TSC Board成员年度工作总结

TSC board member

本年度工作回顾

实际生产应用

1、选定FATE作为银联联邦学习的主方案选型，当前已正式纳入公司联邦学习技术路线
2、组建团队基于FATE进行产品化开发包装，达到生产可用
3、2021年正式投产，当前已与10多家银行金融机构开展合作，为FATE的工业化应用提供了重要案例支撑

社区贡献

1、基于FATE进行产品化研发的过程中，积极反馈所遇到的问题，协助FATE不断进行改进迭代（Spark引擎规模化测试、跨版本互通验证、模型合并、安全漏洞升级、tensor加速等）
2、向社区提交技术文章《助力隐私计算互联互通，一种基于spark的FATE部署方案》
3、参与社区的发版评审讨论

生态影响力

1、在FATE社区活动、行业级大会等场合做过多次报告
2、安全漏洞事件，协助FATE安全运营小组进行应急处理
3、工行牵头的联盟课题《FATE开源框架金融行业技术应用报告》，提供相关的案例与内容补充

互联互通专项

1、在金科联盟牵头40余家行业单位，共同研究互联互通技术、标准、生态，FATE社区以及主要单位深度参与
2、牵头制定《FATE的互联互通路线图》，并在技术专委会讨论，在TSC board会议上汇报审议
3、成果发布：12月16日金融科技锦绣论坛《隐私计算互联互通技术研究报告》发布仪式，12月18日Datafun2022峰会隐私计算分论坛FATE2.0报告

互联互通

银联在FATE社区的工作重点集中于“互联互通”的关键性工作

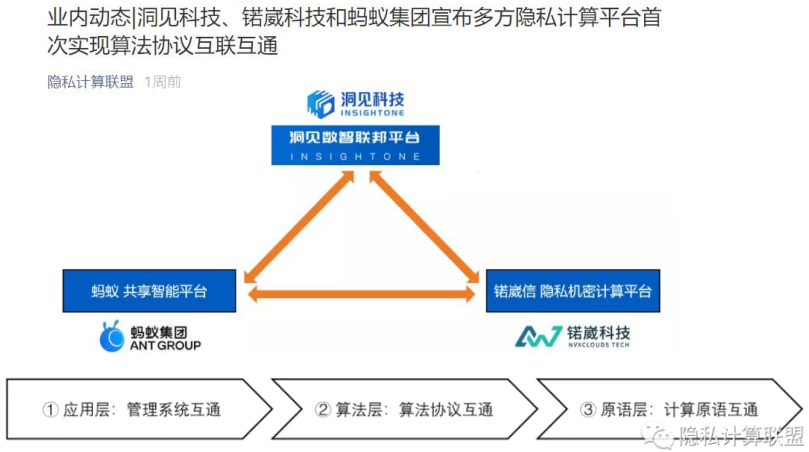
- 联邦学习是当前隐私计算最接近商业落地的一项技术
- 行业内各方互联互通的诉求愈发强烈
  - 应用方：避免烟囱化部署
  - 技术方：方便产品设计与减少与客户互联的适配
- 当前业界已有互联互通的尝试


重大突破！异构联邦学习系统首次实现互联互通

FATE开源社区 4月16日

摘要

日前，在北京金融科技产业联盟的组织下，结合中国工商银行、交通银行、中国农业银行、中国银联等头部金融机构在使用联邦学习的实际场景需要，微众银行AI团队和富数科技隐私计算团队联手破解了不同联邦学习平台之间互联的技术难题，在行业内第一次实现了异构联邦学习平台的互通。这次互联互通实验，初步验证了正在制定中的联邦学习技术互联互通技术标准的可行性，是隐私计算技术发展史上一次里程碑式的突



- 互联互通的推进快于预期，框架性方案愈渐清晰
- 业界头部产品正在推进实质性互联互通
- 各方共同努力实现联网通用的目标

联邦学习互联互通的文本标准

- 北京金融科技产业联盟《金融行业异构隐私计算平台互联互通技术规范》


2.发起签约申请

- 地址: https://{external_info_url}/node/partner/reque
- 方法: POST
- Headers:
  - X-Auth-Key: [X-Auth-Key]
  - X-Auth-Sign: [X-Auth-Sign]
- requestBody:

```
{
    "nid": "95c486d273de43638858
    "enterpriseName": "节点A",
    "nodeAddress":"http://gateway.avata                0003      de1.info"
```

开源社区在API级标准与框架实现中可以扮演重要角色

实质API互联接口的定义

互联互通–金科联盟课题概况

为推动隐私计算互联互通技术发展，促进互联互通统一技术标准形成，北京金融科技产业联盟数据专委会今年启动了《金融行业异构隐私计算平台互联互通技术规范》、《隐私计算互联互通技术研究报告》两项隐私计算重点课题

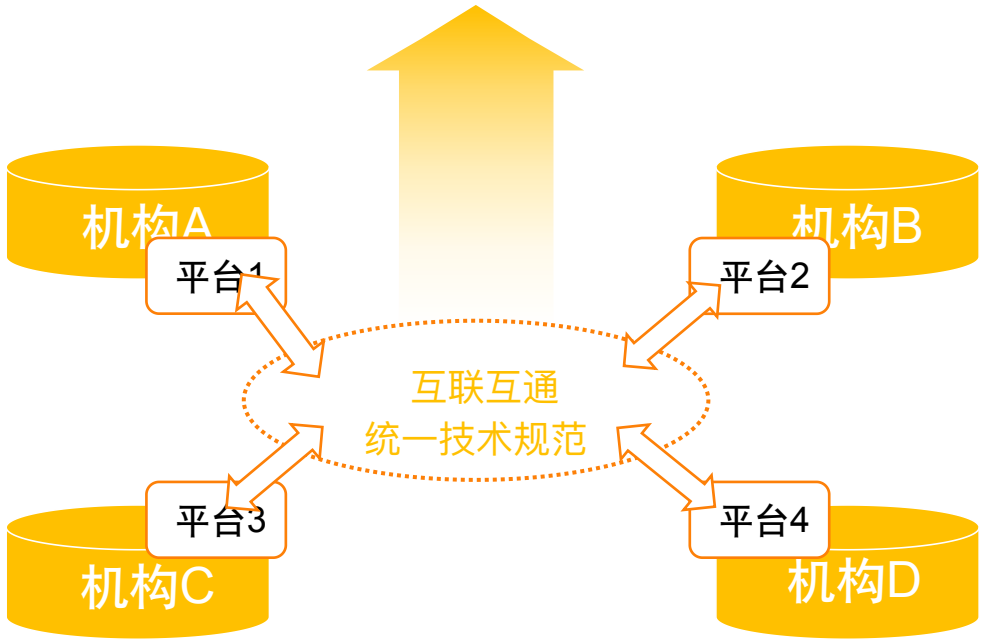
✓ 参与单位：涵盖商业银行等金融机构、科技公司、开源社区、检测机构、电信运营商、科研所等44家单位

北京百度网讯科技有限公司	北京八分量信息科技有限公司	北京冲量在线科技有限公司	北京数牍科技有限公司
成方金融信息技术服务有限公司	度小满科技（北京）有限公司	复旦大学	光大科技有限公司
海光信息技术股份有限公司	华控清交信息科技（北京）有限公司	华为技术有限公司	华夏银行股份有限公司
建信金融科技有限责任公司	交通银行股份有限公司	金融信息化研究所	蓝象智联（杭州）科技有限公司
联易融数字科技集团有限公司	蚂蚁科技集团股份有限公司	上海富数科技有限公司	上海光之树科技有限公司
上海浦东发展银行股份有限公司	上海荣数信息技术有限公司	神谱科技（上海）有限公司	深圳前海微众银行股份有限公司
深圳市洞见智慧科技有限公司	深圳市腾讯计算机系统有限公司	深圳壹账通智能科技有限公司	深圳致星科技有限公司
深圳微言科技有限责任公司	神州融安数字科技（北京）有限公司	天翼电子商务有限公司	同盾科技有限公司
兴业银行股份有限公司	北京银联金卡科技有限公司	银联商务股份有限公司	招商银行股份有限公司
浙商银行股份有限公司	中国工商银行股份有限公司	中国民生银行股份有限公司	中国农业银行股份有限公司
中国银行股份有限公司	中国银联股份有限公司	中金金融认证中心有限公司	中国移动股份有限公司

行业级互联互通

两项隐私计算互联互通课题，以联盟平台为依托，积极推动实现行业级隐私计算互联互通

互联互通 生态支撑体系

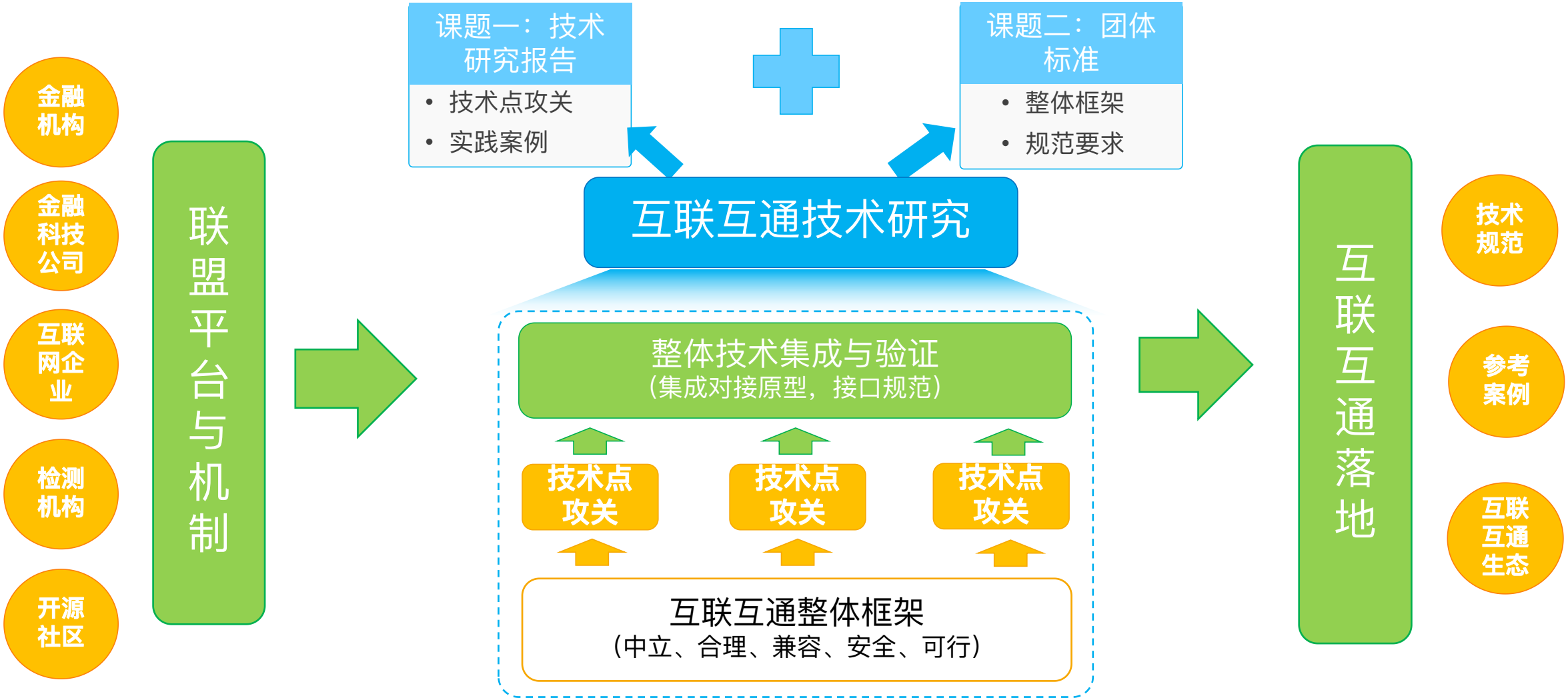


行业级互联互通内涵

- 中立客观，全局视野
- 关照诉求，解决痛点
- 架构合理，凸显安全
- 成果切实，力争推广
- 形成生态，相互促进

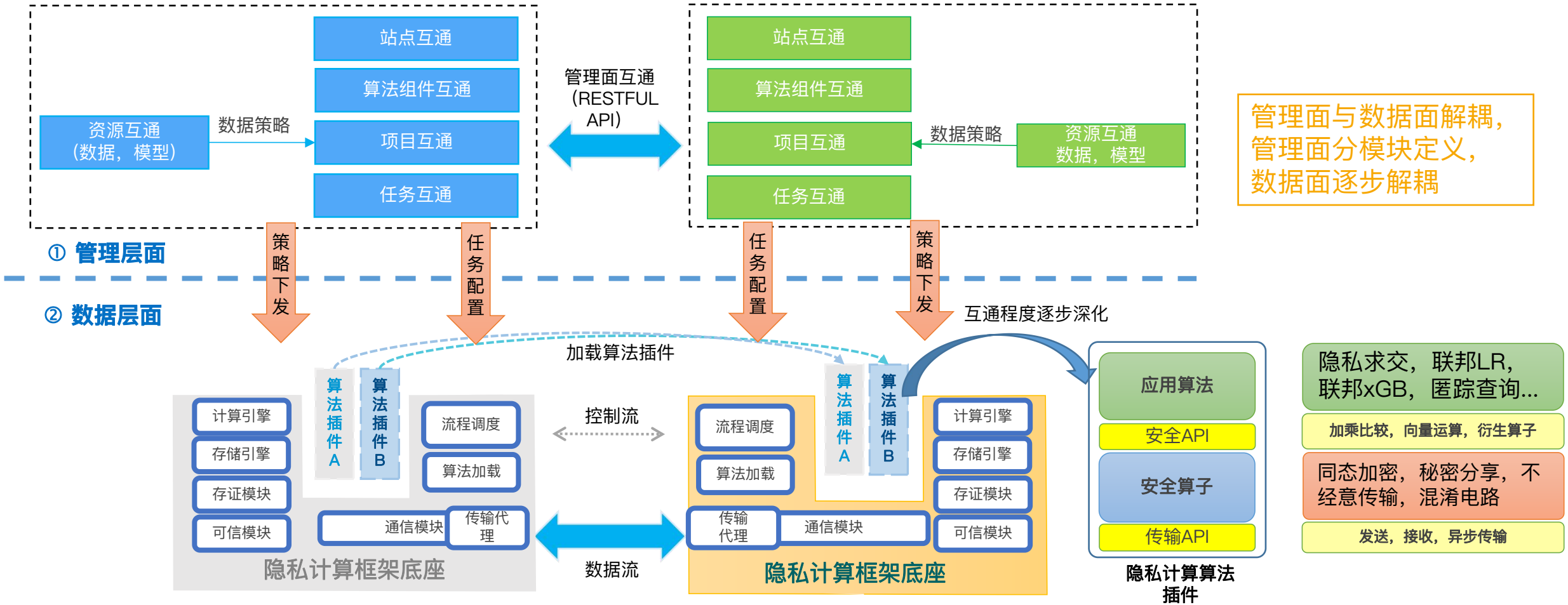
课题整体推进思路

以研究验证为依托，技术+标准双轮驱动的方式，推动行业级互联互通的真正落地



互联互通整体框架

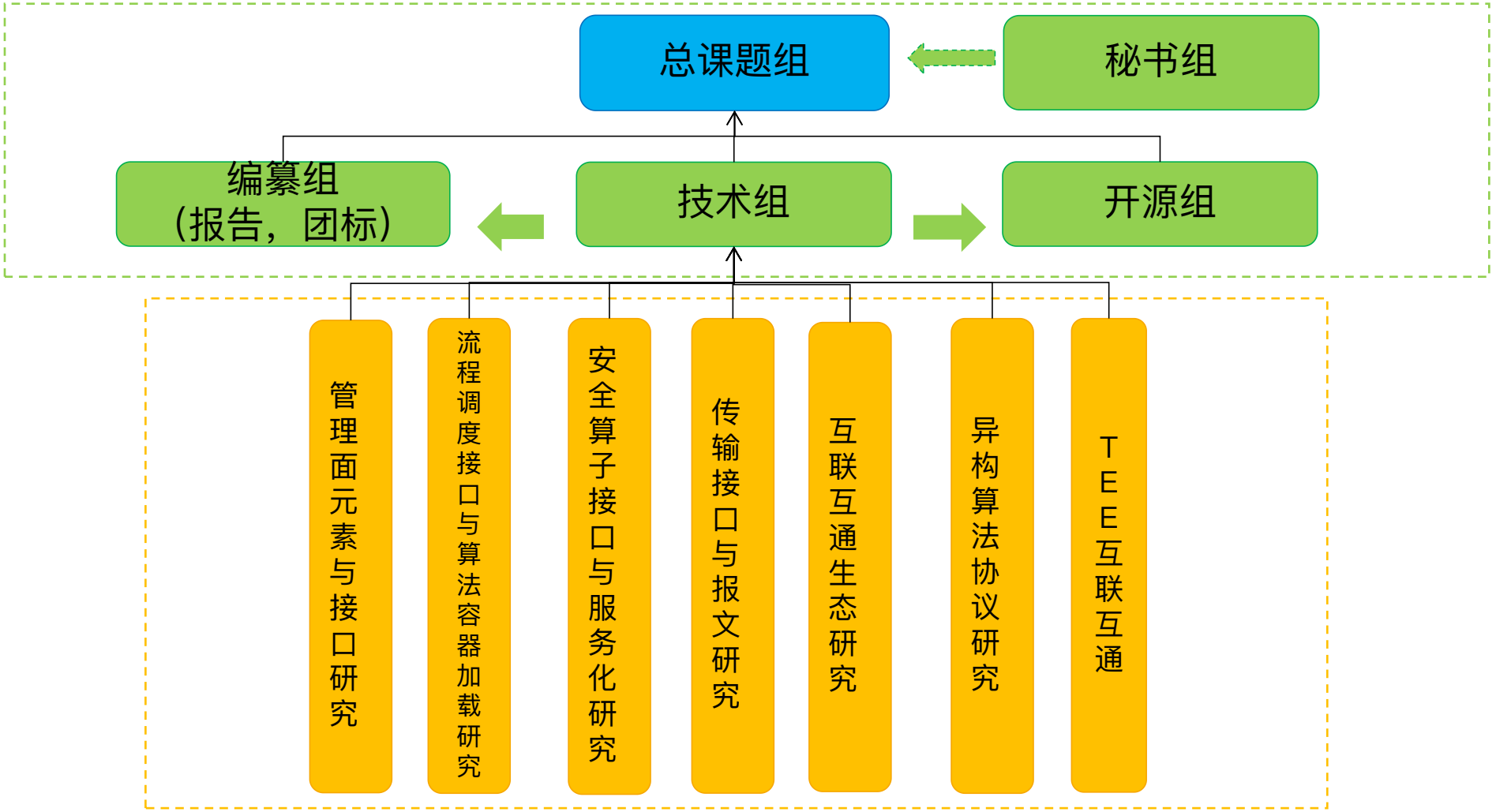
面向金融行业展开深入调研，综合产业各方诉求及技术可行性，研制形成互联互通统一框架



框架特色：全面覆盖MPC、联邦学习、TEE等隐私计算的主流技术路线，完成管理面和数据面低耦合切分，实现算法与框架底座、应用算法与安全算子间的解耦化，做到异构算法灵活可插拔，提升了隐私计算安全属性，更有助于形成良性隐私计算生态

互联互通课题组织

课题组将互联互通框架分解成七个子课题进行分头推进，总课题组主要负责统筹协调与集成验证



子课题分组与技术点攻关

当前各子课题均有序推进，陆续攻关了互联互通中涉及的一系列技术难点

子课题名称	牵头单位	子课题参与单位	主要技术点
管理面元素与接口	招商银行、浦发银行、富数	百度、洞见、度小满、工商银行、光大科技、光之树、交通银行、蓝象、蚂蚁、融安数科、神谱科技、数牍、同盾、兴业银行、星云、中国移动、中国银联、浙商银行、中国银行	“管理面最小必要元素设计” “多方资源访问控制协同策略” “DAG & conf的通用化设计”
流程调度接口与算法容器加载	浦发银行、富数、洞见、百度、微众银行	八分量、度小满、华控清交、蓝象、蚂蚁、融安数科、同盾、星云、中国银联、中国银行	“流程调度互通设计方案” “组件容器化加载方案” “对象注册和发现机制设计”
安全算子接口与服务化研究	蓝象、洞见	BCTC、度小满、富数、工商银行、华控清交、华为、联易融、蚂蚁、浦发银行、融安数科、神谱科技、同盾、星云、中国银联、 招商银行、中国银行	“隐私计算安全算子设计”
传输接口与报文研究	光大科技、蓝象	百度、成方金信、洞见、度小满、富数、华控清交、蚂蚁、 浦发银行、数牍、同盾、微众银行、星云、中国银联、中国银行	“传输层同步异步兼容设计”
互联互通生态研究	CFCA	百度、BCTC、成方金信、电信天翼、富数、工商银行、光大科技、华夏银行、华为、交通银行、蓝象、民生银行、农业银行、蚂蚁、浦发银行、数牍、腾讯、同盾、微言科技、星云、中国银联、招商银行、浙商银行	“互联互通生态研究”
TEE互通技术研究	蚂蚁（主牵头）工商银行	百度、成方金信、冲量在线、电信天翼、富数、光之树、浦发银行、同盾、星云、壹账通、中国银联、招商银行	“TEE统一远程证明流程设计”
异构算法协议研究	蚂蚁	电信天翼、百度、洞见、富数、工商银行、华控清交、华为、联易融、浦发银行、神谱科技、同盾、星云、壹账通、中国银联、招商银行、浙商银行	“异构引擎交互框架设计”

阶段性成果发布

2022年12月16日，在金融科技产业联盟的支持下，《隐私计算互联互通技术研究报告》在金融科技锦绣论坛上正式发布，可为后续进一步开展互联互通标准落地及生态建设提供有力支撑。

北京金融科技产业联盟
BEIJING FINTECH INDUSTRY ALLIANCE

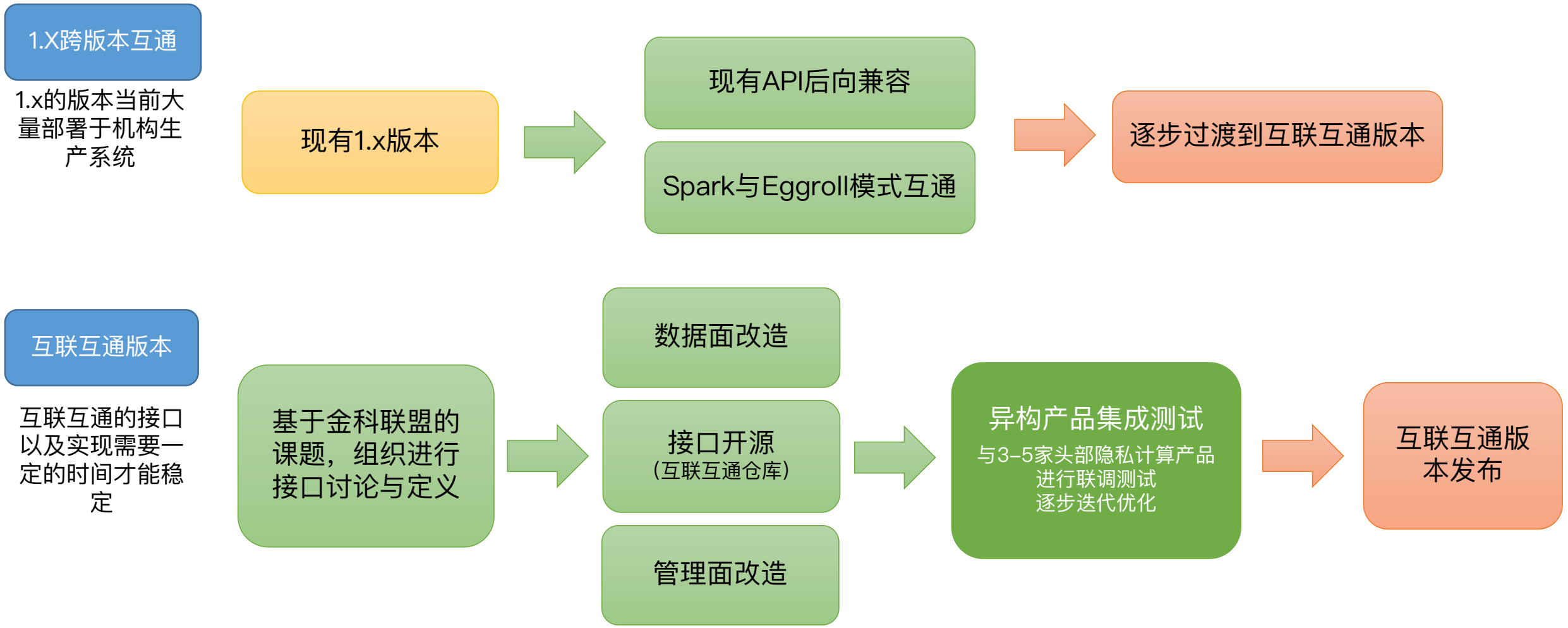
隐私计算互联互通技术研究报告

北京金融科技产业联盟

2022 年 12 月

FATE社区——互联互通路线图

1.x版本与互联互通版本分条线推进



2022 Datafun分会 – 隐私计算与互联互通分论坛

本次DataFun论坛参与单位均为互联互通课题主要贡献单位，演讲内容将涵盖互联互通的主要技术点，并伴有相应技术实践与思考：

报告单位	主题报告	互联互通相关内容
招商银行	隐私计算管理面互联互通设计与应用实践	管理面最小必要元素设计
浦发银行	波塞冬隐私计算平台与数据互联生态建设实践	流程调度与算法加载
微众银行	FATE 助力隐私计算框架互联互通	FATE 2.0互联互通版本方案
富数科技	富数科技隐私计算互联互通成果实践	互联互通实践
洞见智慧	隐私计算互联互通调度层设计和容器管理	流程调度互通设计、组件容器化加载方案
百度网讯	百度互联互通思考与实践	基于最小化约束的算法容器设计
光大科技	隐私计算互联互通传输接口与报文研究	传输层同步异步兼容设计
蓝象智联	蓝象智联隐私计算互联互通实践	多方资源访问控制协同策略、隐私计算安全算子服务设计
蚂蚁科技	异构算法互联互通&TEE互联互通 实践分享	异构平台开放算法协议设计、TEE统一远程证明流程设计
中银金科	中银金科隐私计算平台建设及金融创新应用实践	互联互通实践
电信翼支付	翼支付隐私计算互联互通及在反诈场景的应用实践	互联互通一体机
CFCA	金融行业隐私计算互联互通生态研究	互联互通生态建设
中国银联	银联隐私计算实践与应用	互联互通整体框架

新一年社区工作计划

- **API级的互联互通框架落地于FATE项目**
  - 联合业界应用方、技术方共同推动互联互通落地
  - 借助互联互通，推进FATE架构进一步优化成熟
  - 形成业界可参考的互联互通标杆，与头部隐私计算商业产品形成互联案例
- **技术研究**
  - 半模型的标准化
  - 性能加速 （求交，安全算子，TEE集成）
  - 安全性增强（全匿踪联邦学习，MPC与联邦系统融合）
- **持续生产验证与回馈社区**
- **安全与应急方面做好配合协助**
- **参与社区活动，推广社区影响力**

TSC board member

隐私计算2022年工作成果总结

1. 场景支撑方面

- 累计开展**二十多个**业务场景探索和应用工作，其中**十多个场景**已正式投产运行，**使用FATE的场景两个，即运营商信息（电信）应用于反欺诈场景**和**深圳分行–美团绑卡营销合作场景**使用FATE框架。相关成果获得了工信部“2022年大数据产业发展试点示范项目”，以及信通院隐私计算标杆案例、可信AI标杆案例等多项荣誉。
  - **典型场景**

① **普惠金融**：支持商户贷产品累计新增拓户万余户，放款超数十亿元。

② **信用卡营销**：约十万余个我行信用卡不活跃客户借助京东购物进行优惠营销，已成功激活千余户。

③ **银行卡促活：新增美团支付绑卡客户超百万，相关客户近一个月在美团平台消费总额超千万。**

④ **反欺诈场景：四川地区试点，高风险欺诈账户TOP100较只用行内特征准确率大幅度提升。**

2. 标准和前瞻研究方面

- 在社区的支持下，工行在多个行业联盟组织中**牵头或深度参与了国家、行业等各类标准和研究报告**，在金融科技产业联盟等行业组织中牵头《联邦学习金融应用白皮书》等**7篇报告**、深度参与《金融场景隐私保护计算平台 技术要求与测试方法》等**2篇标准，均已成功发布。**另外**还有10多项标准和研究报告均已取得阶段进展，其中《开源隐私计算框架（FATE）金融行业技术应用与发展报告》已经基本成稿，**正在征求北京金融科技产业联盟意见。

3. 外部发声方面

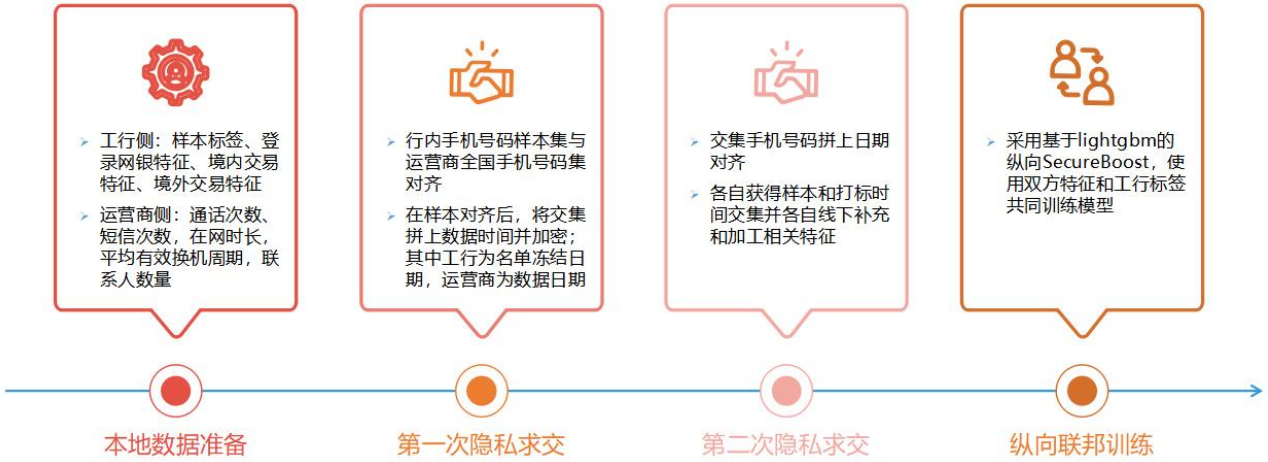
- 联邦学习技术和应用成果在世界人工智能大会（上海）、信通院隐私计算联盟沙龙等**近10个重要会议上进行了隐私计算应用的主旨演讲，介绍了工行在隐私计算领域的建设情况，其中涉及工行使用FATE开展的实践。**

典型场景 — 工行–运营商联合建模反欺诈场景

一、背景和方案

- **背景**
  - **运营商层面特征具有一定前验性**：分析公安部通报案件发现诈骗分子的异常行为在运营商侧更为提前（如更换手机设备、异地联网等），可以帮助我行提前发现风险事件。
  - **企业欺诈特征无法直接输出**：欺诈特征涉及大量隐私数据，无法通过明文方式直接共享数据。
- **方案**
  - 应用联邦学习技术，**联合我行手机银行渠道登陆数据与运营商通话类、短信类、流量类、机主信息类的特征，在数据互不出库的基础上建立工行手机银行登录行为异常识别模型**，旨在通过本次数据合作验证提升行内模型效果，更早地抓出可疑客户，并为进一步分析欺诈风险和优化反欺诈模型提供决策支撑。

二、建模过程



三、模型效果评估

- 四川地区TOP100较只用行内特征准确率提升30%。
- 特征重要性前10中，电信指标有2个，前20中有4个，前30个中有9个。

开源隐私计算框架（FATE）金融行业技术应用与发展报告

参编单位

- 共12家金融单位共同参与编写：北京金融科技产业联盟、中国工商银行股份有限公司、深圳致星科技有限公司、深圳前海微众银行股份有限公司、中国银联股份有限公司、中国银行股份有限公司、建信金融科技有限责任公司、光大科技有限公司、广发银行股份有限公司、北京神州绿盟科技有限公司、中国农业银行股份有限公司、腾讯云计算（北京）有限责任公司

FATE的典型应用案例

- 整体来看，FATE开源框架在金融行业中，主要应用于联合风控、联合营销两大类场景，报告中包括企业信用评估、风险管理、反洗钱、反欺诈、交叉营销、风险识别、智能营销等**10个精选应用案例**：银联关于小微企业信用评估联合建模案例、微众银行关于小微企业信用风险管理中的应用案例、微众银行跨银行反洗钱应用案例、光大科技交叉营销案例、光大科技联合风控案例、广发银行风险识别案例、中国建设银行智能营销应用场景案例、中国工商银行反欺诈风险识别案例、星云关于金融行业异构算力加速案例、腾讯云信贷反欺诈案例。

当前进展与发布计划

- 报告成功通过联盟数据专委会各主任、副主任单位审查，计划报告将于2023年1月在北京金融科技产业联盟公众号平台上发布，**预计对FATE在金融行业的介绍和应用起到抛砖引玉的作用。**

技术发展未来展望

1、FATE与大数据方面

当前在实际应用中，FATE与大数据之间的用数存在不便，系统集成准备工作复杂，甚至部分场景以文件形式支撑，建议FATE与大数据生态HDFS、HIVE、Spark等实现更好的对接，降低用数成本。

2、FATE与大模型方面

大模型的发展方兴未艾，提供了通过“预训练大模型+下游任务微调”方式的通用化解决方案，是当下AI产业发展的一个热点。大模型应用落地需要一定的行业数据进行微调，但是这部分行业数据仍然受到隐私保护和数据安全方面的限制，无法出域，导致大模型和联邦学习的结合存在诸多挑战。建议社区在大模型联邦学习技术方向上加以关注。

3、FATE与软硬件融合方面

隐私计算场景中，超大规模数据计算和模型训练，对软硬件提出了更高的要求，软件与硬件（TEE、GPU或NPU等）的融合发展是必然趋势，尤其是TEE的应用，带来更快计算效率的同时提供更高的安全防护等级，建议FATE社区在相关领域进行关注，能够邀请更多软硬件生态的合作方参与到社区发展中，形成Fate+Tee+xPU的实践方案。——关注到社区在22年12月发布了SPU的成果，期望看到更多同类型成果。

4、FATE与信创生态

在科技自立自强的战略背景下，紧跟信创生态兼容的趋势，建议社区可以对信创相关硬件、操作系统、中间件以及大数据软件等重要的产业链环节开展兼容对接。

TSC board member

2022年度工作成果总结

微众银行作为社区建设主力，始终投入研究、研发和运营，推动项目持续升级，建设社区影响力和先进性。

1. 作为社区项目研发主力之一，持续投入社区核心仓库的研发：

- 作为FATE、FATE-Board、FATE-FLow等仓库的研发主力，完成3个大版本及若干个小版本：
  - v1.8 核心包括无可信第三方的纵向线性回归模型，纵向SecureBoost多分类MO模式支持等
  - V1.9 核心包括高性能的椭圆曲线PSI算法协议，纵向联邦神经网络增加Pytorch后端等，调度引擎生产高可用，异构计算引擎互联互通等
  - V1.10 核心包括横向神经网络支持灵活模型定制化、多数据集类型、及使用业界经典模型；
- 主力负责Research仓库，纳入FATE 开源生态的可信联邦学习研究：
  - 对主要研究成果 FedCG (IJCAI 2022), NFL (ACM TIST), FedIPR (IEEE PTAMI) 进行了详尽的介绍并提供代码；
  - 重点展示高引用论文（引用量>100）；

2. 作为社区治理主力之一，持续投入社区运营和影响力建设：

- 社区生态建设
- 内容建设
- 活动筹办等

2023年度展望

项目规划

- 互联互通：投入FATE互联互通的整体方向（行业互联互通、与大平台互联互通）
- 算法创新：持续集成可信联邦学习算法，拓展其应用场景
- 信创与形态：和业界外部开源生态结合：如TEE，国产化组件等

生态发展

- 社区运营：投入、审视、力求创新
- 开源协同计划：深化技术合作，不拘泥于合作形式，推进隐私计算开源大家庭合作共赢

TSC board member

2022年度社区工作回顾

2022年度，星云Clustar聚焦**技术贡献、社区运营、行研生态**，参与如下共建工作：

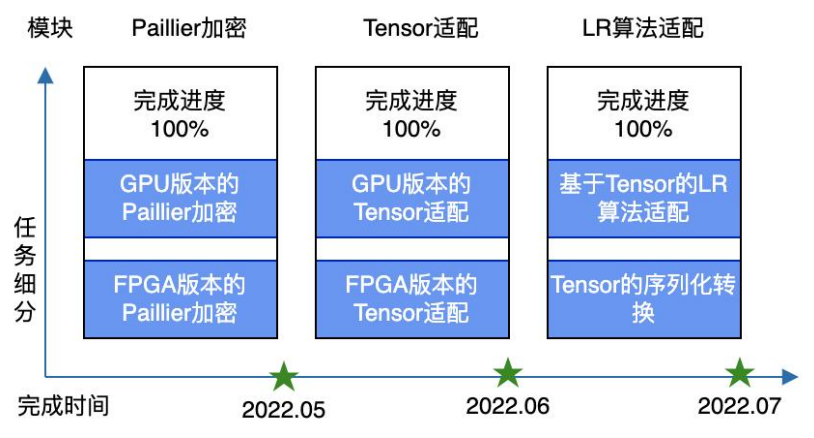
- 技术贡献：**开发层面，**协同设计基于Tensor的重构方案，验证FATE异构硬件适配可行性；FATE全技术栈ARM适配，完善FATE算力生态；参与KubeFATE部署方案贡献；**思路创新层面，**提交《一种基于随机掩码（Mask）的联邦线性回归思路》技术文章，提出相较于同态加密方案更为高效的新思路，并在社区与机器之心联合策划的可信联邦学习论文线上分享活动中详细介绍《FedSVD：10亿规模数据上的无损联邦奇异值分解》论文的研究思考。

- 社区运营：**活动组织方面，**牵头承办FATE LIGHT UP系列公开课第一期法律合规专场、第四期通信运营商专场，并作为分享嘉宾出席第七期产品专场分享；同时，参与了“联邦学习安全效率与开源生态论坛”、“2022年世界人工智能大会数据要素流通技术前沿探索论坛”两场大型论坛，积极助力活跃社区生态建设；**公关传播方面，**聚焦开源影响力、可信联邦学习及隐私计算技术生态，通过经济日报、新京报、金融时报、第一财经等10余家权威媒体，输出《“开源”如何为数字经济提供基础“养料”》、《从“大厂”走向中小微，可信联邦学习如何实现普惠》、《隐私计算期待良性生态》等十余篇行业解读深度报道，以进一步提升可信联邦学习与FATE社区影响力及知名度；
- 行研生态：积极推动可信联邦学习、开源相关行业研究，参与北京金融科技产业联盟《开源隐私计算框架（FATE）金融行业技术应用与发展报告》课题筹备及撰写工作，并重点牵头第一、三、五章节，贡献金融领域FATE项目经典实践案例。

2022年度社区工作回顾

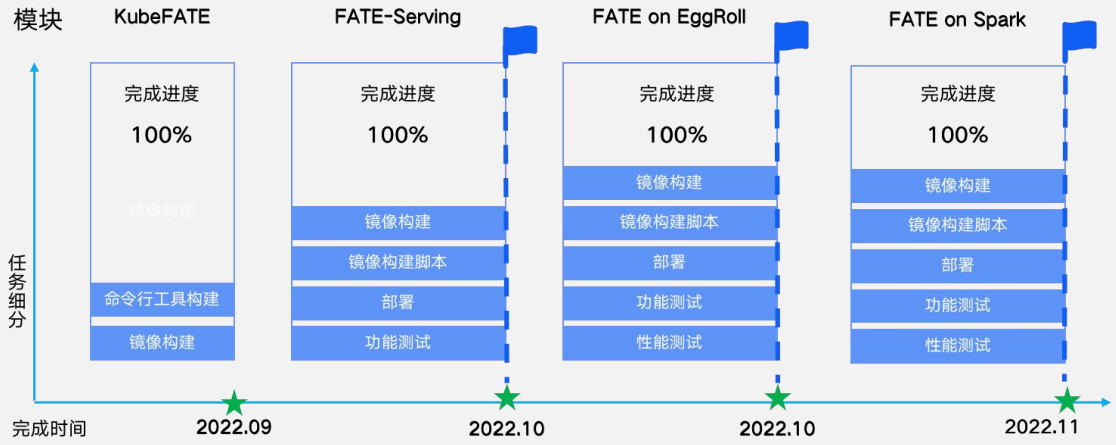
FATE异构硬件适配方案

- 与微众合作设计基于Tensor的重构方案
- 完成Tensor方案的demo版本验证，向社区证明了FATE具备异构硬件加速的能力



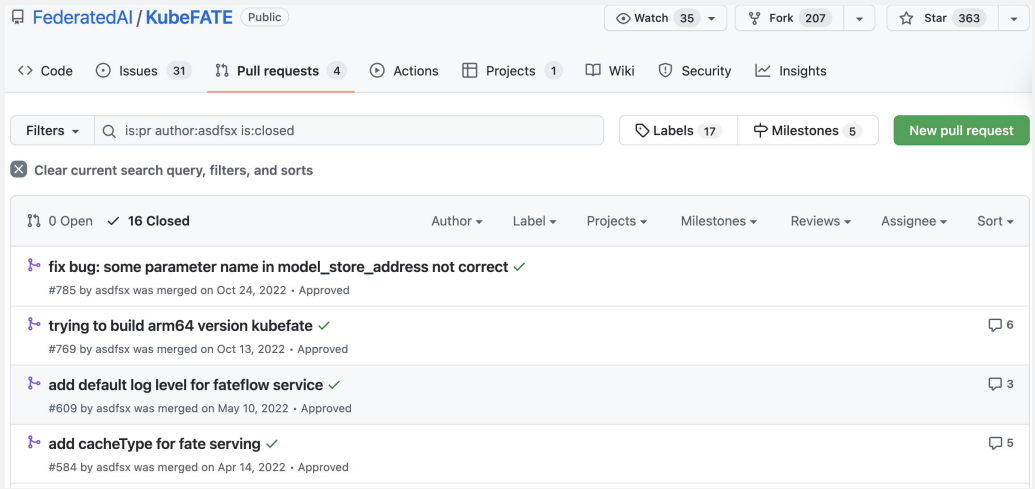
FATE算力生态适配完善

- FATE全技术栈ARM适配
- 搭载基础硬件层华为鲲鹏、系统层OpenEuler欧拉，促进FATE生态在不同技术栈持续完善



KubeFATE部署方案贡献

- 根据星云实践过程中遇到的问题，提交修复或新feature到社区



TSC board member

Summary: VMware's Contribution to FATE Community 2022

- Donated FedLCM project and delivered 2 releases
- Maintained KubeFATE project with 3 major releases, 8 patch releases
- Contributed ~20 improvements and bug-fixes to other core FATE projects
- Coordinated technical articles in WeChat - published 3 articles and coordinated other 6
- Organized community meetings (biweekly), to host meetup in Beijing
- Light Up event - delivered 1 sessions as speaker; host 3 sessions and co-host 2 sessions
- Represented FATE in public events – ACECon, AICON, CCAI, WAIC, CosCon.

- In 2023, VMware will continue to drive adoption of FATE, both locally and globally