BEAS：支持区块链的异步和安全联邦机器学习

BEAS，这是第一个基于区块链的N方FL框架，它使用梯度修剪（与现有的基于噪声和剪裁的技术相比，显示出更好的差异隐私）为训练数据提供严格的隐私保障。

异常检测协议用于最大限度地降低数据中毒攻击的风险，同时使用梯度修剪进一步限制模型中毒攻击的有效性。

BEAS的基本步骤：

1.客户端使用MSP创建加密匿名身份。

2.开始培训流程时，任何客户Ci可以建立一个新的通道c，定义训练参数和模型架构，并通过在本地对自己的私有数据Di进行训练来生成创世区块 Mg。Mg作为频道分类账Lc上的第一个全局块上传。

3.其他客户端连接到背书节点(EP)，从通道分类账请求最新的全局块。他们使用请求的块来初始化预先训练的模型，并通过在自己的私有数据集Di上训练来更新模型，以生成新的局部梯度。

4.客户端Ci将其局部梯度发送给背书节点(EP)，EP创建一个新的局部块，并与订购服务共享。

5.订购服务就区块的订购建立共识，并因此使用点对点协议将其提交到每个背书节点(EP)的账本上。

6.背书节点(EP)检查排队的本地块的数量是否正确≥ 超过合并阈值。如果为true，则会触发合并链码，通过计算异常检测分数来评估每个本地块的质量，并使用联邦平均值聚合块，以生成新的全局块，然后将其发送到通道分类账。

7.重复步骤3至6，直到达到或无限达到共享全局的预期精度。

对抗性中毒

使用FoolsGold防御协议来应对数据中毒攻击。
FG依赖于客户更新之间的相似性，通过比较其梯度更新的相似性来区分诚实的参与者和行为相似的女巫攻击。

Multi-KRUM 防御协议是一种拜占庭弹性梯度聚合算法，可以解决数据中毒攻击。
在每个联邦轮次中，它根据每个本地块与其他所有提交块的偏差对每个本地块进行评分，然后根据评分规则进行相应的梯度聚合。

梯度修剪是一种有效的防御后门子任务上的模型中毒攻击的方法，并将修剪包括在BEA的本地培训回合中。

隐私保护

梯度修剪有助于最小化从共享梯度重建训练数据集的敏感信息