

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

如涉及公众号转发的白名单等事宜，需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，这其中开源项目就以 FATE 为主。

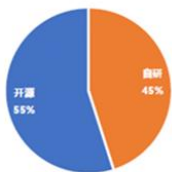


图 10 国内隐私计算平台自研情况

## 【TSC（技术管理委员会）成员】



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



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的，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

## 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

核心框架层

## 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

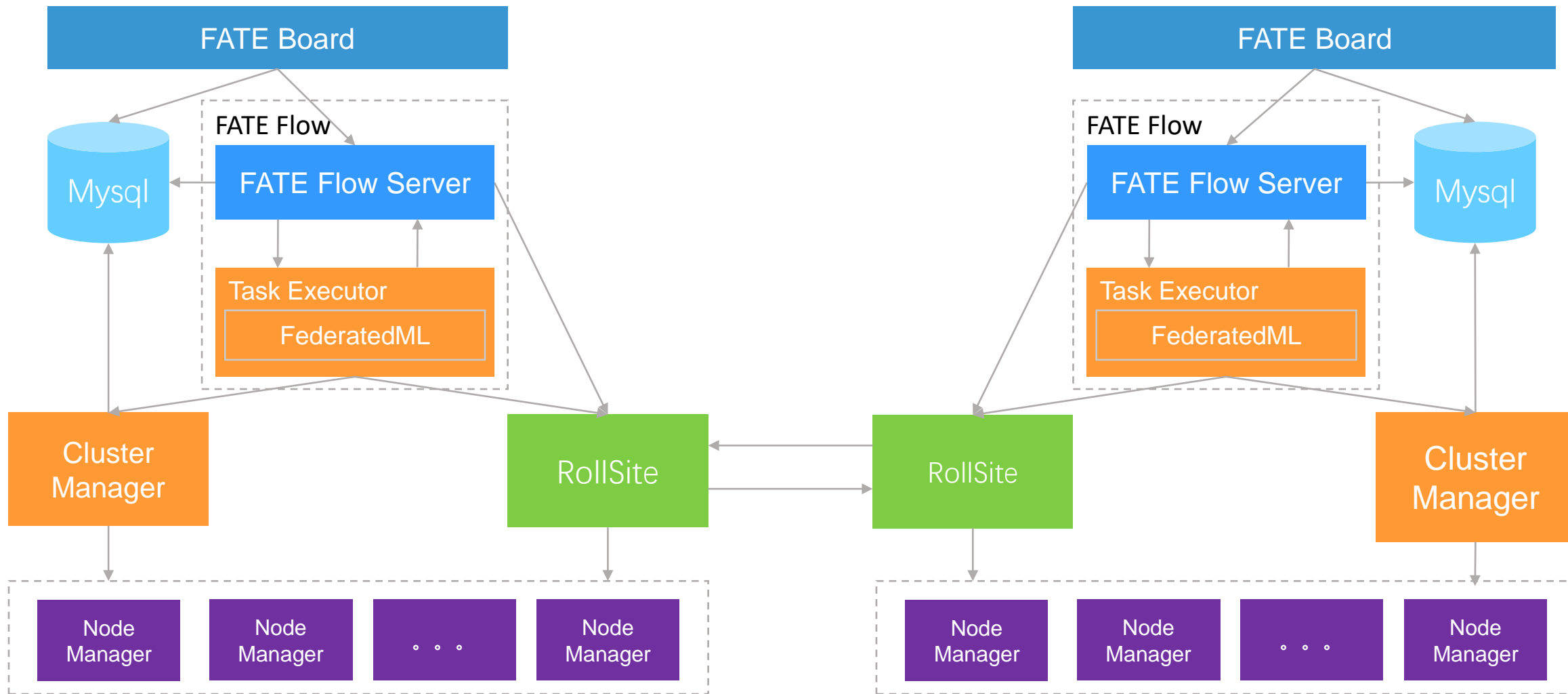
WeBank

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

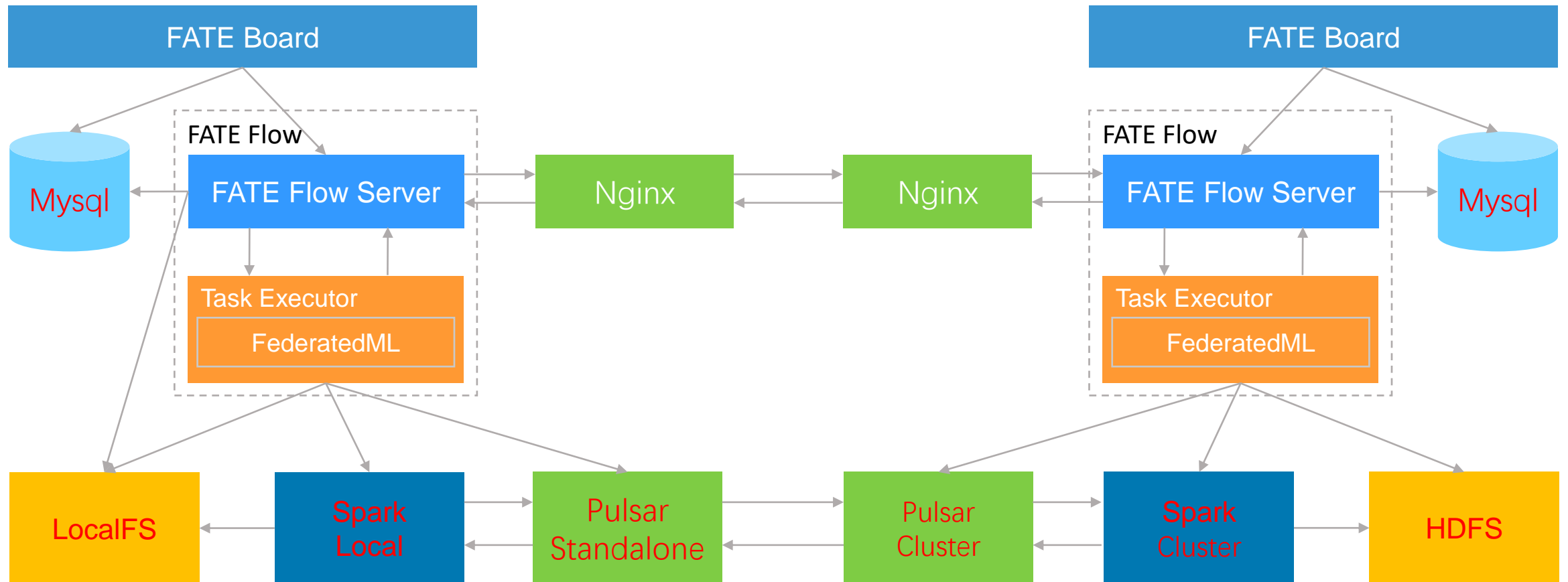
多方联邦通信: 跨站点传输网络  
(RollSite/Pulsar/RabbitMQ)

存储: HDFS/HIVE/MYSQL/LocalFS

# FATE on EggRoll

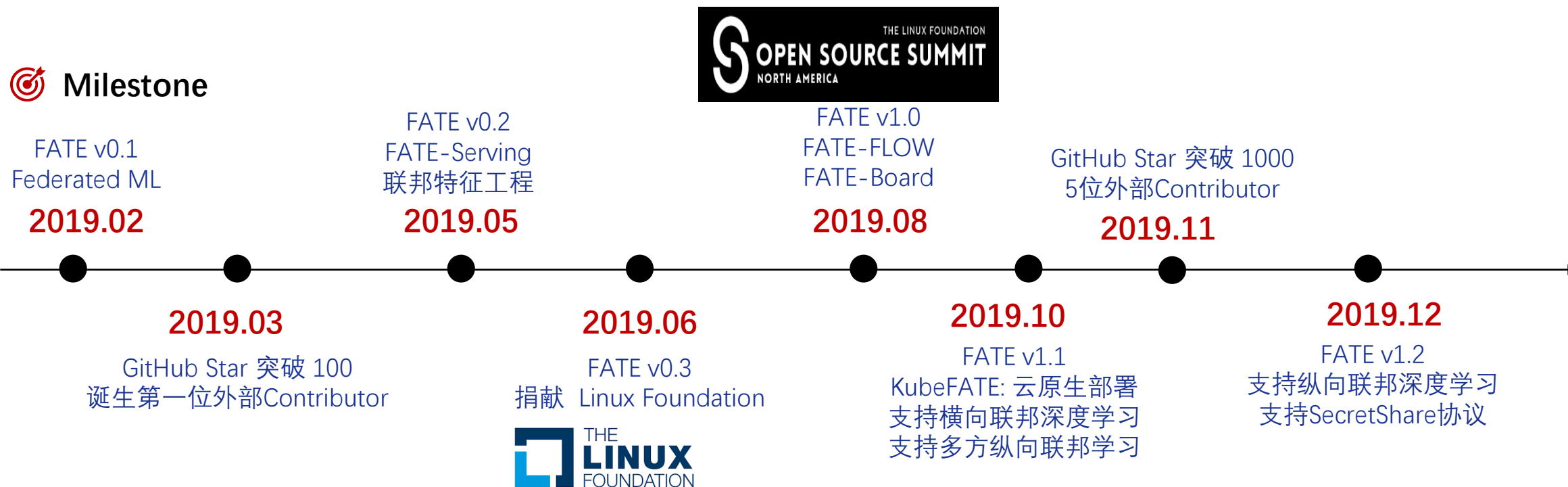


# FATE on Spark



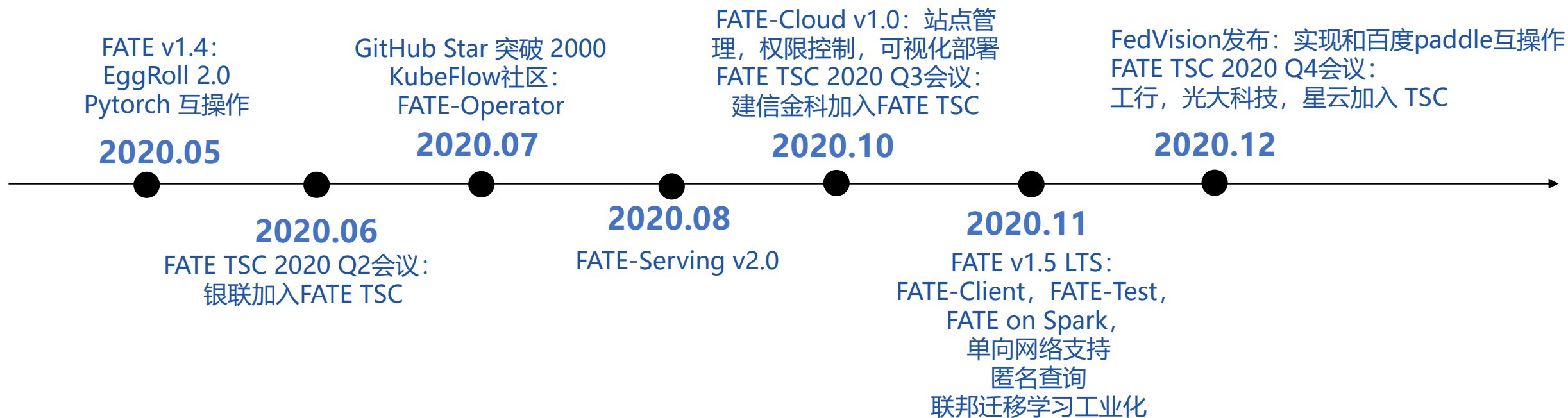
# FATE开源社区里程碑 2019

## Milestone



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

FATE v1.6: 算法近4倍性能提升

FATE-Cloud v1.1: 支持Native方式可视化部署和监控

FATE TSC 2021 Q1会议: 农行加入TSC

FATE-Cloud v1.3: 实现全网任务级别监控统计功能并完成站点端系统代码重构

FATE-1.7: 性能提升5倍+, 无协调方纵向逻辑回顾支持, 秘密分享和同态加密混合协议支持, 多方异构引擎支持, 算法组件多版本支持等

FATE TSC 2021 Q3会议: TSC章程修改, 成立Board

2021.03

2021.06

2021.07

2021.09

2021.11

FATE TSC 2021 Q2会议: 成立互联互通工作组; 中国银行, 中国电信, 富数加入TSC  
FATE-Cloud v1.2: 支持中英双语, 安全证书管理, 纵向/横向场景组网设置

FATE-Cloud v1.4: 实现站点注册流程优化, Exchange站点路由自动更新  
FATE-Serving v2.1: 实现三方以上节点联邦在线预测, 在线集群内多节点间模型同步, 在线集群健康状态一键检测

2021: 企业级产品支持和标准快速推进阶段

# 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》

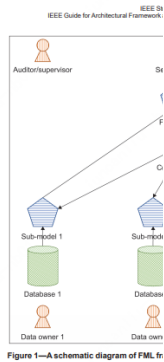


Figure 1—A schematic diagram of FML framework

#### 5. FML data view

##### 5.1 Overview

FML data is often stored in a standard database form and each column represents a feature or label of the set consists of both features, denoted by  $X$ , and label represented as a feature vector  $(X_1, X_2, \dots, X_M)$  sample. In an FML system, data from multiple data attributes. Depending on the extent of overlapping cases are of interest for a federated machine learning

- The overlap of feature attributes  $(X_1, X_2, \dots, (U_1, U_2, \dots))$
- The overlap of sample IDs  $(U_1, U_2, \dots)$  is  $(X_1, X_2, \dots)$
- The overlap of sample IDs  $(U_1, U_2, \dots)$  and

**Participants (entities)**

At the time this draft standard was completed, the SB following membership:

Qian Yang,  
Ji Yong, Piv

**Organization Represented**

#Participant	
AI Singapore	
AI Singapore	
Alipay	
Beijing Huada Netcom Science Technology Co., Ltd.	
Beijing Huada Netcom Science Technology Co., Ltd.	
BGI	
CETC Big Data Research Institute Co., Ltd.	
CETC Big Data Research Institute Co., Ltd.	
China Telecom	
Chinese Academy of Sciences (ICT)	
Chinese Academy of Sciences (ICT)	
Chunor Technology Co., Ltd.	
Chunor Technology Co., Ltd.	
Edureka	
Emulex Co., Ltd.	
Emulex Co., Ltd.	
Hangzhou Qidian Technology Co., Ltd.	
Huawei	
Huawei	
JD (City)	
JD (City)	
JD (City)	
LogiOcean	
LogiOcean	
Qingdao Huasen Electronic Industry Holdings Co., Ltd.	
Qingdao Huasen Electronic Industry Holdings Co., Ltd.	
SenseGlobal	
Sinovation Ventures AI Institute	
Sinovation Ventures AI Institute	
Sinovation Ventures AI Institute	

IEEE SA  
STANDARDS  
ASSOCIATION

IEEE Guide for Architectural Framework and Application of Federated Machine Learning

IEEE Computer Society

Developed by the Learning Technology Standards Committee

IEEE Std 3652.1™-2020

IEEE



STANDARDS

## 【国内标准】

参与编写已发布标准：

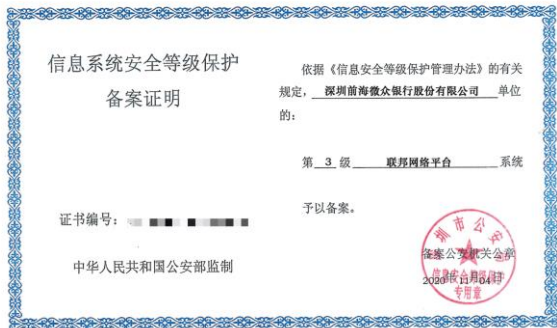
- 参与信通院《基于多方安全计算的数据流通产品技术要求与测试方法》和《联邦学习技术与应用》标准编写
- 金融行业标准：参与央行金融标准化委员会《多方安全计算金融应用技术规划》的标准

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



《信息安全等级保护》三级备案证书



信通院《大数据·联邦学习数据流通产品》认证



信通院《大数据·多方安全计算数据流通产品》认证



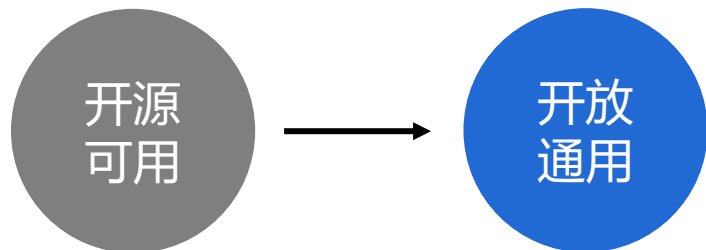
信通院《联邦学习评估专项》



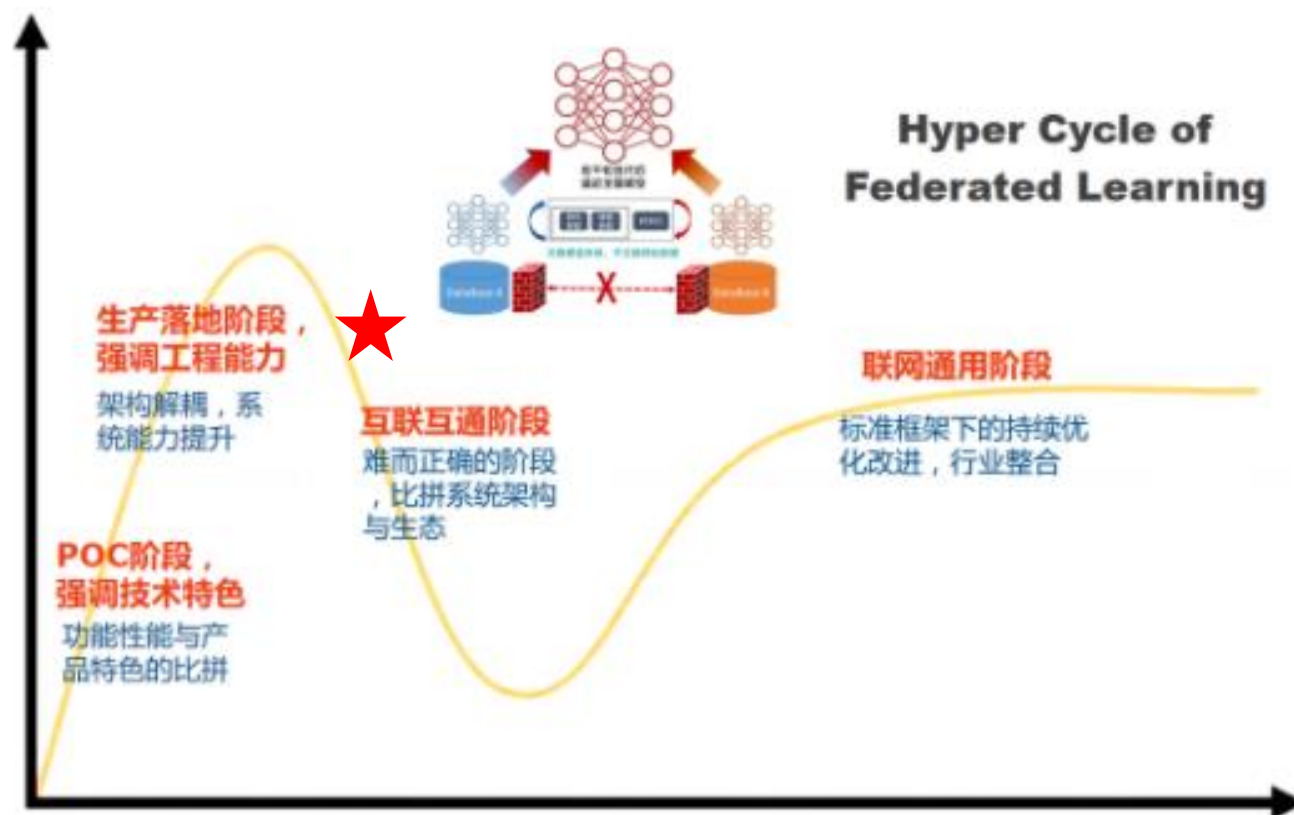
完成银行卡检测中心 (BCTC) 评测

# FATE社区成立互联互通工作组

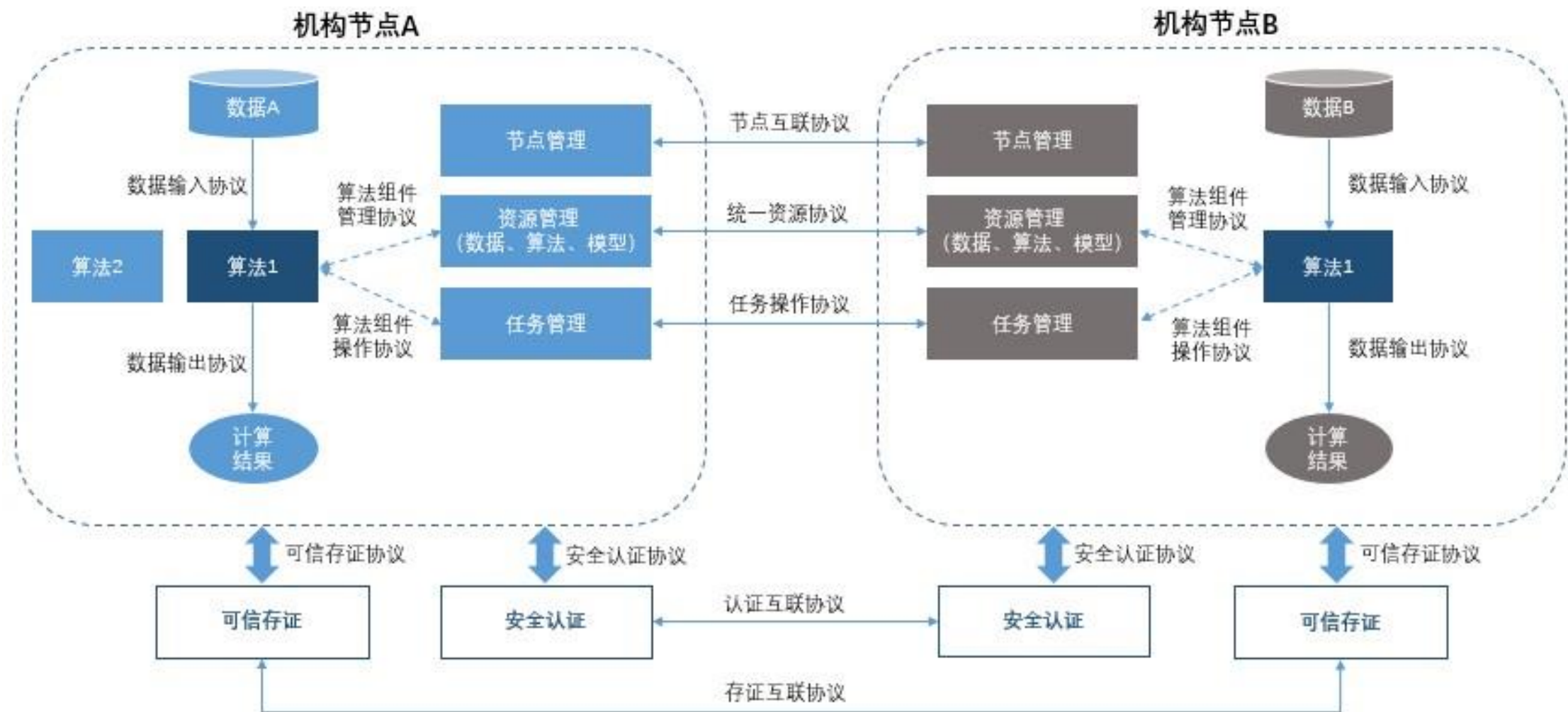
2021年6月24日，联邦学习开源社区 FATE技术委员会召开2021年第二次会议，在中国银联提议下，FATE TSC成立互联互通工作组，由中国银联牵头，成员包括微众银行、VMware、中国电信。标志着联邦学习系统开始从开源可用向开放通用迈进。



【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](mailto: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