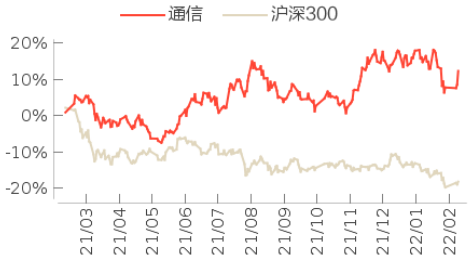
多技术路径齐演进，厂商优先布局隐私计算生态

——区块链系列报告六

行业评级	看好（维持）
国家/地区	中国
行业	通信行业
报告发布日期	2022 年 02 月 22 日



核心观点

- **多条技术路径齐演进，现阶段 MPC、TEE、联邦学习三足鼎立。**隐私计算有许多底层技术可供选择，而隐私计算的实现可能需要多种技术融合应用。现阶段 MPC、TEE 与联邦学习三种技术商用化进程领先，短期内这一技术趋势会被延续。长期来看，MPC、联邦学习需要隐私计算供应商长期积累有效数据并迭代、优化算法，而 TEE 需要在此基础上对于底层芯片做出优化设计。综合而言，TEE 对于供应商的软硬件全栈能力要求极高，现阶段中国厂商仅互联网头部厂商可以实现。出于成本考虑，MPC 与联邦学习的应用占比或将增加。
- **企业难以凭借单一的竞争优势建立隐私计算生态，算法与数据缺一不可。**隐私计算解决方案对其底层技术的成熟度依赖极高。但仅凭借隐私计算底层技术，企业无法为用户提供有效的服务。用户的需求往往对于数据的需求极为定制化、专业化，因此隐私计算供应商需要为用户提供有效的脱敏数据。另一方面，脱离了大量的有效数据，隐私计算的算法演进速度与优化程度也都将受到影响。因此，隐私计算生态的建立需要供应商掌握优秀的算法与丰富的数据资源。互联网大厂、深耕垂直场景的初创企业以及产业内头部企业具备这两种资源，为其成功布局隐私计算提供了可能。
- **隐私计算的通用性局限于底层技术，垂直场景算法区分度较高。**隐私计算的底层技术具备通用性，底层平台的建立存在可能。纵观隐私计算发展生态，主要玩家可分为互联网企业、垂直行业内企业与初创企业三类。互联网大厂最具发展通用性底层平台的可能。未来的生态或将基于此底层平台深入发展基于不同场景的垂直解决方案。
- **隐私计算技术开源程度有限，优先布局的厂商具有先发优势。**现阶段中国隐私计算服务商仅腾讯、微众银行、百度、字节跳动与矩阵元进行开源。互联网大厂腾讯的开源集中于底层框架，而百度的开源也采用逐步开放的形式。总体而言隐私计算源代码的开放程度较低，优先布局的厂商在算法端具备优势。后入局的厂商也可凭借自身数据、生态资源实现算法的快速升级。生态资源更丰富、流量入口更多的后入局者成功概率相对更高。未来发展趋势也存在另一种可能，即当隐私计算开放程度增强或者头部供应商建立隐私计算的底层平台后，一些具备人才资源的初创企业基于底层平台发展专用、垂直的解决方案，占据一定的市场份额。

投资建议与投资标的

- 隐私计算的底层技术具备通用性，底层平台的建立存在可能，从 2018 年开始，头部互联网企业，中国联通、中国电信、中国移动等通信运营商，富数、同盾、星环等成熟的网络安全及大数据公司以及华控清交、锘崴、洞见等初创型科技企业，已接连入局隐私计算。建议关注布局隐私计算技术的运营商中国移动(600941，未评级)、中国联通(600050，未评级)、中国电信(601728，未评级) 。

风险提示

- 安全多方计算、联邦学习、机密计算等技术研发进展不及预期；市场竞争加剧

证券分析师
张颖 021-63325888*6085
zhangying1@orientsec.com.cn
执业证书编号：S0860514090001
香港证监会牌照：BRW773

联系人
周天恩 zhoutianen@orientsec.com.cn
王婉婷 wangwanting@orientsec.com.cn

相关报告

区块链新基建逐步落地，美联储发布首份数字货币白皮书：——区块链双周报（01.12-01.26）	2022-02-06
电力信息系统将受益于电网智能化加速改造进程	2022-01-18
全球 VR/AR 生态逐步完善，平台与内容型厂商加速布局	2022-01-17

目录

图表目录

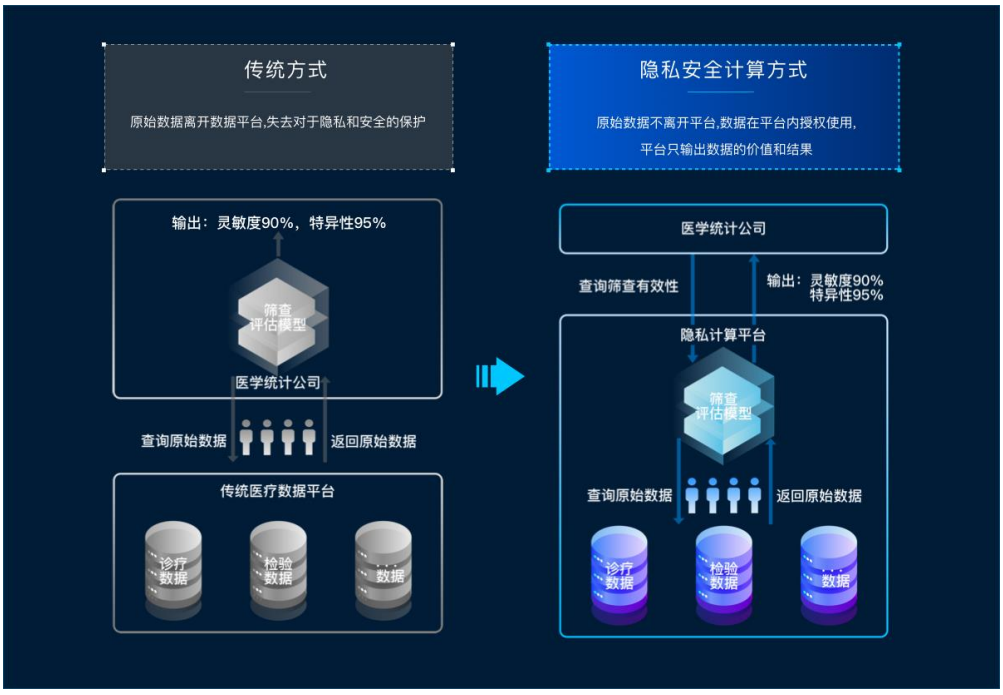
一、 隐私计算融合多领域技术，可实现“数据可用不可见”

1.1、 隐私计算可在对数据形成保护的前提下实现数据价值挖掘

数据是数字经济时代的新型生产要素，其重要意义已被各国政府充分重视。聚合多维、海量数据，挖掘数据内在价值，多元化利用数据价值已成为全球各产业机构的战略重点。**隐私计算指在提供隐私保护的前提下，实现数据价值挖掘的技术体系。**面对数据计算的参与方或其他潜在信息窃取者，隐私计算可实现数据处于加密状态或模糊（非透明）状态下的计算，已实现对各参与方信息的保护。隐私计算在保证数据安全的基础上实现数据的流动与共享，真正实现“数据可用不可见”。

隐私计算技术是人工智能、密码学、区块链、数据科学及计算芯片等领域的交叉融合。隐私计算以现代密码学为核心，协同计算机体系结构、计算复杂性理论、信息论、统计学、抽象代数、数论等理论共同发展。

图 1：隐私计算可以在不分享数据的条件下分享数据的价值



数据来源：翼方健数，东方证券研究所

隐私计算保障的目标覆盖数据应用的全环节，包括：

1. 隐私计算保障数据在数据方的静态存储风险；
2. 隐私计算保障数据从数据方传输至计算方的传输风险；
3. 隐私计算保障数据在计算方计算时的隐私风险；
4. 隐私计算保障数据在计算方计算后的隐私风险；

5. 隐私计算保障计算结果在计算方法的静态存储风险；
6. 隐私计算保障计算结果从计算方法传输至结果方的传输风险；
7. 隐私计算保障计算结果方的静态存储风险。

图 2：隐私计算流程示意

数据来源：中国信通院，东方证券研究所

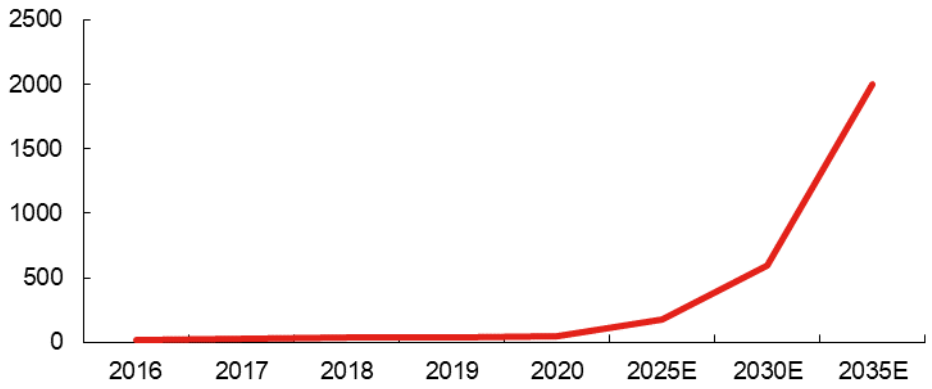
1.2、 隐私计算受到大数据融合应用和隐私保护的双重需求驱动

根据中国信通院数据，全球数据量处于指数增长的阶段。2020 年全球数据产生量约为 48ZB，未来全球数据产生量将迎来爆发式增长，2035 年全球数据产生量预计将超过 2,000ZB。

一方面，大数据在得到使用后才会产生价值，而现阶段全球大数据“数据孤岛效应”显著，数据间缺乏关联性，许多数据库之间彼此无法兼容。此外，企业对于数据信息保护的意识逐渐提升，数据孤立性的降低难度也逐渐提升。但企业和组织需要与产业上下游的业务伙伴通过数据流通实现深度合作、提升决策能力、获取竞争优势的诉求仍将长期存在。隐私计算可以从技术角度实现“原始数据不出库即完成数据价值流通”的目标。

另一方面，大数据的应用面临着越来越多的合规风险。中国《网络安全法》及《民法典》的规定，数据处理者在处理数据时应公开收集、使用规则，并经用户同意。近年来，中国对于数据安全管理的规范程度逐渐提升：2019 年 9 月工信部在《工业大数据发展指导意见<征求意见稿>》中说明将在工业领域积极推广多方安全计算基数；2020 年 12 月发改委、网信办、工信部、能源局联合发布《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》，文件指出要加快构建全国一体化大数据中心，加快数据流通融合，强化大数据安全保障。隐私计算可以防止数据信息泄露，解除信任危机，实现大数据应用流程合规。

图 3：全球数据产生量，2016-2035 年预测（ZB）



数据来源：中国信通院，东方证券研究所

政策驱动隐私计算发展空间。中国隐私计算相关法律政策为隐私计算创造了需求，并鼓励隐私计算相关技术的研发与应用。中国通过颁布相关政策法规促进公众隐私保护体系建立，并维护数据权利主体合法权益。同时，通过政策法规的逐步完善，数据应用与安全保护体系的顶层设计不断完善，数据安全与隐私保护合规要求逐步明确，隐私计算的应用场景预计将进一步拓展。

表 1：中国隐私计算相关政策法规

政策名称	政策类别	发布时间	发布主体	政策意义
网络安全法	法律	2016 年 11 月	全国人民代表大会	对数据形成法律保护
民法典	法律	2020 年 6 月	全国人民代表大会	对个人数据信息形成法律保护
个人信息保护法（草案）	法律	2020 年 10 月	全国人民代表大会	对个人数据信息形成法律保护
大数据产业发展规划（2016-2020 年）	发展规划	2016 年 12 月	工信部	通过多方安全计算等隐私计算技术提升数据流通性
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	加强金融、司法、社保、工商、税务、海关、电力、电信等行业的数据融合应用
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	通过多方安全计算等隐私计算技术提升数据流通性
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	将大数据确定为新型生产要素的一种
个人信息安全规范	技术标准	2017 年 12 月	全国信标委	加强个人信息保护规范
个人金融信息保护技术规划	技术标准	2020 年 2 月	中国人民银行	加强个人金融数据保护规范
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	将大数据确定为新型生产要素的一种
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	加强数据流通融合应用，加强数据安全保障

数据来源：全国人民代表大会，工信部，中国人民银行，中共中央，全国信标委，国务院，发改委，网信办，能源局，东方证券研究所

二、 安全多方计算、联邦学习与机密计算（可信执行环境）是隐私计算主要的技术发展路径，商用落地进展较为领先

隐私计算处于技术多路径探索阶段：隐私计算尚处于技术探索阶段。目前隐私计算主要的技术路径包括多方安全计算、联邦学习、机密计算（包括可信执行环境）、差分隐私（包括本地差分隐私）、同态加密、零知识证明等。从已商用场景分析，安全多方计算、联邦学习与机密计算商用进展较为领先，零知识证明主要被运用于区块链场景中。

表 2：隐私计算技术路径对比

技术路径	计算过程保护	计算结果保护	计算性能	计算精度	硬件依赖	理论支持场景	已商用场景	计算模式
安全多方计算（SMPC）	最好	无	较差	最好	无	任意计算	国际：拍卖、薪资统计、密钥管理； 中国：密钥管理、联合建模	分布式
联邦学习（FL）	较好	无	较好	最好	无	机器学习建模	国际：横向联邦学习（Google GBoard）； 中国：纵向联邦学习（金融风控）	分布式
机密计算（CC）	较好	无	最好	最好	有	任意计算	国际：密钥管理； 中国：联合建模、区块链	中心化
差分隐私（DP）	较差	有	较好	较好	无	任意计算	Google Gboard	中心化
本地差分隐私（LDP）	较好	有	较好	较差	无	数据统计	Google Chrome，Apple iPhone	分布式&中心化
同态加密（HE）	最好	无	较差	较好	无	任意计算	无	中心化
零知识证明（ZKP）	较差	无	较差	较差	无	任意计算	区块链	分布式

数据来源：中国信通院、阿里安全、数牍科技，东方证券研究所

2.1、 安全多方计算（Secure Multi-party Computation，SMPC）

安全多方计算由中国科学院院士姚期智于 1982 年提出，解决一组互不信任的参与方各自持有秘密数据，协同计算一个既定函数的问题。安全多方计算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）与隐私信息检索（Privacy Information Retrieval）等关键计算协议。**安全多方技术正不断提升计算效率，降低实施方案设计复杂度。**基于以上特征，隐私计算的优劣势在于：

- **优势：**安全多方计算让参与方（数据拥有者）对其数据拥有绝对的控制权
- **劣势：**安全多方计算的计算量较大，需要极强的硬件性能支撑，安全多方技术受到网络带宽、延迟等因素制约。安全多方计算通用性有限，需要针对特定问题与场景设计专用协议。

图 4：多方安全计算示意图

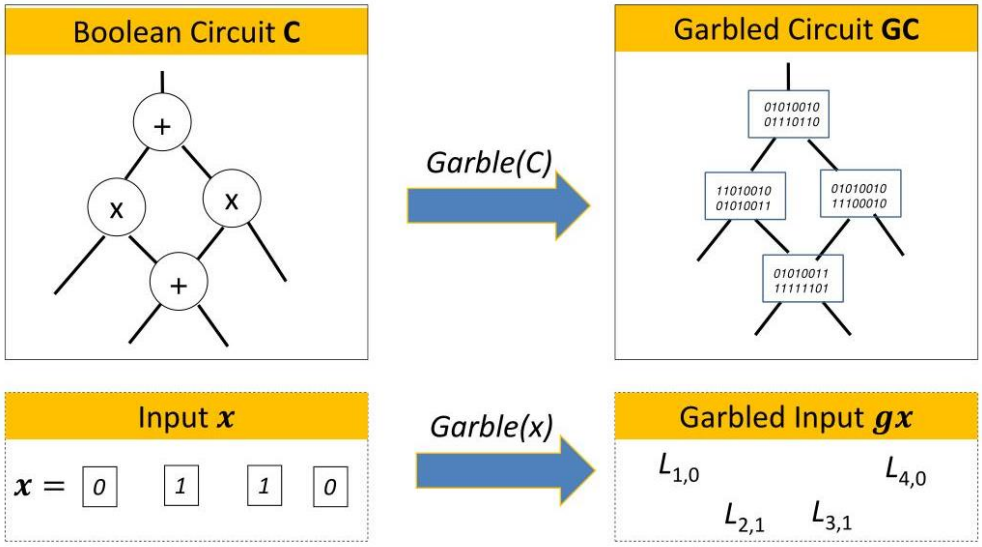
数据来源：中国信通院，阿里安全，数牍科技，东方证券研究所

表 3：安全多方计算关键技术

秘密共享（Secret Sharing）	秘密共享通过将秘密信息分割成若干秘密份额并分发给多人掌管，亿次达到风险分散和容忍入侵的目的
不经意传输（Oblivious Transfer）	发送方拥有若干个秘密消息，但接受者仅能选择并回复其中的一个秘密消息，且无法得到具体是哪一个消息
混淆电路（Garbled Circuit）	核心思想是将任何函数的计算问题转化为由“与”门、“或”门和“非”门组成的布尔逻辑电路，利用加密技术构建加密版本的布尔逻辑电路

数据来源：中国信通院，阿里安全，数牍科技，东方证券研究所

图 5：姚期智院士提出的混淆电路模型

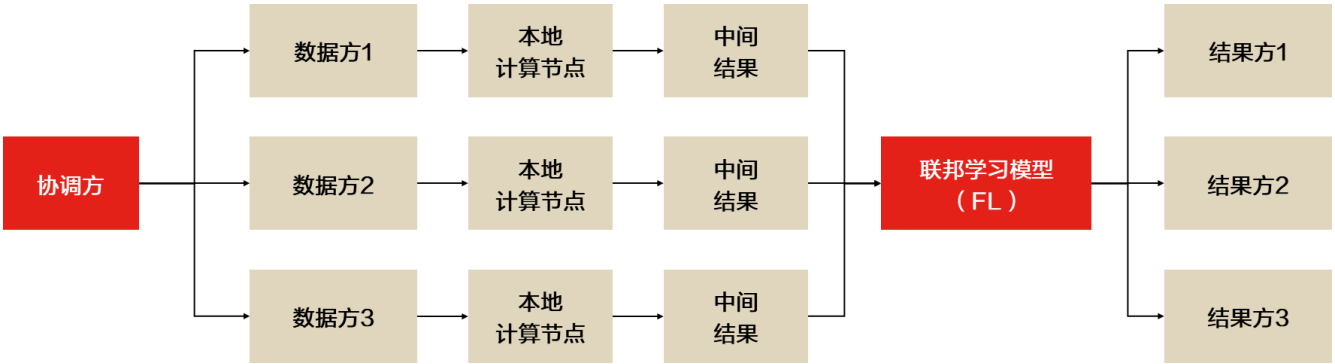


数据来源：Microsoft，东方证券研究所

2.2、 联邦学习（Federated Learning，FL）

联邦学习（Federated Learning）在 2016 年由 Google 最先提出，最先被用于解决安卓手机终端用户在本地更新模型的问题，其设计目标是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。联邦学习可使用的机器学习算法不局限于神经网络，还包括随机森林等重要算法。

图 6：联邦学习架构



数据来源：CSDN，中国信通院，东方证券研究所

针对不同数据集，联邦学习可分为横向联邦学习（Horizontal Federated Learning，HFL）、纵向联邦学习（Vertical Federated Learning，VFL）与联邦迁移学习（Federated Transfer Learning，FTL）：

- **横向联邦学习**主要指在各参与方的数据集特征集重合较大，但是样本重合较小的场景。横向联邦学习把数据集按照横向（即用户维度）切分，并取出双方用户特征相同而用户不完全相同的数据进行训练。Google 在 2016 年提出了一个针对安卓手机模型更新的数据联合建模方案：在单个用户使用安卓手机时，不断在本地更新模型参数并将参数上传到安卓云上，从而使特征维度相同的各数据拥有方建立联合模型。
- **纵向联邦学习**主要指在各参与方的数据集特征集重合较小，但是样本重合较大的场景。纵向联邦学习把数据集按照纵向（即特征维度）切分，并取出双方用户相同而用户特征不完全相同的部分数据进行训练。现阶段，逻辑回归模型、树形结构模型和神经网络模型等众多机器学习模型已经逐渐被证实能够建立在纵向联邦学习体系上。

联邦迁移学习主要指在各参与方的样本和特征重合度都极低的情况下，且在模型训练时各数据集的样本空间与特征空间重叠范围都较小时的场景。联邦迁移学习主要为解决单边数据规模小和标签样本少的问题，从而提升模型的效果。

图 7：星云 Cluster 隐私计算解决方案联邦架构层

数据来源：星云 Cluster，东方证券研究所

2.3、 机密计算（Confidential Computing，CC）/可信执行环境（Trused Execution Environment，TEE）

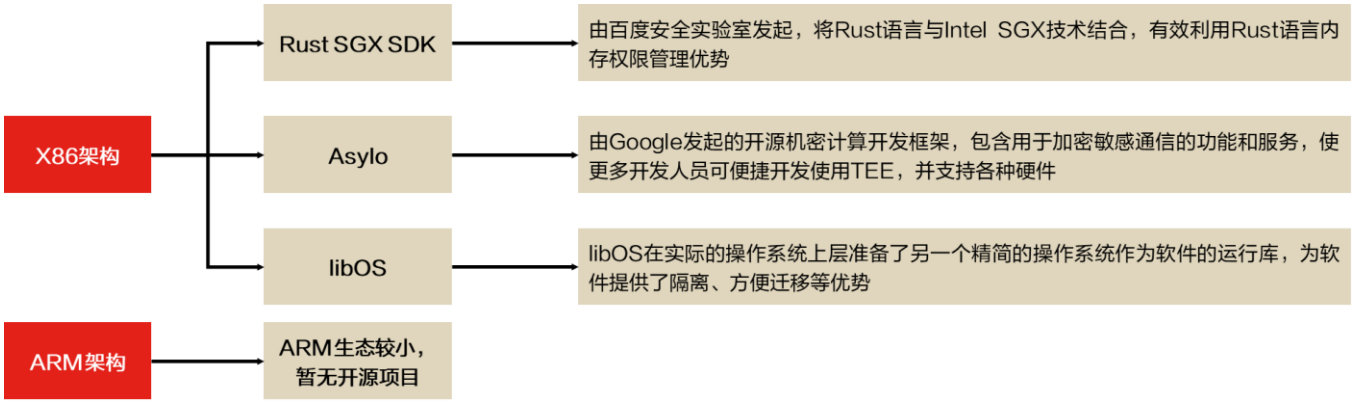
机密计算（Confidential Computing）是一种云计算技术，可在处理期间将敏感数据隔离在受保护的 CPU 区域中。正在处理的数据以及用于处理该数据的技术只能由授权的编程代码访问，并且对任何人或任何其他人（包括云提供商）都是不可见和不可知的。机密计算是一种基于硬件可信执行环境实现数据应用保护的技术。2019 年 8 月，Linux 基金会宣布成立由 Accenture、蚂蚁集团、ARM、Google、Facebook、华为、微软、Redhat 等多家巨头企业组建的机密计算联盟，该联盟针对云服务及硬件生态，致力于保护数据应用中的安全。

机密计算对于隐私计算的意义重大，其主要优势包括：

- 机密计算在使用中也可保护敏感数据，并将云计算的好处延伸到敏感的工作负荷中。
- 机密计算可以有效保护知识产权。机密计算不仅用于数据保护，可信执行环境 TEE 还可用于保护专有业务逻辑、分析功能、机器学习算法或整个应用程序。
- 机密计算可以在新的云解决方案上与合作伙伴安全地进行协作。
- 机密计算可以消除客户在选择云提供商时的担忧。机密计算可以减轻云提供商提供其他竞争性业务服务时的泄密风险。

ARM 与 Intel 在机密运算技术中处于领先地位，ARM TrustZone 与 Intel SGX 是机密计算中较为成熟的两项技术。ARM TrustZone 将系统的硬件与软件资源划分为两个执行环境以确保整体系统的安全性。 Intel SGX 允许应用程序实现一个 Enclave 容器，在应用程序的地址空间划分出一块被保护的区域，将合法软件的安全操作封装在 Enclave 中，为容器内的代码和数据提供机密性和完整性保护，容器之外的任何软件均无法访问 Enclave 内部数据。

图 8：机密计算开源框架



数据来源：全同态加密与区块链，东方证券研究所

图 9：蚂蚁区块链基于 TEE 的隐私保护方案

数据来源：蚂蚁链，东方证券研究所

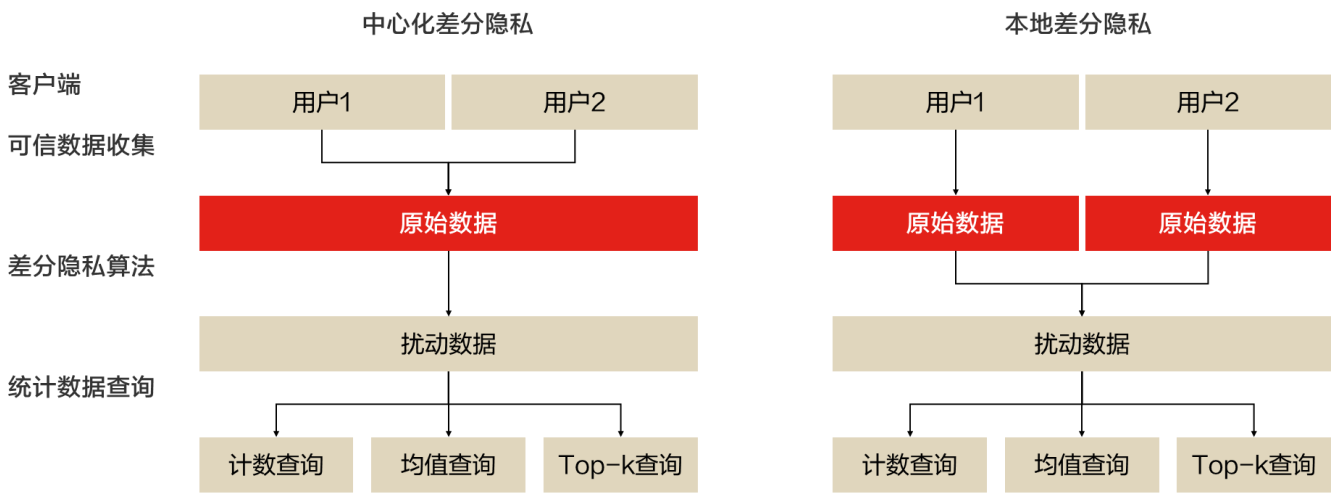
2.4、 差分隐私（Differential Privacy，DP）

差分隐私（Differential Privacy，DP）是密码学中的一种手段，旨在提供一种当从统计数据库查询时，最大化数据查询的准确性，同时最大限度减少识别其记录的机会。差分隐私基于严格的数学理论，通过在计算结果中添加噪声的方法，保证供给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化利用。差分隐私技术也对隐私保护进行了严格的定义并提供了量化评估的方法，对隐私保护水平进行了严谨的证明。

差分隐私通过添加噪声实现隐私保护，这一行为可能对模型的数据可用性及准确率造成影响。过大的噪声会导致数据统计时的可用性和准确度严重受损，因此差分隐私在人脸识别、金融风险剂量等领域无法实现大规模商用。现阶段，差分隐私技术发展的重点为降低噪音对准确率的影响。

本地差分隐私：传统的差分隐私将原始数据集中到一个数据中心，然后在数据中心中对数据施加差分隐私算法，进而对外发布，这种方式也被称为中心化差分隐私（Centralized Differential Privacy，CDP）。但中心化差分隐私需要可信的第三方数据收集者，即保证所收集的数据不会被窃取和泄露。但在实际应用中可信的第三方数据收集者很难被找到。为此，本地差分隐私方案（Localized Differential Privacy，LDP）被提出。本地差分隐私在基于不可信第三方的前提下，其将数据隐私化的工作转移到每个用户，用户自己来处理和保护个人数据，极大地降低了隐私泄露的可能性。本地差分隐私已被 Google、苹果、微软等互联网巨头广泛应用。但相较于传统中心化差分隐私方案，本地查分隐私方案对数据添加的噪声更大，因此在面向数据统计时数据的可用性更低。

图 10：中心化差分隐私与本地差分隐私区别



数据来源：CSDN，东方证券研究所

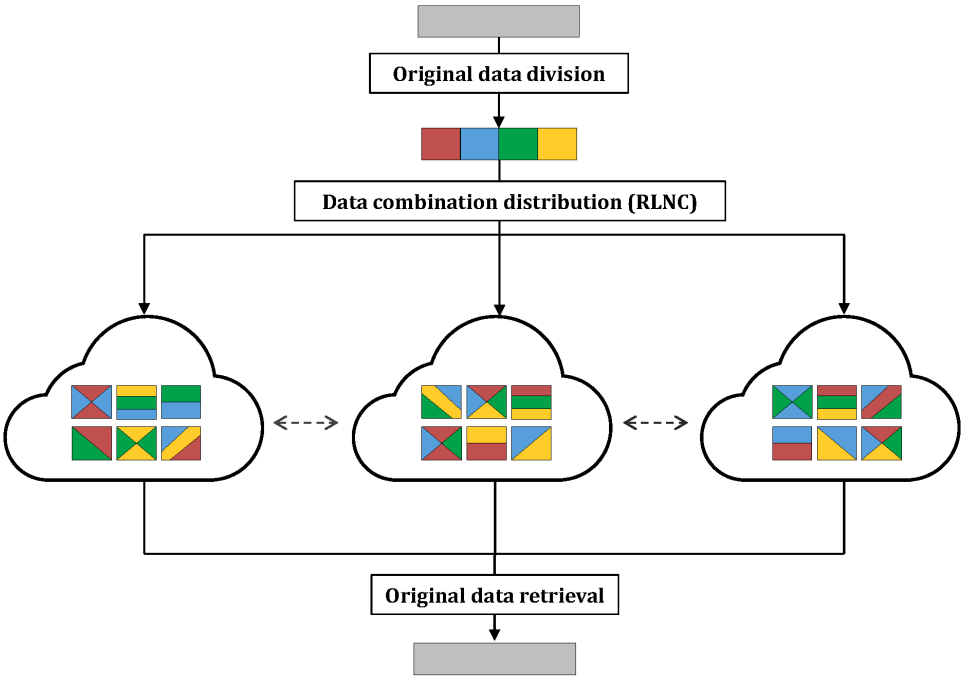
2.5、 同态加密（Homomorphic Encryption，HE）

同态加密（Homomorphic Encryption，HE）系统是一种加密形式，它允许人们对密文进行特定形式的代数运算得到仍然是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果一样。换言之，这项技术令人们可以在加密的资料中进行诸如检索、比较等操作，得出正确的结果，而在整个处理过程中无需对资料进行解密。现阶段同态加密的发展瓶颈在于算法对算力的需求高，且同态加密效率低，因此同态加密暂时不能用于大规模业务。

部分同态加密：现阶段同态加密的实现多通过非对称加密算法，即所有知道公钥的参与方都可以加密、执行密文计算，但只有私钥所有者可以解密。同态加密体系可系统性分为部分同态、近似同态、有限级数全同态与完全同态四类。其中部分同态、近似同态与有限级数全同态均可被划分为部分同态加密方案。部分同态加密（Somewhat Homomorphic Encryption，SHE）只能支持有限的密文计算深度，例如 Paillier 支持密文间的加法运算但不支持密文间的乘法运算，BGN 支持密文间无限次加法运算与一次乘法运算。由于部分同态加密的局限性，一般不会被用于独立建设一个隐私计算方案，而部分同态加密多用于联邦学习方案中的安全增强。

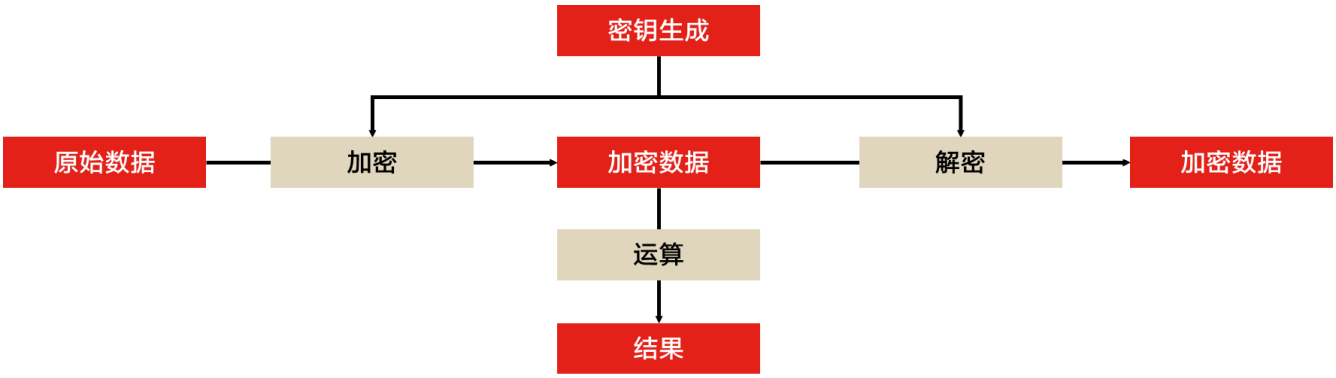
全同态加密（Fully Homomorphic Encryption，FHE）系统没有任何计算方法的限制，用户可以在没有密钥的情况下，把密文任意的组合起来，形成新的密文，并且新的密文可以在任意计算复杂度的情况下被还原成原文。支持近似小数计算的 CKKS 方案相助提升了全同态加密的计算性能，但全同态加密的计算的算力要求仍极高，现阶段尚未大规模商用。

图 11：Google 全同态加密示意图



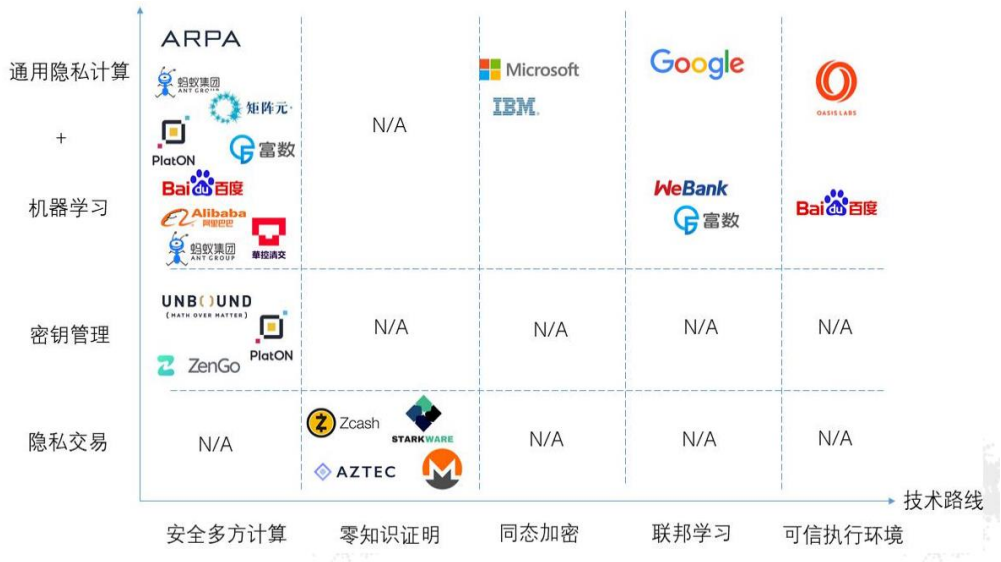
数据来源：MDPI，东方证券研究所

图 12：同态加密流程示意



数据来源：中国信通院，东方证券研究所

图 13：隐私计算技术企业图谱



数据来源：陀螺研究院，矩阵元，东方证券研究所

三、 隐私计算的商用：在可预见的未来，隐私计算将广泛应用于政务、金融、医疗、交通、营销等多个行业

隐私计算是涵盖数据的生产、存储、计算、应用等信息流程全过程中面向隐私保护的计算系统与技术，可在保证原始数据安全隐私性的同时，实现对数据的计算和分析。由于其在多数据流通融合中保护隐私安全的显著效果，隐私计算在政务、金融、医疗、交通、营销等多个行业中均存在广泛的应用场景。

图 14：百度 MesaTEE 开源适用场景

数据来源：百度安全，东方证券研究所

金融：金融与数字化技术的融合程度加深，跨领域的融合应用不断强化，数据的共享与开放正成为金融行业新的趋势。为了保障金融用户与金融企业的隐私安全，隐私计算在金融领域中应用前景广阔，在信贷风险评估、供应链金融、保险业、精准营销、多头借贷中均能发挥重要作用。一般情况下，单一金融机构自有数据量较小，建模样本数量不足，联合多家机构进行联合建模会涉及数据安全风险。而通过联邦学习建模，可以将多家机构数据在不泄露数据的情况下融合应用，提高模型的准确性。而且当金融机构获得新的相关数据时，可及时更新模型，使其他金融机构也可快速具备预测与识别能力。

政务：中国正积极推动政企数据融合、数据生产要素化发展，各地政府也建立了政务数据平台与大数据中心。中国政府中有大量社保数据、公积金数据、税务数据、交通数据等。但这些数据属于不同的部门或地区，存在极强的“数据孤岛”现象，融合应用这些数据需要极为繁琐的审批手续。此外，这些数据涉及公民隐私，将这些数据的价值加以有效利用的难度极大。通过隐私计算与其他技术的结合，可有效保护各部门的数据，部分解决“数据孤岛”问题，提高政府数据使用价值。

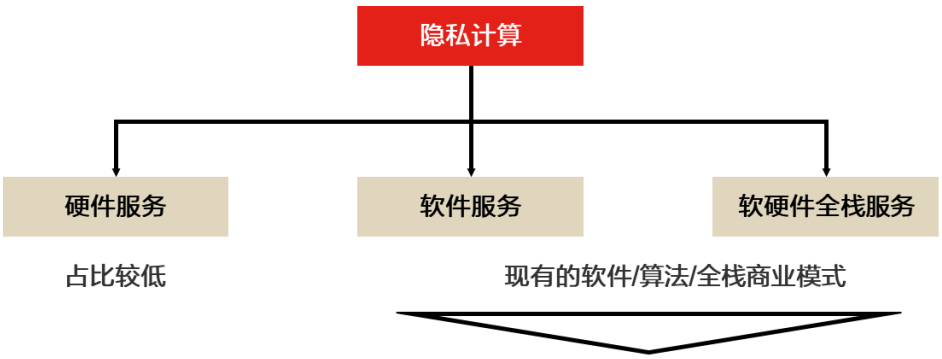
医疗：在医疗健康行业，人工智能与大数据的应用主要是将大规模的病例与病情数据进行深入挖掘，通过建立机器学习与模型训练，提高医疗科研与病情推断的效率，促进整个医疗服务的精确度提升。但医疗数据对于患者而言极为敏感，且现阶段建立全国统一的医疗信息系统成本过高。隐私计算为这一痛点提供了解决方案。通过隐私计算对不同数据源进行横向与纵向的联合建模，保证各方医疗数据安全。医疗机构可以在本地先建立模型，再通过 SMPC 等技术联合其他医疗机构更新模型参数，以最安全、最高效的方式提升模型诊断能力与诊断准确率。

交通：智能交通系统的建立依赖定位数据、个人数据、政务数据、道路数据等多种数据的一体化。由于涉及范围的广泛性以及管理权属的分散性，交通数据极易形成数据孤岛。安全多方计算、零知识证明等隐私计算数据可以帮助交通数据有效打破信息壁垒。隐私计算技术可以通过视频、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。隐私计算也能联合多部门的数据对道路交通状况进行研判，实现车辆路线最优规划，减缓交通拥堵。

营销：联邦学习技术可以帮助营销联合建模，提升营销效果和用户体验。在营销场景中，数据方与营销方均拥有一部分数据，数据方拥有用户画像等流量数据，营销方拥有营销场景数据，而双方均不想共享这一部分核心数据。联邦学习可以在保护双方各自的数据安全的情况下输出建模结果，有效提升营销模型精准性，提高营销效率。

隐私计算尚未广泛商业化应用，商业模式亦处于探索阶段。隐私计算服务分为硬件、软件及全栈服务三类。其中，纯硬件服务在隐私计算的服务中占比极低，软件/全栈服务的商业模式可模仿主流算法/软件成熟的商业模式。

图 15：隐私计算商业模式



销售模式	**一次性付费** 隐私计算供应商为用户搭建隐私计算技术系统/平台/模型后一次性收取所有相关费用，商业模式较简单
服务模式	**定期收费** 隐私计算供应商需要对软件系统进行日常维护及迭代。但这种方式的缺陷是付费方式较为繁琐，客户往往需要反复申请内部项目款审批流程
调用模式	**按需/用量收费** 按需收费在云时代应用占比逐渐增加，调用模式下收费标准会根据数据种类和价值决定，收费标准也会随着时间改变而逐步优化
分润模式	**按结果收费** 分润模式类似代理模式，客户不需要承担初期技术搭建费用，但在新业务开展后需与服务商分成。分润模式多存在于大型集团内部，难以广泛推广

数据来源：中国信通院，东方证券研究所

四、 隐私计算玩家现状：MPC、联邦学习成为主要技术路径

隐私计算主要玩家包括互联网公司与初创企业，MPC、联邦学习成为各企业主要技术路径，TEE、区块链为次要技术路径；现阶段金融为隐私计算主要应用场景，部分企业围绕政务、营销、医疗等垂直场景打造解决方案。

表 4：各公司隐私计算技术路径与主要产品对比

企业	类型	核心产品	技术路径	是否开源	应用行业
微众银行	互联网银行	FATE WeDPR	联邦学习、区块链	是	金融

腾讯	互联网公司	腾讯安全联邦学习 底层框架 Angel PowerFL 神盾联邦学习平台	联邦学习	底层框架开源	金融、政务
蚂蚁	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	MPC、TEE、联邦学习	逐步开源	政务、舆情
字节跳动	互联网公司	Fedlearner	联邦学习	是	金融、教育、营销
京东数科	金融科技公司	Fenlearn	联邦学习	否	金融
同盾科技	金融科技公司	智邦 iBond 平台	MPC、联邦学习	否	金融
光之树	初创企业	天机可信计算框架 云间联邦学习平台	MPC、TEE、联邦学习	否	金融
翼方健数	初创企业	翼数坊	MPC	否	医疗
华控清交	初创企业	PrivPy 多方安全计算平台	MPC	否	金融
数犊科技	初创企业	platone	MPC、联邦学习	否	金融、营销
洞见智慧	初创企业	INSIGHTONE	MPC、TEE、区块链	否	金融、医疗、政务
富数科技	初创企业	Avatar FMPC 安全计算产品	MPC、联邦学习	否	金融、医疗
矩阵元	初创企业	Rosetta PlatONE	MPC、区块链	是	金融

数据来源：微众银行，各公司官网，东方证券研究所

五、 思考：隐私计算发展预测

多条技术路径齐演进，现阶段 MPC、TEE、联邦学习三足鼎立。隐私计算有许多底层技术可供选择，而隐私计算的实现可能需要多种技术融合应用。现阶段 MPC、TEE 与联邦学习三种技术商用化进程领先，短期内这一技术趋势会被延续。长期来看，MPC、联邦学习需要隐私计算供应商长期积累有效数据并迭代、优化算法，而 TEE 需要在此基础上对于底层芯片做出优化设计。综合而言，TEE 对于供应商的软硬件全栈能力要求极高，现阶段中国厂商仅互联网头部厂商可以实现。出于成本考虑，MPC 与联邦学习的应用占比或将增加。

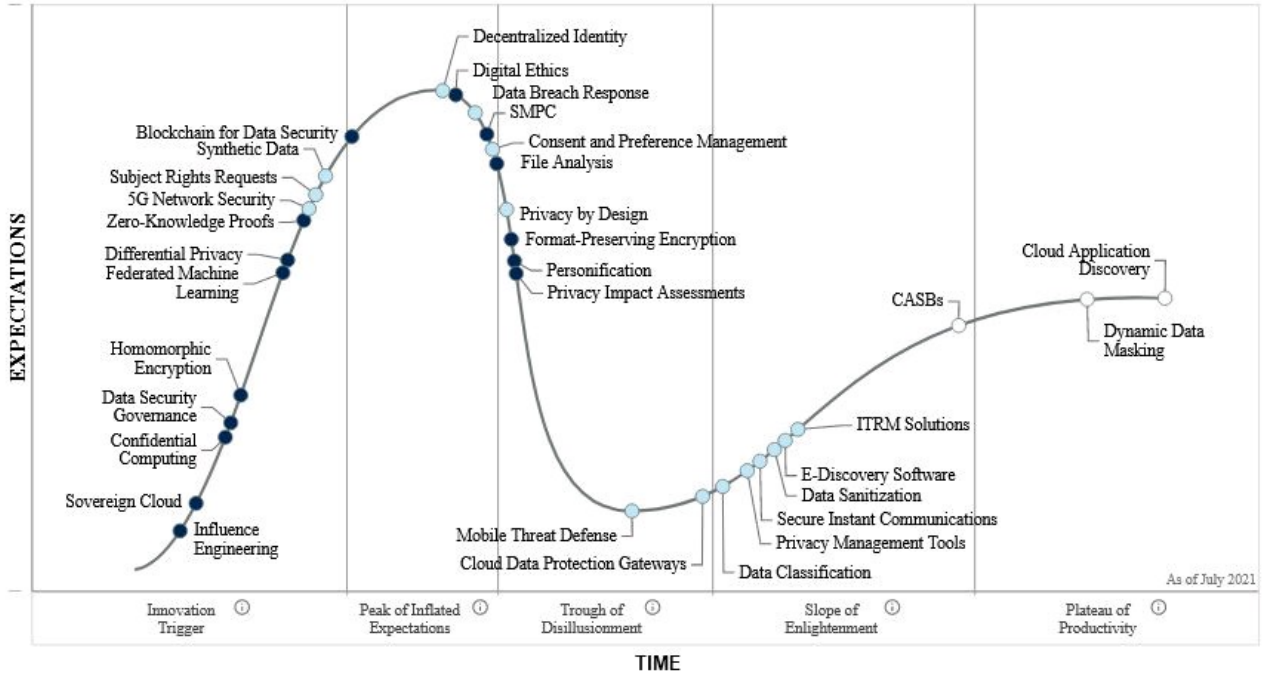
同态加密与差分隐私在隐私计算应用中的落地进程较缓慢。同态加密对于算力资源的需求极高，现阶段常规 GPU 芯片无法满足同态加密所需求的算力，而同态加密的技术演进将不断提升算力需求。因此同态加密的商用可能需要底层根据同态加密算法设计 ASIC 等专用芯片。另一个方面，差分隐私的精准程度不高，长期而言在隐私计算中的独立应用前景较窄，但可成为辅助数据安全与数据加密的增强应用。

企业难以凭借单一的竞争优势建立隐私计算生态，算法与数据缺一不可。隐私计算解决方案对其底层技术的成熟度依赖极高。但仅凭借隐私计算底层技术，企业无法为用户提供有效的服务。用户的需求往往对于数据的需求极为定制化、专业化，因此隐私计算供应商需要为用户提供有效的脱敏数据。另一方面，脱离了大量的有效数据，隐私计算的算法演进速度与优化程度也都将受到影响。因此，隐私计算生态的建立需要供应商掌握优秀的算法与丰富的数据资源。互联网大厂、深耕垂直场景的初创企业以及产业内头部企业具备这两种资源，为其成功布局隐私计算提供了可能。

隐私计算的通用性局限于底层技术，垂直场景算法区分度较高。隐私计算的底层技术具备通用性，底层平台的建立存在可能。纵观隐私计算发展生态，主要玩家可分为互联网企业、垂直行业内企业与初创企业三类。互联网大厂最具发展通用性底层平台的可能。未来的生态或将基于此底层平台深入发展基于不同场景的垂直解决方案。

隐私计算技术开源程度有限，优先布局的厂商具有优势。现阶段中国隐私计算服务商仅腾讯、微众银行、百度、字节跳动与矩阵元进行开源。互联网大厂腾讯的开源集中于底层框架，而百度的开源也采用逐步开放的形式。总体而言隐私计算源代码的开放程度较低，优先布局的厂商在算法端具备优势。后入局的厂商也可凭借自身数据、生态资源实现算法的快速升级。生态资源更丰富、流量入口更多的后入局者成功概率相对更高。未来发展趋势也存在另一种可能，即当隐私计算开放程度增强或者头部供应商建立隐私计算的底层平台后，一些具备人才资源的初创企业基于底层平台发展专用、垂直的解决方案，占据一定的市场份额。

图 16：Gartner 隐私计算技术 Hype Cycle，2021



数据来源：Gartner，东方证券研究所

投资建议与投资标的

隐私计算的底层技术具备通用性，底层平台的建立存在可能，从 2018 年开始，头部互联网企业，中国联通、中国电信、中国移动等通信运营商，富数、同盾、星环等成熟的网络安全及大数据公

司以及华控清交、锘崴、洞见等初创型科技企业，已接连入局隐私计算。建议关注布局隐私计算技术的运营商中国移动(600941，未评级)、中国联通(600050，未评级)、中国电信(601728，未评级)

中国移动

12 月 14 日，在由大湾区中央企业数字化协同创新联盟和中央企业数字化发展研究院共同主办的“首届中央企业数字化转型峰会”上，《中国移动隐私计算应用白皮书》正式发布。《白皮书》以探讨隐私计算的关键技术路径为出发点，聚焦国内外隐私计算应用实践，分析了隐私计算的行业发展现状，重点阐述了中国移动在相关领域的实践情况，并进一步从技术、应用、法律等多角度对隐私计算的发展提出展望。

中国联通

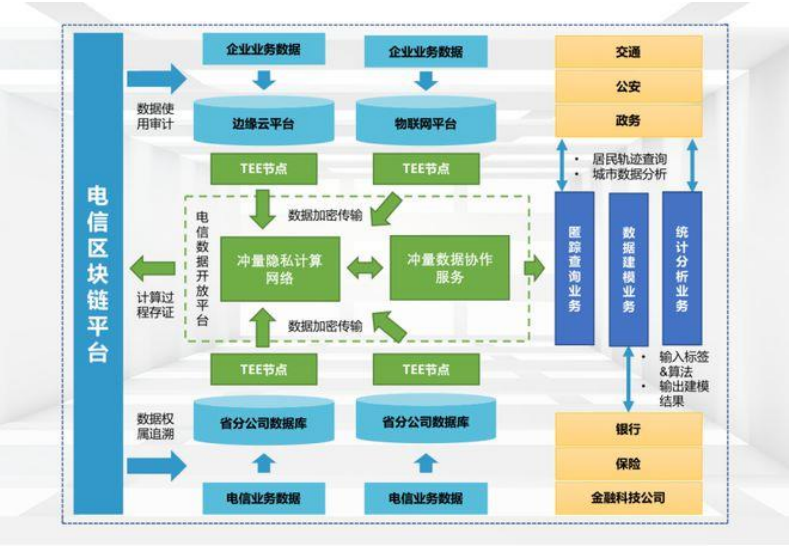
2021 年 8 月，国际电信联盟（ITU）首次发布了隐私计算技术领域的国际标准，该标准由蚂蚁集团、中国联通及之江实验室共同参与制定。

该标准名为 “隐私保护机器学习技术框架”（Technical Framework for Shared Machine Learning System），是以蚂蚁集团的隐私保护机器学习技术为蓝本，定义了参与方角色，功能要求、安全要求，并给出了中心化和分布式两种隐私保护机器学习模式的架构和计算流程。

中国电信

中国电信与冲量在线的合作主要围绕电信集团内部和政企客户之间的数据流通场景展开，基于中国电信自主研发的区块链底层技术，和冲量在线在隐私计算方向的技术创新，通过技术融合解决了数据流通的可信、隐私、安全、公平、可追溯等问题，提供链上数据智能合约化定价与流通的新范式。基于该平台已承载包括电子招投标、清结算、可信财税、国际漫游等多项主要业务场景，已在商用环境下持续稳定运行 2 年以上。

图 17：中国电信区块链平台



数据来源：网易，东方证券研究所

风险提示

- **安全多方计算、联邦学习、机密计算等技术研发进展不及预期：**隐私计算技术路径的研发存在不满足实际业务合规需求的风险；
- **市场竞争加剧：**随着布局隐私计算厂商的数量增加，市场竞争逐渐加剧，可能会挤压企业的利润空间。

分析师申明

每位负责撰写本研究报告全部或部分内容的研究分析师在此作以下声明：

分析师在本报告中对所提及的证券或发行人发表的任何建议和观点均准确地反映了其个人对该证券或发行人的看法和判断；分析师薪酬的任何组成部分无论是在过去、现在及将来，均与其在本研究报告中所表述的具体建议或观点无任何直接或间接的关系。

投资评级和相关定义

报告发布日后的 12 个月内的公司的涨跌幅相对同期的上证指数/深证成指的涨跌幅为基准；

公司投资评级的量化标准

买入：相对强于市场基准指数收益率 15%以上；

增持：相对强于市场基准指数收益率 5%～15%；

中性：相对于市场基准指数收益率在-5%～+5%之间波动；

减持：相对弱于市场基准指数收益率在-5%以下。

未评级 —— 由于在报告发出之时该股票不在本公司研究覆盖范围内，分析师基于当时对该股票的研究状况，未给予投资评级相关信息。

暂停评级 —— 根据监管制度及本公司相关规定，研究报告发布之时该投资对象可能与本公司存在潜在的利益冲突情形；亦或是研究报告发布当时该股票的价值和价格分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确投资评级；分析师在上述情况下暂停对该股票给予投资评级等信息，投资者需要注意在此报告发布之前曾给予该股票的投资评级、盈利预测及目标价格等信息不再有效。

行业投资评级的量化标准：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率在-5%～+5%之间波动；

看淡：相对于市场基准指数收益率在-5%以下。

未评级：由于在报告发出之时该行业不在本公司研究覆盖范围内，分析师基于当时对该行业的研究状况，未给予投资评级等相关信息。

暂停评级：由于研究报告发布当时该行业的投资价值分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确行业投资评级；分析师在上述情况下暂停对该行业给予投资评级信息，投资者需要注意在此报告发布之前曾给予该行业的投资评级信息不再有效。

免责声明

本证券研究报告（以下简称“本报告”）由东方证券股份有限公司（以下简称“本公司”）制作及发布。

本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。本报告的全体接收人应当采取必要措施防止本报告被转发给他人。

本报告是基于本公司认为可靠的且目前已公开的信息撰写，本公司力求但不保证该信息的准确性和完整性，客户也不应该认为该信息是准确和完整的。同时，本公司不保证文中观点或陈述不会发生任何变更，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证券研究报告。本公司会适时更新我们的研究，但可能会因某些规定而无法做到。除了一些定期出版的证券研究报告之外，绝大多数证券研究报告是在分析师认为适当的时候不定期地发布。

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，也没有考虑到个别客户特殊的投资目标、财务状况或需求。客户应考虑本报告中的任何意见或建议是否符合其特定状况，若有必要应寻求专家意见。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投资标的的邀请或向人作出邀请。

本报告中提及的投资价格和价值以及这些投资带来的收入可能会波动。过去的表现并不代表未来的表现，未来的回报也无法保证，投资者可能会损失本金。外汇汇率波动有可能对某些投资的价值或价格或来自这一投资的收入产生不良影响。那些涉及期货、期权及其它衍生工具的交易，因其包括重大的市场风险，因此并不适合所有投资者。

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，投资者自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

东方证券研究所

地址：上海市中山南路 318 号东方国际金融广场 26 楼

电话：021-63325888

传真：021-63326786

网址：www.dfzq.com.cn