的行业应用			
应用领域	解决问题	工作原理	应用效果
金融	数据跨机构互联互通 降低隐私泄露风险	在不泄露各方原始数据的前提下，帮助从事数字化转型与智能化应用过程中的银行、保险公司、互联网金融机构等实现跨机构、跨部门的数据安全融合、联合风控建模、联合营销筛选等，提升金融智能的准确性及完备性	实现数据跨机构流通与应用
医疗	医疗机构间病例数据的互联互通	为医疗机构在保护个人健康与病患隐私数据的前提下，进行疾病的发病趋势、概率预测，治疗效果的统计对比、分析等，实现数据的共享与价值挖掘	实现数据的共享与价值挖掘
广告	流量方和广告主数据共享 优化广告投放效果	在隐私计算技术的帮助下，可以实现以保护双方数据为前提的联合训练、建模、优化模型效果等工作，从而提高计算精度，并完成更精准的投放广告	实现在保护双方数据前提下提高计算精度、精准投放

02
PART

隐私计算的市场实践

2.1 隐私计算关键技术分析

隐私计算行业技术标准逐步完善，四大关键技术路线成为业内共识

- 中国信通院云大所长期聚焦于隐私计算领域，依托大数据技术标准推进委员会于2018年至2020年间陆续牵头制定《基于多方安全计算的数据流通产品技术要求与测试方法》、《基于联邦学习的数据流通产品技术要求与测试方法》、《基于可信执行环境的数据计算平台技术要求与测试方法》、《区块链辅助的隐私计算技术工具技术要求与测试方法》四项针对隐私计算基础功能的标准，并开展评测。
- 由此可见，多方安全计算、联邦学习、可信执行环境和区块链辅助下的隐私计算工具已然成为目前隐私计算产业最重要的四大技术发展方向。经过甲子光年的走访调研，多位业内人士均表示对上述结论的认可，并指出这些关键性技术已经在多个场景中实现落地。

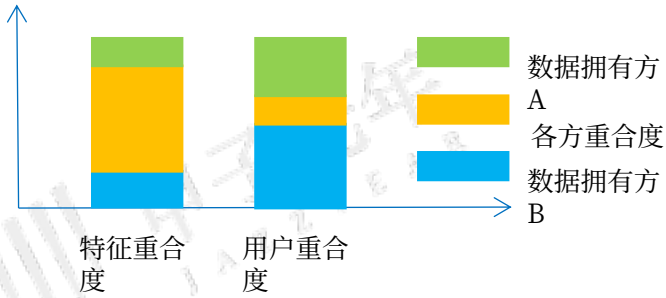
- 多方安全计算（Secure Multi-Party Computation，MPC）有狭义和广义之分。狭义的多方安全计算，最早由图灵奖获得者、中国科学院院士姚期智教授于1982 年通过“百万富翁问题”提出的解决方案，目前所涵盖的范围更加广泛。广义的多方安全计算即指在保障隐私的前提下，多个参与方各自输入信息，并得到一个运算结果。
- 本质上，多方安全计算是利用密码学和分布式特性来实现在交互过程中，让交互的个人或者机构达到身份和行为的匿名，或者无需透漏数据的明文与对方完成协作。多方安全计算的优势在于，各个参与方对其所拥有的数据拥有绝对的控制权，保证基本数据和信息不会泄露，从而保证各方数据的安全和私密。这是实现隐私计算的关键所在。
- 目前，在多方安全计算领域，被大家广泛应用的有以下几项主流技术：秘密共享（secret sharing）、同态加密（Homomorphic Encryption）、零知识证明（Zero—Knowledge Proof）、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（Private Information Retrieval）等，通常这些技术会同时应用在同一个大型项目中，来实现最终目的。安全多方计算具有严格的安全定义，因此可以实现数据流通过程中的隐私性、正确性、公平性（可选）、结果传递保证（可选）等。

2.1 隐私计算关键技术分析

隐私计算行业技术标准逐步完善，四大关键技术路线成为业内共识

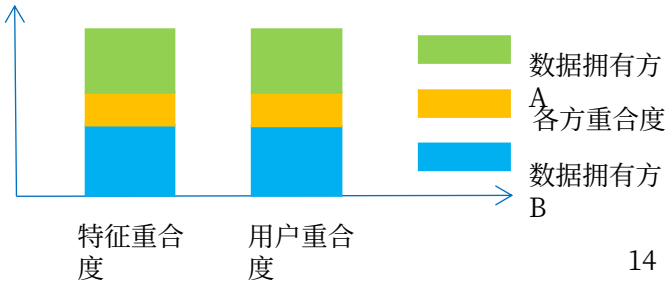
- **联邦学习（Federated Learning, FL）**，又名联邦机器学习，联合学习，联盟学习，最早由谷歌公司于2016年提出，在保障大数据交换时的信息安全、保护终端数据和个人数据隐私、保证合法合规的前提下，在多参与方或多计算结点之间开展高效率的机器学习。主要解决的问题就是，数据拥有方不出本地前提下，构建共有模型。在国内，微众银行是“联邦学习”最早发起者和倡导者之一，开发了全球首个工业级联邦学习开源框架 FATE。
- 联邦学习可以将分布在多个机构之间的数据，在不出库的情况下进行联合学习、建模和预测，充分应用多方异构数据建立更好的模式，为用户提供优质服务。在联邦学习的整个过程中，终端数据始终存储在本地，避免了数据泄露的风险，从而实现共享数据最小化，进而保护数据隐私。此外，联邦学习可使用的机器学习算法包括逻辑回归、神经网络、随机森林等，或将成为下一代人工智能协同算法和协作网络的基础。
- 联邦学习涉及“联邦”和“学习”两部分，是密码学和人工智能相结合的分布式学习技术。微众银行首次将联邦学习应用于金融、推荐等场景，解决人工智能落地中数据孤岛与数据隐私保护难题，将联邦学习总结成三类：横向联邦学习、纵向联邦学习和联邦迁移学习。

（1）横向联邦学习：各方业务场景相似，数据方特征维度相同，用户重合度低，特征重合度高。适用于特征信息重叠较多的场景，通过提升样本数量达到训练模型效果的提升。比如两个异地的银行之间就可以构建横向联邦学习模型。



（2）纵向联邦学习：各方数据方样本ID相同，特征重合度较低，用户重合度较高。适用于参与双方样本重叠较多时的场景，通过丰富样本特征维度，实现机器学习模型的优化。比如银行和商业公司之间可以构建纵向联邦学习模型。

（3）联邦迁移学习：各方特征重合度较低，用户重合度较低。适用于样本和特征重叠都较少时，需要进行数据迁移。

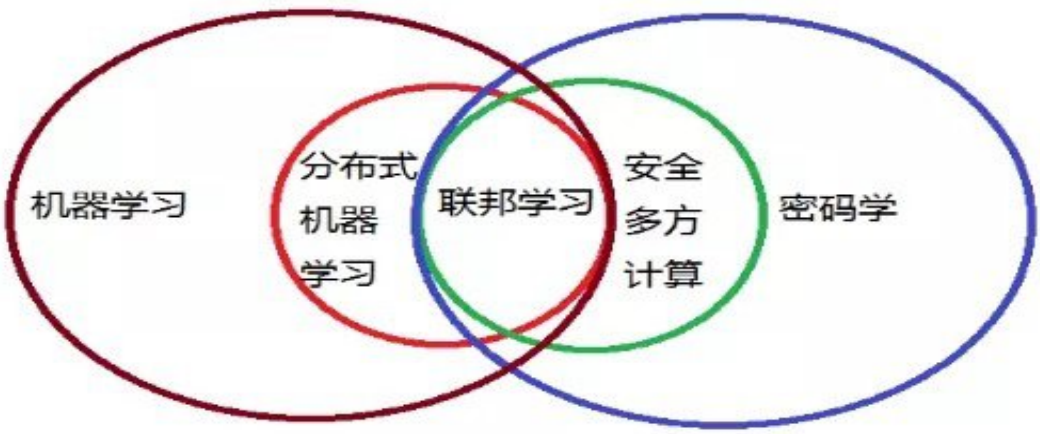


2.1 隐私计算关键技术分析

隐私计算行业技术标准逐步完善，四大关键技术路线成为业内共识

- 从应用场景上来看，根据联邦学习的应用领域及面向服务的受众对象，可将联邦学习的典型应用场景分为：面向个人用户（2C）、面向行业用户（2B）。
- 面向个人用户主要是基于个人终端隐私数据保护情况下的数据共享和协同的应用场景；面向行业用户主要是围绕企业内部以及跨公司跨行业的数据联合建模应用场景。

隐私计算相关技术之间的关系示意图



- **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。通常是在中央处理器中构建一个安全的区域保证其内部加载程序和数据在机密性和完整性上得到保护。
- 可信执行环境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，目前硬件技术被掌握在少数外国核心供应商手中，国内相关技术和产业尚不成熟，所以，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。而且，从国外购买指定的硬件会显著提高该技术的使用成本，不利于该技术的大规模推广。此外，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，但是可信第三方的认定仍备受业内质疑。TEE硬件设备被质疑的还有安全缺陷问题，需要不断改进升级硬件，且相比于软件升级，硬件升级更换的成本较高。

2.1 隐私计算关键技术分析

隐私计算行业技术标准逐步完善，四大关键技术路线成为业内共识

区块链技术与隐私计算技术互为补充、相辅相成。区块链为互联网构建了信任机制，隐私计算为流转在区块链中的信息提供了隐私保护，让链上数据实现“可用不可见”的特点。

在隐私计算行业发展进程中，仍然存在一些技术和应用层面的的难关和问题，区块链技术在一定程度上可以最大限度的解决这些问题，其中包括：

（1）技术：技术的安全可靠、效率、数据孤岛是当下隐私计算要解决的核心问题。

（2）安全：目前的大数据主要存储集中化、规模化的数据中心，数据容易出现被盗、泄露等问题。

（3）效率：大数据时代的到来，让隐私数据的处理成为了一个难题：大规模的加密数据处理导致计算性能下降，而非加密数据处理又极大概率会导致隐私信息的泄露。因为数据隐私技术的不成熟，得不到客户的信任，现在大部分的企业还是自己保存和维护自己的数据，数据无法自由流通和共享，形成数据孤岛。

（4）应用：技术和解决方案还不够完全成熟，与客户的需求可能会存在一定差距；技术标准的不完善会导致客户对采纳技术的安全可靠性有疑虑；市场需求尚未充分展现，在大多数场景下还缺乏明确的拉动型政策和标杆性示范项目；一些行业的数字化程度低，也制约了数据价值挖掘的需求；产业推广需要搭建多方协同的合作方式，而这种模式的建立需要时间，当下各个厂商正走向达成共识的路上。

区块链技术的核心价值在于提供了分布式的信任机制，由此可以实现可信的跨管理域数据存证和防篡改可验证的数据流通。这些价值对于数据生产要素化所必须满足的权属明确、真实可验的技术要求十分关键。

对应地，隐私计算业务由于涉及跨管理域的多方协作，具备天然的分布式特性。一个完整的隐私计算业务除了需要保障计算过程中数据的隐私性之外，还需要提供分布式数字身份、数据审计、数据治理、分布式计算任务协调等一系列分布式配套基础设施。目前来看，区块链技术是提供这些配套基础设施的不二之选。

2.1 隐私计算关键技术分析

隐私计算行业技术标准逐步完善，四大关键技术路线成为业内共识

- 区块链对隐私计算的作用是提升数据的可信度，隐私计算对区块链的作用是找到新的应用场景。
- 隐私计算引入区块链技术，企业可以将自己的数据以加密的形式存在区块链上，当需要与其他人交易数据时，可以直接用加密的形式提供数据。对方将得到的加密信息到区块链中进行验证，这样对方既能确保数据的真实性，又不会让数据在链上被公开。
- 简而言之，区块链技术确立数据的所有权，区块链技术和隐私计算技术一起可以剥离数据的所有权和使用权。
- “隐私计算+区块链”的结合可以打破隐私信任的问题，提高多方协助之间的信任关系以及企业的核心竞争力，促进隐计算在多方之间的信任应用，从而推动隐私计算在具体场景的应用。隐私计算实质上还可以推动企业商业模式的重大改变。
- 综上所述，四大技术路线之间存在较大差异。并且，鉴于可信执行环境的安全可控问题还有待通过自主替代等方式来解决，因此，从隐私计算核心能力来看，构建隐私计算能力体系，目前仍然主要涉及区块链、联邦学习和多方安全计算这三大关键技术支撑。

2.2 隐私计算技术服务体系

隐私计算技术服务体系各有特色，开源框架有突出的竞争力

隐私计算技术如日方升，催生出一系列行业应用，各企业在建设服务体系方面各有特色。随着技术的不断迭代，隐私计算在应用过程中必然会面临更复杂的场景、更多的参与方、更实际的业务需求，实现隐私保护下的互联互通互信也会变得愈发重要。开源框架很可能成为行业内的主流框架，有助于企业在市场上取得领先地位。

在一个典型的隐私计算服务体系当中，通常会包含三类参与方：（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；还有些金融机构有技术，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。

这意味着，各隐私计算企业需要在服务体系当中，在三种角色之间寻找合适的定位。也衍生出，在竞争格局方面，形成各有特色的局面：有的企业比较依赖企业资源生态来打造自身服务体系；有的主要靠技术路线来影响到客户和落地应用选择；有的则主打某一行业，以垂直深入的服务，树立行业内稳固的地位等。

其中，大部分企业采用的是闭源的底层技术框架，但也有少部分如微众银行这样的企业开源了底层框架，以代码透明换取技术信任，以开放的态度推广技术，让更多从业者来开发或改善框架，从而产生更多更好的隐私计算技术，利好整个产业。

2.3 隐私计算效果评估体系

优化隐私计算方案解决能力需立足三大核心要素

综合国家层面的政策法规、行业内多个企业的技术和应用案例可见，成熟的隐私计算方案解决能力需要具备以下 三 个核心要素：**在合法合规的框架下、企业级可支撑大规模商用的易用体验、多方协作牢靠的安全信任关系**。

（1）合法合规

随着互联网爆发式的发展，数据的自由流动明显加快，随之容易引发一系列问题，比如数据的确权问题、安全问题、隐私问题等。在这样的背景下，隐私计算使得数据无需离开机构，仍能实现机构与机构之间的协作，满足数据的自由流动和挖掘数据价值，其重要性日益凸显。但是，隐私计算本身是一项综合的技术，一方面，它需要推动数据流动，另一方面更需要保护数据被合规合法地使用。这也意味着必须在合法合规的框架下探索隐私计算的应用价值才有实际意义。

2021年6月，全国人大常委会第二十九次会议正式通过了我国首部数据安全领域的基本法——《中华人民共和国数据安全法》，要求通过采取必要措施，保障数据得到有效保护和合法利用，并持续处于安全状态的能力，主张坚持维护数据安全和促进数据开发利用并重，以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

随着立法，其对使用数据使用的合规性提出了更为严格的要求，许多数据可能将无法再通过传统的技术获得，否则存在违背法律法规的风险。这对于隐私计算而言，也是新的发展机会。

（2）产品体验

当前，隐私计算技术的可用性大大增强，使用场景逐渐丰富，产品化程度逐步成熟。参照中国信息通信研究院云计算与大数据研究所公布的隐私计算相关测评结果，从互联网头部企业、电信运营商、知名大数据公司到隐私计算技术研发初创公司，越来越多类型的企业加入隐私计算技术提供者的行列中。技术及应用的发展也使得隐私计算相关产品的架构、功能逐渐成熟。产品呈现出相关技术深度融合，以及工具化、模块化、高易用的特点。

2.3 隐私计算效果评估体系

优化隐私计算方案解决能力需立足三大核心要素

整个隐私计算的开发模型需得是可视化编程。从其依托的其中两项关键技术来看，一是企业需在底层技术上，通过区块链核心技术，以及智能合约相关的技术体系，来构建多方分布式协作环境；二是引入基于密码学的安全多方计算，也由一系列核心技术支撑，具备较高深的认知门槛，所以，如何使用它对于企业和开发者来说，是一个很大的挑战。

因此，在打造平台的过程中，需要非常注重的一个投入就是，如何让用户更敏捷地实现安全多方计算场景的落地。在这个过程中，构建可视化的、可拖拽的组件，帮助不同的业务、不同的角色去实现安全计算的一些尝试：比如业务部门可以对可视化的组件进行拖拽，像拼图、拼积木一样地敏捷实现搭建；数据分析的部门可以像写传统的SQL类型的语句一样，写一些基本的脚本代码就可以实现基本数据分析；开发部门要把场景完全实现，还可以提供高级语言的方式来编程落地整个解决方案。整体上，一整套适用于不同角色，不同场景下的组件和方案，可以更好地辅助安全多方隐私计算的落地。

（3）安全信任

过去，传统生产要素自身较为固定，基本上受物理、地域、时间等条件制约，事前承诺、事中取证、事后维权均有支撑。此时，大家探讨安全可信，也往往是从系统安全的角度出发，探讨数据的机密性、完整性、可用性等。

然而，对于数据这个新的生产要素，传统信任机制的适用性有限，数据要素“复用无损耗、使用无限制、用后无痕迹”的特点，使其难以真正有效地进行承诺、取证、维权。由此一来，缺乏技术手段的各数据业务主体只能用信誉等虚拟信用进行背书、担保，公正公平意义缺失。换言之，应该有技术力量，尤其是开源技术力量的注入，打破传统信任机制的藩篱，通过开源的形式促成技术信任，建立新式信任机制。

利用开源技术的特性，无论是代码包还是技术协议，都是开源的，数据所有者能够自主评估技术本身的可靠性、隐私性、可控性，从而决定自己是不是要分享数据，信任机制将越来越可靠稳定。总之，从基于信誉、基于补偿的信任，再到基于技术以及基于开源技术的信任，可信数据权益体系的信任基础发生着深刻变化。

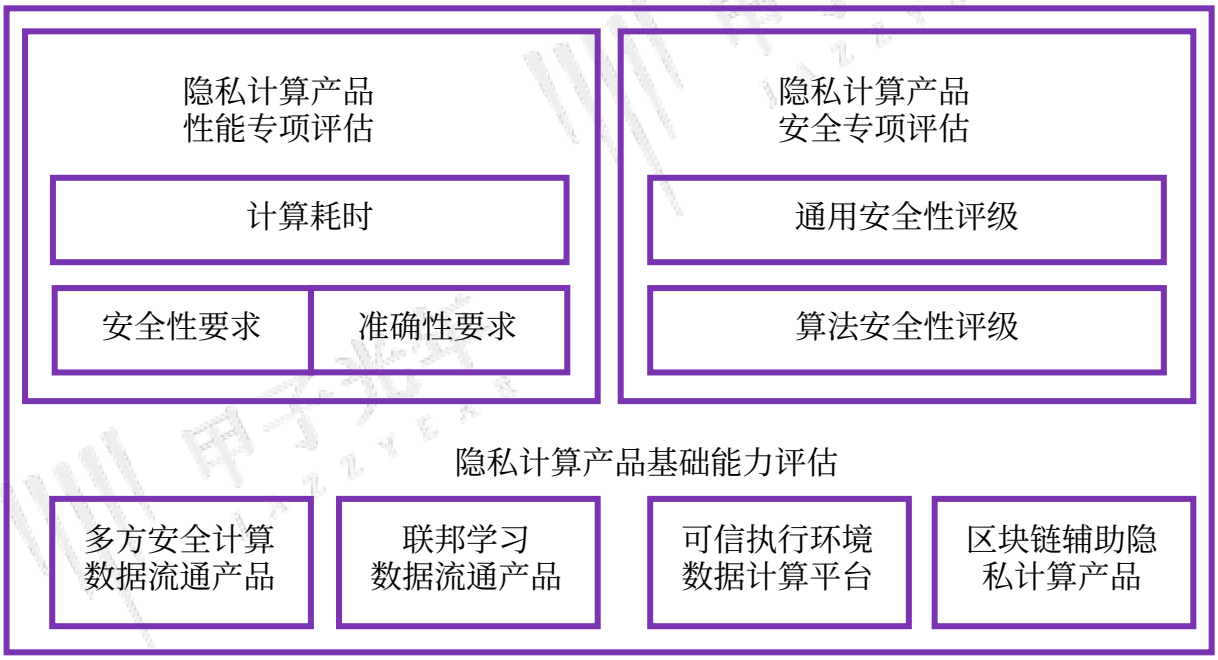
在探讨隐私计算应用的安全信任机制时，一个更值得关注的视角便是从“开源构建信任”出发，来考量如何通过技术的开源开放达成技术信任，进而构建隐私计算应用的安全可信网络和生态。

2.3 隐私计算效果评估体系

行业内隐私计算效果评估体系初步落地，供给端和用户端双向验证

- 当前，隐私计算技术的可用性较之前有很大的提升，使用场景也逐渐丰富，隐私计算的产品化程度逐步成熟，产品数量呈现爆发式增长，产品类型也日趋丰富，隐私计算产业已初步形成。作为新兴的技术，使用者难以综合的判断选择的隐私计算产品的应用效果，因此市场需要建立一套隐私计算产品的规范和产品评估体系。
- 制定共性的评估体系和标准，能够将各类复杂的隐私计算产品转化为易于理解的指标形态。从**供应商**角度来看，共性的评估体系能够有效促进厂商之间的有序发展，建立行业的技术门槛，提升供应商的服务能力。从**用户**角度来看，共性的评估体系能够帮助用户理解技术特点与能力，便于用户选型。
- 根据《隐私计算产品评估体系》（中国信息通信研究院云计算与大数据研究所，北京100191）研究显示，隐私计算评估体系包含基础能力评估、性能专项评估、安全专项评估。基础能力评估能够反映出隐私计算产品功能的通用性程度；性能专项评估能够反映出隐私计算产品在满足安全性和准确性门槛下的计算效率；安全专项评估能够反映出隐私计算产品在各安全维度下的安全等级。

隐私计算产品评估体系



2.3 隐私计算效果评估体系

通过应用实践，可实践、实操性强的评估体系终成型

- 经过对隐私计算行业内头部企业的实地走访调研，以及对隐私计算产品在实际工作中的应用见证，甲子光年总结提炼出了一套隐私计算产品效果评估体系，并对隐私计算产品评估进行了展望。
- 以下，从市场需求、收付模式、产品体验、应用效果的等详细的维度来定性和定量的进行评估：

- 综合来看，隐私计算的效果评估宗旨一定是要合法合规合理的，既需要具备一些普适应的特征，又需要帮助客户提升运营效率，提供差异化的服务和价值实现价值转化，才能实现最终更好的服务客户的目的。
- 以金融行业为例，在营销或者风控场景，对于模型效果的评估常用AUC或者KS来衡量，其中代表着模型对于特定场景中响应客群或者风险客群的刻画能力，越高代表着刻画能力越强。特定到营销场景，一个更为精准的模型会在同等营销预算的情况下，获得更多获客、更多活客、更多召回等，在精准营销环节提供更精准的武器。特定在风控场景，一个更为精准的模型能够识别更多高风险客群、提供更高的授信依据、清退更多高风险客户等，为风控管理提供更多维度的判断。

2.4 隐私计算行业格局

隐私计算技术市场应用广泛，政务、金融、医疗等领域抢先落地

- 在政策和市场需求的双重驱动下，隐私计算行业市场逐渐打开，国内隐私计算市场规模有望超千亿，未来市场规模或将呈指数级增长。
- 隐私计算业务场景的参与方一般会包含三类，即数据的提供方（如移动运营商）、数据的使用方（如金融机构）和隐私计算技术服务提供商（包含集成商）。
- 从系统/软件销售与服务收入角度看，隐私计算作为下一代IT系统的数据合规的刚需，这部分功能升级会占有不同类型IT系统投资的5%-10%左右。在具体的公共服务、智慧城市、数字乡村、数字生活、数字政府、智慧医疗、智慧交通等方面，2021年IT服务市场规模会突破1万亿元，相应的隐私计算系统/软件销售和服务的市场每年在350亿到700亿之间。
- 从隐私计算平台上产生的业务运营分润收入角度看，主要包括（1）不同行业内的低频（如按月/季度调用）的数据建模分析服务；（2）不同行业的高频（近实时调用）的数据模型应用服务；（3）赋能区块链业务服务。

整个隐私计算市场的规模体现在业务上，如图所示：

新药研发、临床辅助诊断、医保风控、科研、医疗AI等

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

联合征信、精准营销、联合风控、客户画像等

精准获客、品牌营销、跨域营销、联名品牌策划等

2.4 隐私计算行业格局

隐私计算技术与能力提供者，及基于关键能力目前国内的市场竞争格局

- 目前，国内隐私计算领域不仅有包括BAT在内的互联网大厂，也有来自于垂直行业的机构（网络安全与大数据企业）以及独立创业公司。各个企业的资源生态、技术路线和行业布局均有所不同，也衍生了不同的战略打法，但起决定性作用的考核标准在于能否为客户带来足够的、特有的数据源以及提供完整解决方案的能力。

- 本报告选取具有典型代表性的企业作为案例进行分析，从而更加清晰地了解目前行业内厂商的综合实力。

隐私计算行业典型企业					
代表企业	资源生态	核心能力	主要技术路线	典型应用行业	价值评估分析
微众银行	开源生态、金融机构	多方大数据隐私计算平台WeDPR-PPC、联邦学习平台FATE	区块链、联邦学习、多方安全计算	金融、政务、医疗等	三大核心技术构建隐私计算能力体系，以最大开源联盟链生态圈、全球首个联邦学习工业级开源框架FATE开源社区服务全行业应用场景
腾讯	腾讯生态、互联网公司	腾讯联邦安全学习、神盾联邦学习平台、底层框架Angle PowerFL	联邦学习	金融、政务等	生态型平台，数据自产自销
蚂蚁	阿里生态、互联网公司	蚂蚁摩斯	TEE、多方安全计算、区块链	金融等	生态型平台，数据自产自销
华控清交	创业公司	PrivPy 多方安全计算平台	多方安全计算	政务、金融、能源等	综合硬实力较强算法安全性、通用性和应用性较强
蓝象智联	创业公司	金融级隐私计算平台GAIA	多方安全计算、联邦学习和区块链	金融、广告等	行业深耕型企业，提供联邦AI和多方安全计算双引擎平台，拥有企业级IT服务能力和资深数据运营能力
翼方健数	创业公司	翼数坊	TEE、多方安全计算、联邦学习	医疗、政务 、金融等	技术精专，从深耕一个行业起步逐步拓展多行业，产品体验感强
洞见科技	创业公司	洞见数智联邦平台（INSIGHTONE）	联邦学习、安全多方计算	政务、金融（银行、保险）等	基于混合计算引擎的硬核技术平台与产品体系，左加数据，右加场景，与异构平台间的互联互通性突出
富数科技	创业公司	FMPC安全计算产品	联邦学习、安全多方计算	金融、医疗、政务等	专注于联邦学习、多方安全计算等，通用性较强
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、TEE	金融、政务等	拥有较丰富的商业化和开发经验
同盾科技	金融垂直行业公司	智邦iBond平台	联邦学习	金融等	在联邦学习、深度学习方面探索，专注智能分析与决策

2.4 隐私计算行业格局

国内代表企业-微众银行

- 隐私计算是涵盖众多学科的交叉融合技术，目前主要的三大支撑技术为区块链、联邦学习和安全多方计算。近些年，微众银行深耕隐私计算，在隐私计算三大支撑技术方面均形成了丰富的实践成果。

- 区块链因其智能合约、共识机制等技术特性，可实现隐私计算过程中可信的跨管理域数据存证和防篡改可验证的数据流通，非常适合隐私计算多边信任关系的建立，成为隐私计算技术中必不可少的选项。隐私计算在区块链基础上，可进一步实现数据价值有序流通、协同生产的自然延伸，这是完善数据基础设施、构建数据价值闭环的关键技术能力。
- 基于多年在区块链领域的攻关和沉淀，微众银行有发展隐私计算的先发优势。目前，微众银行发布的区块链开源核心项目已超过 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，可为隐私计算提供分布式数字身份、数据审计、数据治理、分布式计算任务协调等一系列分布式配套基础设施。
- 微众银行牵头研发的金融级区块链底层开源平台FISCO BCOS，于2017年正式对外开源，具备高性能、安全可控、功能丰富等优势，从国密算法、操作系统、芯片架构到服务器平台，实现全链路国产化支持，为开展区块链应用提供安全可靠的基础设施。其成为国家信息中心顶层设计的国家级区块链基础设施BSN中首个国产联盟链底层框架，汇聚2000+企业机构、40000+开发者建成最大最活跃的国产开源联盟链生态圈，支撑生态内企业数百个应用项目的研发，已有超120个应用投入使用，覆盖健康码跨境互认、政务、监管科技、社会治理、版权保护等业务场景。

- 以联邦学习为代表的人工智能与隐私保护技术的融合衍生是目前主流的隐私计算技术主要方向之一。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，能够在本地原始数据不出库的情况下，通过对中间加密数据的流通与处理来完成多方联合的机器学习训练，能够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，进行数据使用和联合建模。
- 2019 年 2 月，微众银行将自主研发的全球首个工业级联邦学习框架 FATE予以正式发布并全面开源。该项目不仅提供了一系列开箱即用的联邦学习算法、比如LR、GBDT、DNN等，还给开发者提供了实现联邦学习算法和系统的范本，使得大部分传统算法都可以经过一定改造适配到联邦学习框架中来。同时，FATE提供了一套友好的跨域交互信息管理方案，解决了联邦学习信息安全审计难的问题，大幅提升了隐私计算的性能。

2.4 隐私计算行业格局

国内代表企业-微众银行

- 安全多方计算是多种密码学基础工具的综合应用，可基于密码学的算法协议来实现隐私计算，其可在各方不泄露输入数据的前提下完成多方协同分析、处理和结果发布。
- 在安全多方计算方面，微众银行给出了场景式隐私保护解决方案WeDPR，其强项在于安全多方计算、零知识证明、同态加密等密码学技术。
- WeDPR方案组合多种隐私保护策略，满足多变业务流程，适用于联合报表、联合预测、密文投票、密文排名、密文摇号、密文对账等众多需要实现数据隐私保护的典型场景。

安全合规	基于联盟链的可信数据治理，全面支持国密算法，支持身份认证、准入规则、权限控制、监管审计等
全面隐私	可以做到明文数据不出库，相关密文数据用途可限，同时密文计算结果可验，并且密文协作贡献可计量
功能丰富	全面涵盖主流协作模式，不用依赖可信第三方，能够支持任意数量机构的同时参与，也可以进行恶意模型+区块链提供全流程正确性验证
性能优异	5 分钟可以完成亿级数据隐私求交，3 毫秒内可以完成万次联合乘法计算
易学易用	采用模块化算法封装，高级语言和类 SQL 业务逻辑编写，可以实现可视化拖拽和即用即搭
部署灵活	可以实现容器化镜像快速部署，无 TEE 硬件依赖，无平台绑定依赖，且适配小程序/APP客户端

- 基于WeDPR，微众银行自主研发了多方大数据隐私计算平台WeDPR-PPC。这是一个支持多方平等协作和大数据复杂逻辑密文计算的高性能隐私计算平台，并基于区块链和安全多方计算的优势，实现在确权、授权和维权的全生命周期管理下，达到多方数据的联合报表、联合计算、隐私查询、联合建模和预测等。该平台具备十亿级别的大数据处理能力，支持任意多方的隐私数据跨域协作，同时提供横向通用性计算能力和纵向定制型计算能力覆盖全域场景，满足海量数据商业应用场景需求。
- 拥抱开放，微众银行于2021年8月创新性地将WeDPR-PPC的核心功能开放体验，提供开箱即用的隐私计算业务探索体验，在降低隐私计算应用门槛的同时，拉近隐私计算技术和行业潜在应用的距离，更有力地推进有影响力的隐私计算标杆应用落地。

2.4 隐私计算行业格局

国内代表企业-蚂蚁集团

- 蚂蚁链是蚂蚁集团代表性的科技品牌，融合包括区块链、AIoT、智能风控等技术，通过链接各个产业网络，扎实解决行业实际问题，推动区块链技术平民化。在实际应用上，蚂蚁链已携手生态合作伙伴，解决了50余个场景的信任难题。

- 在区块链方面，蚂蚁链 BaaS 平台是其自主研发的具备高性能、强隐私保护的区块链技术平台。平台依托蚂蚁集团支付宝的海量并发技术经验，交易支持秒级确认，提供海量数据存储，具备万级 TPS 的处理能力。

- 蚂蚁链摩斯多方安全计算平台是其自主研发的多方安全计算商用平台，具备功能丰富、扩展性强的多方安全算子库和多方安全计算的高效机器学习算法库，可以实现多方安全联合建模、联合分析、联合规则。平台已规模化在金融行业中实践，赋能数十家金融机构实现联合风控。

- 蚂蚁隐私计算智能服务平台是其基于自主研发 Fascia 联邦学习开发框架与多方安全计算、差分隐私等技术结合实 现更安全的联邦学习产品，可实现联合统计、联合建模。在医疗 行业中，联合阿里云已与大型跨国医疗企业合作应用在疾病诊断、 检查推荐、用药推荐、罕见病预测、质控规则管理等场景中，为 医疗数据治理、全院质控、医学研究、医保风控和临床核心业务 中的痛点难点问题提供解决方案。

- 蚂蚁集团研发了结合虚拟化隔离技术和可信平台模块技术的新型 TEE 技术 HyperEnclave ，支持由用户自主掌控 TEE 信任根；HyperEnclave 可集成国内外内存加密硬件引擎，实现各项 TEE 技术目标。蚂蚁集团开源了 Occlum 项目，并捐赠给机密计算联盟成为联盟官方产品。

- 蚂蚁集团可证去标识适用于多方开展大规模离线数据挖掘以及高性能在线数据分析场景。可证去标识是一种全新的隐私计算技术，允许多方依法合规的使用数据，安全可控的进行数据分析 和计算，同时支持大规模数据和实时计算。

- 蚂蚁集团旗下隐私计算智能服务平台将差分隐私与多方安全计算、联邦学习技术结合，实现全链路的计算隐私保护，已在医疗行业的联合诊断增强中进行探索性应用。

03 PART 隐私计算的发展趋势

3.1 隐私计算技术发展方向

面向市场应用与行业需求，隐私计算的发展方向

根据Gartner的预测，到2025年全球将有一半的大型企业机构在不受信任的环境和多方数据分析用例中使用隐私计算处理数据。虽然目前隐私计算的应用场景主要聚焦于金融、医疗等领域，但随着其产品化、商业化的进程的加速，用户对于隐私计算概念的接受度进一步提升，加之政策领域支持，隐私计算的应用已向交通、教育、工业等领域延伸，并且将形成跨机构、跨行业、跨企业的多类型应用场景，有望在更多地领域进行拓展应用。

（1）政务领域-推进政企数据融合

在国家积极推动政企数据融合、数据生产要素化的大方向下，各地政府积极建立政务数据开放平台、大数据中心，致力于服务各行各业。政务数据通常涉及社保数据、公积金数据、税务数据、生活数据、交通数据等。但是这些数据属于不同部门，“数据孤岛”情况严重，想要共享这些数据存在协调困难、审批手续繁杂等问题。同时这些数据涉及大量公民隐私，管控更加严格，进一步阻碍政务数据在部门之间、政企之间的合作。

通过隐私保护计算和其他技术的结合，可以有效保护各部门的数据，在一定程度上解决政务“数据孤岛”问题，提高政府治理能力。例如通过视频、位置、交通等多部门数据对治安防控、突发事件进行研判，合理调配资源，提高应急处理能力和安全防范能力。此外，还可以联合多部门的数据对道路交通状况进行预判，实现车辆路线最优规划，减缓交通拥堵。

区块链技术在“电子政务”中的应用

- 构建可信区块链，实现数据安全共享

通过区块链技术独特的密码学机制和共识机制可实现数据的确权、授权，厘清数据责权关系，解决数据交换和流通环节中数据归属不明的痛点。

数据拥有方与数据使用方的所有办事流程交付智能合约，多个节点共同运行和检验，建立可信区块链，实现数据跨层级、跨区域、跨部门、跨业务、跨系统安全共享。

3.1 隐私计算技术发展方向

面向市场应用与行业需求，隐私计算的发展方向

- 降低办事成本，实现数据自动流转

智能合约是基于这些可信的不可篡改的数据，可以自动化地执行一些预先定义好的规则和条款。

由于智能合约嵌在所有数据都以分散的分布式方式存储的区块链中，因此直到流程履行完成，没有人能够控制。

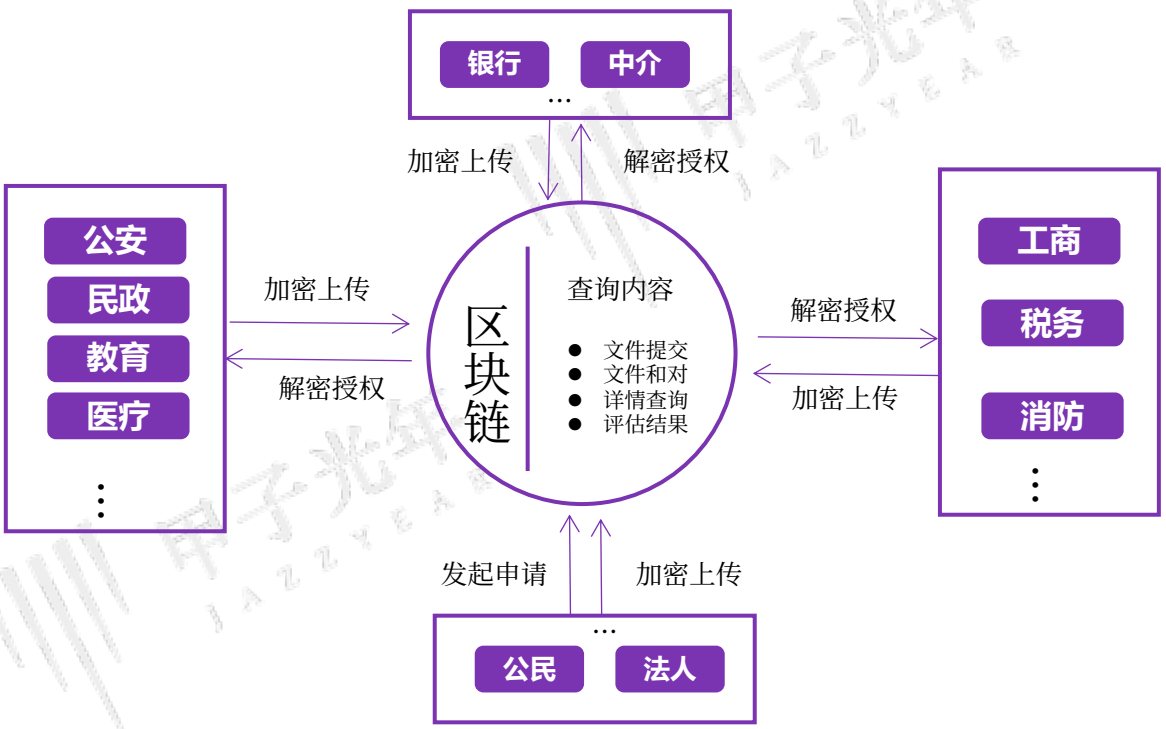
基于区块链技术智能合约，数据将按照数据拥有部门和数据使用部门签订的物理契约自动处理并流转，顺利完成所有流程，让“数据跑路”取代传统的“人跑路”。

- 实现数据全程可追溯信息化监管

分布式账本指的是交易记账由分布在不同地方的多个节点共同完成，而且每一个节点记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证。

以区块链分布式账本为载体，数据使用方和数据拥有方的签发、使用记录、验证记录、状态存储到区块链上，实现数据信息不可篡改，不可伪造且公开透明可监管。

区块链技术在政务中的应用



3.1 隐私计算技术发展方向

面向市场应用与行业需求，隐私计算的发展方向

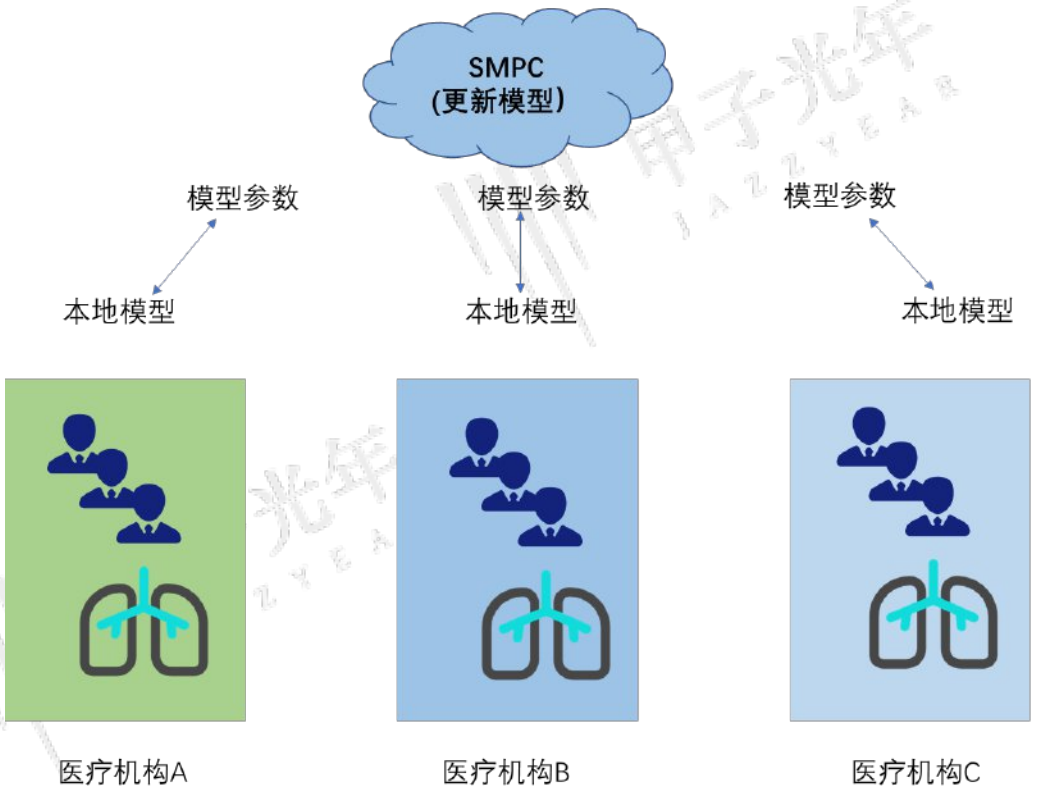
（2）医疗领域-构建新型诊断模式

随着互联网以及电子病历的大量普及，各家医疗机构积累了大量的医疗数据，这些数据对于病人来说是极其敏感的。随着人工智能和医疗的紧密结合，越来越多的个人数据被用于临床诊断、医学研究、公共健康等各个方面，这就增加数据泄露的可能性。

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。

为了应对新冠肺炎疫情带来的医疗挑战，医疗机构需要在全球范围内共享新冠肺炎疫情数据。如通过人工智能识别肺部X 光图像来诊断新冠肺炎。各医疗机构先在本地建立模型，再通过SMPC等技术联合其他医疗机构更新模型参数，在保护各方数据隐私安全前提下，提高图像模型诊断能力。

新冠人工智能联合诊断示意图



3.1 隐私计算技术发展方向

面向市场应用与行业需求，隐私计算的发展方向

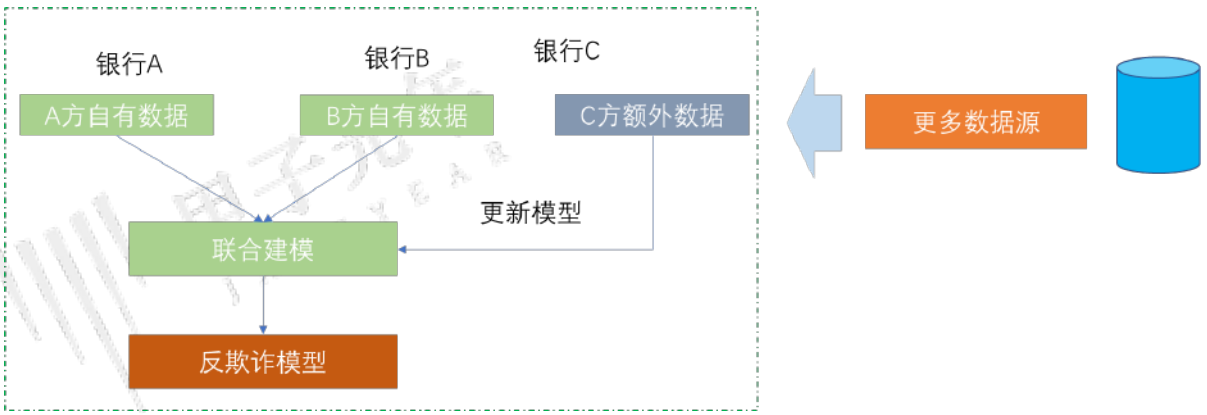
（3）金融领域-提升客户模型精准度

尽管金融数据在体量、维度、价值等方面具有一定优势，但是这部分数据更多涉及客户金融相关的数据，缺少客户的行为数据、场景数据等。具体到某一个金融机构时，其数据的丰富程度更大打折扣。而客户的行为数据和场景数据往往掌握在一些互联网公司和其他数据源公司手中。在信贷风险评估、供应链金融、保险业、精准营销、多头借贷等方面，金融机构都需要和这些数据源公司联合建模，提升模型的精确度。

但是金融数据的安全及风险防范一直是金融机构关注的重点，国家也相继出台金融安全相关政策，不断强化对金融数据安全的重视程度。在传统的数据合作中，通常采用数据脱敏的方式将一方数据给到另一方，并由其进行本地建模。虽然数据脱敏方案实现了一定程度的隐私保护，但仍然能通过收集到的相关数据，损害数据方的利益，甚至侵害客户的个人隐私。此外，经过脱敏处理的数据可用性会受到严重影响。在数据合作之前，传统方案需要通过比较哈希值的方式进行撞库，这样一方就会留存大量的哈希值造成对方客户名单的泄露。

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。

反欺诈联邦学习示意图



3.1 隐私计算技术发展方向

隐私计算面临个人与机构、机构与机构两大场景上的技术发展方向

- 在分布式的商业场景中，数据出现自由流动，如电商的采购行为、社交平台上的交流行为以及在支付场景中的支付行为等。未来，在各个场景中，数据可能会被联合进行挖掘，从而释放出更大的价值。

- 这背后是数据隐私、数据流动的双循环，即个人和机构之间的循环，机构和机构之间的循环。两个双循环推动了整个数据产业的发展，所以隐私计算必然也绕不开这个双循环，其价值就在于要支撑两个循环中的应用场景。

- **从个人与机构的循环来看**，个人和机构之间会有各种数据往来。个人在享受机构提供的各种产品服务的过程中，数据不断地流向机构，同时又不断地会有新的数据产生。在此场景中，已经有非常多的法规要求，在收集用户数据的时候必须经过用户授权。

- **从机构与机构的循环来看**，随着互联网的发展，信息化时代迈向了智能化时代，与此同时，很多产品的服务能力需要多个机构之间相互协作来实现。在此场景中，机构之间需要有很多的相互协作，以进行服务质量的提升和服务能力的挖掘，这意味着未来机构之间可能是联合的数据使用者。

- **这便引申出隐私计算的一个非常重要的落地价值：可实现选择性授权情况下的最小使用，以加强个人隐私信息的保护**。此外，“**坚持最大开放原则，促进公共数据价值的释放**”是隐私计算价值评估的另一重要原则。其主要源自于国家政策的引导，如《数据安全法》就明确，对公共数据鼓励和提倡最大化地去释放和挖掘，鼓励构建政务数据开放平台，将政务的公开数据更大地释放给全社会、全产业。基于未来政务数据公开的大背景下，如何使用好公共数据来推动产业的发展，隐私计算在这块的落地是非常重要的。

3.2 成为隐私计算产业技术与服务的引领者

- 隐私计算领域既有“初生牛犊不怕虎”的创业公司，也有亲自下场的互联网大厂和金融机构。如何在其中脱颖而出，并成为产业技术与服务的引领者，这是业内所有参与者都关心的问题。关于如何构建隐私计算企业的核心竞争力，我们认为有四个方向工作仍需“发力”：

- **合法合规是前提**。随着《中华人民共和数据安全法》发颁布，“合法合规”这一数字经济大背景不仅促进了隐私计算产业的发展，同样也成为隐私计算企业必须要遵守的原则。其中，两个细分问题需要注意：①目前聚焦于隐私计算的合规红线尚不明确，隐私计算企业仍需厘清技术方案与管理实践中的潜在风险点。② 坚持道德操守固然重要，而将这种信念传递给其他利益相关者，包括用户、员工、股东、行业监管者等，同样是相关企业不容忽视的内容，信任关系的建立与此密不可分。

- **技术实力是基础**。打造过硬的技术实力无疑是隐私计算企业脱颖而出的重要条件，尤其是在产业发展的“基建期”。目前，隐私计算的技术效率还有进一步提升的空间。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，计算和建模效率还不能令人满意；同态加密的计算有严重的性能瓶颈。另外，由于计算效率和安全等问题，现有系统产品比较复杂，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低，但单纯售卖系统成本与收益完全不成正比。

- **方案优化是要求**。客户在实际应用场景中，往往需要的是一个业务问题的整体解决方案，如客户需要拉新促销的市场营销技术，而不仅仅是在隐私计算模式下产生新的数据。隐私计算通常为方案中的某一模块，但要满足客户整体需求还存在一定的差距，因为某些需求并不是现有技术就能够解决，有些需求还需要其他合作厂商协作，共同解决问题。

- **信任关系是关键。**作为新技术和新产业，隐私计算的潜在用户及其他利益相关者对它的认识还不充分。目前，在金融风控和市场营销等领域，模型的可解释性、规则简单性是监管机构非常关心的问题，这也是阻碍技术应用的较大障碍。此外，隐私计算计算的安全可靠性是制约用户使用的另一个关键因素。

- 从目前发展阶段而言，隐私计算的技术效果和安全性仍然不能够令人满意，放心大胆地使用。另外，国家还未发布明确的监管文件和技术标准认可隐私计算的安全可靠程度。所以，如何降低客户对于技术应用风险的疑虑，是隐私计算厂商亟待解决的问题，也是成为行业领军者的关键。

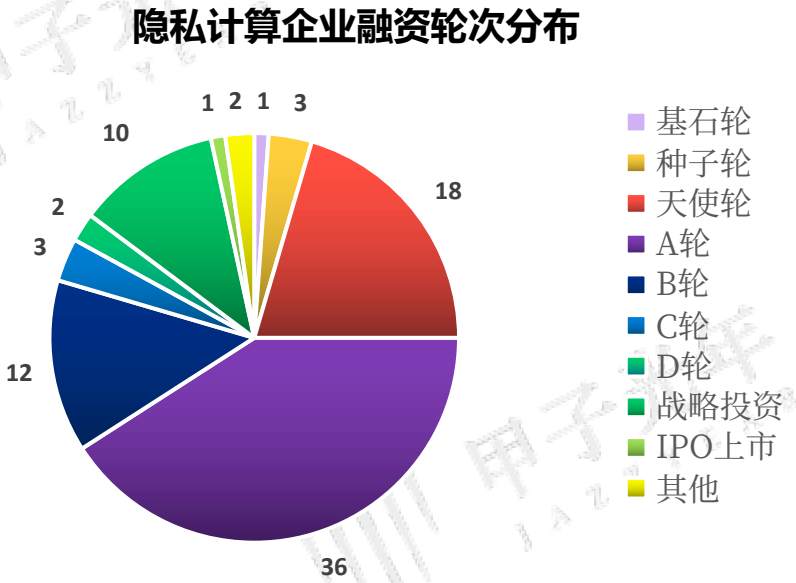
3.3 隐私计算行业融资全貌

隐私计算自2019年以来，受到资本市场密切关注，截至目前获百亿美元级融资

- **全球40余家隐私计算相关企业，超8成获得过融资，近4成处于A轮**

➢ 多位隐私计算从业人员表示，目前隐私计算产业的发展还处于较为早期的阶段，在此阶段，相应的技术厂商数量还不算多，竞争少，赛道相对宽松；大多数企业处于起步阶段，技术相对不够成熟，需要较长时间的迭代和完善。

➢ 根据全网公开数据不完全统计，目前全球隐私计算相关企业超过40家，一共获得过88起融资。从融资轮次来看，较多企业融资分布在天使轮、A轮和B轮，共计66起。



- **获融企业平均每起融资数千万元，中国资方投遍全球隐私计算企业**

➢ 经统计，过往隐私计算行业相关企业共计获得超100亿美元融资，其中千万级别的融资频次最高，占比约7成。

➢ 从隐私计算行业投资方来看，中国的VC/PE机构出手频繁，其中出手频次较多的有高瓴创投、金沙江创投，经纬中国、红杉资本中国、IDG资本、启明创投、中航资本等。

3.3 隐私计算行业融资全貌

企业名称	融资时间	融资轮次	融资金额	投资机构
金融壹账通	2018/1/16	A轮	6.5亿美元	IDG资本（领投）、SBI投资(思佰益)、和暄资本 Hermitage Capital
	2019/12/13	IPO上市	3.59亿美元	
同盾科技	2013/11/1	天使轮	1000万人民币	IDG资本、华创资本
	2014/8/1	A轮	1000万美元	宽带资本CBC（领投）、线性资本、以太创服（以太资本）
	2015/5/20	B轮	3000万美元	启明创投、宽带资本CBC、IDG资本、华创资本、线性资本
	2016/4/13	B+轮	3200万美元	尚城资本（领投）、元禾控股、启明创投、宽带资本CBC、华创资本、IDG资本、线性资本、华兴资本（财务顾问）
	2017/10/10	C轮	7280万美元	信达汉石（领投）、淡马锡Temasek（领投）、天图投资（领投）、尚城资本
	2019/4/25	D轮	1亿美元	招商局资本（领投）、国泰创投（领投）、光大控股（领投）、GGV纪源资本（领投）、信达汉石
	2019/6/30	D+轮	数千万美元	中航资本、浙商创投、广发全球投资基金
华控清交	2018/10/11	天使轮	数千万人民币	清华控股、中互金投资基金管理
	2019/5/30	Pre-A轮	数千万人民币	高榕资本、中关村协同创新基金、海淀园创业中心
	2019/9/4	战略投资	未透露	港交所
锘崴科技	2020/3/17	A轮	数千万人民币	启明创投
翼方健数	2020/7/6	B轮	数千万美元	奇绩创坛、聚源资本-中芯聚源、LDV Partners复盛创投
	2021/7/29	B+轮	超3亿元人民币	未披露
富数科技	2016/9/3	天使轮	未透露	易兴资产、金顾恒资产
	2017/12/1	A轮	5000万人民币	达泰资本、伯藜创投、晨山资本
	2018/5/31	A+轮	数亿人民币	晨山资本（领投）、达泰资本、麦达数字、伯藜创投
	2019/8/14	Pre-B轮	近亿人民币	达泰资本（领投）、宽带资本CBC
	2020/12/30	B轮	数千万人民币	亚信科技、晨山资本
	2021/7/15	C轮	数亿人民币	中国互联网投资基金、同创伟业、义柏资本（财务顾问）
众安科技	2019/7/19	战略投资	19.61亿人民币	百仕达、众安在线
光之树科技	2018/3/13	天使轮	1000万人民币	心元资本Cherubic Ventures、策源创投、巢生资本
	2020/2/19	A轮	数千万人民币	险峰旗云

数据来源：IT桔子、鲸准、天眼查等公开数据，甲子光年整理

3.3 隐私计算行业融资全貌

云象区块链	2016/7/12	天使轮	300万人民币	临潮资产管理有限公司
	2017/9/13	Pre-A轮	数千万人民币	多维资本、中经合集团
	2018/11/19	A轮	数千万人民币	深创投、中经合集团
	2019/9/26	A+轮	数千万人民币	永喜资产
	2019/12/26	A++轮	数千万人民币	未披露
	2020/4/19	Pre-B轮	未披露	竑观投资
	2021/5/27	B轮	过亿人民币	复星集团、深创投
趣链科技	2016/9/1	战略投资	1750万人民币	信雅达、浙大网新、君宝通信
	2017/12/16	A轮	数千万人民币	亚东星辰（领投）、方广资本
	2018/6/3	B轮	15亿人民币	新湖中宝-新湖控股、国投创业、树兰医疗、理想国际、景喆投资、汇仁文曲投资、永滴投资
	2018/10/8	B+轮	数千万人民币	协创资本
	2021/4/9	C轮	数亿人民币	易方达基金（领投）、龚虹嘉、银宏基金
布比区块链	2015/4/6	天使轮	数百万人民币	点亮资本、亦庄互联基金
	2016/8/31	Pre-A轮	3000万人民币	启赋资本、招商局创投、创新工场、界石投资、分布式资本
	2017/11/1	A轮	1亿人民币	长江国弘、博将资本、盘古创富VANGOO、新链创投、步长集团
宇链科技	2018-09-07	天使轮	数百万人民币	浙江清华长三角研究院、勤桦投资
	2020/3/11	Pre-A轮	未披露	思得投资
	2020/10/28	A轮	未披露	享誉时代、天津正泰嘉诚企业管理合伙企业（有限合伙）
	2021/2/19	A+轮	千万级人民币	杭州奈姬企业管理合伙企业（有限合伙）
达朴汇联	2018/3/27	天使轮	未透露	惠能资本
链安科技	2018/3/3	种子轮	数百万美元	分布式资本
	2018/11/7	天使轮	数百万美元	界石投资、盘古创富VANGOO
	2019/11/29	战略投资	1000万人民币	任子行
	2020/1/16	战略投资	未透露	联想创投、分布式资本、盘古创富VANGOO、界石投资、成都创投、复星集团
	2020/2/25	战略投资	未透露	前海母基金
数秦科技	2016/6/23	种子轮	1000万人民币	未透露
	2017/4/26	天使轮	2500万人民币	鼎峰资本、杭州水木基金、嘉慧泽、卢春泉
	2020/4/1	Pre-A轮	数千万人民币	考拉基金、天使投资人、链兴资本（财务顾问）
	2021/5/28	A轮	数千万人民币	万马集团、易方科达、链兴资本（财务顾问）
溪塔科技	2020/9/11	A轮	未透露	招银国际、现在支付iPaynow、大湾区共同家园发展基金
算数力科技	2019/5/15	Pre-A轮	千万级人民币	真格基金、高兴资本
Chainlink	2017/9/22	战略投资	3200万美元	未透露
ARPA	2018/8/20	基石轮	数百万美元	GBIC、Ledger Capital、Arrington XRP、LYVC、Coefficient Ventures、Connect Capital
Phala Network	2020/9/2	战略投资	未透露	币世界、水滴资本waterdrip capital、Blue Mountain Labs、Exoplanet Capital、Incuba Alpha、无极链、瑞新资本、SNZ、IOSG Ventures、Candaq Group

数据来源：IT桔子、鲸准、天眼查等公开数据，甲子光年整理

3.3 隐私计算行业融资全貌

星云 Clustar	2018/5/7	天使轮	数千万人民币	红杉资本中国
	2019/6/4	A轮	数千万人民币	基石资本（领投）、红杉资本中国、山景资本（财务顾问）
	2021/4/15	A+轮	300万美元	基石资本（领投）、香港科技园（领投）
	2021/5/12	A+轮	800万美元	华泰创新（领投）、招银国际
链飞科技	2020-04-26	股权融资	未透露	利欧股份、YEE
洞见科技	2020/6/22	天使轮	2000万人民币	中诚信、心元资本等
	2021/3/18	Pre-A轮	数千万人民币	元起资本、数字中国（飞凡创投）领投，心元资本等老股东跟投
Oasis Labs	2018/7/10	A轮	4500万美元	Pantera Capital、NGC Ventures、高榕资本、Foundation Capital、Data Collective、Accel Partners、Andreessen Horowitz、Polychain Capital、MetastableCapital、Electric Capital
Qedit	2019/5/7	A轮	1000万美元	MizMaa Ventures（领投）、蚂蚁集团、RGAx、Collider Ventures、Meron Capital
数牍科技	2019/9/4	天使轮	数千万人民币	红杉资本中国
Findora Foundation	2020/12/16	战略投资	数千万美元	Polychain Capital（领投）、Powerscale Capital、Cabin VC、Axia8 Ventures、Krypital Group、Allchaineed、Jack Lee
PlatON	2020/10/9	A轮	1200万美元	高山资本（领投）、Hash Global Capital （领投）、新加坡 OUE 集团
蓝象智联	2020/7/16	天使轮	数千万人民币	万向、金沙江创投、联想之星
竹云科技	2014/12/18	天使轮	未透露	中孵创投
	2015/8/15	Pre-A轮	数千万人民币	易合资本、茗晖基金
	2017/1/20	A轮	未透露	粤科创投界、粤科金融
	2018/5/22	A+轮	数千万人民币	中孵创投
	2019/5/13	B轮	数亿人民币	东方富海（领投）、达晨财智（领投）、子于资本
	2019/8/28	B+轮	数千万人民币	投控东海、首建投资本、东海投资
	2020/10/13	战略投资	3亿人民币	红杉资本中国、昆仑资本
冲量在线	2020/11/23	天使轮	数百万美元	IDG资本、源合资本（财务顾问）
数蓬科技	2018/9/21	Pre-A轮	500万美元	经纬中国
	2020/1/7	A轮	1300万美元	时代资本领投，基石资本、松禾资本，经纬中国
	2021/1/5	B轮	2800万美元	高瓴创投领投、金沙江创投跟投，经纬中国、时代资本（Jeneration Capital）

数据来源：IT桔子、鲸准、天眼查等公开数据，甲子光年整理

3.3 隐私计算行业融资全貌

融数联智	2019/12/18	天使轮	未透露	水木清华校友基金、英诺天使基金
	2020/5/1	Pre-A轮	1000万人民币	投资方未透露
	2021/6/1	A轮	未透露	云上大数据基金
Integritee	2021/6/17	种子轮	200万美元	了得资本LD Capital（领投）、FBG Capital、AU21 Capital、DFG、OKEx Blockdream Ventures
矩阵元	2018/6/28	天使轮	未透露	分布式资本、万向控股
同态科技	2020/5/20	股权融资	未披露	金沙江创投
兆物信链	2019/6/18	股权融资	未披露	安医生
	2019/11/9	Pre-A轮	千万级人民币	起源资本、麓谷高新创投
	202年12月16日	股权融资	未披露	麓盛投资
未获得融资企业：慢雾科技、摩联科技、MYKEY、Enigma、MaskBook等。				

甲子光年
JAZZYEAR

鸣谢名单

李辉忠　微众银行区块链隐私计算技术负责人

严 强　微众银行区块链安全科学家

姚 明　洞见科技创始人、董事长

赵 玺　翼方健数联合创始人、首席技术官

黄 斌　华控清交 副总裁

毛仁歆　蓝象智联首席科学家

王 超　蓝象智联技术总监

法律声明

甲子光年
JAZZYEAR

北京甲子光年科技服务有限公司是一家科技智库，包含智库、媒体、社群、企业服务版块，立足于中国科技创新前沿阵地，动态跟踪头部科技企业发展和传统产业技术升级案例，致力于推动人工智能、大数据、物联网、云计算、AR/VR交互技术、信息安全、金融科技、大健康等科技创新在产业之中的应用与落地。

谢谢
THANK YOU