iDML：激励式去中心化机器学习

Haoxiang Yu*、Hsiao-Yuan Chen*、Sangsu Lee*、Sriram Vishwanath*、Xi Zheng†、Christine Julien*
*德克萨斯大学奥斯汀分校电气与计算机工程系{hxyu, littlecircle0730, sethlee, sriram, c.julien}@utexas.edu
†计算系，麦考瑞大学，james.zheng@mq.edu.au

arXiv:2304.05354v1 [cs.LG] 10 Apr 2023

摘要—随着去中心化和机会式学习方法在机器学习中的日益兴起，终端设备越来越多地被要求使用其自行收集的众包数据，在设备上训练深度学习模型。从资源消耗和隐私保护的角度来看，这些方法都颇具吸引力。当设备直接受益于训练后的模型时，激励是隐性的——参与设备的资源因协作所产生的更高准确率模型的可用性而得到激励。然而，当终端用户设备被要求为主要使他人受益的任务贡献其资源（例如计算、通信和数据）时，就必须提供明确的激励机制，例如为邻居设备所需、但设备所有者并不感兴趣的任务训练模型。在本项目中，我们提出了一种基于区块链的新型激励机制，用于完全去中心化和机会式学习架构。我们利用一个智能合约，不仅为终端设备参与去中心化学习提供明确的激励，还创建了一种完全去中心化的机制，用于检查和反思学习架构的行为。

索引词——普适计算、去中心化机器学习、区块链、激励机制、智能合约

I. 引言

随着机器学习技术的不断发展，以及个人设备计算能力的日益增强，机器学习已广泛应用于各种面向用户的任务，例如图像分类、输入预测、智能家居系统等 [1]。这些任务通常依赖深度神经网络（DNN），从大型数据集中学习模式。要在这些任务中实现高准确率，需要大量训练数据。然而，由于隐私问题，以及终端用户设备与云端之间通信带宽有限，收集足够的数据来训练稳健的模型颇具挑战性 [2]。

为提升用户隐私，并让应用能够在通信受限的环境中运行，机器学习已拓展出多种分布式学习方法，在这些方法中，终端设备承担了部分训练负担。最广为人知的是联邦学习方法：中央服务器协调大量终端用户设备，迭代训练共享的全局模型。终端设备接收模型快照，使用本地可用的数据对模型进行若干轮训练，然后向中央服务器发送模型更新。服务器聚合收到的更新，生成一个新的全局模型，然后重复这一过程。在纯联邦学习设计中，中央服务器没有自己的任何训练数据，这使其难以检测终端节点对共享模型的贡献是否有效。

在某些情况下，依靠中央服务器来协调分布式终端设备集的学习过程，要么不可行（例如，设备无法良好连接到互联网），要么并非最优选择（例如，设备希望学习更加个性化的模型，而非单一的全局模型）。因此，出现了一些方法，它们将学习过程完全去中心化，转而仅依靠终端用户设备之间机会式的设备间协作。现有研究表明，在多种条件下，这些去中心化方法都能实现较高的模型准确率 [3],[4]。本文将仅依靠设备间相遇在设备端训练模型的方法称为去中心化机会式学习。去中心化机会式学习利用短暂相遇，与相遇到的邻居及其本地（隐私）数据协作，支持设备端训练。一个简单的例子是，八卦学习 [4]将整个学习过程去中心化，仅通过节点之间机会式的成对交换，逐步学习与集中式方法所学习的相同共享全局模型。另一个例子是机会式协作学习 （OppCL） [3], 。设备并不交换为收敛到全局模型而学习的梯度，而是学习个体模型，这些模型受到设备自身数据与其交互中遇到的数据的独特组合的影响。在 OppCL 中，一台设备遇到另一台设备时，会将自己的个人模型参数分享给邻居；邻居随后使用自己的本地数据，针对发起学习的设备的目标计算一次特定更新。

去中心化机会式学习需要终端设备开展许多活动，而每项活动都需要设备贡献资源。从本质上说，任何去中心化学习方法都依赖终端设备捐出其数据、计算和通信资源。因此，激励参与 学习过程中的参与仍然是实现去中心化机 会式学习实践应用的一项重大未解决挑战。为了支持设备端训练，设备必须收集训练数据，而这些数据可能需要使用有效标签进行标注。例如，如果应用是训练目标检测系统 [5],，所收集的数据是照片，并且每张照片都必须标注有所

框架中的主要对象。如果应用是下一个词预测 [6], 所收集的数据是用户输入的可能敏感的文本，而标签则根据输入的词语序列“免费”获得。数据收集和标注会明确地（例如，用户主动标注数据）或根据标注所需的计算量隐式地消耗资源。数据必须被存储，并且必须用于训练，这需要每个终端节点提供计算资源。随着参与设备开展协作，它们之间的交换也会消耗宝贵的通信资源。

此外，虽然去中心化机会式学习的设计通过避免直接共享原始数据来保护用户隐私，但模型更新的接收方很难确认其他参与方是否忠实履行了对算法的义务。此外，由于整个过程是去中心化且机会式的，因此很难检查和反思模型的溯源——这需要存储并共享训练期间发生的情况、模型准确率的变化、用于训练模型的数据等。更一般地说，由于采用了去中心化架构，要避免或检测各种攻击者可能颇具难度，其中包括试图中断训练以及试图破坏训练的攻击者。

这一问题完全去中心化且分布式的特性，使其自然适用于区块链 [7],——一种分布式账本技术，以及与之相关的智能合约。智能合约一词最初指法律合同的自动化 [8], 如今通常指在分布式账本的多个节点上同步运行的代码脚本 [9]。区块链以去中心化方式进行存储和计算的天然机制，使其非常适合与去中心化机会式学习相结合。具体而言，我们提出将去中心化机会式学习的优势与智能合约相结合，以：(1) 有力激励各方参与机会式学习；(2) 提供一种在去中心化学习中记录和反思模型溯源的方法；以及 (3) 探索一种能够抵御明确定义的攻击模型的新型去中心化机会式学习流程。本文作出了以下具体贡献：

- 我们开发了一种基于区块链的 智能合约 ，可应用于去中心化机会式学习架构，以激励参与者为学习过程做出贡献。
- 我们在智能合约中设计了相关机制，使其能够记录和检查与完全去中心化学习执行进度相关的重要信息。
- 我们展示了如何利用该智能合约防范针对新激励机制和去中心化机会式学习算法的攻击。
- 我们通过模拟评估了激励系统，并采用了不同的机会式但完全去中心化的学习算法。开发的技术将以开源成果的形式发布。

本文的组织如下：在第二节中，我们讨论去中心化学习、智能合约和激励机制。在第三节中，我们介绍系统设计和智能合约工作流程。在第四节中，我们使用模拟系统，通过两种不同的学习算法、两个不同的数据集，以及去中心化学习中的两种典型数据分布（独立同分布/非独立同分布），对我们提出的系统的行为进行基准测试。在论文的最后一节中，我们总结全文并探讨未来可能的工作。

II. 相关工作

近年来，研究界提出了若干新的分布式学习模型，为利用用户数据和计算资源提供了新的机会，同时将隐私泄露风险降至最低。本研究的相关工作主要包括四个方面：(1) 分布式与去中心化学习方法；(2) 区块链和智能合约；(3) 分布式与去中心化学习的激励机制；以及 (4) 针对激励机制和去中心化学习算法的攻击。

A. 分布式学习

移动设备能力的提升以及对数据隐私的需求，推动了联邦学习和去中心化学习的发展。在联邦学习中，设备协作构建全局模型，同时保护每台设备的数据隐私 [10], [11]。联邦学习在普适计算中的应用包括唤醒词检测（在智能家居语音助手中也称为关键词检测），此类应用中，联邦学习能够保护用户终端设备收集的、可能涉及隐私的音频数据 [12]。另一个经典的联邦学习应用是在移动设备键盘上进行下一个词预测 [13]。其他应用还探索了设备端图像分类和图像处理 [14]。

这些传统的联邦学习方法假设存在一个单一的中央协调器，而模型聚合中各设备的目标是协同学习一个由所有参与者共享的全局模型。这不同于去中心化和机会式方法，在这些方法中，学习过程仅通过设备之间的机会性相遇推进。在本研究中，我们探讨两种不同的去中心化机会式学习方式：基于 Gossip 的学习 [4] 和机会式协作学习 [3]。在基于 Gossip 的学习中，每当设备与另一台设备相遇时，就会执行一个合并-更新-发送周期。在此过程中，遇到的邻居会分享其本地训练的模型，接收设备将收到的模型合并到自己的本地模型中，然后仅使用本地数据对合并后的模型进行训练。当然，这通常是一个双向过程；在双向相遇中，两台设备会分别独立执行合并-更新-发送流程。在基于 Gossip 的学习中，目标是让一组间歇互连的节点最终学会一个一致的共享全局模型。相比之下，在机会式协作架构中，每台设备都致力于学习自己的个性化模型，同时根据需要机会性地整合基于邻居本地数据的学习成果。在机会式协作学习中，一台设备

与另一台设备相遇时，会执行一个发送-训练-返回-合并周期。在此过程中，当设备与邻居相遇时，它会向邻居发送一份本地存储模型的副本。邻居使用自己的本地数据对该模型进行一轮训练，然后返回更新后的模型。设备将更新后的模型与已存储的模型合并，并继续使用本地数据进行训练。

从这些描述可以看出，这两种模型都要求设备贡献本地资源，以支持自身及其他设备的学习过程。设计这样一个去中心化且机会性的系统所面临的重大挑战，是激励设备以安全的方式为共同利益贡献其本地资源。这正是本文所要解决的主要问题。

B. 区块链和智能合约

在本文中，我们使用智能合约作为程序，以公平性、安全性和可审计性执行我们的方法。在此背景下，智能合约是一种能够在区块链平台上自动执行的计算机程序。具体而言，我们利用区块链对智能合约执行的支持，实现本文所述的激励机制。智能合约部署后，所有参与者都可以查看该合约是否公平，以及执行该合约是否符合自身最佳利益。此外，参与者所采取的所有行动也可由智能合约中的其他参与者查看；现有研究还表明，在区块链上执行智能合约可以保证投票结果的正确性 [15]。

虽然区块链通常与数字货币联系在一起，但如今已有多个平台将区块链应用于数字货币之外。尤其是，以太坊生态系统允许用户在区块链上运行自定义程序 [16]。例如，用户可以使用以太坊将合约转换为编程语言，将程序编译为字节码，并在以太坊虚拟机（EVM）上执行。由于以太坊虚拟机（EVM）中的合约能够自行执行，我们将这种程序称为智能合约。

C. 激励机制

本研究旨在提供数字激励，鼓励用户为去中心化学习算法贡献自己的资源。现有研究已将博弈论应用于为集中式联邦学习设计激励机制 [17]–[20]。在博弈论中，参与者会做出影响其他参与者行动的个人决策。Zhang 等人将斯塔克尔伯格博弈用于激励参与联邦学习，并由服务器担任领导者、边缘节点担任跟随者 [21]。该系统分两个阶段运行：首先，服务器公布总奖励；随后，边缘节点根据该信息制定训练策略，以最大化各自的奖励。Lim 等人运用合作博弈论，通过根据模型所有者对模型聚合过程的边际贡献给予奖励，分层激励联邦学习 [22]。

研究人员还考虑了通过拍卖来支持联邦学习场景中的激励。先前的研究探索了多种不同的拍卖策略，包括密封投标、正向拍卖、反向拍卖、双向拍卖和组合拍卖 [17], [23], [24]。此外，Zhu 等人还探讨了拍卖过程的不同方面，包括与联邦学习相关的算力、感知、数据资源和训练资源 [20]。然而，博弈论和拍卖方法存在局限，因为它们假设所有参与者的行为方式都相同。此外，这些方法并不安全，也缺乏可审计性。例如，它们无法检测攻击，也无法记录学习进度所需的关键信息。

除了博弈论和基于拍卖的机制之外，近期研究还探索了区块链在设计激励机制中的应用，尤其是针对涉及中央协调方的联邦学习方法。Wang 等人设计了一种联邦学习框架，允许客户端将本地梯度作为交易在区块链上共享。指定的工作节点会验证这些交易，并将其打包成区块 [18]。类似地，Bao 等人提出的 FLChain 是一个基于区块链的生态系统，可确保溯源并维护联邦学习模型的可审计性 [25]。这些研究展示了如何有效发现并移除不诚实节点。它们还展示了在保障用户隐私的同时，使学习过程具备可审计性的可能性。更一般地说，这些研究阐明了保密性、可审计性和公平性这几个目标 [25], ，我们也将用它们来构建研究框架。

然而，这些将区块链应用于分布式学习激励的方案，只关注涉及中央协调方的联邦学习场景；对于完全去中心化的学习结构，这些方案并不直接适用，因为我们不假设所有设备都会请求全局模型以开展下一轮训练。此外，它们为支持学习过程本身而采用的信息共享方案严重依赖区块链，这会带来极高的成本，并将其潜在适用范围限制在能够承担这笔成本的应用中。相比之下，我们提出仅通过智能合约与区块链进行与模型溯源和激励相关的必要交互。这样一来，我们便将分布式学习协议本身置于区块链之外，从而能够采用更灵活且注重资源效率的实现方式。

D. 激励型去中心化学习场景中的攻击者

一般而言，本文提出的去中心化学习和激励机制面临两种主要类型的攻击，我们将其称为激励机制攻击和学习攻击。尽管本文侧重于为参与者提供激励，但该设计也能保护系统免受这两类攻击。

激励机制攻击。 激励机制攻击 是由激励机制本身的设计所引发的攻击。在此类攻击中，攻击者受到激励机制所提供奖励的驱使，这里只精品

可能会试图不付出实际努力就获取奖励（例如，提供虚假或无用的训练信息）。为挫败激励机制攻击，我们精心设计了激励机制，以检测并防止此类攻击，具体内容将在下文第三节中介绍。

学习攻击。去中心化学习的分布式特性使其容易受到各种可能扰乱该过程的攻击。具体而言，这些攻击可分为：（1）规避攻击，攻击者旨在通过使用对抗性测试数据使模型做出错误预测 [26]；（2）投毒攻击，攻击者污染训练数据以使模型错误分类输入 [27]；以及（3）探索性攻击，攻击者逆向分析模型，试图恢复有关训练数据的信息 [28]。在本文所讨论的去中心化机会式学习方法中，投毒攻击最为相关；在本文余下部分，我们将此类攻击简称为学习攻击。

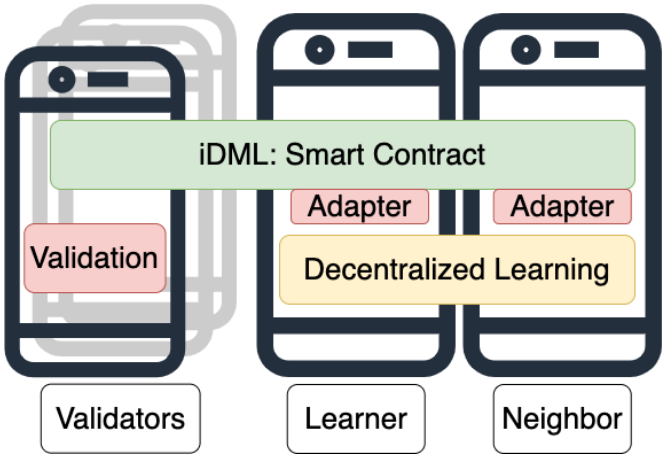

图 1：系统架构

目前已有一些用于检测这些学习攻击的解决方案，但截至目前，它们仅被设计用于集中式联邦学习场景。例如，Sun 等人识别了联邦学习中的后门攻击，并提出了范数阈值法，其中中央服务器会拒绝任何范数大于某个阈值 M [29] 的模型更新。他们表明，其性能取决于系统中对手节点所占的比例。Blanchard 等人提出的 Krum 是一种聚合规则，可用于使分布式随机梯度下降计算能够抵御拜占庭故障 [30]。

由于在去中心化环境中，客户端完全掌控数据，因为它们是数据的唯一所有者，因此也可以通过简单地将目标类别 [27] 中训练样本的标签翻转，再进行训练，发起一种简单的学习攻击。

现有针对这些攻击的研究主要从节点或模型层面来应对，而非从去中心化系统层面着手。此外，现有解决方案依赖中央服务器的全局视图，也就是说，它们支持中心化联邦学习，而非去中心化方法。相比之下，我们的方法通过智能合约和投票机制，使任何参与者都能识别并丢弃无法提高其他参与者所提供模型准确率的模型。在系统层面，随着时间推移，持续作出有害贡献或未能改进的用户将受到惩罚，并自动从环境中移除。

III. 系统设计

本研究提供了一个通用平台，以激励用户参与去中心化机会式学习。在去中心化机会式学习中，参与者贡献计算、通信和数据等资源，这对学习过程的成功至关重要，尤其会影响所学模型能够达到的准确率。图 1 抽象地展示了这一激励机制，称为 iDML用于激励的去中心化机器学习，涉及现有的去中心化机会式学习算法实现。

在 iDML 中，有三种角色：(1) **学习者** 是参与设备，它希望从去中心化机会式学习算法中的某次交互中获益；(2) **邻居** 是参与设备，它贡献自身资源以供学习者学习；(3) **验证者**是负责验证邻居贡献的参与者。设备可以在不同时间承担多个角色；对于某次交互，验证者必须与学习者和邻居不同。不过，在对称协议（例如八卦学习）中，交互中的两个节点可以同时从彼此处获益。在这种情况下，iDML 将这次交互视为两次交互：每次都由其中一台设备担任学习者，另一台相遇设备担任邻居。

如图 1 所示，我们将 iDML 设计为一个插件；智能合约的实现与去中心化学习的核心功能分离，使其具有可移植性和可泛化性。为了让 iDML 能够与现有的去中心化学习算法互操作，我们实现了一个算法专用的适配器，其作用实际上是协调上层 iDML 与下层去中心化学习实现之间的交互。此外，我们还实现了算法专用验证器。如下文将进一步详述，验证的具体步骤会根据所使用的学习算法而有所不同。在上层，iDML 负责维护智能合约，并协调三种角色的参与者之间的协作。

A. 激励参与去中心化学习

我们系统的主要目标是激励参与者积极参与去中心化机会式学习过程，并为他们贡献的资源提供补偿。iDML 方法的整体流程如图 2 所示。尽管图中展示了许多步骤，但整体而言，该过程直观易懂，包含九个步骤：

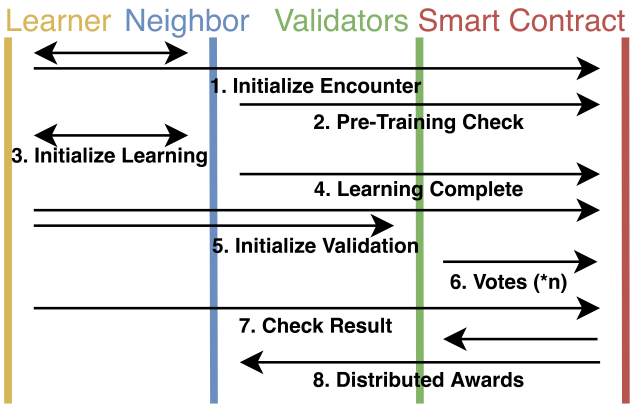

图2：iDML 的系统视图。除步骤 1 和 3 外，其他所有步骤均属于 iDML。

1) 学习者与邻居相遇，底层的去中心化学习协议随即触发。2) 在学习开始之前，调用iDML适配器，并要求学习者向智能合约支付预先设定且双方同意的代币金额。邻居设备在重新开始学习活动之前检查该预付款。3) 预付款完成并经验证后，学习者与邻居完成去中心化学习算法所要求的任何协作任务。4) 协作任务完成后，学习者与邻居双方通知智能合约。5)验证者收到验证请求后，使用特定算法验证实现执行验证。6) 验证者验证模型后，通过将结果发送至智能合约进行投票。7) 当智能合约收到预先设定数量的投票，或最长时间已过后，任一方请求获取智能合约中的结果。8)然后，智能合约根据预先设定的方法和共识，向邻居和验证者分发奖励或实施惩罚。

接下来，我们介绍以智能合约为核心的方案工作流程。在全文中，我们将每个步骤都与 Fig. 2中的编号步骤对应起来，不过省略了步骤3，因为该步骤着重于去中心化学习过程，而非智能合约的作用。

步骤 0（初始化）：为初始化智能合约的使用，在图 2 所示的任何步骤之前，拥有参与去中心化机会式学习的设备的个人必须通过将其数字货币兑换为代币（一种数字货币）来加入该流程；我们的智能合约支持符合 ERC-20 代币标准[1]的代币。智能合约预设了与一种数字货币的兑换率，但可以将该数字货币用作桥梁，以便彩票娱乐

[1]https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

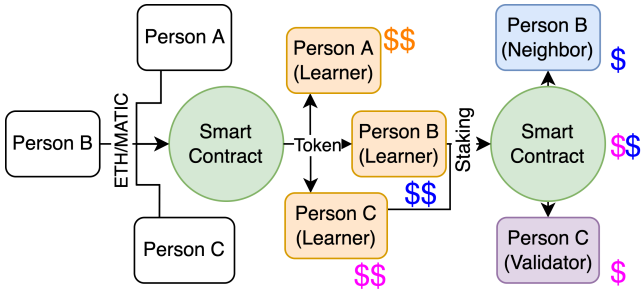

图 3：初始化智能合约（**步骤 0**）。

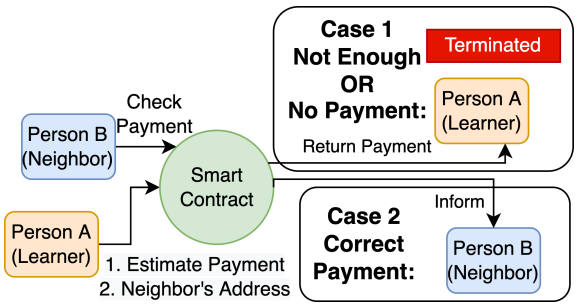

图 4：在启动由相遇驱动的训练过程（**步骤 1 和 2**）之前进行预付款并检查预付款。

可与其他数字货币兑换。要在 iDML 中担任**邻居** 或**验证者**，参与者需要向智能合约质押预先设定数量的代币作为保证金。一旦某个特定的机会式学习过程成功完成，**学习者** 便会向**邻居** 和**验证者** 支付奖励。完整的初始化过程如图 3 所示。

步骤1（初始化相遇）和步骤2（训练前检查）：在发起相遇且两名参与者初步同意进行协作后，两名参与者（即将从相遇中受益的**学习者** 和将提供资源以支持去中心化学习算法的**邻居** ）都会在继续之前向智能合约报到。具体而言，**学习者**会将其将要协作的邻居身份告知智能合约，并授权预付款（图 2中的第二条箭头）。计算适当付款金额的方法基于邻居与学习者之间达成的共识。预付款取决于去中心化学习过程对通信和计算资源的要求，可以由所有参与者全局定义，也可以在相遇步骤中私下协商。**邻居**将通过智能合约检查预付款的有效性。如果预付款不足，**邻居** 可以拒绝协作，预付款将退回智能合约中**学习者**的账户。否则，**学习者** 和**邻居** 将按照去中心化学习算法的定义进行协作。这一与智能合约进行的训练前报到过程如图 4 所示。

步骤4（学习完成）：步骤3（初始化学习）中

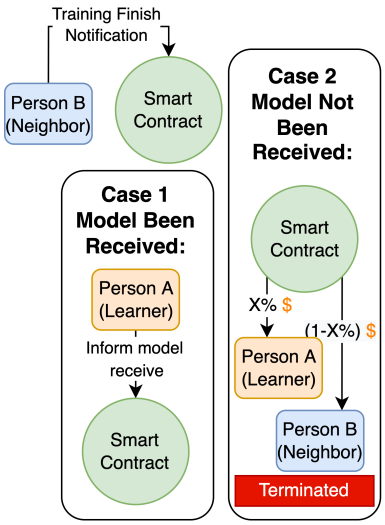

图5：完成学习任务（**步骤4**）。

图 2 中的去中心化机会式学习算法已完成，且未与智能合约进行任何交互。然而，当协作过程完成且**学习者** 获得结果（例如模型参数）时，**邻居** 上的 iDML 适配器层会拦截并复制该结果，然后向 iDML 中的智能合约发送“学习完成”信号和结果的 MD5。此外，**学习者**也会通过学习者侧的 iDML 适配器层向智能合约报告结果的 MD5。在此步骤中，可能出现两种结果。第一种情况（图 5 中的情况 1）是，假设**学习者**和**邻居** 的结果一致，则可以开始验证过程。另一方面（图 5 中的情况 2），有几种不同的可能性会导致流程无法继续。由于去中心化学习的特性，**学习者** 或**邻居**可能无法连接，也可能无法发送或接收学习过程的结果。在这种情况下，由于**邻居**很可能已为训练过程贡献了资源，因此会将部分预付款支付给**邻居** ，以示诚意。另一方面，由于**学习者** 未能从协作中获益，剩余的预付款将退还给**学习者**。

在确定向一名**学习者**支付的小额款项的金额时，我们寻求一种平衡，以防止恶意学习者和/或邻居参与。随着时间的推移，如果某个**邻居** 或**学习者** 在智能合约中积累了未完成的交互记录，则可以在继续未来的交互之前，在第2 步使用这些信息。例如，智能合约可以在底层区块链中逐区块检查某个**邻居**的记录，以进行更深入的验证。

第 5 步（模型验证）： 要启动验证步骤，**学习者**会将学习输入和结果分享给验证者（第 5步的第一条箭头），并通知智能合约验证已初始化（第 5 步的第二条箭头）。然后，验证者开始验证**邻居**的贡献是否可靠。验证者是根据

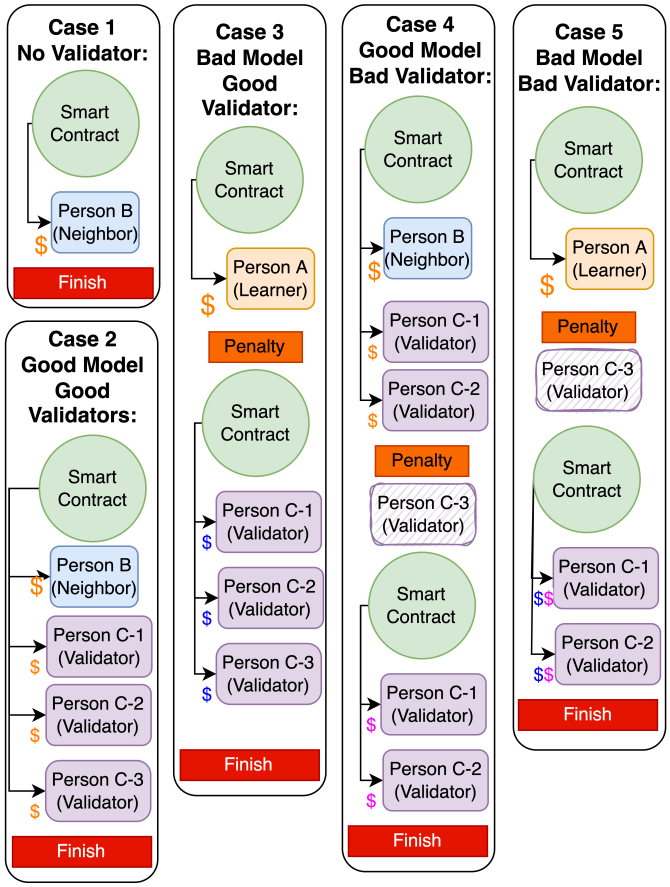

图 6：完成相遇（**步骤 6-8**）。

与邻居相同的标准。在智能合约上，通过使用模型权重和验证者 ID 的 MD5 哈希对学习结果进行索引，这可以防止学习者向验证者发送错误的模型。如图 1所示，验证方法取决于所使用的特定去中心化学习算法。此步骤会调用若干适用于该学习算法的验证者（例如，根据经验进行调优）。每个验证者投票 判断他们是否认为该结果有效，依据是评估更新后的模型相对于**学习者**先前模型的表现。也就是说，验证者会检查**邻居**对学习的贡献是否为正。由于我们允许结果存在一定程度的不确定性，因此引入了容差 (τ)这一概念。此外，随着去中心化学习训练的模型准确率提高，模型改进的空间会缩小。然而，在这种情况下，纳入相遇的邻居设备的学习贡献仍然可以帮助学习者的模型变得更具可泛化性。基于这些发现，如果更新后的学习模型所得到的准确率要么高于输入模型的原始准确率，要么不比输入模型低超过 τ，则认为该模型有效。虽然我们在原型中以明文传输投票结果，但现有研究表明，可以保护投票以避免结果受到偏差影响 [15]。

步骤 6 至 8（最终确定）： 在最后几个步骤中，如果满足以下两个条件之一，则可以计算投票结果。

	说明
r	学习者请求支付的奖励金额。
r_n	邻居收到的奖励金额。
r_v^t	投赞成票的验证者获得的奖励金额。
r_v^f	投反对票的验证者获得的奖励金额。
p_r^n	邻居应获得的奖励比例。
p_r^v	验证者应获得的奖励比例（$p_r^v = (1 - p_r^n)$）。
n_v^t	投赞成票的验证者人数。
n_v^f	投反对票的验证者人数。
V	投票阈值；完成定案所需的票数
τ	模型准确率容差。

满足以下条件之一：1)投票数超过 V （投票阈值），或 2)可在智能合约中预先设定的最大投票时间已过。 p_r^n 是将给予邻居的奖励百分比， p_r^v 是将在所有验证者之间分配的奖励百分比。去中心化学习算法在智能合约中均可配置 p_r^n 和 p_r^v ，并且$p_r^v + p_r^n = 1$。我们使用 n_v^t 表示投票认为模型具有合理贡献的验证者数量，而 n_v^f表示投反对票的数量。系统中的任何参与者都可以请求最终确定，其可能结果如下所示，图 6 也对此进行了总结。请注意，在图中，棕色美元符号表示从**学习者**处分配的奖励，蓝色美元符号表示来自邻居的惩罚，粉色美元符号表示来自验证者的惩罚。为简单起见，在图 4 和图 5中，我们将验证者 C-1 和 C-2 视为良性验证者，而将 C-3 视为恶意验证者。

情形 1： 如果系统中没有投票（$n_v^t = n_v^f = 0$），我们就假设该模型做出了实质性贡献。

$$r_n = r \tag{1}$$

情形 2： 如果所有验证者都认为**邻居** 提供了合理的贡献（即 $n_v^t \neq 0; n_v^f = 0$），则奖励将按以下方式发放：

$$r_n = p_r^n * r \quad \text{and} \quad r_v^t = \frac{p_r^v * r}{n_v^t} \tag{2}$$

情形 3： 如果所有验证者都认为**邻居** 未提供合理的贡献（即 $n_v^t = 0; n_v^f \neq 0$），则预付款将退还给**学习者**，奖励/惩罚将按以下方式发放：

$$r_n = -r \quad \text{and} \quad r_v^f = \frac{r}{n_v^t} \tag{3}$$

情形 4： 如果多数验证者认为**邻居** 提供了合理的贡献，但其他一些验证者并不认同（即 $n_v^t \geq n_v^f > 0$），则奖励/惩罚将按以下方式发放：

$$r_n = p_r^n * r \quad \text{and} \quad r_v^t = \frac{p_r^v * r - n_v^f * r_v^f}{n_v^t} \qquad r_v^f = -\frac{p_r^v * r}{n_v^t + n_v^f} \tag{4}$$

情况 5： 如果大多数验证者认为**邻居**的贡献**并非**合理的改进，但有些其他人则认为是合理的（即 $0 < n_v^t < n_v^f$）。预付款将退还给**学习者**，奖励/惩罚如下：

$$r_n = -r \quad \text{and} \quad r_v^t = -\frac{r}{n_v^t + n_v^f} \qquad r_v^f = \frac{r - n_v^t * r_v^t}{n_v^f} \tag{5}$$

B. 恶意模型防范

如前所述，针对 iDML 这类系统的攻击主要分为两类：激励机制攻击和学习攻击。我们的方法旨在防范这两类攻击。

激励机制攻击。 激励机制攻击是由激励机制本身引发的攻击。在这类情况下，攻击者试图在没有实际参与有意义的协作的情况下，获得与学习过程相关的奖励。假设系统中的所有参与者都能在没有恶意意图的情况下训练模型，并与其他参与者共享模型，这并不现实，因为参与者可能会通过返回随机模型权重来破坏训练；这种行为源于单个参与者层面的模型训练既非最优，也缺乏效率。遗憾的是，现有系统没有配备检测此类恶意行为的手段，因此整个学习系统的准确率和实用性都会下降。此类攻击可以通过利用 iDML 的验证步骤（图 2 中的步骤 5 和 6）来应对。

此外，验证结果可能导致对攻击者施加惩罚。图 3 中的步骤 0 要求邻居在协作前质押其代币，这为智能合约惩罚不诚实的**邻居**参与者提供了一种机制。在式 3 和式 5 中，我们保证攻击者可能受到的惩罚等于或略高于其可能获得的收益（例如，当**邻居** 也是一名“正向”验证者时），这使得激励机制攻击的数学期望小于或等于 0。

学习攻击。 学习攻击旨在使学习过程的输出对某个输入进行错误分类，这通常也称为投毒攻击。在 iDML 中，质押和验证步骤也能有效防止此类学习攻击。如果**邻居** 参与者在任何操作中存在不诚实行为，则其质押给智能合约的代币将受到惩罚。

IV. 评估

本节中，我们使用两种最先进的去中心化学习算法对 iDML 进行评估：八卦学习 [4] 和机会式协作学习（OppCL） [3]。

A. 数据集和模型

我们的评估依赖于两个广泛使用的分类数据集：CIFAR-10 [31], ，由 10 个类别的 60,000 张32*32彩色图像组成；以及 Fashion-MNIST [32],, 包含10 个类别的 70,000 张28x28 灰度图像。我们将每个数据集中的10,000 张图像用作测试数据集。对于训练数据，我们将剩余样本分配给潜在的训练设备（即**邻居** 参与者）

在 iDML 中采用两种方法：(1) 独立同分布（IID）：训练数据均匀分配给所有模拟参与者，且彼此不重叠；(2) 非独立同分布（Non-IID）：每位**邻居** 参与者拥有相同数量且彼此不重叠的数据，但每位邻居的数据仅包含 2 个类别。

对于两种学习算法，我们选择足够小、能够在资源受限设备上训练且适用于不同模型规模的学习模型。对于我们采用的八卦学习方法 [4],，所有参与者都依赖相同的模型结构；设备相遇时，只需交换当前模型参数的快照，并在继续训练之前在本地进行聚合。我们使用 10 个卷积层、最大池化和丢弃层。相比之下，对于我们的机会式学习模型，我们采用三种不同规模的卷积神经网络（CNN）模型，分别包含 6、10 和 14 层，以及最大池化和丢弃层。

去中心化机会式学习依赖参与节点之间的相遇。我们依托常用的接触模式数据集 [33]–[35]。然而，这些数据集偏向于某些热门节点，不适用于我们的实验。我们没有直接使用这些相遇模式，而是利用这些数据集中的洞见，随机生成更大规模的相遇模式，为 50 名模拟参与者提供均匀分布的接触模式。

B. 评估平台与设置

我们使用 Solidity[2] 实现智能合约，并将其部署在 Ganache[3]，这一智能合约工具上。去中心化机会式学习模拟系统使用 Python 和 TensorFlow 实现。模拟运行于一台工作站上，配备 Ubuntu 18.04 LTS 系统、i7-9800X CPU、128G 内存和 NVIDIA GeForce RTX 2080 Ti GPU。

iDML 的验证过程取决于去中心化学习算法。因此，我们针对每种算法分别实现了验证过程。对于八卦学习，我们让**学习者**在执行接收-合并-训练循环之前保留一份模型副本，并将旧模型和新模型都分享给**验证者**。对于 OppCL，**学习者**收到模型后不会进行合并，而是将模型分享给**验证者** 进行验证。对于这两种算法，**验证者** 都会评估模型的准确率，并根据评估结果进行投票。实验中使用的其他参数列于表 I。

C. 实验结果

在我们的第一个也是主要的实验中，我们的目标是评估 iDML 在为参与去中心化机会式学习提供激励方面的有效性。具体而言，我们评估了八卦学习和 OppCL 在不同数量的验证者和训练容忍度（τ）设置下的投票准确率。请注意，容差值给出了训练模型准确率的下界（τ 定义见步骤

表 I：模拟参数

参数	**值**
用户成为 **邻居** 或**验证者**所需的质押阈值	100
投票阈值 V	3
最大投票等待时间（区块）	50000
每位参与者交换的代币数量	1000000
每个**邻居/验证者** 最初质押的代币数量	200
F-MNIST 的容差 τ IID ‖ OppCL（图 8 和 9）	0.030

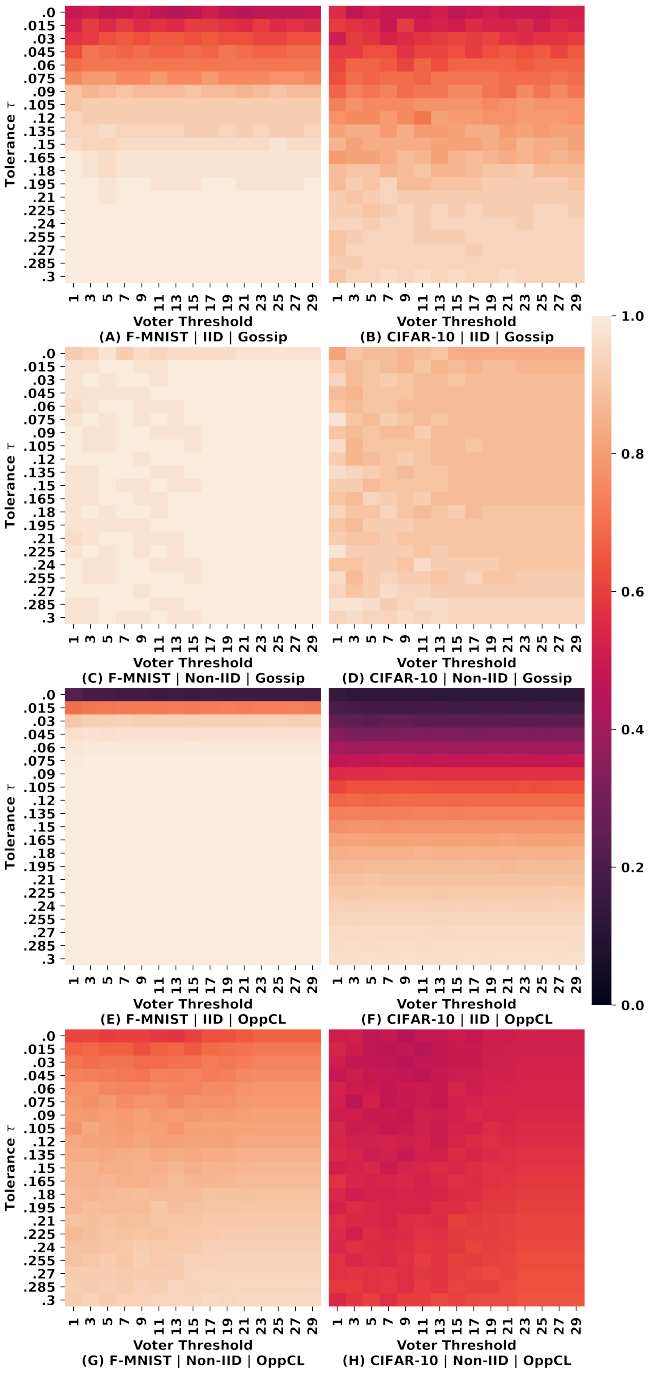

图 7：不同 τ 和投票者设置下的投票准确率

[2]https://soliditylang.org/ [3]https://trufflesuite.com/ganache/

5). 投票准确率反映了有多少训练实例通过我们的验证算法得到验证。如果模型在验证集上的准确率满足容差设置，则该实例被视为已验证。如果模型的可泛化能力更强，则更有可能通过我们的验证。

具体而言，图 7 展示了 iDML 在给定特定阈值和一定数量的**验证者**（即投票者）的情况下，验证**邻居**是否为**学习者**创建了有效贡献的效果。图 7 显示，在独立同分布设置下，两种学习算法在投票者数量不同时，投票准确率都呈现稳定的模式。通过另一项采用极少投票者的深入研究（因篇幅所限未予展示），我们发现，在这些设置下，三名投票者是一个不错的选择。尽管在非独立同分布设置下，投票准确率会随投票者数量变化而略有波动，但考虑到增加投票者所需的成本，投票者数量较少更为理想（例如 3 名）。

我们还观察到 Gossip 和 OppCL 在独立同分布与非独立同分布设置下表现不同。这表明，我们为两种学习算法设计的适配器能够发挥作用，因为结果趋势体现了这两种算法固有的特性。例如，Gossip 学习采用合并-更新-发送循环，而 OppCL 采用共享-训练-返回循环。二者的差异（每个训练实例中，Gossip 比 OppCL 更具可泛化性）使得 OppCL 模型的投票准确率方差比 Gossip 学习模型更大。

iDML的一项实际价值在于，在假设参与者的行为将受到明确定义的激励驱动的前提下，我们所定义的明确激励机制将促使系统参与者有效参与，并通过协作获得更高的模型准确率。多轮模拟表明，当前系统设计会奖励付出大量劳动的**邻居**参与者，而那些以任何方式阻碍训练的参与者则会被排除在系统参与之外。在现实世界的应用中，人类行为确实可能更加复杂，也未必像机器那样受到直接驱动。然而，许多应用案例表明，明确界定的奖励（例如金钱价值和晋升）能够鼓励人们采取期望的行为。

在最终实验中，我们评估 iDML在多大程度上也能防止学习攻击。我们分配不同数量的学习攻击者。这些攻击者中的每一个都会翻转其数据集中的图像标签（例如，他们将卡车标记为飞机和/或将鹿标记为狗）。我们将这些攻击者随机注入系统，并使用测试数据集检查每一轮相遇后所有参与者的模型准确率。

作为基线，我们首先在不使用 iDML 的情况下进行实验。我们分别在系统中植入 0、3 和 10 个攻击者。图 8 显示，在 OppCL 下，攻击者数量增加会导致系统准确率提升延迟。此外，经过几轮交互后，系统的学习准确率不再提升。系统中的攻击者越多，最终模型的平均准确率越低。然后，我们使用 iDML 对 10 个攻击者的情况重新进行实验；结果以图 8 中的红色虚线表示。结果显示，iDML 起初呈现出与 10 个攻击者实验相似的趋势。

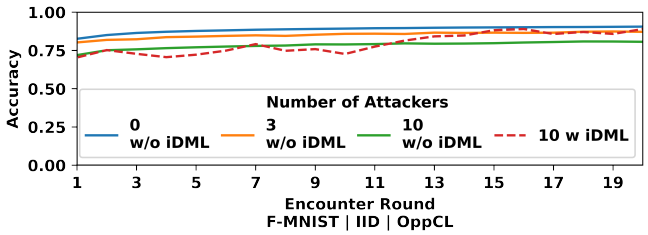

图 8：不同攻击者数量下的模型准确率

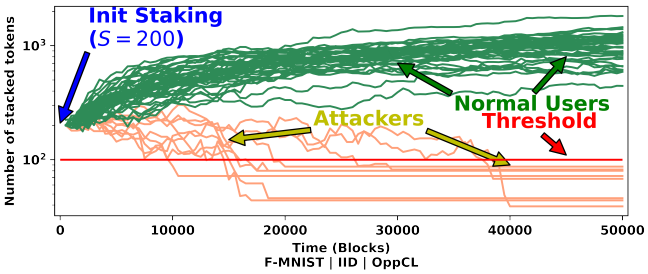

图 9：训练过程中参与者质押代币的变化情况

随后恢复。为了解这一行为的原因，我们考察了每次与所有参与者相遇前后智能合约中的质押量（图 9）。使用不同算法和数据集组合得到的结果与图 8 和图 9 类似，因此为简洁起见不再列出。

我们认为，在第一阶段（40000 个区块之前），尽管 iDML 拒绝了攻击者的一些模型，但这些攻击者仍然活跃于学习系统中。与此同时，iDML 继续惩罚那些提供恶意模型和/或充当恶意“正面”验证者的攻击者。在转折点（40000个区块）之后，攻击者的质押降至阈值以下，他们将无法再在系统中协作。此后，iDML 从攻击中恢复学习系统，模型准确率开始再次提升。

D. 讨论

虽然这些结果展现了诸如iDML这类方法的潜力，但仍存在一些额外的约束和局限性，这些约束和局限性既与其对区块链的依赖有关，也与系统本身的设计有关。

1) 区块链： 所提出的系统是一个去中心化平台，利用区块链网络提供安全高效的数据存储与共享。然而，使用区块链技术也存在某些局限性。

- **操作成本**：区块链网络中的大多数操作（例如（EVM 操作码），包括栈（POP、PUSHX、DUPX、SWAPX）、内存（CALLDATACOPY、CODECOPY 等）以及存储（SLOAD 和 SSTORE）[36],）都会产生一种称为“燃料费”的成本；所使用的燃料费随后会转换为货币费用，而该费用取决于

表 II：示例成本iDML 中一次学习相遇的成本（基线成本数据来自 2023 年 1 月 17 日 04:27 UTC　　）

Step	已使用的燃料费	成本（以太坊网络）	成本（Polygon 网络）
2. 训练前检查（学习者）	43919	$0.9623	$0.0025
4. 学习完成 (邻居)	96172	$2.1072	$0.0055
4. 学习完成（学习者）	46921	$1.0281	$0.0027
6. 投票（验证者）	78869	$1.7281	$0.0045
7. 结果检查和 8. 分发奖励（任何一方）	191344	$4.1925	$0.0109
总计	457225	$10.0182	$0.0261

所使用网络的基线成本。表 II 展示了在 iDML 中进行一次相遇时，两个示例网络所使用的燃料费。在采用 iDML 时，应用设计者必须权衡部署激励所带来的收益与其成本之间的关系——iDML 并不适用于所有应用，但表 II 表明，这些成本（1）可以控制在合理范围内，并且（2）可以预先估算。近期，随着 Polygon Miden 等新技术的发展，成本可能会降低 [4]。

- **安全风险：** 由于所提出的系统依赖于区块链的安全性和可靠性，区块链上发生的任何安全问题也可能影响所提出的系统。例如，如果黑客成功发动 51% 攻击并控制区块链，就有可能篡改存储在所提出系统中的数据 [37]。

- **隐私受限**：如果智能合约部署在公共链上，例如 ETH 或Polygon，那么信息就可能被公众访问，这可能会引发敏感数据泄露方面的担忧，例如个人相遇信息。因此，在 iDML的设计中，我们有意将模型权重和数据分布保留在区块链之外，以降低隐私风险。

2) 系统： 系统依靠验证者来确定邻居的贡献是否有效，但由于机器学习任务的性质以及数据集和学习过程的随机性，准确率的波动是自然现象，并不一定表明贡献无效。根据学习者所遇到的具体验证者，验证结果可能会有所不同。我们采用了验证容差值（τ）来减少这一问题，但无法将其完全消除。此外，准确率可能并不总能充分反映模型的改进情况。其他评估指标，如召回率、精确率、F1值和损失，可能更好地反映改进效果。未来的工作可以探索选择更适合特定学习任务的性能指标，并且可以更新 iDML，使不同的学习者能够要求使用不同的指标。然而，在本研究中，我们依靠准确率来展示 iDML 激励邻居参与的潜力。

最后，iDML 专门设计为一种去中心化机器学习的激励机制。我们纳入了一些设计组件，用于防止或缓解系统可能遭受的攻击，但这些措施并不全面。例如，iDML 按照设计能够缓解（但不能完全防止）恶意邻居发起的模型投毒攻击，因为验证者会对每个邻居的贡献进行签名。另一方面，如果一群攻击者串通起来，伪装成恶意邻居和验证者，系统就无法缓解这种攻击。未来，我们可以在移动网络的真实相遇模式背景下评估 iDML，从而测试发起此类攻击的难度、成本和潜在危害。再举一个更细致的例子，容差 τ 很有用，因为它允许模型准确率出现一些预期波动；但持续攻击者可能会试图在容差范围内操纵模型，使模型方向发生偏移。不过，要成功发动此类攻击，邻居必须能够在一段时间内反复影响学习者的模型（假设 τ 合理地小），因此缓解此类攻击的简便方法是确保所选邻居具有多样性。

[4]https://polygon.technology/solutions/polygon-miden

V. 结论与未来工作

我们提出了一个名为 iDML 的框架，用于激励去中心化的机会式机器学习。评估结果表明，该系统能够有效补偿那些提供通信和计算资源、以协助其他参与者完成模型学习任务的邻近设备。此外，结果还表明，系统能够检测其中的攻击者，并避免将恶意模型合并到用户的模型中。对采用不同数据和数据分布的各种去中心化学习算法进行评估后发现，我们提出的 iDML 系统适用范围广泛。未来可以使用大规模的现实世界合约模式对该系统进行评估。另一方面，为了更好地激励参与者，也可以考虑数据项稀有性，并据此提供相应奖励。

参考文献

[1] T. S. Ajani、A. L. Imoize 和 A. A. Atayero，“嵌入式和移动设备中的机器学习综述——优化与应用”，传感器，第 21 卷，第 13 期，第 4412 页，2021年6月 [在线]。可访问：http://dx.doi.org/10 3390 21134412 。/s Y. Zhan、J. Zhang、[2] Z. Hong、L. Wu、P. Li 和 S. Guo，“联邦学习激励机制设计综述”，*IEEE* 新兴计算主题汇刊，第 10 卷，第 2 期，第 1035–1044 页，2022年。[3] S. Lee、X. Zheng、J. Hua、H. Vikalo 和 C. Julien，“机会式联邦学习：探索面向普适计算应用的自我中心协作”，载于*2021*年 *IEEE* 普适计算与通信国际会议（*PerCom*），2021年，第 1–8 页。[4] I. Colin、A. Bellet、J. Salmon 和 S. Cl´emenc,on，“用于成对函数去中心化优化的 Gossip对偶平均”，载于国际机器学习会议。PMLR，2016年，第 1388–1396 页。

[5] Z.-Q. Zhao,P. Zheng,S.-t. Xu, 和 X. Wu，“基于深度学习的目标检测：综述”，《IEEE 神经网络与学习系统汇刊》，第30卷，第 11 期，第 3212–3232 页，2019年。[6] T. Yang, G. Andrew, H.Eichner, H. Sun, W. Li, N. Kong, D.Ramage, 和F. Beaufays，“应用联邦学习：改进 Google键盘查询建议”，CoRR，第abs/1812.02903 卷，2018年。[7] [ ] 1812 02903 在线。可用：http://arxiv.org/abs/。Z. Zheng,S. Xie,H.-N.Dai,X.Chen,和 H.Wang，“区块链的挑战与机遇：综述”，《国际网络与网格服务期刊》，第14卷，第 4 期，第 352–375页，2018年。[8] N. Szabo，“在公共网络上形式化并保障关系安全”，First Monday，1997年。[9] W.Zou, D. Lo, P.S.Kochhar,X.-B.D. Le, X. Xia, Y. Feng, Z. Chen, 和B. Xu，“智能合约开发：挑战与机遇”，《IEEE 软件工程汇刊》，第47卷，第 10 期，第 2084–2106 页，2021年。[10] P. Kairouz, H.B.McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles,G.Cormode, R. Cummings等，“联邦学习的进展与开放问题”，《机器学习中的基础与趋势》，第14卷，第1–2 期，第1–210 页，2021年。[11] B.McMahan,E. Moore, D. Ramage,S.Hampson,和B. A. y.Arcas，“从去中心化数据中进行通信高效的深度网络学习”，载于《第 20 届国际人工智能与统计学会议论文集》，系列：《机器学习研究论文集》，A. Singh 和 J. Zhu 编，第 54卷。PMLR，2017年 4月20–22 日，第 1273–1282 页。 [在线]。可用：https://proceedings.mlr.press/v54/mcmahan17a.html[12] D. Leroy, A. Coucke,T. Lavril, T. Gisselbrecht, 和 J.Dureau，“用于关键词检测的联邦学习”，载于ICASSP 2019-2019 IEEE国际声学、语音与信号处理会议（ICASSP）。IEEE，2019年，第 6341–6345 页。[13] A. Hard, K. Rao, R. Mathews, S. Ramaswamy, F. Beaufays, S. Augenstein, H. Eichner, C.Kiddon, 和D.Ramage，“用于移动键盘预测的联邦学习”，arXiv预印本 arXiv:1811.03604，2018年。[14] Y. Xiong, H. J.Kim, 和V.Hedau，“Antnets：用于资源高效图像分类的移动卷积神经网络”，arXiv预印本 arXiv:1904.03775，2019年。[15] J. Lyu, Z. L. Jiang,X. Wang,Z.Nong, M.H. Au, 和 J.Fang，“基于智能合约的安全去中心化无信任电子投票系统”，载于2019年第18 届 IEEE 计算与通信中的信任、安全与隐私国际会议/第13 届 IEEE 大数据科学与工程国际会议（TrustCom/BigDataSE），2019年，第 570–577 页。[16] G. Wood 等，“以太坊：安全的去中心化通用交易账本”，以太坊项目黄皮书，第151卷，第 2014年 期，第 1–32 页，2014年。[17] Y. Jiao,P.Wang, D. Niyato, B. Lin,和 D. I. Kim，“面向无线联邦学习服务市场的自动化拍卖框架”，《IEEE 移动计算汇刊》，第20 卷，第10 期，第 3034–3048 页，2021年。[18] G.Wang,C. X.Dang,和 Z. Zhou，“衡量联邦学习参与者的贡献”，载于 2019年 IEEE 大数据国际会议（BigData），2019年，第 2597–2604 页。[19] T. Song,Y. Tong, 和 S. Wei，“联邦学习的利润分配”，载于 2019年 IEEE 大数据国际会议（BigData），2019年，第 2577–2586 页。[20] X. Tu, K. Zhu, N. C.Luong,D.Niyato,Y.Zhang, 和 J.Li, “联邦学习的激励机制：经济学与博弈论视角”，《IEEE 认知通信与网络汇刊》，第8 卷，第 3 期，第1566–1593 页，2022年。[21] T. Zhang, Z. Shen, J. Jin,X. Zheng,A.Tagami, 和 X. Cao，“在边缘智能中实现民主：一种基于雾计算的协同学习方案”，《IEEE物联网期刊》，第 8卷，2761，2021年4 月，2751 第 页–。[22] W.Y. B. Lim,Z. Xiong, C. Miao, D. Niyato, Q. Yang, C. Leung, 和 H.V. Poor，“移动网络中联邦机器学习的分层激励机制设计”，《IEEE 物联网期刊》，第7 卷，第10 期，第 9575–9588 页，2020年。[23] S. Fan, H. Zhang,Y.Zeng, 和 W. Cai，“边缘计算中用于联邦学习的混合区块链资源交易系统”，《IEEE 物联网期刊》，第8 卷，第 4 期，第 2252–2264页，2021年。[24] Y. Deng, F. Lyu, J. Ren, Y.-C. Chen, P.Yang, Y.Zhou,和 Y. Zhang，“Fair：具有精准用户激励的质量感知联邦学习与模型聚合”，载于 *IEEE INFOCOM2021 -IEEE*计算机通信会议，2021年，第1–10页。[25] X. Bao、C. Su、Y. Xiong、W. Huang和Y. Hu，“Flchain：一种具有信任和激励机制、可审计的联邦学习区块链”，载于 *2019*年第*5*届大数据计算与通信国际会议（*BIGCOM*），2019年，第151–159页。[26] B. Biggio、I. Corona、D.Maiorca、B.Nelson、N. ˇSrndi´c、P. Laskov、G. Giacinto和F. Roli，“测试时针对机器学习的规避攻击”，载于数据库中的机器学习与知识发现，H.Blockeel、K.Kersting、S.Nijssen和F. ˇZelezn´y编。柏林、海德堡：Springer Berlin Heidelberg，2013年，第387–402页。[27] A.Shafahi、W. R. Huang、M. Najibi、O. Suciu、C. Studer、T. Dumitras和T. Goldstein，“毒蛙！针对神经网络的目标性干净标签投毒攻击”，2018年。[28] X. Zhou、M. Xu、Y. Wu和N. Zheng，“联邦学习中的深度模型投毒攻击”，未来互联网，第13卷，第3期，2021年。 [在线]。可用地址：https://www.mdpi.com/ 1999 5903 13 3 73 - / //Z. Sun、P. Kairouz、[29] A.T.Suresh和H.B. McMahan，“你真的能对联邦学习植入后门吗？”2019年。 [在线]。可用地址：https://arxiv.org/abs/ 1911 07963 。[30] P. Blanchard、E. M. El Mhamdi、R.Guerraoui和J. Stainer，“与对手进行机器学习：拜占庭容错梯度下降”，神经信息处理系统进展，第30卷，2017年。[31] A. Krizhevsky、G. Hinton等，“从微小图像中学习多层特征”，2009年。[32] H.Xiao、K. Rasul和R. Vollgraf。（2017年）Fashion-MNIST：用于评测机器学习算法的新型图像数据集。[33] L.Ozella、D.Paolotti、G. Lichand、J. P. Rodr´ıguez、S.Haenni、J. Phuka、O.B.Leal-Neto和C. Cattuto，“使用可穿戴接近传感器刻画马拉维农村村庄中的社会接触模式”，*EPJ*数据科学，第10卷，第1期，第46页，2021年。[34] R. I.Ciobanu和C. Dobre，“CRAWDAD数据集 upb/mobility2011（版本2012-06-18）”，从 https://crawdad.org/upb/mobility2011/ 20120618下载，2012年6月。[35] ——，“CRAWDAD数据集 upb/hyccups（版本2016-10-17）”，从 https://crawdad.org/upb/hyccups/20161017下载，2016年10月。[36] “以太坊虚拟机（EVM）。” [在线]。可用地址：https://ethereum.org/en/developers/docs/evm/[37] I.Eyal和E. G. Sirer，“多数并不足够：比特币挖矿易受攻击”，*Commun. ACM*，第61卷，第7期，第95–102页，2018年6月。 [在线]。可用地址：https://doi.org/10.1145/3212998