(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112714050 A
(43)申请公布日 2021.04.27

(21)申请号 202011525604.X

(22)申请日 2020.12.22

(71)申请人 齐鲁工业大学
地址 250353 山东省济南市长清区大学路3501号

(72)发明人 禹继国 周广林 闫碧薇 韩玉冰 王桂娟

(74)专利代理机构 济南信达专利事务所有限公司 37100
代理人 冯春连

(51)Int.Cl.
H04L 12/28(2006.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)
G06F 21/62(2013.01)
G06Q 40/08(2012.01)

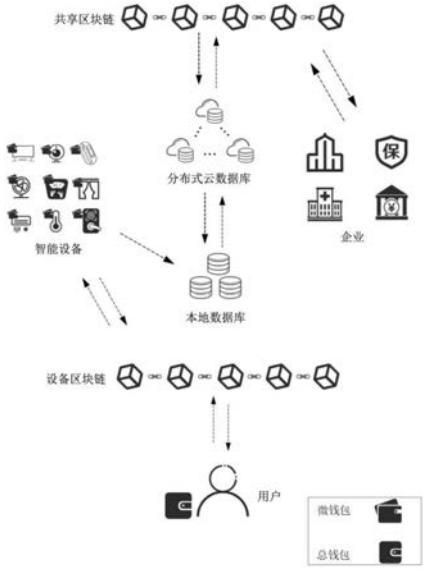
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于区块链和联邦学习的数据共享与隐私保护方法

(57)摘要

本发明公开一种基于区块链和联邦学习的数据共享与隐私保护方法,涉及数据安全技术领域,其包括:在同一用户的智能家居场景下,建立设备区块链来管理智能设备的权限,并在多个智能设备之间建立共识机制;在不同用户的智能家居场景下,建立共享区块链来接收上传数据,并管理数据的所有权,随后利用智能合约,实现企业对用户数据的共享交易;完成交易后,企业根据自身业务需求与共享区块链上的用户数据进行联邦学习,进而预测得到服务模型,并存储于模型区块链一,在用户想要获得服务时,在模型区块链一上申请关联服务模型,随后将关联数据作为关联服务模型的输入,得到推荐结果。本发明可以在保护数据安全的前提下实现数据共享。



CN 112714050 A

1.一种基于区块链和联邦学习的数据共享与隐私保护方法,其特征在于,其实现内容包括:

(1)在同一用户的智能家居场景下,建立所有智能设备的设备区块链,基于设备区块链管理智能设备的权限,并在多个智能设备之间建立共识机制,避免有作恶或故障的智能设备上传数据;

(2)在不同用户的智能家居场景下,建立所有智能设备的共享区块链,共享区块链接收智能设备上传的数据,并管理所接收数据的所有权,随后利用智能合约,实现企业对用户数据的共享交易,同时保证交易过程中数据的完整性和可审计性;

(3)企业通过共享区块链与用户完成共享交易后,企业根据自身业务需求与共享区块链上的用户数据进行联邦学习,进而预测得到与用户需求相关的服务模型,并存储于模型区块链一,在用户想要获得A服务时,用户直接在模型区块链一上申请A服务的相关联服务模型,随后将A服务的相关联数据作为申请所得相关联服务模型的输入,最终得到A服务的推荐结果,用户即可根据推荐结果进行选择,并完成后续交易。

2.根据权利要求1所述的一种基于区块链和联邦学习的数据共享与隐私保护方法,其特征在于,在同一用户的智能家居场景下,

基于设备区块链管理智能设备的权限,当设备区块链上新加入一个智能设备或是撤出一个智能设备时,在设备区块链上更新该智能设备的证书和密钥;

在多个智能设备之间建立共识机制后,当多个智能设备要上传收集的数据到共享区块链时,多个智能设备之间进行验证,避免有作恶或故障的智能设备上传数据到共享区块链。

3.根据权利要求2所述的一种基于区块链和联邦学习的数据共享与隐私保护方法,其特征在于,每个智能设备都有一个微钱包,所述微钱包即智能设备的地址和公私钥对,微钱包用于实现匿名的数据共享交易;

每个用户都有一个总钱包,用户通过总钱包和设备区块链管理其智能家居场景下所有智能设备的微钱包;

智能设备上传收集的数据到共享区块链时,还会将智能设备的地址和公钥一起广播到共享区块链中。

4.根据权利要求3所述的一种基于区块链和联邦学习的数据共享与隐私保护方法,其特征在于,企业利用共享区块链的智能合约进行数据的共享交易,交易过程中,企业首先到共享区块链查找需要的数据,然后根据查找结果向共享区块链申请共享交易,交易成功后,相应的报酬直接由智能合约转到数据绑定的地址,即智能设备的微钱包;智能设备所属的用户即可通过总钱包和设备区块链管理该智能设备的微钱包。

5.根据权利要求1-4中任一项所述的一种基于区块链和联邦学习的数据共享与隐私保护方法,其特征在于,设置一个本地数据库,智能设备收集数据,并对数据进行签名和地址绑定,随后上传至本地数据库,本地数据库对数据进行脱敏和加密处理,以使数据不具备用户的私密信息;

设定间隔时间,本地数据库将脱敏和加密处理后的数据按照间隔时间自动上传至分布式云数据库,随后,还把脱敏和加密处理后数据的摘要信息自动上传至共享区块链。

6.根据权利要求5所述的一种基于区块链和联邦学习的数据共享与隐私保护方法,其特征在于,用户将申请得到的相关联服务模型下载到本地数据库进行存储。

7.根据权利要求1或6所述的一种基于区块链和联邦学习的数据共享与隐私保护方法，其特征在于，企业通过共享区块链与用户完成共享交易后，企业与企业之间根据自身业务需求进行联邦学习，得到最终模型，并存储于模型区块链二，企业利用最终模型预测相关业务的潜在客户群。

8.根据权利要求7所述的一种基于区块链和联邦学习的数据共享与隐私保护方法，其特征在于，企业与企业之间根据自身业务需求进行联邦学习时：

首先，使用基于加密的数据样本对齐技术，对企业的加密数据进行对齐；

随后，训练加密模型，通过预先指定轮次的迭代生成最终模型。

9.根据权利要求8所述的一种基于区块链和联邦学习的数据共享与隐私保护方法，其特征在于，企业与企业之间根据自身业务需求进行联邦学习过程中，还会产生中间模型，中间模型存储于模型区块链二，且中间模型仅用于相关或相似企业与同一企业进行联邦学习的过程中。

10.根据权利要求7所述的一种基于区块链和联邦学习的数据共享与隐私保护方法，其特征在于，设定联邦学习的间隔时间，企业根据自身业务需求与共享区块链上的用户数据进行联邦学习，企业与企业之间根据自身业务需求进行联邦学习。

一种基于区块链和联邦学习的数据共享与隐私保护方法

技术领域

[0001] 本发明涉及数据共享和保护技术领域，具体的说是一种基于区块链和联邦学习的数据共享与隐私保护方法。

背景技术

[0002] 随着当下软件、硬件及通讯技术的高速发展，这对物联网的发展可以说是锦上添花。有预测指出，在物联网发展到一定时期，其产业规模将是互联网的30倍，还有 预测指出，到2025年物联网设备的数量将达到1000亿左右，而与个人联系最为密切 的场景之一就是智能家居。据统计，2018年全球智能家居设备的出货量超过8亿，预 计到2023年全球智能家居设备的出货量将增长到13亿部。

[0003] 毫无疑问，这些物联网设备将产生及其庞大和复杂的数据，在智能家居场景中还会产生关联性强、隐私性高的数据。基于这种现状，当下最主要的问题在于，个人用 户当下对这些数据完全没有所有权，数据都被设备厂商收集，且大多都采用中心化的 数据存储方式。长此以往，这就会产生不良后果：如果设备厂商被黑客攻击或由于其 他原因导致数据被窃取和泄露，这将对个人用户产生不可估量的伤害。

[0004] 在现有的智能家居场景解决方案中，尚没有特别针对数据的隐私保护做相关的研究。目前各个厂商在智能家居中做的最多的工作主要有以下两个方面：首先是在通信 方面，也就是传感器到网关再到智能电器间的通信连接，主要有zigbee、wifi、蓝牙 等；另一方面是在智能设备操控方面，随着人工智能的发展，语音助手也是各大厂商 竞相开发的领域，作为国内在智能家居领域领先的小米科技更是在2020年10月份发 布一指连的超宽带技术，赋予手机与智能设备空间感知能力，在手机指向设备时即可 定向操控。对于用户的使用体验来说，短时间内看是向着利好发展，但这种牺牲隐私 换取便利是不可取的；对于厂商和相关科研机构来说，技术要发展，研究要深入，而 这一切都离不开数据，一味的保护隐私将导致数据无法收集、无法流通，这是不符合 时代发展趋势的。

发明内容

[0005] 本发明针对目前技术发展的需求和不足之处，提供一种基于区块链和联邦学习的数据共享与隐私保护方法，解决当下智能家居场景下各智能设备收集用户关联性强、隐私性高的数据时，导致用户隐私泄露且对数据没有所属权的问题。

[0006] 本发明的一种基于区块链和联邦学习的数据共享与隐私保护方法，解决上述技术问题采用的技术方案如下：

[0007] 一种基于区块链和联邦学习的数据共享与隐私保护方法，其实现内容包括：

[0008] (1)在同一用户的智能家居场景下，建立所有智能设备的设备区块链，基于设 备区块链管理智能设备的权限，并在多个智能设备之间建立共识机制，避免有作恶或 故障的智能设备上传数据；

[0009] (2)在不同用户的智能家居场景下，建立所有智能设备的共享区块链，共享区 块

链接收智能设备上传的数据，并管理所接收数据的所有权，随后利用智能合约，实 现企业对用户数据的共享交易，同时保证交易过程中数据的完整性和可审计性；

[0010] (3)企业通过共享区块链与用户完成共享交易后，企业根据自身业务需求与共 享区块链上的用户数据进行联邦学习，进而预测得到与用户需求相关的服务模型，并 存储于模型区块链一，在用户想要获得A服务时，用户直接在模型区块链一上申请A 服务的相关联服务模型，随后将A服务的相关联数据作为申请所得相关联服务模型的 输入，最终得到A服务的推荐结果，用户即可根据推荐结果进行选择，并完成后续交 易。

[0011] 进一步的，在同一用户的智能家居场景下，

[0012] 基于设备区块链管理智能设备的权限，当设备区块链上新加入一个智能设备或是撤出一个智能设备时，在设备区块链上更新该智能设备的证书和密钥；

[0013] 在多个智能设备之间建立共识机制后，当多个智能设备要上传收集的数据到共享区块链时，多个智能设备之间进行验证，避免有作恶或故障的智能设备上传数据到共 享区块链。

[0014] 更进一步的，每个智能设备都有一个微钱包，所述微钱包即智能设备的地址和公私钥对，微钱包用于实现匿名的数据共享交易；

[0015] 每个用户都有一个总钱包，用户通过总钱包和设备区块链管理其智能家居场景下所有智能设备的微钱包；

[0016] 智能设备上传收集的数据到共享区块链时，还会将智能设备的地址和公钥一起广播到共享区块链中。

[0017] 更新一步的，企业利用共享区块链的智能合约进行数据的共享交易，交易过程中，企业首先到共享区块链查找需要的数据，然后根据查找结果向共享区块链申请共享交 易，交易成功后，相应的报酬直接由智能合约转到数据绑定的地址，即智能设备的微 钱包；智能设备所属的用户即可通过总钱包和设备区块链管理该智能设备的微钱包。

[0018] 更进一步的，设置一个本地数据库，智能设备收集数据，并对数据进行签名和地址绑定，随后上传至本地数据库，本地数据库对数据进行脱敏和加密处理，以使数据 不具备用户的私密信息；

[0019] 设定间隔时间，本地数据库将脱敏和加密处理后的数据按照间隔时间自动上传至分布式云数据库，随后，还把脱敏和加密处理后数据的摘要信息自动上传至共享区块 链。

[0020] 优选的，用户将申请得到的相关联服务模型下载到本地数据库进行存储。

[0021] 进一步的，企业通过共享区块链与用户完成共享交易后，企业与企业之间根据自身业务需求进行联邦学习，得到最终模型，并存储于模型区块链二，企业利用最终模 型预测相关业务的潜在客户群。

[0022] 更进一步的，企业与企业之间根据自身业务需求进行联邦学习时：

[0023] 首先，使用基于加密的数据样本对齐技术，对企业的加密数据进行对齐；

[0024] 随后，训练加密模型，通过预先指定轮次的迭代生成最终模型。

[0025] 更进一步的，企业与企业之间根据自身业务需求进行联邦学习过程中，还会产生中间模型，中间模型存储于模型区块链二，且中间模型仅用于相关或相似企业与同一 企业进行联邦学习的过程中。

[0026] 优选的，设定联邦学习的间隔时间，企业根据自身业务需求与共享区块链上的用

户数据进行联邦学习，企业与企业之间根据自身业务需求进行联邦学习。

[0027] 本发明的一种基于区块链和联邦学习的数据共享与隐私保护方法，与现有技术相比具有的有益效果是：

[0028] (1)本发明基于区块链管理智能设备的权限，可以避免单点故障，也使得信息 完整性和可信性更高，基于区块链进行数据的上传和交易，使得用户可以在匿名的前 提下对数据拥有一定的所有权，并通过智能合约自动处理交易，使得其安全性和效率 更高；

[0029] (2)本发明基于联邦学习在不泄露个人数据和企业数据的前提下，实现用户与 企业、企业与企业之间的数据共享，且不影响数据共享后的服务效果。

附图说明

[0030] 附图1是本发明中企业与用户进行数据共享交易的示意图；

[0031] 附图2是本发明中企业与企业、企业与用户分别进行联邦学习的示意图。

具体实施方式

[0032] 为使本发明的技术方案、解决的技术问题和技术效果更加清楚明白，以下结合具体实施例，对本发明的技术方案进行清楚、完整的描述。

[0033] 实施例一：

[0034] 参考附图1，本实施例提出一种基于区块链和联邦学习的数据共享与隐私保护方法，其实现内容包括：

[0035] (1)在同一用户的智能家居场景下，建立所有智能设备的设备区块链，基于设 备区块链管理智能设备的权限，并在多个智能设备之间建立共识机制，避免有作恶或 故障的智能设备上传数据。

[0036] 这一过程中，基于设备区块链管理智能设备的权限，当设备区块链上新加入一个智能设备或是撤出一个智能设备时，在设备区块链上更新该智能设备的证书和密钥；

[0037] 在多个智能设备之间建立共识机制后，当多个智能设备要上传收集的数据到共享区块链时，多个智能设备之间进行验证，避免有作恶或故障的智能设备上传数据到共 享区块链。

[0038] (2)在不同用户的智能家居场景下，建立所有智能设备的共享区块链，共享区 块链接收智能设备上传的数据，并管理所接收数据的所有权，随后利用智能合约，实 现企业对用户数据的共享交易，同时保证交易过程中数据的完整性和可审计性。

[0039] 为了更好的实现数据的共享交易，每个智能设备都有一个微钱包，微钱包即智能设备的地址和公私钥对，微钱包用于实现匿名的数据共享交易；

[0040] 每个用户都有一个总钱包，用户通过总钱包和设备区块链管理其智能家居场景下所有智能设备的微钱包；

[0041] 智能设备上传收集的数据到共享区块链时，还会将智能设备的地址和公钥一起广播到共享区块链中。

[0042] 此时，企业利用共享区块链的智能合约进行数据的共享交易，交易过程中，企业首先到共享区块链查找需要的数据，然后根据查找结果向共享区块链申请共享交易， 交易成功后，相应的报酬直接由智能合约转到数据绑定的地址，即智能设备的微钱包； 智能设

备所属的用户即可通过总钱包和设备区块链管理该智能设备的微钱包。

[0043] 当然,实现上述(1)、(2)的过程中,还可以设置一个本地数据库,智能设备 收集数据,并对数据进行签名和地址绑定,随后上传至本地数据库,本地数据库对数 据进行脱敏和加密处理,以使数据不具备用户的私密信息;设定一个间隔时间,本地 数据库将脱敏和加密处理后的数据按照间隔时间自动上传至分布式云数据库,随后, 还把脱敏和加密处理后数据的摘要信息自动上传至共享区块链。

[0044] (3)企业通过共享区块链与用户完成共享交易后,参考附图2,企业根据自身 业务需求与共享区块链上的用户数据进行联邦学习,进而预测得到与用户需求相关的 服务模型,并存储于模型区块链一,在用户想要获得A服务时,用户直接在模型区块 链一上申请A服务的相关联服务模型,申请得到的相关联服务模型可以下载到本地数 据库进行存储,随后将A服务的相关联数据作为申请所得相关联服务模型的输入,最 终得到A服务的推荐结果,用户即可根据推荐结果进行选择,并完成后续交易。此过 程需要补充的是,每个企业与共享区块链上的用户数据进行联邦学习时,至少产生一 个服务模型,用户在模型区块链一上申请A服务的相关联服务模型时,申请得到的相 关联服务模型也不限于一个,进一步的,用户得到的推荐结果也不限于一个。

[0045] 执行(3)时,可以设定一个联邦学习的间隔时间,企业根据自身业务需求与共 享区块链上的用户数据按照间隔时间进行联邦学习,以提高预测所得服务模型的后续 使用率。

[0046] 实施例二:

[0047] 参考附图2,在实施例一的结构基础上,本实施例的一种基于区块链和联邦学习的数据共享与隐私保护方法,其在企业通过共享区块链与用户完成共享交易后,企业 与企业之间根据自身业务需求进行联邦学习,得到最终模型,并存储于模型区块链二, 企业利用最终模型预测相关业务的潜在客户群。

[0048] 企业与企业之间根据自身业务需求进行联邦学习时,可以设定一个联邦学习的间隔时间,以提高训练所得最终模型的预测效果。

[0049] 企业与企业之间根据自身业务需求进行联邦学习时:

[0050] 首先,使用基于加密的数据样本对齐技术,对企业的加密数据进行对齐;

[0051] 随后,训练加密模型,通过预先指定轮次的迭代生成最终模型。

[0052] 企业与企业之间根据自身业务需求进行联邦学习过程中,还会分别产生中间模型,中间模型存储于模型区块链二,且中间模型仅用于相关或相似企业与同一企业进 行联邦学习的过程中。比如说,保险公司A和电商公司B之间进行联邦学习,其产生 的中间模型共享到模型区块链二,当保险公司C因为业务需求要跟电商公司B进行联 邦学习时,双方就可以到模型区块链二上申请中间模型,并把该中间模型加入保险公 司C与电商公司B的联邦学习过程中,使得最终模型的效果更好,同时也令之前的数 据得到了更大的利用。

[0053] 综上可知,采用本发明的一种基于区块链和联邦学习的数据共享与隐私保护方法,可以在保护数据安全的前提下实现数据共享,还不影响用户主动获取服务时的效 果。

[0054] 以上应用具体个例对本发明的原理及实施方式进行了详细阐述,这些实施例只是用于帮助理解本发明的核心技术内容。基于本发明的上述具体实施例,本技术领域的 技术人员在不脱离本发明原理的前提下,对本发明所作出的任何改进和修饰,皆应落 入本发明

的专利保护范围。

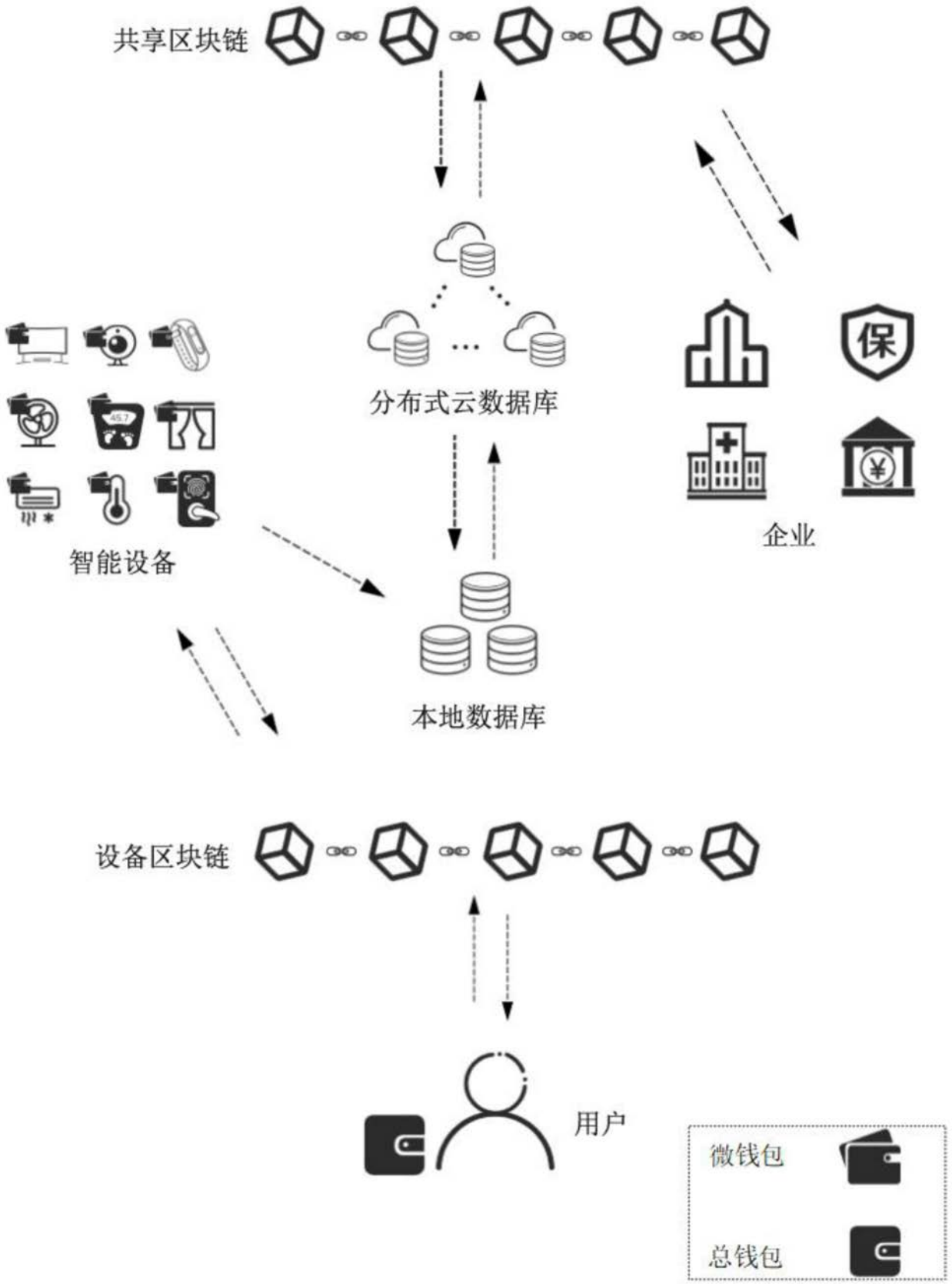


图1

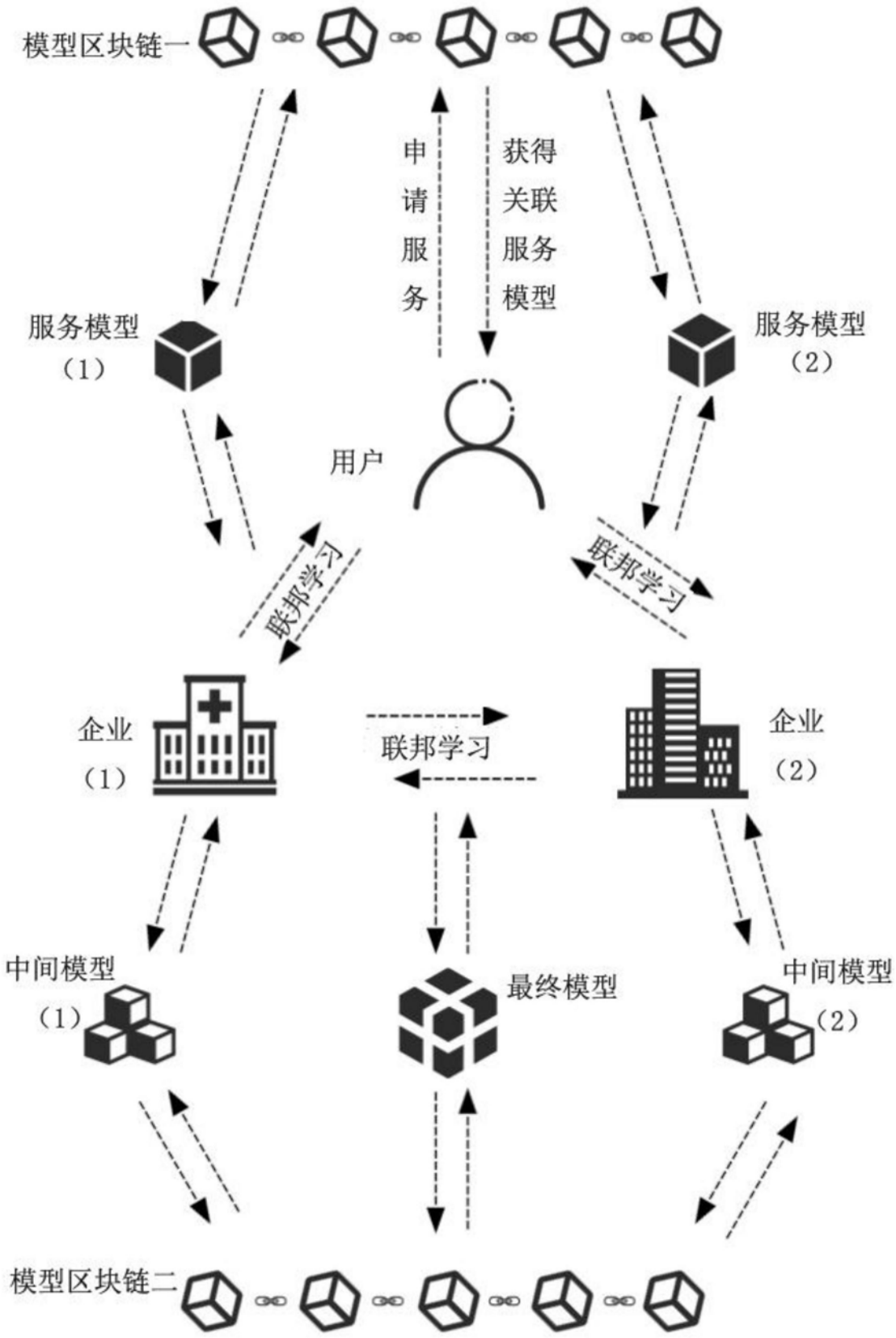

模型区块链一
申请服务
获得关联服务模型
服务模型（1）
服务模型（2）
用户
联邦学习
联邦学习
企业（1）
联邦学习
企业（2）
中间模型（1）
最终模型
中间模型（2）
模型区块链二

图2