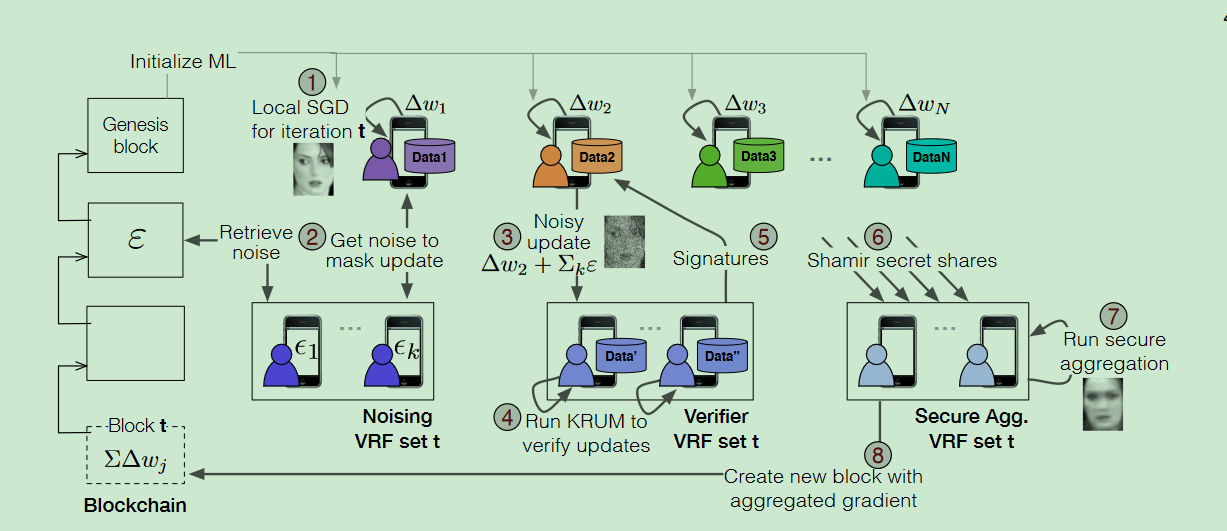
本篇论文提出了一种基于区块链的联邦学习系统——Biscotti。其目的是在一个完全去中心化的联邦学习系统中，利用密码学抵御投毒攻击和梯度泄露攻击的同时，确保系统的可扩展性和容错性。



Biscotti系统通过proof-of-federation（类似于PoS）选举以下四种角色，普通节点、噪声节点、验证节点和聚合节点。系统的设计主要分为噪声添加阶段、梯度验证阶段和梯度聚合阶段三部分。噪声添加阶段中，节点从噪声委员会处获取噪声（差分隐私）以隐藏自己的梯度。梯度验证阶段中，验证委员会利用Multi-Krum过滤掉投毒梯度。梯度聚合阶中，聚合委员会利用安全聚合算法聚合梯度，消除噪声，防止训练效率下降。最后将包含聚合梯度的区块进行广播。

Biscotti与其他区块链不同之处在于，由于每一次基于最新区块的选举对于所有节点来说是相同的，区块链几乎不会分叉，节点之间的竞争也不会像Bitcoin系统那样激烈。

Biscotti具有以下局限性：

1. Multi-Krum在节点大量波动的环境下可能失效，因为其需要大量的诚实梯度才能生效。且Multi-Krum会筛掉基于non-iid数据训练出来的诚实梯度。
2. 受到网络的限制，系统不能训练参数多且复杂的大型神经网络。
3. 因为聚合的模型是没有噪声的，系统可能会受到基于全局模型的信息泄露攻击。
4. 系统基于的一大假设是权益多的节点不会尝试颠覆系统。如果某权益多的节点是为了颠覆系统而先假装成诚实节点的话，系统将被攻破。