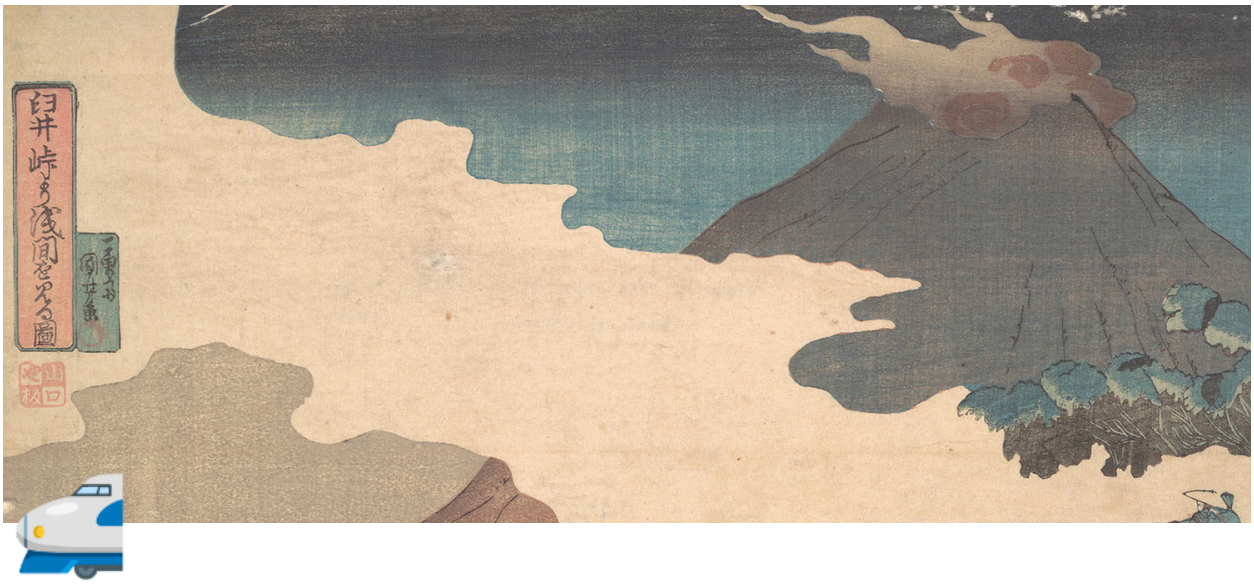


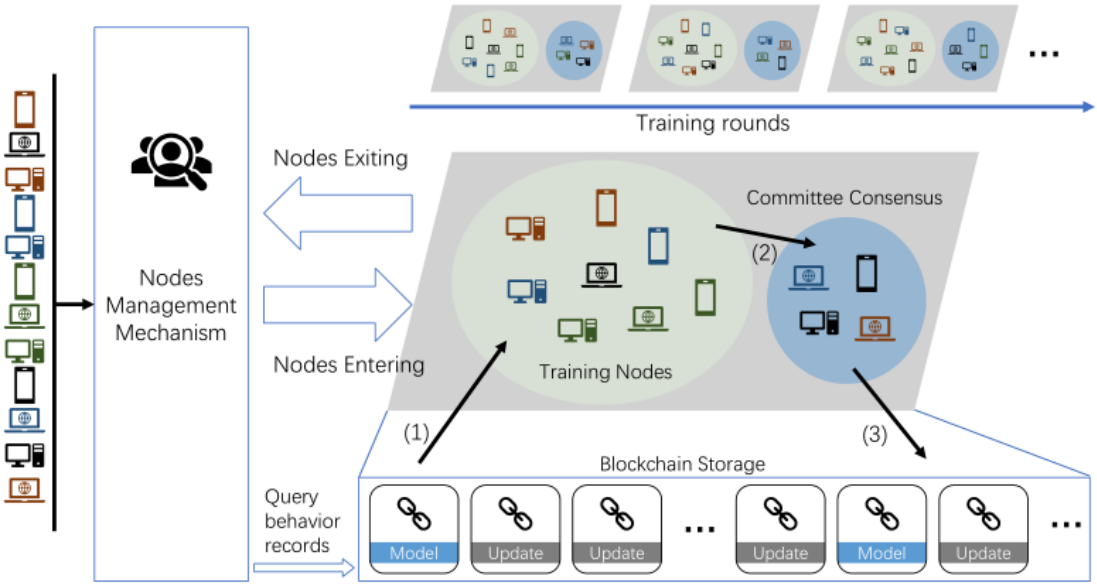
# 基于区块链的委员会共识去中心化联邦学习框架

提出了一种基于区块链的去中心化联邦学习框架，即基于区块链的委员会共识联邦学习框架(BFLC)。框架使用区块链进行全局模型存储和本地模型更新交换。

为了实现BFLC，还设计了一种创新的委员会共识机制，该机制可以有效地减少共识计算量，减少恶意攻击。然后我们讨论了BFLC的可伸缩性，包括理论安全性、存储优化和激励措施。最后，我们使用真实数据集进行实验，以验证BFLC框架的有效性。

在本文中，提出了一种分散的、自治的基于区块链的FL体系结构来解决这些挑战。在FL节点的管理方面，基于联盟链的体系结构确保了节点的权限控制。

在存储方面，我们在模型和更新链上设计了存储模式，通过这种模式，节点可以快速获得最新的模型。每个验证的更新都被记录下来，并在区块链上保持原样。考虑到区块链占用的存储空间较大，部分节点可以放弃历史块以释放存储空间。在块共识机制方面，提出了一种新颖的委员会共识机制，该机制在恶意攻击下仅能增加少量的验证消耗，实现更大的稳定性。在每一轮FL中，更新由少量节点(即委员会)进行验证和打包。委员会共识机制让最诚实的节点相互加强，不断完善全球模式。少量错误或恶意的节点更新将被忽略，以避免破坏全局模型。




## BFLC框架的培训过程。

(1)训练节点获取最新的全局模型并进行局部训练。
(2)训练节点向委员会发送本地更新。
(3)委员会对更新进行验证，并记录新的模型或更新到区块链。

BFLC的存储为联盟区块链系统，只有被授权的设备才能访问FL培训内容。
节点访问当前模型并进行局部训练，将验证后的局部梯度放入新的更新块中。当持续有足够的更新块时，智能合约触发聚合，并生成下一轮的新模型并放置在链上。

## 委员会共识机制(CCM)

CCM将在局部梯度附加到链上之前对其进行验证。
首先由几个诚实节点组成一个委员会，负责局部梯度的验证和块的生成。同时，其余节点进行局部训练，并将局部更新发送给委员会。然后，委员会对这些更新进行验证，并给它们打分。只有合格的更新将打包到区块链。
在下一轮开始时，根据上一轮节点的分数选出新的委员会，这意味着委员会不会再次当选。委员会成员通过将他们的数据作为一个验证集来验证本地更新，验证的准确性成为评分。在综合各个委员会成员的分数后，中位数将成为这次更新的分数。

## CCM的优势：

(1)效率高:只有少数节点会验证更新，而不是向每个节点广播并达成协议。
(2)交叉验证:委员会成员不参加本轮训练。因此，将委员会的本地数据作为验证集。随着每轮委员会成员的轮换，验证集也会发生变化。在这种情况下，实现了对FL模型的交叉验证。
(3)反恶意节点:智能合约将根据验证分数选出性能较好的相应节点，组成下一轮训练的新委员会。这意味着所选的本地数据分布是群居的，节点不是恶意的。

## 节点管理与激励：

为了控制权限，我们指定了组成培训社区的初始节点来负责节点管理，即成为管理员。每个设备在加入培训社区之前必须经过管理人员的验证。该验证方式为黑名单模式:如果设备因错误行为(如提交误导性更新、传播私机)被社区踢出，设备将被拒绝。

## 激励机制：分红机制

许可费:每台设备需要支付全局模型的访问许可费，这些费用由管理人员保管。
利润分配:每轮汇总后，管理者根据提交的更新得分，将奖励分配给相应的节点。
频繁提供更新可以获得更多的奖励，不断更新的全球模型将吸引更多的节点参与。

## 存储优化：

存储开销削减方案:容量不足的节点可以在本地删除历史块，只保留当前轮的最新模型和更新。这样可以解决部分节点存储空间不足的问题，同时保留核心节点的灾难恢复能力和块校验能力。

可信和可靠的第三方存储可能是一个更好的解决方案。区块链只维护每个型号或更新文件所在的网络地址和修改操作的记录。其他节点与存储云服务器进行交互，获取最新型号或上传更新。这种集中存储将负责灾难恢复备份和分布式文件存储服务。