WeBank

FATE项目简介

范涛

微众银行联邦学习研发负责人

2021年 11月

FATE：全球首个工业级联邦学习开源框架

- ✓ FATE是微众银行人工智能团队发起的全球首个联邦学习工业级开源框架，可以让企业和机构在保护数据安全和数据隐私的前提下进行数据协作
- ✓ FATE于2019年2月首次对外开源，并于2019年6月捐献给Linux基金会，并成立FATE TSC对FATE社区进行开源治理，成员包含国内主要云计算和金融服务企业
- ✓ 核心功能包括联邦特征工程，联邦统计，联邦机器学习，联邦深度学习，联邦迁移学习等

GitHub: https://github.com/FederatedAI/

FATE开源治理

【FATE社区概况】

570+ 家企业机构，**350+** 所高校

8个FATE社群**3000+**人，**3400+** GitHub Star

如涉及到公众号转发的白名单等事宜，需要与信通院沟通确认的，随时沟通。

13	KubeTEE	2020 年 9 月	蚂蚁集团	可信执行环境

从开源项目的活跃度和影响力来看，联邦学习的开源生态为工业化的落地应用贡献了强劲力量，特别是 FATE，2020 年及之后出现的很多联邦学习类产品都或多或少的吸收和借鉴了 FATE 供给的营养。在中国信通院调研统计中，55%的国内隐私计算产品是基于或参考开源项目开发的[9]，这其中开源项目就以 FATE 为主。

图 10 国内隐私计算平台自研情况

【TSC（技术管理委员会）成员】

WeBank 微众银行 · Tencent · UnionPay 银联 · vmware · 中国电信 CHINA TELECOM · 光大科技有限公司 EVERBRIGHT TECHNOLOGY CO. LTD · 中国银行 BANK OF CHINA · 中国农业银行 AGRICULTURAL BANK OF CHINA · ICBC 中国工商银行 · 建信金融科技 CCB Fintech · 富数 FUDATA.CN · CLUSTAR 星云

信通院《隐私计算白皮书（2021年）》发布，根据白皮书中国信通院的调研，**55%的国内隐私计算产品是基于或者参考开源项目开发，这其中开源项目就以FATE为主。**

FATE：联邦学习一站式解决方案

企业解决方案层

FATE-Studio
面向企业开发者提供零门槛联邦学习开发平台
集交互式联邦建模，联邦查询统计，数据管理，模型部署为一体解决方案

FATE-Cloud
面向企业开发者提供联邦数据合作网络搭建平台
集联邦站点注册，站点监控，站点集群可视化部署，合约管理，交易管理为一体解决方案

核心应用组件层

联邦区块链 FATE-Chain
- 身份认证/可信授权
- 日志协作/审计
- 数据/模型激励追踪

联邦查询统计 FATE-SQL
- 联邦SQL解析器
- 横向/纵向查询统计算子
- 查询安全审计

联邦建模可视化 FATE-Board
- 联邦模型可视化
- 联邦任务dashboard
- 任务/日志管理

联邦建模调度 FATE-Flow
- 多方任务协同调度
- 联邦任务生命周期管理
- 联邦模型管理

联邦在线推理 FATE-Serving
- 实时在线联邦推理
- 集群管理与监控
- 在线模型管理

核心框架层

联邦学习算法库 FederatedML
- 纵向联邦特征工程
- 纵向联邦学习
- 横向联邦学习
- 联邦深度学习
- 联邦迁移学习
- 纵向联邦统计
- 安全信息检索（PIR）
- 安全求交（PSI）
- 横纵融合
- 异步联邦学习
- 模型加密预测

联邦安全协议Secure Protocols
- Paillier同态加密
- 仿射同态加密
- Secret-Sharing（SPDZ）
- OT
- 可交换加密
- 安全聚合
- RSA
- DH密钥交换

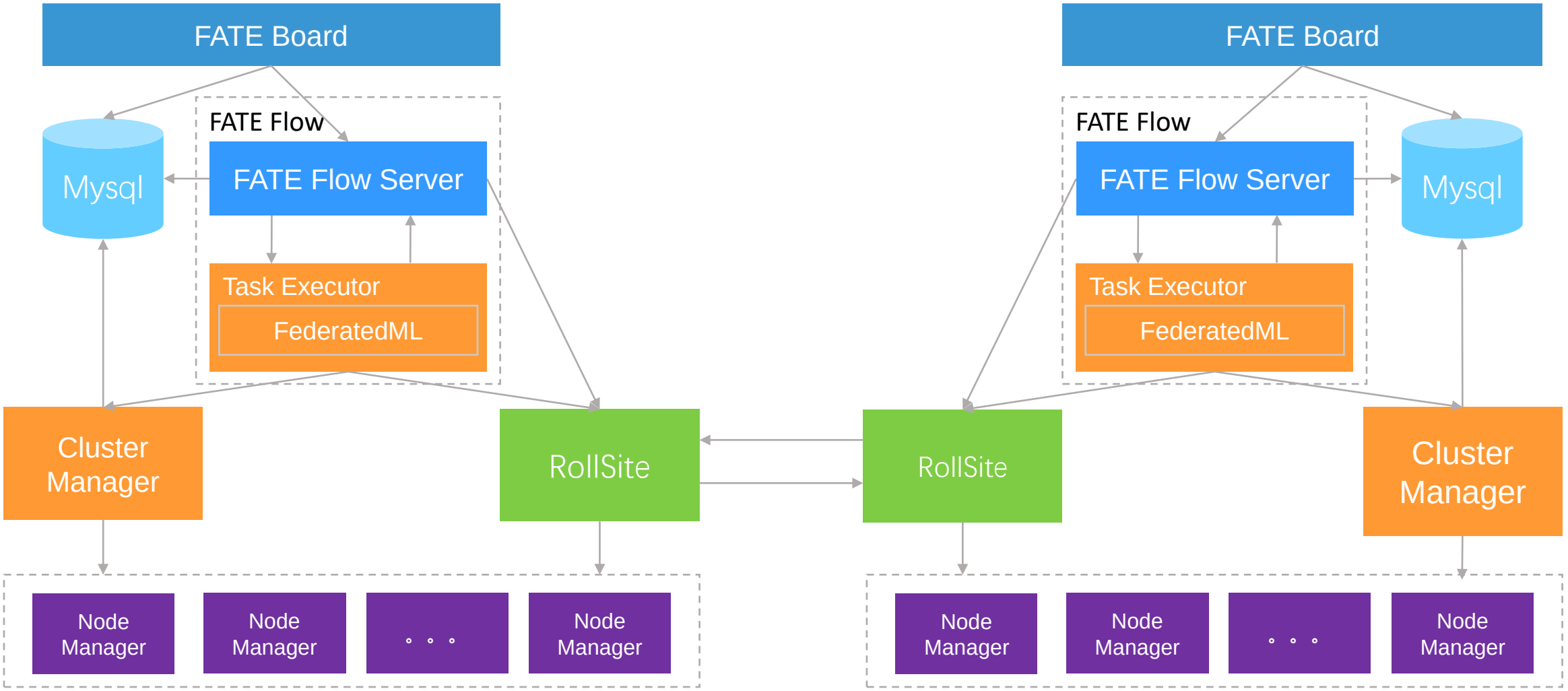
计算： Tensorflow / Pytorch (深度学习) EggRoll / Spark (分布式计算框架)

多方联邦通信：跨站点传输网络（RollSite/Pulsar/RabbitMQ）

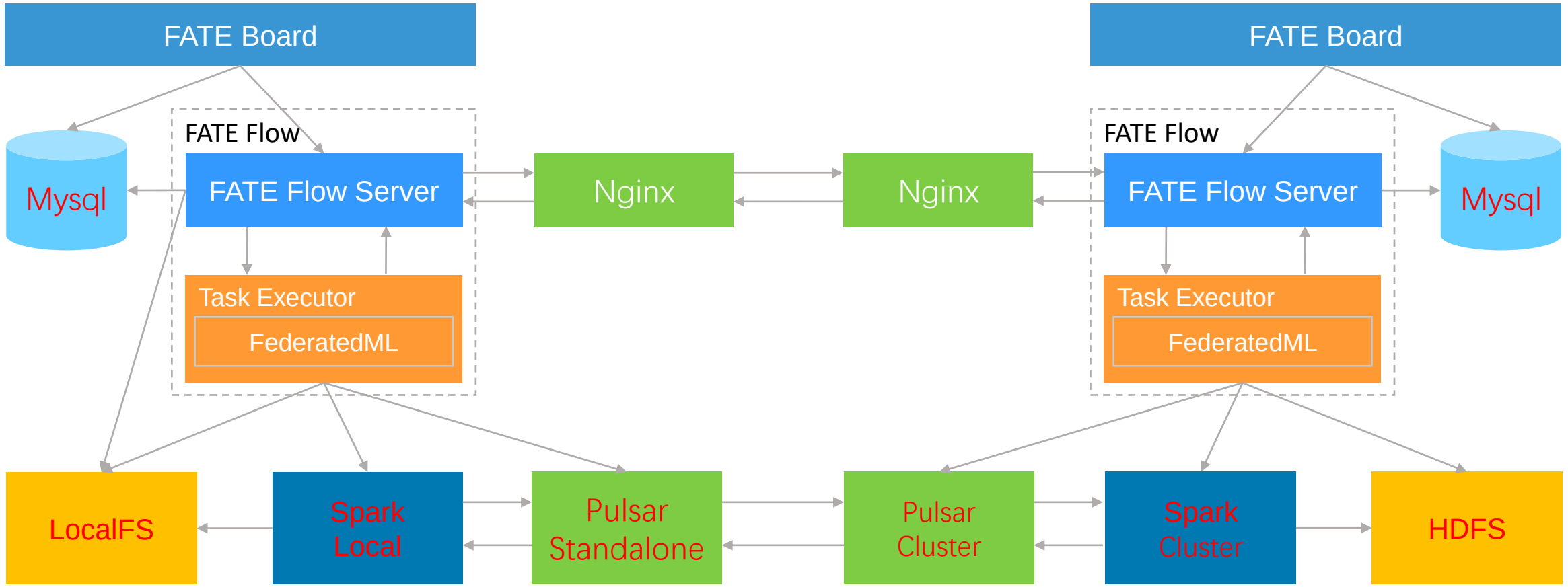
存储：HDFS/HIVE/MYSQL/LocalFS

WeBank

FATE on EggRoll



FATE on Spark



FATE开源社区里程碑 2019

Milestone

FATE v0.1
Federated ML
2019.02

2019.03
GitHub Star 突破 100
诞生第一位外部Contributor

FATE v0.2
FATE-Serving
联邦特征工程
2019.05

2019.06
FATE v0.3
捐献 Linux Foundation

THE LINUX FOUNDATION OPEN SOURCE SUMMIT NORTH AMERICA

FATE v1.0
FATE-FLOW
FATE-Board
2019.08

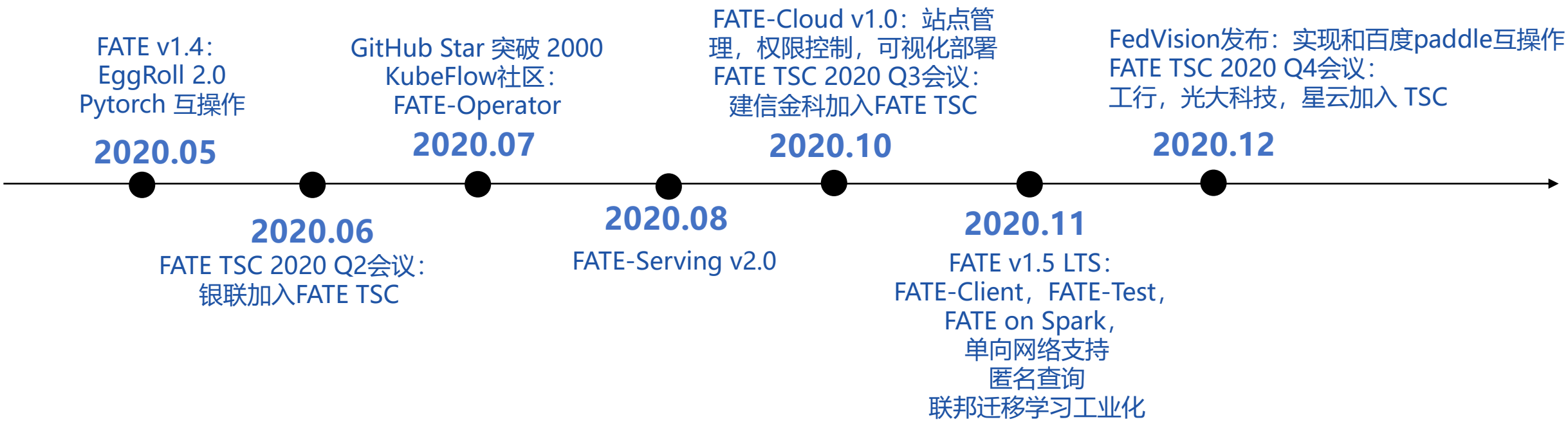
2019.10
FATE v1.1
KubeFATE: 云原生部署
支持横向联邦深度学习
支持多方纵向联邦学习

GitHub Star 突破 1000
5位外部Contributor
2019.11

2019.12
FATE v1.2
支持纵向联邦深度学习
支持SecretShare协议

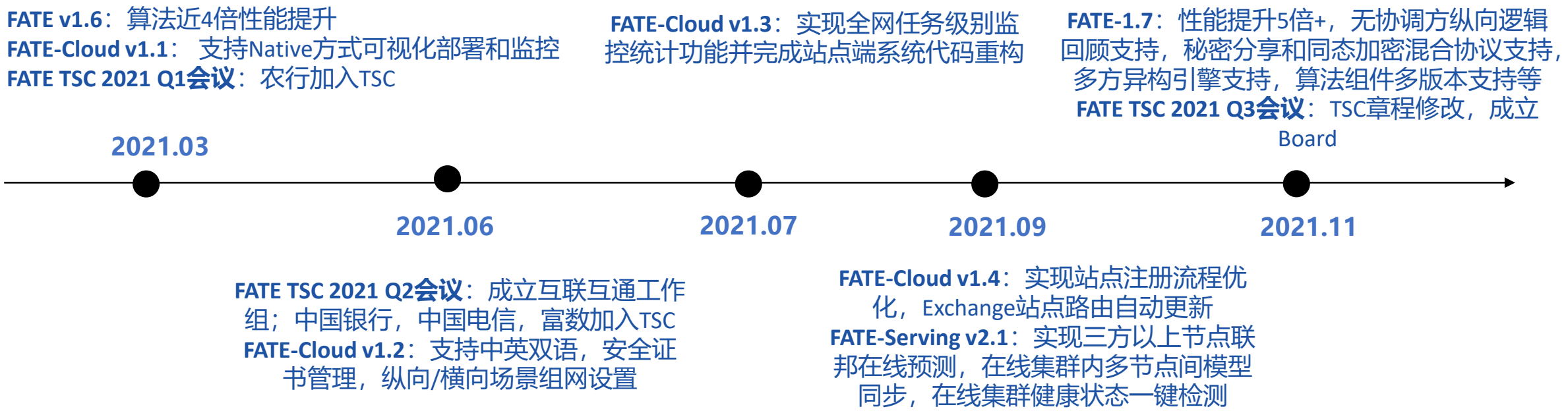
2019：开源社区初创，功能丰富阶段

FATE开源社区里程碑 2020



2020：开源社区生态快速发展阶段

FATE开源社区里程碑 2021



2021：企业级产品支持和标准快速推进阶段

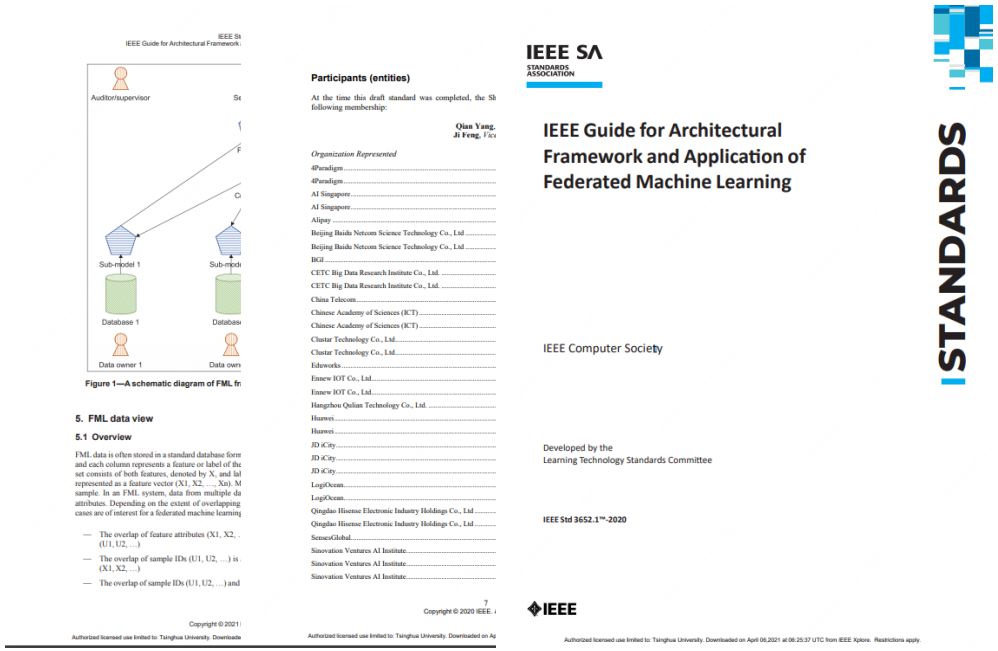
WeBank

微众联邦学习产品标准建设情况

【国际标准】

发布全球第一个联邦学习相关国际标准

IEEE P3652.1《IEEE Guide for Architectural Framework and Application of Federated Machine Learning》



【国内标准】

参与编写已发布标准：

- 参与信通院《基于多方安全计算的数据流通产品技术要求与测试方法》和《联邦学习技术与应用》标准编写
- 金融行业标准：参与央行金融标准化委员会《多方安全计算金融应用技术规划》的标准

参与编写中的标准：

- 金融行业标准《联邦学习金融应用与互联互通标准规范》
- 通信行业标准（CCSA-TC1/TF1）：《联邦学习的安全评测技术要求及测试方法》《联邦学习跨框架互操作技术要求》
- 团体标准（CCSA-T601）：《联邦学习跨平台互联互通标准》

微众联邦学习产品安全认证

- 系统通过**《信息安全等级保护》三级备案**
- 通过中国信通院《大数据 · 联邦学习数据流通产品》、《大数据 · 多方安全计算数据流通产品》、《联邦学习评估专项》认证
- 完成国家金融科技评测中心（银行卡检测中心）多方安全计算金融应用技术测评


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，深圳前海微众银行股份有限公司单位的：

第 3 级 联邦网络平台 系统

予以备案。

证书编号：[redacted]

中华人民共和国公安部监制

备案公安机关公章

2020 年 6 月 24 日

《信息安全等级保护》三级备案证书


大数据产品能力评测

证书编号：IVB-2020-00180

颁发日期：2020年12月18日

多方安全计算
基础能力专项评测证书

深圳前海微众银行股份有限公司

信通院《大数据 · 联邦学习数据流通产品》认证


大数据产品能力评测

证书编号：IVB-2020-00179

颁发日期：2020年12月18日

联邦学习
基础能力专项评测证书

深圳前海微众银行股份有限公司

信通院《大数据 · 多方安全计算数据流通产品》认证


信通院《联邦学习评估专项》


国家金融科技测评中心
National FinTech Evaluation Center
银行卡检测中心
Bank Card Test Center

多方安全计算金融应用评测证书

深圳前海微众银行股份有限公司

完成银行卡检测中心（BCTC）评测

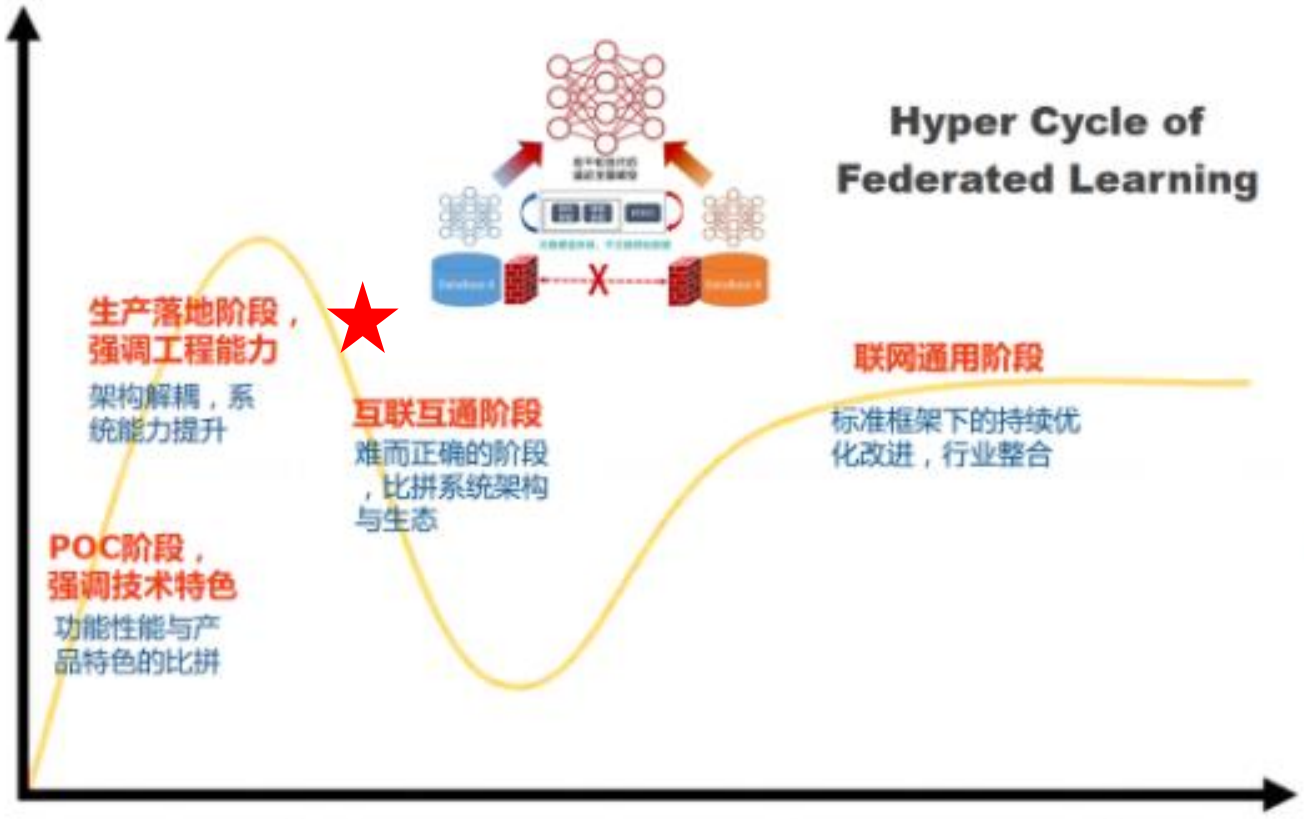
FATE社区成立互联互通工作组

2021年6月24日，联邦学习开源社区FATE技术委员会召开2021年第二次会议，在中国银联提议下，FATE TSC成立互联互通工作组，由中国银联牵头，成员包括微众银行、VMware、中国电信。标志着联邦学习系统开始从开源可用向开放通用迈进。

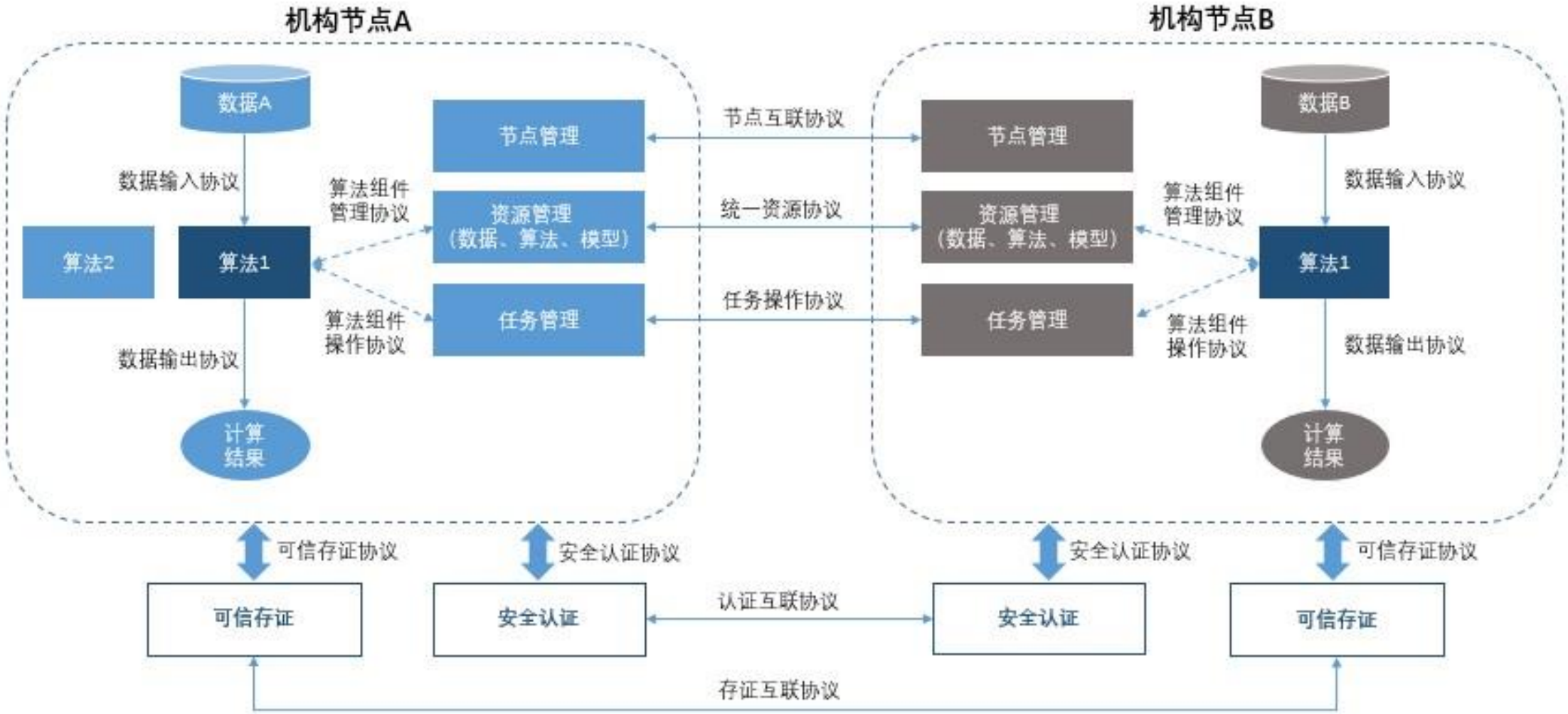
WeBank UnionPay 银联 vmware 中国电信 CHINA TELECOM

开源可用 → 开放通用

【联邦学习系统拟演进方向】



FATE与异构框架互联互通解决方案



关注FATE

欢迎来GitHub 加入FATE建设
star我们，第一时间接收项目进展

官网：**https://www.fedai.org/**
邮箱：contact@fedai.org

国内首个联邦学习官方社区，这里有

- 高价值贡献者激励计划
- **10+**顶尖算法工程师实时答疑解惑
- 超**500**家企业机构开发者共同交流学习
- 国内最新联邦学习产品资讯抢先获取