隐私计算核心技术架构与行业最佳实践

同盾科技有限公司
陈涛

Agenda

- Overview
- 隐私计算核心技术
- 智邦：工业级平台
- 行业最佳实践

同盾科技：专注决策智能

同盾科技 www.tongdun.cn

专注决策智能

同盾科技是中国领先的人工智能科技企业，总部位于浙江省杭州市余杭区，**专注决策智能先进技术研发和应用**，致力于帮助政企客户防范风险、提升决策效率。多年来同盾科技坚持自主科技创新，多项算法和软件系统已达全球领先水平，并形成了**“基于人工智能的决策智能平台-智策”** 和 **“基于隐私计算的共享智能平台-智邦”** 两大平台，公司聚焦于金融风险、安全风险、政府治理风险三大场景，助力政企客户实现更大的社会价值和商业价值的同时，与客户共同成长。

北京　上海　深圳

广州　成都　新加坡

印尼　马来西亚　阿联酋

客户覆盖

20+	120+	10000+
大行业	细分场景	企业客户

科研实力

300+	300+	数十篇
专利申请	软件著作权	权威期刊收录论文

同盾科技 www.tongdun.cn

同盾智邦：隐私计算多个细分领域的供应商代表

优势：深耕金融领域

- 懂业务，懂产品，懂建模
- 服务上万家客户，长期积累的行业内业务经验有助于帮助客户落地

优势：独家的数据运营能力

- 依托同盾丰富的智能决策产品体系、万级客户生态体系
- 深度融合隐私计算+数据运营，完善的数据要素生态壁垒

优势：场景化联邦平台

- 平台能力“可拆可合”，支持单一/组合场景产品配置
- 场景覆盖全，涵盖联合风控、联合营销、联合运营、智慧政务、智能医疗、智能交通、智慧能源、智慧教育等
- 全链路联邦化，支持联邦评分卡、联邦建模、联邦统计、安全查询、联邦推理等

爱分析《2022隐私计算厂商全景报告》

隐私计算相关测评与获奖情况

测评结果

- ISO/IEC 27701:2019隐私信息管理体系认证
- 信通院多方安全计算产品评测
- 信通院联邦学习产品评测
- BCTC：联邦学习金融应用评测证
- BCTC：多方安全计算金融应用评测证书
- 公安部信息安全等级保护（等保三级）
- 公安三所信息系统安全测评
- 信创：飞腾处理器、银河麒麟高级服务器操作系统V10、红旗服务器操作系统V7.5系列国产信创兼容认证

研发成果

- 20+篇学术论文
- 100+项专利

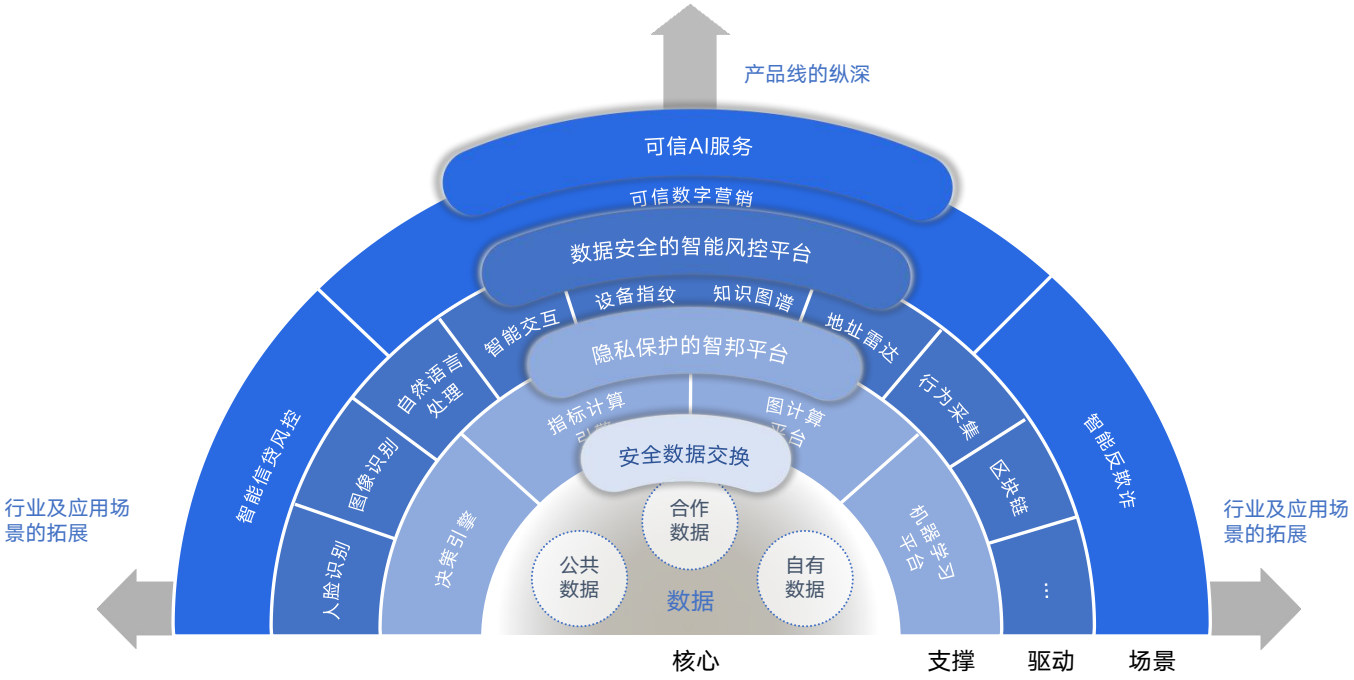
获奖情况

- 第六届世界智能大会：**2022 WIC智能科技创新应用优秀案例**
- 第五届全球人工智能与机器人峰会「AI最佳成长棒-最佳新基建成长奖」「联邦学习探索奖」
- 信通院2020、2021星河案例：隐私计算优秀案例
- AIIA2022可信人工智能实践优秀案例
- 北数所-北京经信局：2022数据安全流通创新应用解决方案竞赛一等奖
- **科技部国家科技创新2030“新一代人工智能”重大项目**
- **全球隐私计算发明专利榜百强**
- **中央网信办人工智能企业典型应用案例**
- 第一届长三角金融科技创新与应用全球大赛「最佳技术创新十佳」
- 算力智库「隐私计算产业30强」「最具价值数据智能产品/解决方案」
- 2021CCF-GAIR峰会 [最佳AI安全产品奖]
- 人工智能产业发展联盟-2021人工智能[创新之星]

隐私计算在决策智能体系中的基础地位

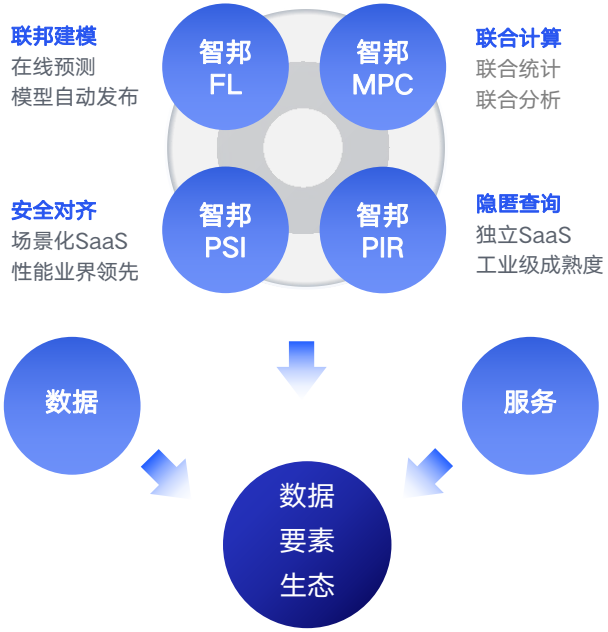
智邦iBond在智能分析决策场景中的支撑作用

基于隐私计算的共享智能平台（智邦） 场景化支撑可信AI服务的开放平台



智邦iBond：基于隐私计算的共享智能平台

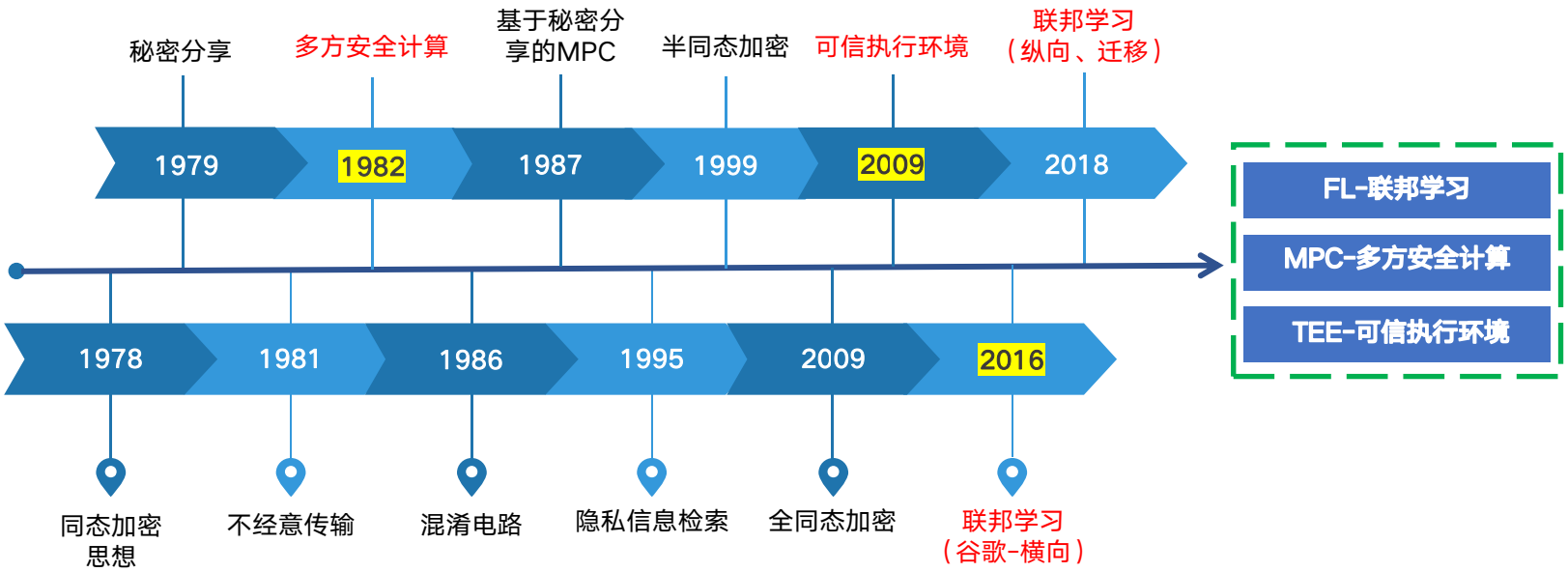
智邦iBond产品矩阵



基于知识联邦的共享智能生态系统

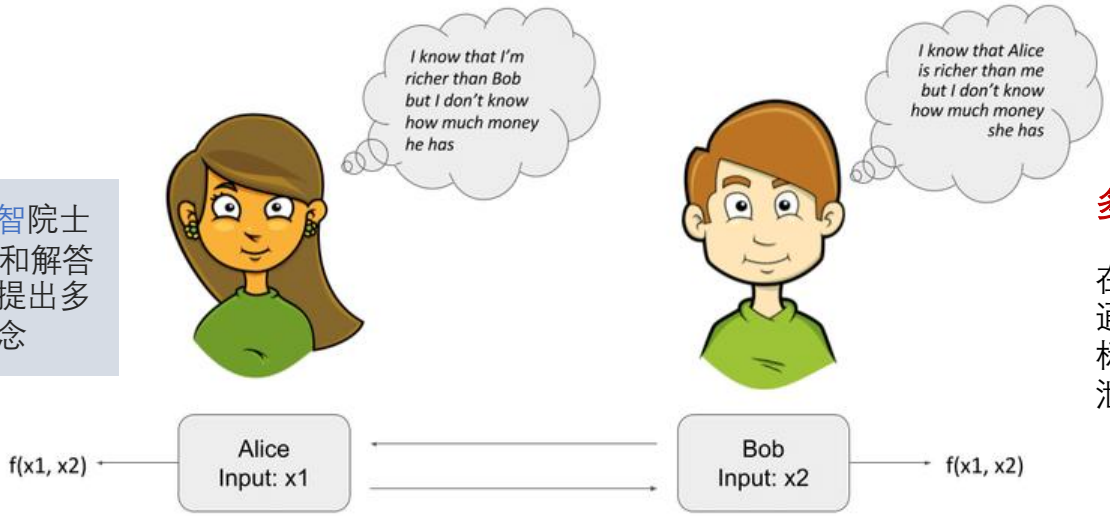
多种场景	智能金融	智能医疗	智能政务	智能城市	智能教育
五大功能	联邦共享	联邦计算	联邦学习	联邦预测	联邦推理
各层典型解决方案	多头共债	智能风控	反欺诈	企业征信	
四大层次	信息层：安全计算、安全查询、密文推理、密文训练	模型层：线性模型、树模型、回归模型、深度模型	认知层：迁移学习、跨媒体表达、集成学习、知识蒸馏	知识层：知识推理、图神经网络、知识融合、知识表达	
智能	机器学习	深度学习	强化学习	元学习	知识工程
数据	跨样本	跨特征	复合型		
技术	联邦学习	多方安全计算	可信执行环境	区块链	
安全	密码学	数据安全	网络安全	分布式系统	

核心技术：隐私计算技术发展历程



核心技术：多方安全计算（MPC）

图灵奖获得者姚期智院士于1982年通过提出和解答百万富翁问题首次提出多方安全计算概念



多方安全计算（MPC）

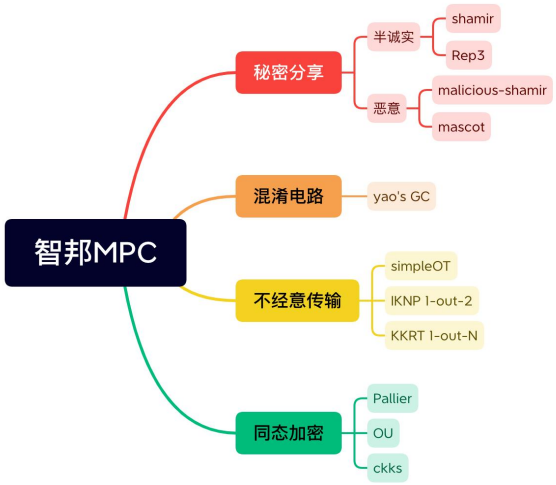
在无可信第三方情况下，通过多方协同完成计算目标，实现除计算结果外不泄露各方的隐私数据

著名的百万富翁难题：
两个富翁比谁更有钱，但不想让对方知道自己有多少钱

多方安全计算技术获取数据使用价值，却不泄露原始数据
实现“数据可用不可见”

核心技术：多方安全计算（MPC）

基于多方安全计算(MPC)技术实现多方的**安全联合统计**、**联合建模**等业务场景需求



第一层次

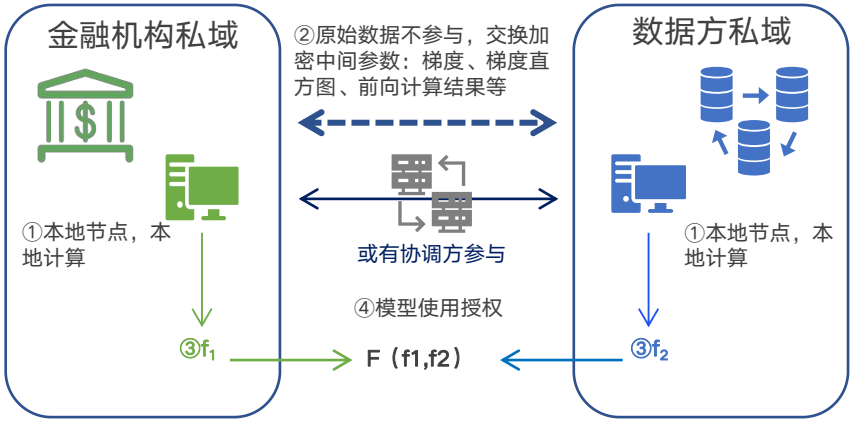
第二层次

第三层次

核心技术：联邦学习（FL）

联邦学习（Federated Learning）：

一种隐私保护的分布式机器学习框架，各个参与方在保证各自原始数据不出域的前提下，通过交互中间数据，协作完成某项机器学习任务



A：数据安全方面：

1）原始数据不出门，参与各方本地建模；

2）没有敏感数据流通，交互加密中间值；

B：模型安全方面：

1）参与方只有自己模型权重，整个模型被保护；

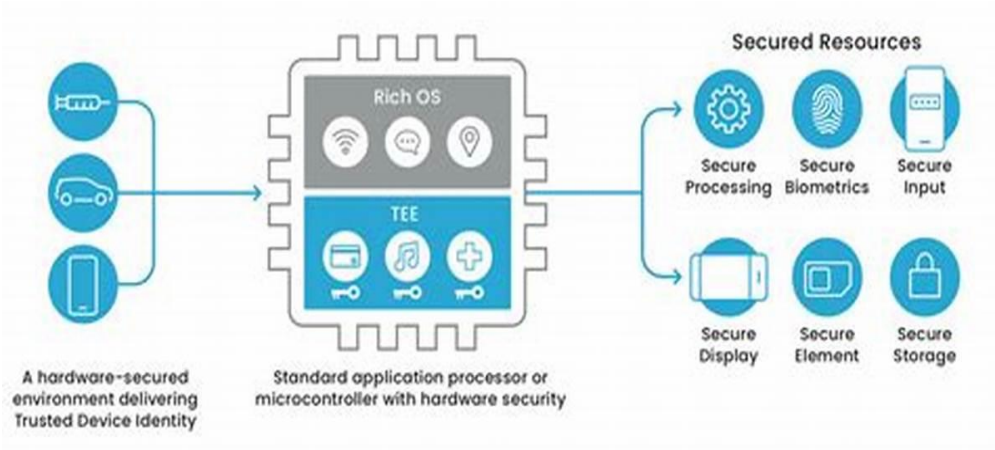
2）当采用多方安全计算的方式，模型以碎片化方式存储；

核心技术：可信执行环境（TEE）

可信执行环境（Trusted Execution Environment）：

一种通过软硬件方式构建一个安全隔离区域，保证在安全隔离区域内部加载的代码和数据的机密性和完整性得到保护

典型TEE：Intel的SGX，ARM的TrustZone、AMD的SVE、海光CSV等



底层硬件：

TEE将多方数据集中到可信硬件构造的可性执行环境中一起进行安全计算

基础算法：

为保证传输至可信执行环境中数据的安全性，常结合密码学算法来实现加密和验证方案

应用角度：

TEE可支持多方数据的联合统计、联合查询、联合建模及预测等多种安全计算应用

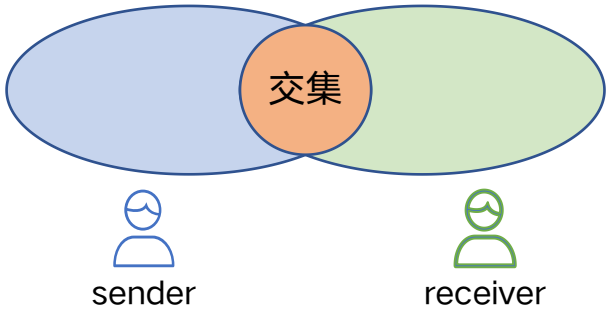
核心技术：安全隐私求交（PSI）

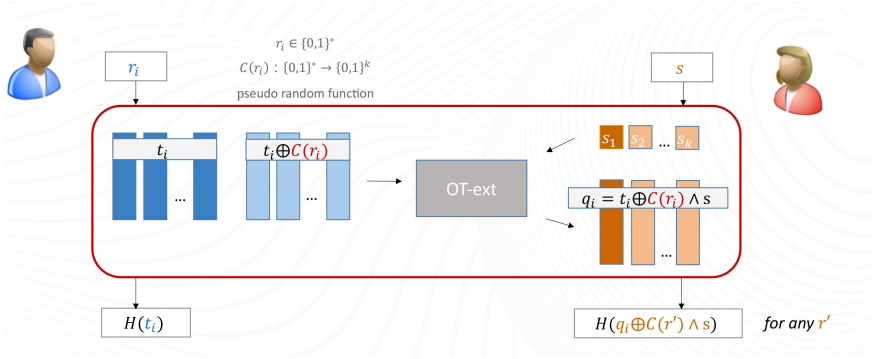
安全隐私求交(PSI)目的：

- 获得交叉用户，进行营销推广
- 获得交叉用户，进行跨特征联邦学习

方案特点：

- 保护交集外的用户信息





核心技术：隐匿查询（PIR）

隐匿查询(PIR)的目标：

保证需求方向服务方(数据提供方)提交查询请求时，在查询信息(查询ID或查询条件)不被感知或泄露的前提下完成查询

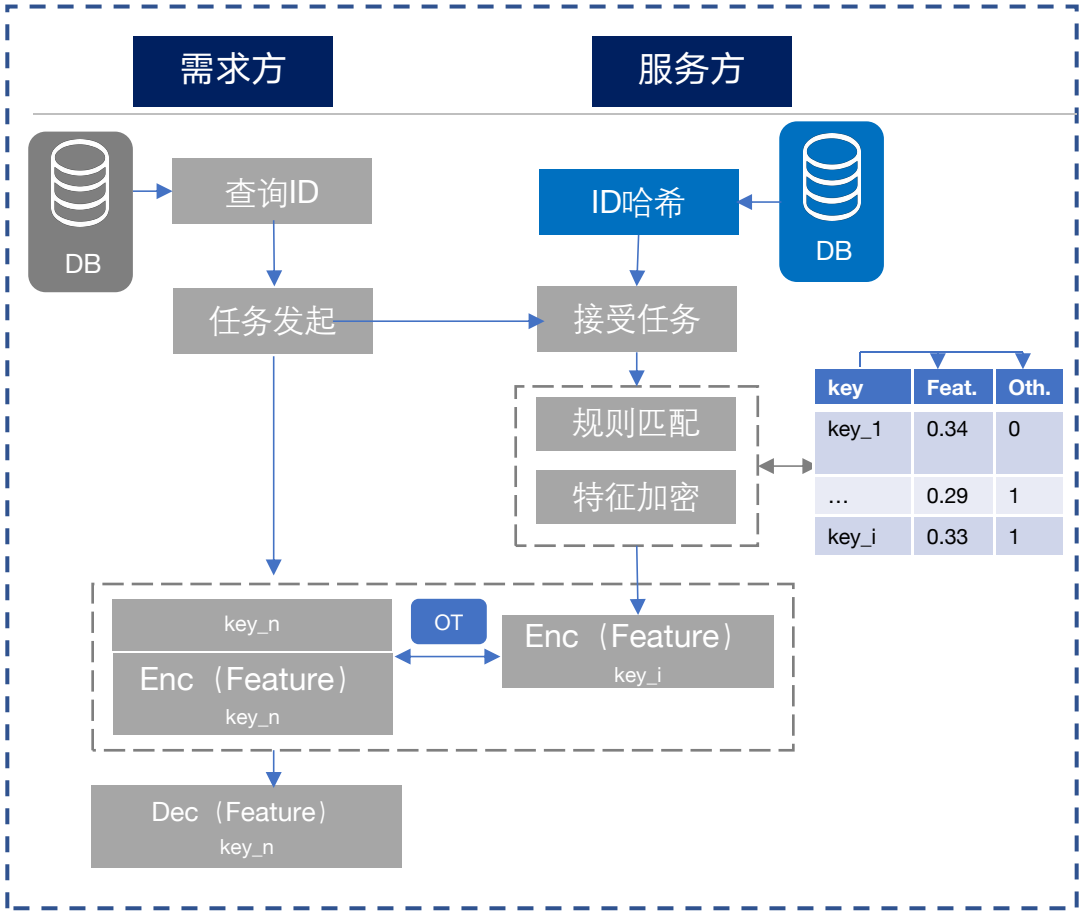
查询效果：

需求方(查询方)：

- 得到预期查询结果

服务方(被查询方)：

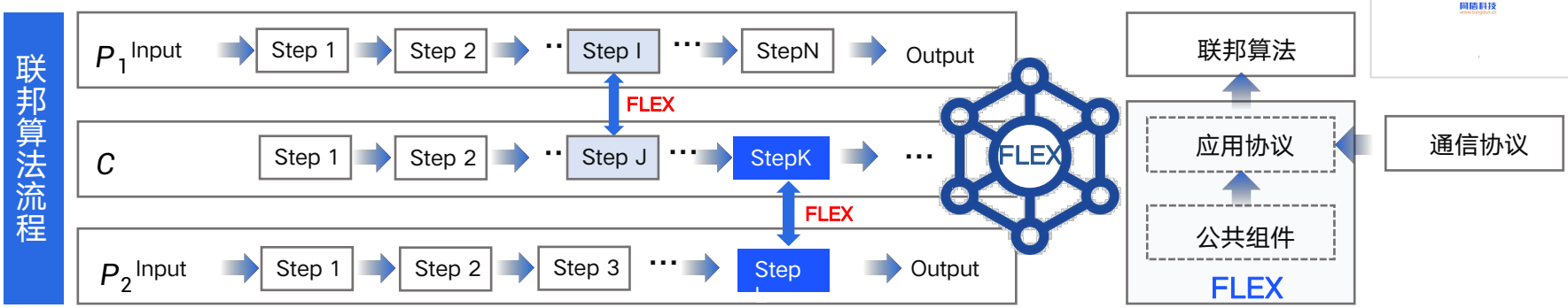
- 无法获知具体查询ID或查询条件
- 返回多条混淆加密结果，但查询方只能解密唯一的目标查询结果，无法获得查询结果外的其他信息



联邦数据安全交换协议FLEX，打破平台孤岛，引领行业规范

FLEX (Federated Learning EXchange) 是一套开源的标准化联邦协议，是可信AI的HTTPS

联邦算法有多方参与，需要在多方之间进行数据交换，业界首个联邦平台互联互通协议和开源参考实现



实现方式：

FLEX协议通过约定联邦过程中参与方之间数据交换顺序，以及在交换前后采用的数据加解密方法，来实现打破平台孤岛。

协议包括两层

- 应用协议：面向联邦算法的，为联邦算法提供多方数据交换的应用支撑。联邦过程中采用的通信协议也会被封装在这里。
- 公共组件：是上层应用协议所依赖的基础密码算法和安全协议，比如同态加密、秘密分享等。

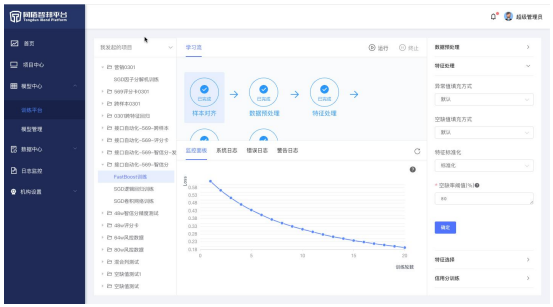
https://github.com/tongdun/iBond-flex

同盾科技 www.tongdun.cn

智邦iBond：面向数据安全的智能金融风控底座

多方安全计算MPC

数据不暴露，可用不可见
规则模型密态计算引擎，不拿数据拿结果

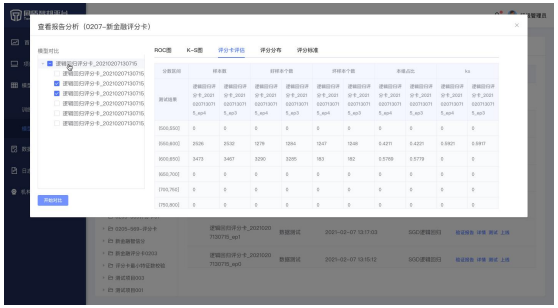


联邦学习建模FL

数据不出门，算法模型满地跑
不聚数据聚能力

安全求交PSI

计算双方共同客户，避免暴露对方没有的客户D



匿踪查询PIR

隐匿共享查询不留痕，联合统计

监控展示指挥舱大屏

智邦平台 Tongdun iBond

兼顾数据隐私安全和价值挖掘

- 数据不出门且能联合计算或机器学习，挖掘大数据隐含的信息和知识；
- 杜绝数据复制转移风险，或缓存泄漏、贩卖滥用。

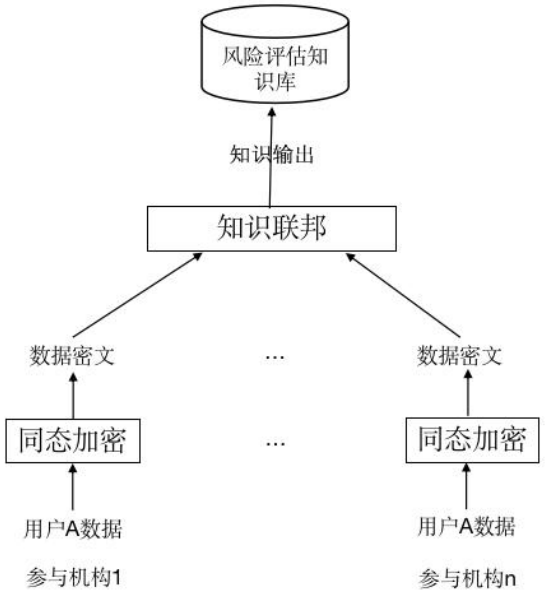
解决数据开放共享和数据安全可控两难

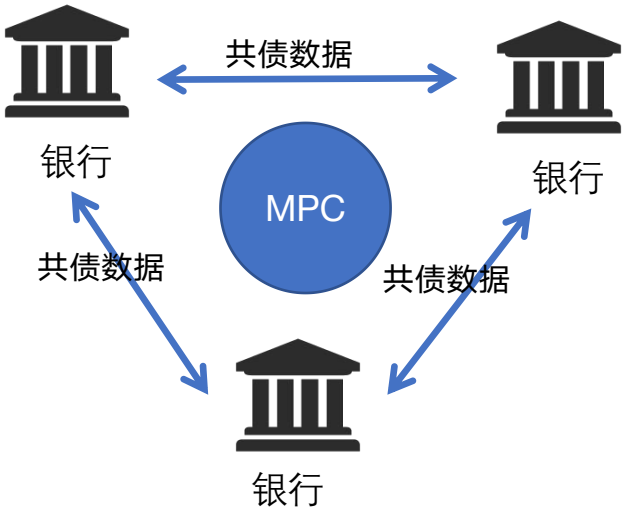
- 数据服务过程中客户信息被泄露
- 数据孤岛，无法发挥数据应有价值
- 大数据科技公司面临湿手沾面的合规问题
- 数据资产复制流失和模型知识无法得到保护

同盾科技 www.tongdun.cn

最佳实践：智邦iBond的典型应用场景

场景一：多头共债（多方安全计算）



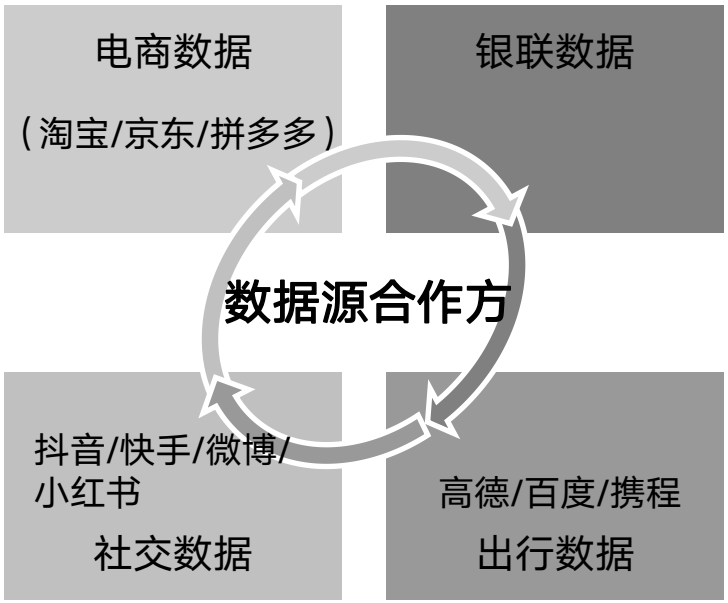


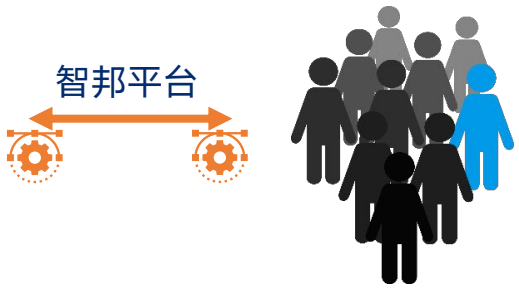
- 数据管理：智能金融风控平台支持多种数据导入方式和数据格式以快速接入参与方数据，并对数据进行管理。
- 用户指标对齐：由于各参与机构持有的用户数据在指标维度、命名以及顺序上存在着较大的差异，因此，各参与机构通过智能风控平台导入数据后，平台需完成基于用户的各参与方数据指标对齐。
- 加密方法：智能风控平台提供多种加密技术，如同态加密，一次一密，MONN加密，各参与方经协商后，采用统一的加密策略，在私有域中对用户数据进行加密，并将密文发送至智能风控平台。
- 知识联邦：智能风控平台对多头贷业务进行知识抽象，形成知识公式，并根据公式，在密文基础上计算最大授信额度，已授信额度，已使用额度，申请贷款次数，贷款审批通过次数等。然后将计算结果和风险评估模型输出，构建风险评估知识库。

最佳实践：智邦iBond的典型应用场景

场景二：个人评分（联邦学习）

跨不同数据源的联邦学习建模

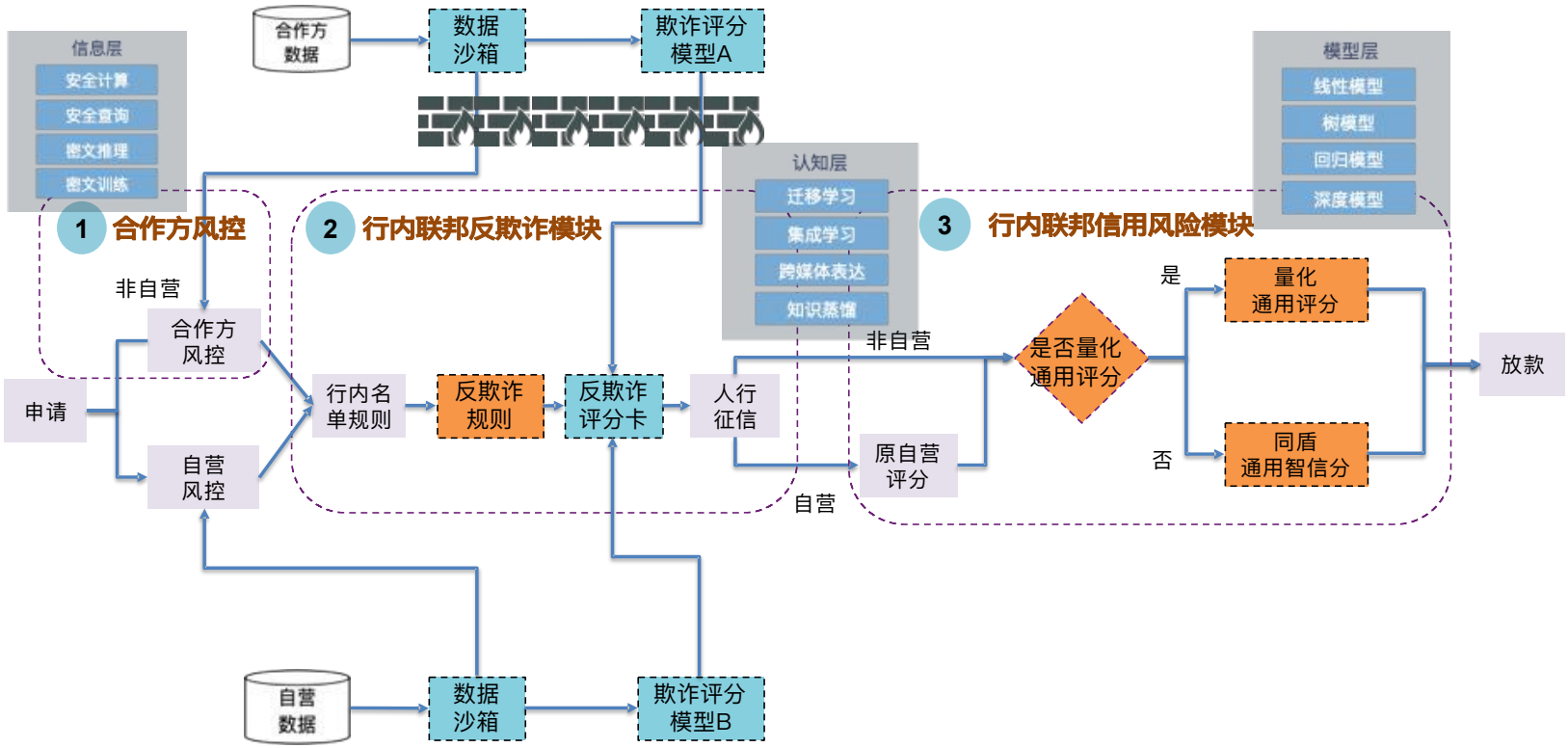




解决方案：通过行内客户的数据与行外的不同类型数据做联邦学习建模，完成行内现有客户的信用评分。

最佳实践：智邦iBond的典型应用场景

场景三：反欺诈（安全多方预测）



最佳实践：智邦iBond的典型应用场景

场景四：企业征信（安全多方推理/决策）

从公司经营能力、资本实力、绿色指数、信用因子、司法诉讼5大类（共近百个细分维度）对企业进行综合评价，得到的一系列用于表征企业信用和实力的金融评分体系。

商业案例：智邦iBond助力银保智能营销

- 背景：某国有银行与某保险公司基于紧密的业务联系，需要从银行上亿客群中挖掘潜在保险用户，有效提升银保营销转化率，进而提高保险销量。

健康险场景

保险意识/保险消费能力/保险偏好

年金险场景

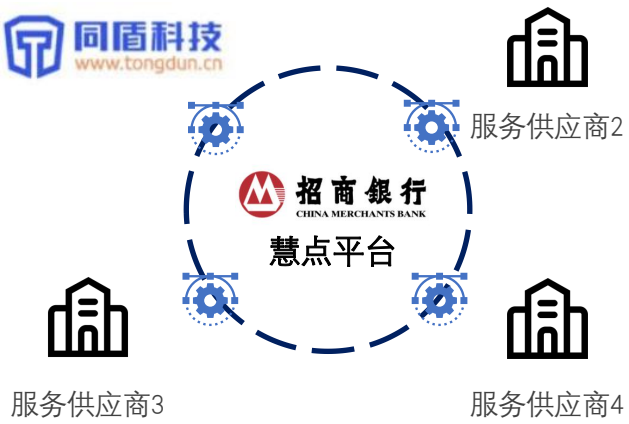
借贷情况/投资理财/信用风险

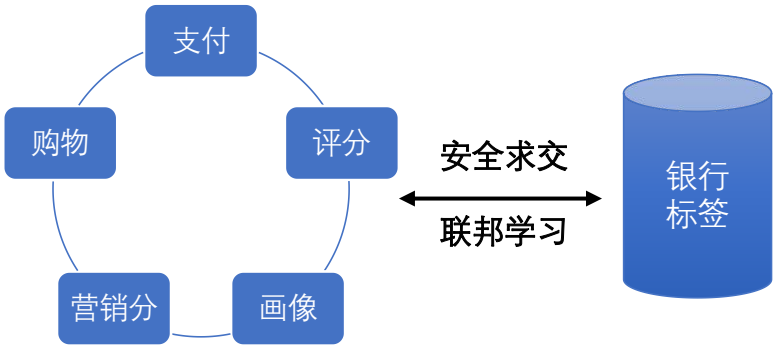
车险场景

是否有车/汽车品牌/新车/二手车/车险偏好

- 基于种子用户画像寻找相似人群，找到高质量、高潜力用户！
- 筛选、识别、扩展更多相似人群，进一步大规模增加客户量级，找到更多精准用户！
- 全流程银行、保险公司的特征、标签不出本地，无隐私泄漏的风险！
- 效果提升明显：验证集上模型指标（Recall）较之前模型，提升300%！

商业案例：智邦iBond携手大型金融机构 异构隐私计算平台间互联互通





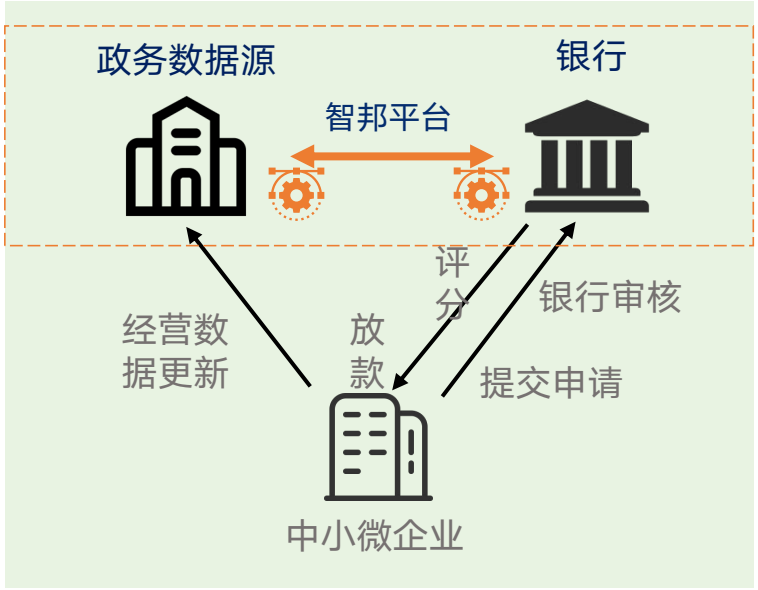
互联互通：

- 与招行慧点隐私计算平台实现对接，基于信通院互联互通标准、行方标准，联通数据、模型、应用。
- 系国内首个由大型股份制商业银行参与，与多家头部隐私计算厂商共同合作，实现跨异构平台互联互通。行业的开放互联互通典型示范项目。

“可信数字营销”应用场景：

- 现金消费贷产品：无额度用户促建额、额度有效用户促支用。
- “可信数字营销”：通过隐私计算+同盾营销分，迭代营销策略，提升银行存量客户的营销转化效果，促进业务增长。
- 打通数据求交、查询、建模训练、联邦共享等隐私计算流程，实现在风控、营销等应用场景落地。

商业案例：智邦iBond助力政务数据价值挖掘 赋能普惠金融



- 背景：银行机构在对中小企业进行普惠金融时，通常受限于以下问题：
  - 银行拥有的数据维度不足
  - 人工评估、效率低
  - 企业缺少渠道申请服务
  - 未充分发挥大数据作用

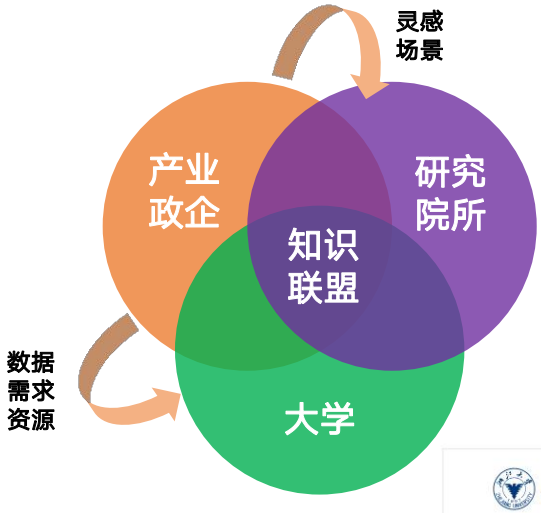
  → 普惠金融受阻

- 目标：
  - 打破数据孤岛，充分发挥地方政务数据价值
  - 数据惠民，调动金融机构积极性
  - 打通普惠金融路径，促进地方经济增长

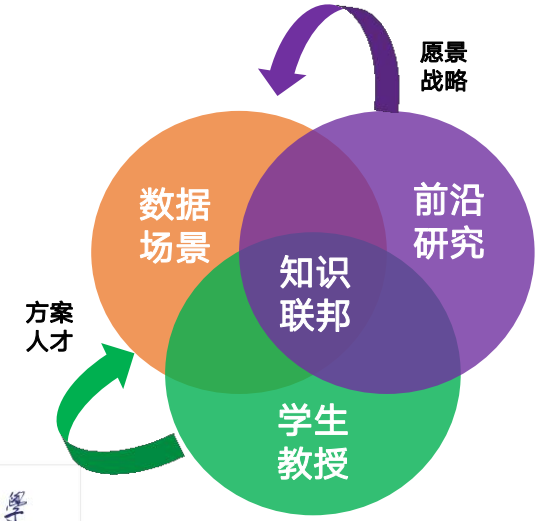
协助政务信息机构搭建金融公共服务平台，中小微企业可在平台上申请金融服务
通过智邦平台，打通政务数据源与金融机构，构建符合银行机构的企业评分模型，丰富企业信用评分维度，
便于银行机构对金融服务进行营销和风险侧的判断

产学研联盟AKF

下一代可信人工智能



AKF
知识联邦产学研联盟
Industry-University Research Alliance for Knowledge Federation



同盾科技 www.tongdun.cn

浙江大学 ZHEJIANG UNIVERSITY | 中国科学院 CHINESE ACADEMY OF SCIENCES | 复旦大学

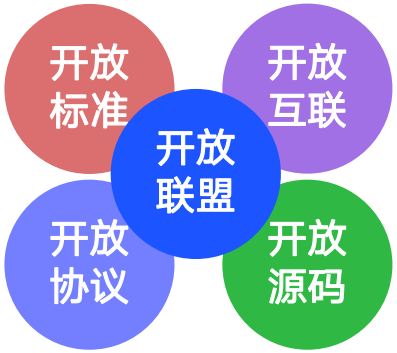
哈尔滨工业大学 HARBIN INSTITUTE OF TECHNOLOGY | 華東師範大學 EAST CHINA NORMAL UNIVERSITY | Baidu 百度

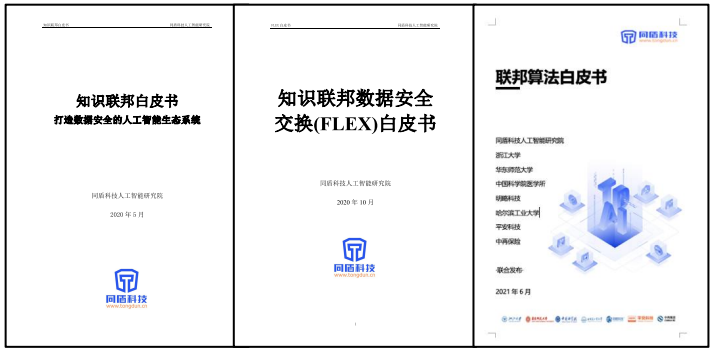
360 www.360.cn | 平安科技 PING AN TECHNOLOGY | 明略科技 MININGLAMP Technology

知识联邦产学研联盟 AKF
(Industry-University Research Alliance for Knowledge Federation)

参与建设国家新一代人工智能开放创新平台

产学研联盟AKF





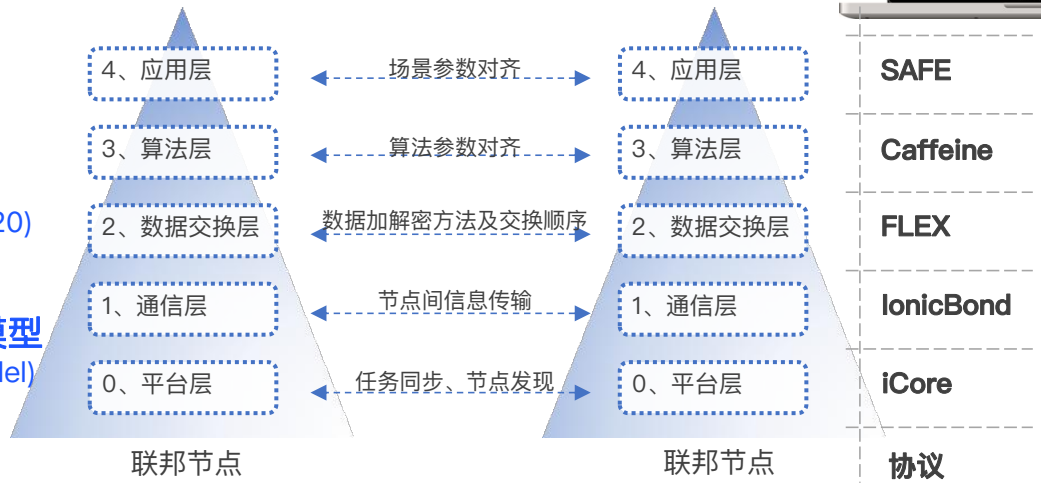
FLEX

iApp 应用商店
iModel 模型商店
iAlgo 算法商店
iData 数据要素市场
InceptionAI

AKF
知识联邦产学研联盟
Industry-University Research Alliance for Knowledge Federation

2021 全球人工智能技术大会可信AI专题论坛
2020 NeurIPS 联邦学习研讨会 (SpicyFL 2020)

开放联邦系统互联参考模型: FIRM模型
(Federated Interconnection Reference Model)



同盾科技
www.tongdun.cn

麦思博(msup)有限公司是一家面向技术型企业的培训咨询机构，携手2000余位中外客座导师，服务于技术团队的能力提升、软件工程效能和产品创新迭代，超过3000余家企业续约学习，是科技领域占有率第1的客座导师品牌，msup以整合全球领先经验实践为己任，为中国产业快速发展提供智库。

高可用架构主要关注互联网架构及高可用、可扩展及高性能领域的知识传播。订阅用户覆盖主流互联网及软件领域系统架构技术从业人员。高可用架构系列社群是一个社区组织，其精神是“分享+交流”，提倡社区的人人参与，同时从社区获得高质量的内容。