一、联邦学习的定义

2016 年是人工智能（AI）成熟的一年。随着 AlphaGo 击败了顶尖的人类围棋玩家，我们真正见证了 AI 的巨大潜力，并开始期望在许多包括无人驾驶汽车、医疗保健、金融等的应用中，使用更复杂、尖端的人工智能技术。如今，人工智能技术在几乎所有行业都能发挥其优势。2016 年，AlphaGo 使用了总计 300000 盘比赛作为训练数据，以取得优异的成绩。

随着 AlphaGo 的成功，人们自然希望像 AlphaGo 这样的大数据驱动的人工智能能够在我们生活的各个方面很快实现。然而，现实情况有些令人失望：除了少数行业外，大多数领域的数据都很有限或质量较差，使得人工智能技术的实现比我们想象的要困难。是否可以通过跨组织传输数据，将数据融合到一个公共站点中？事实上，在许多情况下，打破数据源之间的障碍即使不是不可能的，也是非常困难的。一般来说，任何人工智能项目所需的数据涉及多种类型。例如，在人工智能驱动的产品推荐服务中，产品销售商拥有产品信息、用户购买数据，但没有描述用户购买能力和支付习惯的数据。在大多数行业中，数据以孤岛的形式存在。由于行业竞争、隐私安全和复杂的管理程序，甚至同一公司不同部门之间的数据集成也面临着巨大的阻力。几乎不可能将分散在全国各地的数据和机构进行整合，否则成本是难以承受的。

联邦学习（Federated Learning）是一种新兴的人工智能基础技术，在 2016 年由谷歌最先提出，原本用于解决安卓手机终端用户在本地更新模型的问题，其设计目标是在保障大数据交换时的信息安全、保护终端数据和个人数据隐私、保证合法合规的前提下，在多参与方或多计算结点之间开展高效率的机器学习。其中，联邦学习可使用的机器学习算法不局限于神经网络，还包括随机森林等重要算法。联邦学习有望成为下一代人工智能协同算法和协作网络的基础。

令 N 个数据所有者为{F1, …, FN}，他们都希望整合各自的数据{D1, …, DN}来训练出一个机器学习模型。传统的方法是把所有的数据放在一起并使用 D =

D1∪…∪DN 来训练一个模型 MSUM。联邦学习系统是一个学习过程，数据所有者共同训练一个模型 MFED，在此过程中，任何数据所有者 Fi 都不会向其他人公开其数据 Di。此外，MFED 的精度表示为 VFED，应该非常接近 MSUM 的性能，VSUM。设 δ 为非负实数，如果|VFED - VSUM| < δ，我们可以说联邦学习算法具有 δ -accuracy 损失。

根据参与各方数据源分布的情况不同，联邦学习可以被分为三类：横向联邦学习、纵向联邦学习、联邦迁移学习。

横向联邦学习：在两个数据集的用户特征重叠较多而用户重叠较少的情况下，我们把数据集按照横向(即用户维度)切分，并取出双方用户特征相同而用户不完全相同的那部分数据进行训练。比如业务相同但是分布在不同地区的两家企业，它们的用户群体分别来自各自所在的地区，相互的交集很小。但是，它们的业务很相似，因此，记录的用户特征是相同的。

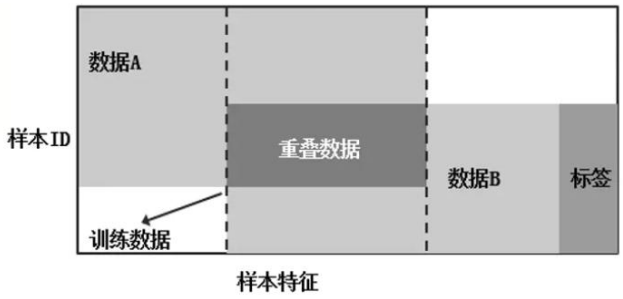

图 1.1

纵向联邦学习：在两个数据集的用户重叠较多而用户特征重叠较少的情况下，我们把数据集按照纵向（即特征维度）切分，并取出双方用户相同而用户特征不完全相同的那部分数据进行训练。比如有两个不同机构，一家是某地的银行，另一家是同一个地方的电商。它们的用户群体很有可能包含该地的大部分居民，因此用户的交集较大。但是，由于银行记录的都是用户的收支行为与信用评级，而电商则保有用户的浏览与购买历史，因此它们的用户特征交集较小

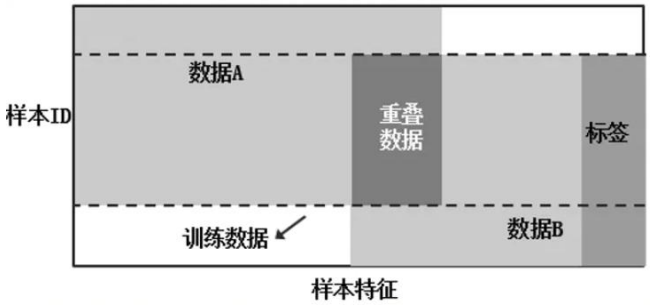

图 1.2

联邦迁移学习：在两个数据集的用户与用户特征重叠都较少的情况下，我们不对数据进行切分，而可以利用迁移学习来克服数据或标签不足的情况。这种方法叫做联邦迁移学习。

比如有两个不同机构，一家是位于中国的银行，另一家是位于美国的电商。由于受到地域限制，这两家机构的用户群体交集很小。同时，由于机构类型的不同，二者的数据特征也只有小部分重合。在这种情况下，要想进行有效的联邦学习，就必须引入迁移学习，来解决单边数据规模小和标签样本少的问题，从而提升模型的效果。

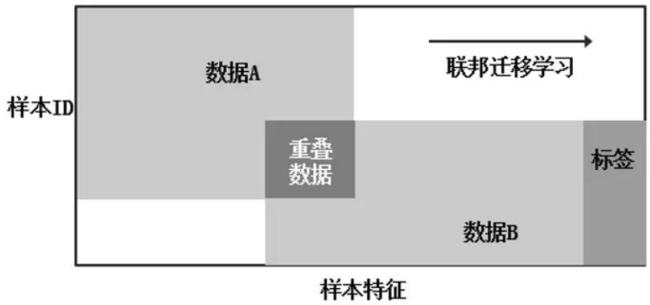

图 1.3

二、联邦学习的流程

客户端-服务器架构的联邦学习流程

在物理层面上，联邦学习系统一般由数据持有方和中心服务器组成。各数据持有方的本地数据的数量或特征数可能并不足以支持一次成功的模型训练，因此需要其他数据持有方的支持。而联邦学习中心服务器的工作类似于分布式机器学习的服务器，其收集各数据持有方的梯度，并在服务器内进行聚合操作后返回新

的梯度。在一次联邦学习的合作建模过程中，数据持有方对本地数据的训练仅发生在本地，以保护数据隐私，迭代产生的梯度在脱敏后被作为交互信息，代替本地数据上传给第三方受信任的服务器，等待服务器返回聚合后的参数，对模型进行更新[8]。图 2 展示了客户端-服务器架构的联邦学习流程。

步骤 1：系统初始化。首先由中心服务器发送建模任务，寻求参与客户端。客户端数据持有方根据自身需求，提出联合建模设想。在与其他合作数据持有方达成协议后，联合建模设想被确立，各数据持有方进入联合建模过程。由中心服务器向各数据持有方发布初始参数。

步骤 2：局部计算。联合建模任务开启并初始化系统参数后，各数据持有方将被要求首先在本地根据己方数据进行局部计算，计算完成后，将本地局部计算所得梯度脱敏后进行上传，以用于全局模型的一次更新。

步骤 3：中心聚合。在收到来自多个数据持有方的计算结果后，中心服务器对这些计算值进行聚合操作，在聚合的过程中需要同时考虑效率、安全、隐私等多方面的问题。比如，有时因为系统的异构性，中心服务器可能不会等待所有数据持有方的上传，而是选择一个合适的数据持有方子集作为收集目标，或者为了安全地对参数进行聚合，使用一定的加密技术对参数进行加密，这些方法将会在后面的章节中详细讨论。

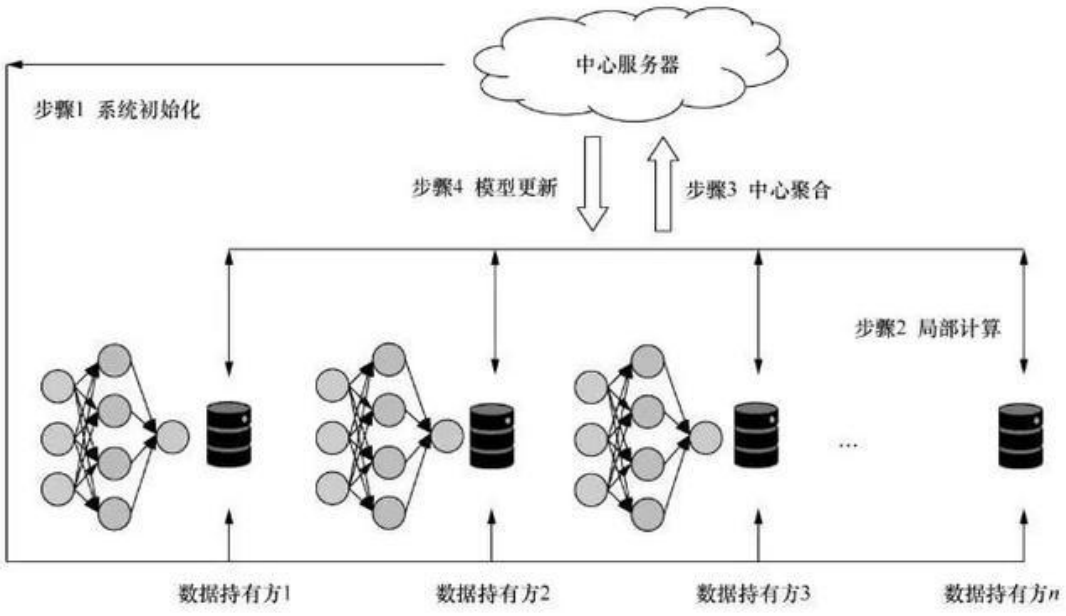

图 2.1 客户端-服务器架构的联邦学习流程

步骤 4：模型更新。中心服务器根据聚合后的结果对全局模型进行一次更新，并将更新后的模型返回给参与建模的数据持有方。数据持有方更新本地模型，并开启下一步局部计算，同时评估更新后的模型性能，当性能足够好时，训练终止，联合建模结束。建立好的全局模型将会被保留在中心服务器端，以进行后续的预测或分类工作。

上述过程是一个典型的基于客户端服务器架构的联邦学习过程。但并不是每个联邦学习任务都一定要严格按照这样的流程进行操作，有时可能会针对不同场景对流程做出改动，例如，适当地减少通信频率来保证学习效率，或者在聚合后增加一个逻辑判断，判断接收到的本地计算结果的质量，以提升联邦学习系统的鲁棒性。

三、应用场景

联邦学习作为一种创新的建模机制，可以在不影响数据隐私和安全的情况下，对来自多个方面的数据进行统一的建模，在销售、金融和许多其他行业中有着很好的应用前景，在这些行业中，由于知识产权、隐私保护和数据安全等因素，数据不能直接汇聚用来训练机器学习模型。

智能零售

以智能零售为例。其目的是利用机器学习技术为客户提供个性化服务，主要包括产品推荐和销售服务。智能零售业务涉及的数据特征主要包括用户购买力、用户个人偏好和产品特征。在实际应用中，这三个数据特性可能分散在三个不同的部门或企业中。例如，一个用户的购买力可以从他的银行存款中推断出来，他的个人偏好可以从他的社交网络中分析出来，而产品的特征则由一个电子商店记录下来。在这种情况下，我们面临两个问题。首先，为了保护数据隐私和数据安全，银行、社交网站和电子购物网站之间的数据壁垒很难打破。因此，不能直接聚合数据来训练模型。第二，三方存储的数据通常是异构的，传统的机器学习模型不能直接处理异构数据。目前，传统的机器学习方法还没有有效地解决这些问题，阻碍了人工智能在更多领域的推广应用。

联邦学习和迁移学习是解决这些问题的关键。首先，利用联邦学习的特点，可以在不导出企业数据的情况下，为三方建立机器学习模型，既充分保护了数据隐私和数据安全，又为客户提供个性化、有针对性的服务，还顺便实现了互惠互利。同时，我们可以利用迁移学习来解决数据异质性问题，突破传统人工智能技术的局限性。因此，联邦学习为我们构建跨企业、跨数据、跨域的大数据和人工智能生态圈提供了良好的技术支持。

可以使用联邦学习框架进行多方数据库查询，而无需公开数据。例如，假设在金融应用程序中，我们有兴趣检查多方借款，这是银行业的一个主要风险因素。当某些用户恶意向一家银行借款以支付另一家银行的贷款时，就会发生这种情况。多方借款是对金融稳定的威胁，因为大量的此类非法行为可能导致整个金融体系崩溃。为了找到这样的用户而不在银行 A 和银行 B 之间公开用户列表，我们可以利用联邦学习框架。特别是，我们可以使用联邦学习的加密机制，对每一方的用户列表进行加密，然后在联邦中找到加密列表之间的交集。最终结果的解密提供了多方借款人的列表，而不会将其他“好”用户暴露给另一方。正如我们将在下面看到的，这个操作对应于纵向联邦学习框架。

智慧医疗

智慧医疗是另一个领域，我们预计这将大大受益于联邦学习技术的兴起。疾病症状、基因序列、医学报告等医学数据是非常敏感和私密的，然而医学数据很难收集，它们存在于孤立的医疗中心和医院中。数据源的不足和标签的缺乏导致机器学习模型的性能不理想，成为当前智慧医疗的瓶颈。我们设想，如果所有的医疗机构都联合起来，共享他们的数据，形成一个大型的医疗数据集，那么在该大型医疗数据集上训练的机器学习模型的性能将显著提高。联邦学习与迁移学习相结合是实现这一愿景的主要途径。迁移学习可以应用于填补缺失的标签，从而扩大可用数据的规模，进一步提高训练模型的性能。因此，联邦迁移学习将在智慧医疗发展中发挥关键作用，它可能将人类健康保健提升到一个全新的水平。

网络数据分析

网络数据分析(Network Data Analytics Function, NWDAF) 是 5G 技术中一项重要的内容，它允许网络中的设备利用人工智能技术监测和分析网络的运行情况。为了实现这一功能，NWDAF 可以获取网络中的各部分数据内容。然而，网络中的很多数据会涉及较为敏感的信息，完全开放的数据内容将会带来较高的安全风险。采用本文所提出的基于区块链的联邦学习架构，每个核心网的实体可以在其内部运行联邦学习算法，仅将所学习的本地模型发送给 NWDAF 功能实体，从而在保护数据安全的同时，提升网络的性能表现。

四、联邦学习与区块链

联邦学习不仅是一种技术标准，也是一种商业模式。当人们意识到大数据的影响时，他们首先想到的是将数据聚合在一起，通过远程处理器计算模型，然后下载结果供进一步使用。云计算就是在这种需求下产生的。然而，随着数据隐私和数据安全的重要性越来越高，以及公司利润与其数据之间的关系越来越密切，云计算模型受到了挑战。然而，联邦学习的商业模式为大数据的应用提供了一个新的范例。当各个机构所占用的孤立数据不能产生理想的模型时，联邦学习机制使得机构和企业可以在不进行数据交换的情况下共享一个统一的模型。此外，在区块链技术的共识机制的帮助下，联邦学习可以制定公平的利润分配规则。无论数据拥有的规模如何，数据拥有者都会被激励加入数据联盟，并获得自己的利润。我们认为，建立数据联盟的业务模型和联邦学习的技术机制应该一起进行。我们还将为各个领域的联邦学习制定标准，以便尽快投入使用。

针对谷歌提出的安卓设备上联邦学习模型的局限性进行了探讨。谷歌提出的联邦学习模型 Vanilla FL(图 4.1 a)由每个设备在本地进行模型训练和参数上传，通过一个中央服务器来进行模型的更新，使得用户数据只在本地设备上进行处理，以此来保证用户的数据隐私。其局限性在于该模型只依赖于一个单一的中央

服务器，容易受到服务器故障的影响。同时也没有合适的激励基本来激励用户提供数据训练和上传模型参数。为了解决上述这些问题，作者提出了基于区块链的区块链联邦学习（BlockFL），用区块链网络来替代中央服务器，区块链网络允许交换设备的本地模型更新，同时验证和提供相应的激励机制。

如图 4.1 所示，BlockFL 的逻辑结构由设备和矿工组成。矿工在物理上是随机选择的设备或单独的节点。每个设备在 BlockFL 网路中计算并上传本地模型更新到相关联的矿工，矿工交换和验证所有的本地模型更新，然后运行工作量证明机制 POW。当矿工完成 POW，将生产一个新的区块，区块里记录了验证的本地模型的更新，然后将存储本地聚合模型更新的区块添加到区块链中，再由每个设备下载，设备从新的块中计算全局模型更新。本地设备上的全局模型更新可以确保在矿工或者设备故障时不会影响其他设备的全局模型更新。这样普通设备用户和矿工用户都能得到最新的全局更新模型，以此形成对用户的激励机制。同时作者还对 BlockFL 由区块链网络引起的延迟进行了分析。考虑通过调整块的生成速率即 POW 难度来使延迟最小化，以此增加系统的实用性。

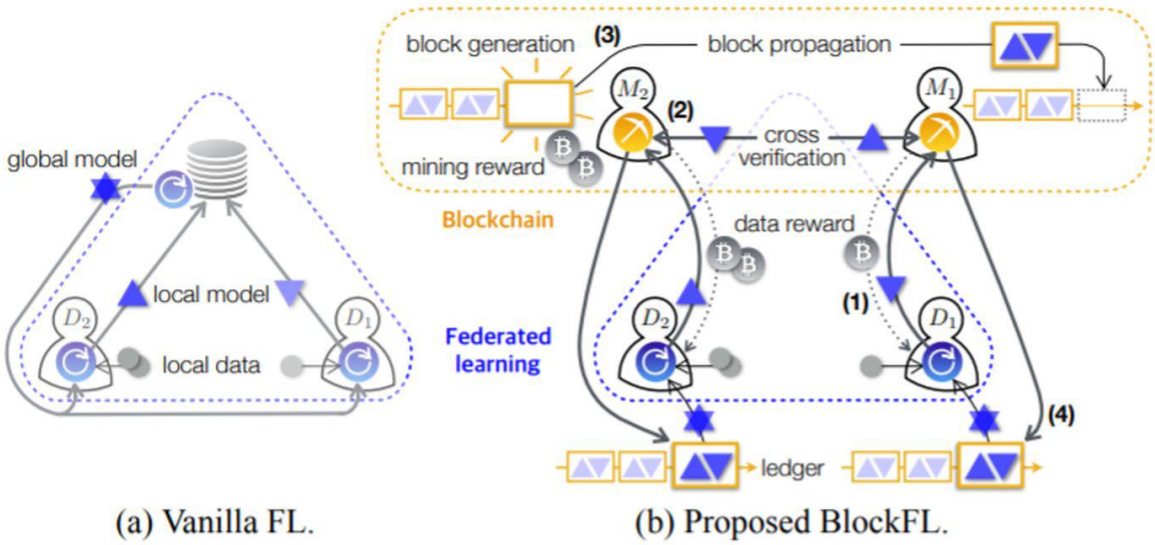

图 4.1　Vanilla FL 和 BlockFL 的系统结构

1、资源共享

在下一代无线网络中，终端设备数量的迅猛增长以及大量低时延应用的出现，使得网络的频谱、数据等资源变得日趋紧张。资源共享是解决资源紧缺问题的有效手段。如何建立有效的资源感知、管理机制，确定资源优化分配的方案，是实现资源高效共享的关键。

利用空闲的资源信息进行分析预测可以高效地进行资源的动态共享。而中心化的资源信息数据库具有较高的维护及通信成本，同时面临单点故障等安全风险。通过利用区块链进行资源信息动态认知，不仅可以降低成本，其分布式特性还可以支持更多的用户接入。但在实际应用中，还需要统筹考虑业务特性、资源信息以及节点能力等，实现资源的动态分配。而区块链本身难以达成上述功能。考虑无线环境中设备计算和存储资源的限制，基于本文所提出的技术方案，我们将联邦学习与区块链相融合，实现资源的智能共享。首先从区块链获取并分析可共享的资源信息；进而依据可用资源、业务负荷、用户特性以及服务质量(QoS)要求等，设计系统的资源共享效用函数；最后以效用函数最大化为目标，通过联邦学习计算适用于分布式边缘场景的资源优化分配策略。在所提出的区块链赋能联邦学习的资源共享场景中，有闲置频谱、数据等资源的用户成为资源提供者，有相应资源使用需求的用户则作为消费者。多个资源提供者通过区块链节点网络，为资源请求者提供相应的共享资源。资源共享的事件同时作为交易被记录在区块链中，资源使用者可以通过区块链支付资源的使用费用。

2、智能交通

将区块链与联邦学习的融合方案应用于智能交通领域，可以提升用户的驾驶体验、车辆运行安全以及交通效率。其中，车辆作为用户层，持有数据并运行本地联邦学习训练。路边单元(Road Side Unit, RSU) 则作为边缘服务层，维护区块链并执行模型参数的聚合。具体而言，联邦学习所训练的模型，可用于车联网中交通流量预测、车辆间多媒体资源共享策略制定以及车辆的驾驶路径智能规划等。而区块链可以在多个参与方之间建立一个可信机制，并且确保所传递数据的可靠性。