FLchain：通过支持MEC的区块链网络进行联合学习

Umer Majeed和Choong Seon Hong

# 韩国京熙大学计算机科学与工程系，17104，电子邮件：{umermajeed，cshong}@khu.ac.kr

*摘要*-在本文中，我们提出了一种基于区块链网络的体系结构FLchain，以增强联邦学习的安全性。我们利用渠道的概念来学习FLchain上的多个全局模型。每个全局迭代的本地模型参数作为一个块存储在特定于频道的分类帐上。我们引入了“全局模型状态trie”的概念，它基于从移动设备收集的本地模型更新的聚合，存储和更新在区块链网络上。定性评估表明，FLchain比传统的FL方案更为稳健，因为它以不变的方式保证了FL模型的出处和可审计方面。

*索引术语*-区块链、分布式计算、联合学习、多址边缘计算。

# 一、 简介

机器学习（ML）经常应用于相关的用户数据，以增强底层服务。传统的ML方案需要在集中式云上聚合训练数据，这就增加了对用户个人数据隐私和滥用的担忧[1]。联邦学习（FL）是分布式ML的一种协作方式，由于没有任何原始数据从用户设备中传出，FL中用户数据的隐私性保持不变。因此，外语学习是学习模式隐私保护的发展之路。

在传统的FL中，移动设备根据设备数据样本计算本地模型更新并将其发送到中央服务器。中心服务器聚合从不同设备接收的本地模型更新，并更新全局模型。更新后的全局模型由移动设备获取，以计算其下一次修订的本地模型[2]。循环将继续，直到中央服务器达到所需的精度。这种方法的缺点是

完全依赖于中央服务器的可靠性来存储和计算全局模型更新。任何恶意行为都会导致有缺陷的全局模型更新，不利于后续局部模型更新的准确性，从而导致整个FL过程变得错误。

区块链已经成为一种按时间顺序、去中心化、保留出处和不变的账本技术[3]。在不安全的环境下替换易受攻击的中心服务器是一种有效的解决方案。减轻安全性

这项工作得到了信息与通信研究所的支持

韩国政府资助的技术规划与评估（IITP）赠款-

ment（MSIT）（编号：2019-0-01287，进化式深度学习模型生成

边缘计算平台）。\*作者是通讯员洪博士。

FL中涉及中央服务器的问题，区块链可以与FL集成。

以下是论文的组织结构。第二节分析了区块链支持的FL的文献综述。在第三节中，我们简要解释了与拟议工作相关的准备工作。第四节设计了系统模型。第五节列举了FLchain的详细操作规范。第六节对FLchain进行了评价，第七节总结了本研究。

# 二。相关工作

本节讨论了最近在区块链网络上即兴FL的努力。

区块链和FL的耦合通过提出一种超实用的鲁棒分散学习模型训练方案来保证用户数据的隐私性。经过训练的学习模型参数可以以不变的方式安全地存储在区块链上，并具有防止未经授权的访问和恶意行为的傻瓜防护能力。此外，区块链安全地保存了学习模型的出处和时间方面[4]。

在[5]中，作者讨论了FL与区块链的联合。从地理位置分散的站点将训练数据收集到一个集中的服务器上很容易受到网络攻击、隐私泄露和网络延迟。区块链为FL程序提供了一种安全的交换学习模型参数的方法。区块链能够审核FL中全球模型每个时代的学习模型。此外，发现基于区块链的FL的性能几乎与独立FL相当[6]。

Kim等人。在[7]中，提出了基于区块链（BlockFL）的设备FL架构。对用户设备上可用的数据样本执行本地模型更新。本地模型更新在区块链上的区块中累积。全局模型更新也由用户设备从最新的块计算出来，从而建立了设备上FL的概念。他们考虑全局学习模型的可伸缩性、鲁棒性和延迟最小化。该模型假设所有参与设备在指定的等待时间内向区块链网络提交本地模型更新。由于用户移动性、网络延迟、电源问题和间歇性可用性问题，在预定时间内从所有参与设备获取本地模型更新实际上是不可行的。*吐温*

# 三、 序言和定义

本节简要说明了所提议的体系结构及其操作的准备工作。

## A、 渠道

Fabric引入了通道的概念，这些通道是用于在至少两个对等点之间实现隔离通信的专用子网。只有与通道关联的对等方有权读取、提交和验证通道中的事务。每个频道都有单独的分类帐。共识也适用于每个通道[8]。在FLchain中，对于每个全局学习模型，创建一个带有genesis块的新通道，该通道存储通道特定的分类账。genesis块存储全局学习模型的初始权值、权值的维数、超参数、激活函数和偏差。

## B、 全局模型状态Trie

与以太坊[9]中追求账户状态的“账户状态Trie”类似，我们提出了在FLchain中追求全局学习模型权重的“全局模型状态Trie”。每个通道都有自己的全局模型状态trie，其形式为Merkle Patricia树。全局模型状态trie将权重存储在键值对中，其中key是权重位置（表示权重指标的下标），value是实际权重系数。在FLchain中，权重系数在生成块的同时进行更新。在协商一致后，全局模型状态trie为全局学习模型提供更新后的权重系数。

# 四、 系统模型

在这一部分中，我们提出了一个通过集成多址边缘计算（MEC）和区块链网络的FL系统模型。如图1所示，FLchain的物理基础设施包括移动设备和边缘设备。移动设备使用设备上的数据样本计算本地模型更新。边缘设备有两个用途。首先，它们为资源受限的移动设备提供网络资源。第二，它们在FLchain的区块链网络中充当节点。

每个全局模型在单独的通道上训练。FLchian的可用信道集用{1,2,3，…，Cn}表示。其中，是FLchain上可用信道的总数，表示在信道∈C注册的设备数量。由边缘设备组成的区块链网络将用户设备的本地模型更新以块的形式存储在特定信道的单独区块链上。区块链网络还计算并安全地将全球模型更新存储在特定于频道的Merkle Patricia树中。图2显示了给定信道的FL区块链的简化架构。FLchain的底层区块链平台应定制开发，具有Hyperledger Fabric[10]和以太坊[11]的功能。*乔丹C中国Djj*

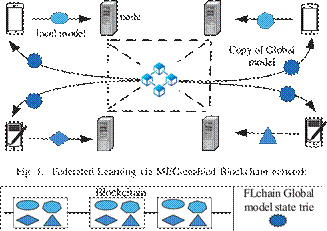


图2。FLchain：联邦学习的简化区块链架构

# 五、 FLCHAIN中的区块链操作

在本节中，我们将介绍FLchain的操作。算法1给出了信道FLchain的整体过程。图3是FLchain对设备和信道的操作顺序图。*j我j*

## A、 初始化

为每个新的全球学习模型的培训创建了一个新的渠道。初始重量参数和其他必要的配置被设置并存储在genesis块中。让我们成为一个新的全球学习模式的渠道。*j乔丹*

FLchain可以应用于任何学习模型。然而，我们认为全局学习模型是一个线性回归问题。让我们为通道设置相关设备。是通道设备上的数据样本集*乔丹DjjSi，j我j*. 然后，用。学习目标是

在所有数据样本上使损失函数（w）最小化∈*我深圳*

*Sj公司*带={xz，yz}*深圳*，其中。通过寻找最优权重参数使损失函数最小化*威斯康星州*∗，在哪里*d*-维列向量，表示信道的全局模型权重向量。*j*

*wj酒店*∗=阿格明（wj），（一）



                    哪里*,* （二）

和

全局迭代=0时的初始权重参数从预先选择的范围中随机选择。器件（0）、wi、j（0）∈[0，wj，max]和全局梯度∇l（wj（0））∈（0，1）的全局权重（0）和局部权重参数（0）。损失函数的全局梯度定义为：*t威斯康星州威斯康星州我威斯康星州*

*.* （四）

## B、 渠道查询

当一个设备想要加入特定频道的FLchain时，首先进行频道查询，然后通过区块链网络将可用频道列表发送给移动设备。*我C*

## C、 频道选择

当一个设备想要为特定的全局模型贡献FL时，它执行信道查询。一旦可访问通道列表可用，它将为该特定全局模型选择相关通道。设设备选择的通道为j。*我Cci我ci*

## D、 设备注册

如果该设备尚未注册，则该设备需要为其预先选择的信道注册自己。在注册之后，用户设备被分配私钥和公钥，通过这些私钥可以向信道提交修改后的本地模型权重。分别表示设备和信道分配的私钥和公钥。*我普里，j普比，j我j*

## E、 本地模型更新

完成设备注册程序后，或重新-

接收到计算本地模型下一次更新的通知后，设备通过其关联的边缘节点从区块链网络下载最新的全局模型参数（t−1）。而，是需要在通道上计算的当前全局模型迭代。对于每个全局模型迭代，设备上的本地模型都会针对时间段进行更新。在局部模型时代，用随机方差缩减梯度（SVRG）对器件的局部模型进行更新，如[12]：*威斯康星州tjtDi公司五五我*

哪里*η >*我们有0个本地纪元（t）=wi，jV（t）。本地模型更新（t）由设备决定，并以交易形式转发至区块链网络。（t） 是设备在迭代时为通道生成并由设备私钥签名的事务*威斯康星州威斯康星州我transi，j我jt普里，j*. 事务数据包括。

## F、 交易池

提交的事务在事务池（mempool）中累积。特别是，区块链网络中的每个节点都有自己的通道特定内存池。交易经过验证、验证和认证。对于每个全局模型迭代，通道上的对等方等待时间，等待mempool中事务的累积。*j特瓦特，j*

内存池中可能存在由于网络延迟而延迟的事务。原本打算在先前的全局模型更新中集成的事务不能用于计算下一个全局模型更新，因此这些事务被丢弃。

算法1:FLchain通道运算*j*

1： 全局模型2的设置通道：初始化：=0；（0），wi，j（0）∈[0，wj，max]；*j乔丹t威斯康星州*

3： 所有∈Dj do并行*我*

|  |  |
| --- | --- |
| 9： 十： | ∈*j*  从频道下载（t）到设备*威斯康星州j我* |
| 十一： | *t*←t+1；（t）=wj（t）；*威斯康星州*0 |

第四章：查询可用频道选择频道

将设备注册到的通道端*我j*

8： 所有人都是并行的*身份证*

对于=1，…，V do*五*

*wi，合资公司*（t） =wi，jv−1（t）−η∇Φ，和式（6）

结束

15： （t）=wi、jV（t）、生成（t）并转发到区块链网络*威斯康星州transi，j*

16： 等待来自通道的通知*j*

17： 结束

18： 使用公式（7）计算（t）*威斯康星州*

19： 全局模型状态trie更新、块生成和一致性

20： 结束时间



## G、 全局模型更新

当等待时间超过时，通道中的对等节点（边缘节点）通过捆绑事务从其自己的内存池中进行迭代来竞争生成下一个块。确定全局模型状态trie，安全地存储全局模型参数（t）。全局模型状态trie的根被添加到具有块高度的块的块头中。全局模型权重使用分布式近似牛顿法（DANE）[13]进行更新，如下所示：*吐温，吐温jt威斯康星州t*



其中，是一组设备，它们的事务由winner miner接收并包含在具有块高度的块中。是迭代时装置∈Dj，t贡献的数据样本数*Dj，ttNk、t、jkt*. 此外，还有

. 在此处，为通道的样本集贡献了个样本。*Si，t，jtj*

可能有设备无法在指定时间内将其本地模型更新报告给winner miner。在更新全局模型时，FL必须具有处理这些离散设备的协议[14]。

## H、 协商一致议定书

在矿工广播最新区块后，区块链中的对等方必须验证区块交易，并检查更新的全局模型状态trie的正确性。对等方根据块内的事务计算自己的全局模型状态trie，并根据广播块验证全局模型状态trie的根。如果区块被发现是有效的，区块链网络必须就区块链达成共识，直至各区块和

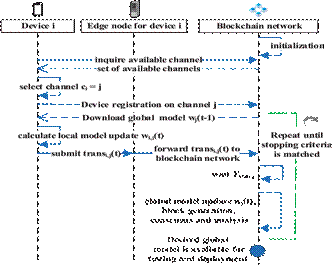


图3。FLchain：FL通过区块链进行操作的序列图，相应的矿工被视为赢家矿工。但是，如果块无效，则拒绝该块。winner miner广播的最新区块将在协商一致期间附加到特定频道的分类账上。由于每个区块链节点都会计算、验证和验证全局模型状态trie以获得一致性，因此基于区块链的FL比典型的FL更可靠和健壮。当需要终止新的区块生成时，底层共识协议可以修改为实际拜占庭容错（pBFT）和工作证明（PoW）一旦全局模型满足停止条件。

## 一、 分析

在每次全局模型迭代后，进行分析，以检查FL是否已达到预期结果或需要执行更多轮。停止标准可根据每个FL任务定义。

对于，FL过程将继续进行全局迭代*乔丹T*对于一个预定义的常数*ε阈值，j>*0当达到所需的标准时，就可以对全局模型进行测试和部署。

# 六、 评价

FLchain为FL在区块链网络上提供了一个合适的平台。FLchain的主要优点如下：

•FLchain为每个全局模型的学习提供了一个单独的通道。存储本地模型更新的共识和分类帐是特定于渠道的。全局模型状态trie也基于每个通道进行维护。全局模型状态trie可以安全无瑕地将全局模型权重存储在Merkle-Patricia树中。全局模型状态trie可以在从genesis块到特定通道的区块链的顶部块的任何迭代中重新生成和验证。•

•在FLchain中，全局模型更新由区块链网络而不是单个中央服务器计算、验证、验证和存储。因此，它比典型的FL更健壮。

# 七。结论和今后的工作

在本文中，我们设计了一种通过边缘设备组成的区块链网络来实现FL的体系结构。我们确定，可以为区块链网络中的每个全球模型分配一个单独的通道。我们提出了全局模型状态trie的概念，将全局模型安全地存储为Merkle-Patricia树。该方法的局限性在于，用户设备依赖于其相应边缘设备的完整性来将事务转发到区块链网络。未来，我们的目标是在延迟、计算和存储需求方面优化FLchain。此外，我们还将设计一个用户设备和矿工节点参与FLchain的奖励机制。

参考文献

[1] Zhao，Zhang，Zhang，Zhang，Zhang，Zhang，Zhang，第48Y卷，第1卷“隐私保护”和第48W卷“隐私保护”第1卷。

[2] A.Zappone、M.Di Renzo和M.Debbah，“深度学习时代的无线网络设计：基于模型、基于AI，还是两者兼而有之？《IEEE通讯事务》，2019年。

[3] S.Nakamoto，“比特币：对等电子现金系统”，2008年。[在线]。可用：http://bitcoin.org/bitcoin.pdf

[4] 第27卷，美国电子工程师协会（IEEE）第101H卷，第101H页。

[5] D.Dillenberger，P.Novotny，Q.Zhang，P.Jayachandran，H.Gupta，

S、 Mehta、S.Hans、S.Chakraborty、M.Walli、J.Thomas、R.Vaculin、K.Sarpatwar和D.Verma，“区块链分析和人工智能”，IBM研发杂志，2019年。

[6] D.Preuveneers、V.Rimmer、I.Tsingenopoulos、J.Spooren、W.Joosen和E.Ilie Zudor，“联合学习的连锁异常检测模型：入侵检测案例研究”，应用科学，第8卷，第12期，第2663页，2018年。

[7] H.Kim、J.Park、M.Bennis和S.Kim，“区块链在设备上的联合学习，出版中”，《IEEE通信快报》，2019年。

[8] P.Thakkar、S.Nathan和B.Viswanathan，“性能基准和优化超级账本结构区块链平台”，第26届IEEE计算机和电信系统建模、分析和仿真国际研讨会（吉祥物），密尔沃基，美国，2018年9月，第264-276页。

[9] V.Buterin，“以太坊中的默克林”，发表在以太坊博客上，2015年，访问时间：2019-05-15。[在线]。可用：https://blog。以太坊。org/2015/11/15/ethereum中的merkling/

[10] E.Androulaki，A.Barger，V.Bortnikov，C.Cachin，K.Christidis，A.De Caro，D.Enyeart，C.Ferris，G.Laventman，Y.Manevich等人，“超级账本结构：许可区块链的分布式操作系统”，载于第十三届欧洲系统大会论文集。葡萄牙波尔图：ACM，2018年。

[11] G.Wood等人，“以太坊：一个安全的分散式通用交易账本”，以太坊项目黄皮书，第151卷，第1-32页，2014年。

[12] J.Konecnˇy，H.B.McMahan，D.Ramage，和P.Richt`arik，“联邦优化：设备智能的分布式机器学习”，arXiv预印本arXiv:1610.025272016年。

[13] O.Shamir、N.Srebro和T.Zhang，“使用近似牛顿型方法的通信高效分布式优化”，in Proc。第31届机器学习国际会议，中国北京，2014年，第1000-1008页。

[14] K.Bonawitz，H.Eichner，W.Grieskamp，D.Huba，A.Ingerman，V.Ivanov，C.Kiddon，J.Konecny，S.Mazzochi，H.B.McMahan等人，“在规模上走向联邦学习：系统设计”，arXiv预印本arXiv:1902.010462019年。