(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 110050474 A
(43)申请公布日 2019.07.23

(21)申请号 201780074210.7

(22)申请日 2017.12.28

(30)优先权数据
62/441,070 2016.12.30 US

(85)PCT国际申请进入国家阶段日
2019.05.30

(86)PCT国际申请的申请数据
PCT/US2017/068828 2017.12.28

(87)PCT国际申请的公布数据
WO2018/126075 EN 2018.07.05

(71)申请人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 N·M·史密斯 M·诺兰
D·卡尔博尼 M·凯利

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 李炜 黄嵩泉

(51)Int.Cl.
H04W 4/70(2006.01)
H04L 29/12(2006.01)
H04L 9/32(2006.01)
H04W 84/18(2006.01)
H04W 4/08(2006.01)
H04L 29/08(2006.01)

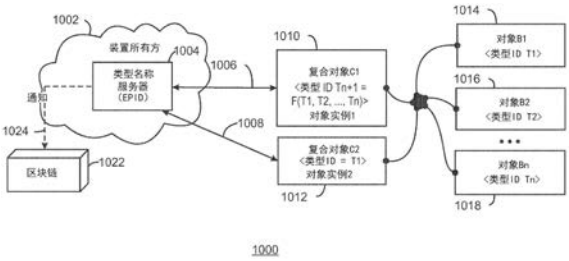
权利要求书3页 说明书53页 附图43页

(54)发明名称

用于物联网网络中的复合对象的子对象的类型命名和区块链

(57)摘要

物联网(IoT)网络复合对象包括:装置所有方,其具有名称服务器和子对象列表;子对象;以及记录子对象的区块链。IoT网络复合对象包括装置所有方和区块链,该装置所有方具有复合对象类型名称服务器。IoT网络联盟小组包括联盟小组名称服务器、联盟小组成员列表、以及区块链。IoT网络设备包括设备身份生成器、消息发布方、网络申请器、装置描述器和打包器发送器。IoT网络设备包括用于通过到第二网络的门户将装置注册到第一网络的装置注册器、装置加入器、令牌请求器、以及验证请求发送器。IoT网络设备包括用于校验验证请求的身份的身份校验器、以及验证请求响应返回器。IoT网络设备包括调用程序实体凭证下发器、对象实体提供器、凭证呈现器和访问控制列表策略申请器。



CN 110050474 A

1.一种设备,包括复合对象,所述设备包括:

装置所有方,所述装置所有方包括用于创建用于所述复合对象的类型名称的类型名称服务器;以及

区块链,所述区块链包括事务,所述事务包括形成所述复合对象的子对象的类型。

2.如权利要求1所述的设备,包括类型检查器,所述类型检查器用于确定包括所述复合对象的子对象的类型。

3.如权利要求2所述的设备,其中,所述类型检查器包括类型自检系统。

4.如权利要求2所述的设备,其中,所述类型检查器包括类型证明系统。

5.如权利要求1所述的设备,包括类型图生成器,所述类型图生成器用于生成形成所述子对象的子子对象的类型的类型图。

6.如权利要求5所述的设备,包括类型名称计算器,所述类型名称计算器用于根据所述类型图生成类型名称。

7.如权利要求1所述的设备,其中,所述事务包括类型图。

8.如权利要求1所述的设备,其中,对象包括类型凭证。

9.如权利要求8所述的设备,其中,所述类型凭证包括制造商的密钥。

10.如权利要求8所述的设备,其中,所述类型凭证由名称服务器提供。

11.如权利要求1-10中的任一项所述的设备,其中,子对象包括子子对象,并且所述子对象的类型名称根据所述子子对象的类型来确定。

12.如权利要求11所述的设备,包括由包括所述子子对象的类型的子对象生成的类型图。

13.一种用于在IoT网络中创建对象类型的方法,包括:

请求由名称服务器创建类型组;

执行组成复合对象的子对象的类型检查以构建形成所述复合对象的对象的类型图;

根据所述类型图计算类型组名称;以及

访问区块链以判定类型组名称是否已经被创建。

14.如权利要求13所述的方法,包括:通过将包括所述类型图的事务写入所述区块链来创建所述类型组名称。

15.如权利要求13所述的方法,包括:从所述名称服务器向所述复合对象下发EPID加入请求。

16.如权利要求15所述的方法,包括:向形成所述复合对象的子对象下发类型凭证。

17.如权利要求13所述的方法,其中,所述名称服务器请求所述复合对象执行所述类型检查。

18.如权利要求13-17中的任一项所述的方法,其中,所述类型检查包括对形成所述复合对象的子对象的递归自检。

19.如权利要求18所述的方法,其中,所述递归自检包括:

向形成所述复合对象的子对象中的每一个子对象发送类型自检请求;

执行类型自检以确定形成子对象的每个子子对象的类型;

在由子子对象形成的子对象中的每一个子对象处构建类型图;

将所述类型图返回至所述复合对象;以及

校验所述类型图上的签名。

20.如权利要求13-17中的任一项所述的方法,包括:

从每个子子对象到层级结构中的更低级别的对象执行递归类型自检;

为所述层级结构的每一个级别处的对象构建类型图;以及

将所述类型图返回到所述层级结构的下一个更高级别。

21.如权利要求13-17中的任一项所述的方法,其中,所述类型检查包括执行对形成所述复合对象的子对象的递归证明。

22.如权利要求21所述的方法,其中,所述递归证明包括:

从每一级别向在下一更低级别处的对象发送类型证明请求;

将在层级结构的特定级别处组成对象的所有对象的类型图返回到下一更高级别;以及

在所述复合对象中构建整体类型图。

23.一种非暂态机器可读介质,包括指令,所述指令用于引导处理器:

构建形成复合对象的对象的类型图;

计算所述复合对象的类型名称;以及

将所述类型名称和类型图记录在区块链中。

24.如权利要求23所述的非暂态机器可读介质,包括引导处理器执行以下操作的指令:执行对形成所述复合对象的对象的递归类型自检。

25.如权利要求23所述的非暂态机器可读介质,包括引导处理器执行以下操作的指令:执行对形成所述复合对象的对象的递归类型证明。

26.如权利要求23所述的非暂态机器可读介质,包括引导处理器执行以下操作的指令:如果所述类型名称不存在于所述区块链中,则创建所述类型名称。

27.如权利要求23-26中的任一项所述的非暂态机器可读介质,包括:向具有类型凭证的子对象发送EPID加入请求。

28.一种用于在IoT网络中创建对象类型的设备,包括:

用于请求由名称服务器创建类型组的装置;

用于执行组成复合对象的子对象的类型检查以构建形成所述复合对象的对象的类型图的装置;

用于根据所述类型图计算类型组名称的装置;以及

用于访问区块链以判定类型组名称是否已经被创建的装置。

29.如权利要求28所述的设备,包括:用于通过将包括所述类型图的事务写入所述区块链来创建所述类型组名称的装置。

30.如权利要求28所述的设备,包括:用于从所述名称服务器向所述复合对象下发EPID加入请求的装置。

31.如权利要求30所述的设备,包括:用于向形成所述复合对象的子对象下发类型凭证的装置。

32.如权利要求28所述的设备,包括:用于请求所述复合对象执行所述类型检查的装置。

33.如权利要求28-32中的任一项所述的设备,其中,所述类型检查包括对形成所述复合对象的子对象的递归自检。

34.如权利要求33所述的设备,其中,所述递归自检包括:

用于向形成所述复合对象的子对象中的每一个子对象发送类型自检请求的装置;

用于执行类型自检以确定形成子对象的每个子子对象的类型的装置;

用于在由子子对象形成的子对象中的每一个子对象处构建类型图的装置;

用于将所述类型图返回至所述复合对象的装置;以及

用于校验所述类型图上的签名的装置。

35.如权利要求28-32中任一项所述的设备,包括:

用于从每个子子对象到层级结构中的更低级别的对象执行递归类型自检的装置;

用于为所述层级结构的每一个级别处的对象构建类型图的装置;以及

用于将所述类型图返回到所述层级结构的下一个更高级别的装置。

36.如权利要求28-32中的任一项所述的设备,其中,所述类型检查包括用于执行对形成所述复合对象的子对象的递归证明的装置。

37.如权利要求36所述的设备,其中,所述递归证明包括:

用于从每一级别向在下一更低级别处的对象发送类型证明请求的装置;

用于将在层级结构的特定级别处组成对象的所有对象的类型图返回到下一更高级别的装置;以及

用于在所述复合对象中构建整体类型图的装置。

用于物联网网络中的复合对象的子对象的类型命名和区块链

相关申请的交叉引用

[0001] 本申请要求于2016年12月30日提交的Ned M.Smith等人的题目为“THE INTERNET OF THINGS(物联网)”的美国专利临时申请序列号62/441,070的申请日的权益,并且所述美国专利临时申请通过引用结合于此。

技术领域

[0002] 本技术总体上涉及物联网(IoT)装置。更具体地,本技术涉及可以执行遥感和致动功能的装置。

背景技术

[0003] 互联网的当前视图是将客户端(诸如个人计算机、平板计算机、智能电话、服务器、数码相框和许多其他类型的装置)连接到服务器群中托管的可公开访问的数据中心。然而,此视图表示全球连网网络的总体使用情况的一小部分。目前存在非常大量的、但不可公开访问的连接资源。示例包括企业网络、私有组织控制网络和跨越全球的监控网络,通常使用点对点型中继器来匿名。

[0004] 据估计,到2020年,物联网(IoT)可能会为超过150亿台装置带来互联网连接。对于组织,IoT装置可以提供监测、跟踪或控制其他装置和物品的机会,所述其他装置和物品包括其他IoT装置、其他家庭和工业装置、制造和食品生产链中的物品等。IoT网络的出现成为推动互联网演变发生深刻变化的催化剂。在未来,互联网很可能从主要以人为本的公用事业演变为基础设施,在这个基础设施中,人类可能最终成为互连装置世界中的少数参与者。

[0005] 在这个视图中,互联网将成为装置和装置网络的通信系统,从而不仅与数据中心通信而且与彼此通信。装置可以形成功能性网络或虚拟装置以执行功能,一旦执行完功能,这些功能性网络或虚拟装置就可以解散。在实现可靠、安全且可标识的装置方面存在挑战,这些装置可以根据需要形成网络以完成任务。

附图说明

[0006] 图1是根据一些实施例的可以存在于互联网中的互连的图。

[0007] 图2是根据一些实施例的针对通过骨干链路耦合至网关的多个物联网(IoT)网络的网络拓扑的图。

[0008] 图3是根据一些实施例的与多个IoT装置通信的云计算网络或云的图。

[0009] 图4是根据一些实施例的与IoT装置的网状网络通信的云计算网络或云的图,所述IoT装置可以被称为雾装置、在云边缘操作。

[0010] 图5是示出根据一些实施例的由多个原子对象形成复合对象的示意图。

[0011] 图6是根据一些实施例的由原子对象和复合对象集形成组对象的示意图。

[0012] 图7是根据一些实施例的使用对象集来进行组创建的示例方法的处理流程图。

[0013] 图8是根据一些实施例的可以存在于IoT装置中用于卸载数据的组件的示例的框

图。

[0014] 图9是根据一些实施例的包括用于引导处理器形成组对象的代码的非暂态机器可读介质的框图。

[0015] 图10是示出根据一些实施例的使用用于对象类型身份的增强隐私标识(EPID)的示意图。

[0016] 图11是根据一些实施例的用于动态创建对象类型的示例方法的梯形图。

[0017] 图12是根据一些实施例的使用递归进行类型自检的示例方法的梯形图。

[0018] 图13是根据一些实施例的用于递归类型证明的示例方法的梯形图。

[0019] 图14是根据一些实施例的可以存在于IoT装置中用于当形成复合对象时将类型分配给所述复合对象的组件的示例的框图。

[0020] 图15是根据一些实施例的包括用于引导处理器形成组对象的代码的非暂态机器可读介质的框图。

[0021] 图16是根据一些实施例的形成联盟小组的示意图。

[0022] 图17是根据一些实施例的用于在联盟小组中登记成员的示例方法的处理流程图。

[0023] 图18是根据一些实施例的可以存在于IoT装置中用于创建联盟小组的组件的示例的框图。

[0024] 图19是根据一些实施例的包括用于引导处理器创建联盟小组的代码的非暂态机器可读介质的框图。

[0025] 图20是展示根据一些实施例的跨公共域、私密域、和公共-私密域的互操作性的示意图。

[0026] 图21是根据一些实施例的跨有线网络和无线网络的异构网络的互操作性的示意图。

[0027] 图22是根据一些实施例的用于任务定义和委托的示例方法的示意图。

[0028] 图23是根据一些实施例的用于由协议转换中介进行的协议转换中介的示例方法的处理流程图。

[0029] 图24是根据一些实施例的可以存在于IoT装置中用于定义任务和委托节点的组件的示例的框图。

[0030] 图25是根据一些实施例的包括用于定义任务和委托节点的代码的非暂态机器可读介质的框图。

[0031] 图26是根据一些实施例的用于分散式网络访问代理来使用功能的示例组织的示意图。

[0032] 图27是根据一些实施例的用于分散式网络访问代理来使用功能的示例方法的处理流程图。

[0033] 图28是根据一些实施例的可以存在于IoT装置中用于与有价值数据单元协商的组件的示例的框图。

[0034] 图29是根据一些实施例的包括用于定义任务和委托节点的代码的非暂态机器可读介质的框图。

[0035] 图30是根据一些实施例的用于利用许可指南来提供认证、授权和计费的分散式版本的示例组织的示意图。

[0036] 图31是根据一些实施例的用于利用许可指南来提供认证、授权和计费的分散式版本的示例方法的处理流程图。

[0037] 图32是根据一些实施例的可以存在于IoT装置中用于利用IoT装置进行分散式授权、认证、和计费的组件的示例的框图。

[0038] 图33是根据一些实施例的包括用于利用IoT装置进行分散式授权、认证和计费的代码的非暂态机器可读介质的框图。

[0039] 图34是根据一些实施例的用于使用远程认证拨号用户服务(RADIUS)或DIAMETER协议在IoT装置上进行分散式授权、认证和计费的技术的示意图。

[0040] 图35是根据一些实施例的图34的组件通过分散式RADIUS代理起作用以在IoT装置上进行授权、认证和计费的动作图的示意图。

[0041] 图36是根据一些实施例的图34的组件通过分散式API 3406起作用以在IoT装置上进行授权、认证和计费的示例方法的梯形图。

[0042] 图37是根据一些实施例的用于在IoT装置上进行分散式授权、认证和计费的动作图的示意图。

[0043] 图38是根据一些实施例的可以存在于IoT装置中用于利用IoT装置进行分散式授权、认证、和计费的组件的示例的框图。

[0044] 图39是根据一些实施例的包括用于引导处理器利用IoT装置进行分散式授权、认证和计费的代码的非暂态机器可读介质的框图。

[0045] 图40是根据一些实施例用于IoT对象中的访问控制的逻辑划分的示意图。

[0046] 图41是根据一些实施例的用于IoT对象中的调用程序凭证与访问控制请求之间的逻辑划分的示意图。

[0047] 图42是根据一些实施例用于在IoT对象中使用层进行访问控制的对象能力之间的逻辑划分示意图。

[0048] 图43是根据一些实施例的用于IoT对象中的访问控制的示例方法的处理流程图。

[0049] 图44是根据一些实施例的可以存在于IoT装置中用于IoT对象中的访问控制的组件的示例的框图。

[0050] 图45是根据一些实施例的包括用于引导处理器在IoT对象中进行访问控制的代码的非暂态机器可读介质19600的框图。

[0051] 贯穿本公开和附图使用相同的数字来引用相似的组件和特征。100系列的数字指代最初见于图1的特征;200系列的数字指代最初见于图2的特征;依此类推。

具体实施方式

[0052] 物联网(IoT)是一种系统,其中大量计算装置彼此互连并且与通信网络(例如,互联网)互连,以在网络中在非常低的级别处提供诸如数据采集和致动等功能。低级别指示可以位于网络边缘处或附近的装置,例如在网络结束前的最后装置。如本文使用的,IoT装置可以包括执行诸如感测或控制等功能的装置,所述装置与其他IoT装置和通信网络进行通信。IoT装置可以包括被配置用于执行一个或多个功能的自主装置或半自主装置。通常,IoT装置可能在存储器、大小或功能方面受到限制,允许针对与较少数量的较大型装置类似的成本来部署更大的数量。然而,IoT装置可以是智能电话、膝上型计算机、平板计算机、PC和/

或其他较大型装置。进一步地，IoT装置可以是虚拟装置，诸如智能电话或其他计算装置上的应用。IoT装置可以包括IoT网关，用于将IoT装置耦合到其他IoT装置和云应用，用于数据存储、过程控制等。

[0053] IoT装置的网络可以包括商业和家庭装置，诸如配水系统、配电系统、流水线控制系统、工厂控制系统、灯开关、恒温器、锁、相机、报警器、运动传感器等。可以通过控制器(诸如计算机、服务器和其他系统)访问IoT装置，例如，以控制系统或访问数据。控制器和IoT装置可以彼此远程地定位。

[0054] 互联网可以被配置用于向大量物联网(IoT)装置提供通信。因此，如本文所述，针对未来互联网的许多创新被设计用于解决从中央服务器到网关、下到边缘装置对网络层的需求，以不受阻碍地增长、发现相连接资源并使其可获得、并且支持隐藏和划分相连接资源的能力。可以使用任何数量的网络协议和通信标准，其中每个协议和标准被设计用于解决特定目标。进一步地，协议是支持人类可访问服务的结构的一部分，所述服务无论位置、时间或空间如何都运行。这些创新包括服务交付和相关联的基础设施，诸如硬件和软件。可以根据服务级别和服务交付协议中指定的服务质量(QoS)条款来提供服务。IoT装置和网络的使用在异构的连接网络中提出了许多新的挑战，包括如例如在图1和图2中所描绘的有线和无线技术的组合。

[0055] 图1是根据一些实施例的可以存在于互联网100与IoT网络之间的互连的图。互连可以将较小的网络102、下到单独的IoT装置104耦合到互联网100的骨干106。为了简化附图，并非每个装置104或其他对象都被标记。

[0056] 在图1中，可以被称为层1(“T1”)提供商108的顶级提供商通过互联网的骨干106耦合到其他提供商，诸如二级或层2(“T2”)提供商110。在一些方面，骨干106可包括光纤链路。在一个示例中，T2提供商110可以例如通过另外的链路、通过微波通信114或通过其他通信技术耦合到LTE蜂窝网的塔112。塔112可以通过LTE通信链路116(例如通过中心节点118)耦合到包括IoT装置104的网状网络。各IoT装置104之间的通信也可以基于LTE通信链路116。

[0057] 在另一示例中，高速上行链路119可以将T2提供商110耦合到网关120。多个IoT装置104可以与网关120通信，并且例如经由蓝牙低功耗(BLE)链路122通过网关120彼此通信。

[0058] 骨干106可以将诸如层3(“T3”)提供商124等较低级别的服务提供商耦合到互联网。T3提供商124可以被认为是例如从T2提供商110购买对骨干106的访问并提供对企业网关126及其他客户的访问的通用互联网服务提供商(ISP)。

[0059] 通过企业网关126，无线局域网(WLAN)可以用于通过Wi-Fi®链路128与IoT装置104通信。Wi-Fi链路128还可以用于耦合到低功率广域(LPWA)网关130，所述LPWA网关可以通过例如可与LoRa联盟颁布的LoRaWan规范兼容的LPWA链路132来与IoT装置104通信。

[0060] T3提供商124还可以通过协调器装置136提供对网状网络134的访问，所述协调器装置使用任何数量的通信链路(诸如LTE蜂窝链路、LPWA链路或基于IEEE 802.15.4标准(诸如Zigbee®)的链路138)与T3提供商124通信。其他协调器装置136可以提供形成链接装置的一个或多个集群树的链接链。

[0061] 在一些方面，一个或多个IoT装置104包括用于与其他装置通信的适当收发机。进一步地，一个或多个IoT装置104可以包括其他无线电收发机、光学收发机或声学收发机，以及有线网络接口，用于使用附加协议和频率的通信。在一些方面，一个或多个IoT装置104包

括关于图8描述的组件。

[0062] 技术和网络可以促进装置和网络的发展。随着技术发展，可以开发网络用于自我管理、功能演进和/或协作，而无需直接的人为干预。因此，这些技术可以使网络在没有集中控制系统的情况下运行。本文描述的技术可以使网络管理和操作功能自动化超出当前能力。进一步地，这些方法可以提供灵活性以具有在没有人为干预的情况下操作的集中控制、自动化的集中控制或其任何组合。

[0063] 图2是根据一些实施例的可以用于通过骨干链路202耦合至网关204的多个物联网(IoT)网络的网络拓扑200的图。类似编号的项如关于图1所描述的那样。进一步地，为了简化图，并非每个装置104或通信链路116、122、128或132都被标记。骨干链路202可以包括任何数量的有线或无线技术，并且可以是局域网(LAN)、广域网(WAN)或互联网的一部分。

[0064] 虽然图2中的拓扑是中心辐射型并且图1中的拓扑是点对点型，但可以观察到这些拓扑没有冲突，而是点对点型节点可以通过网关表现为中心辐射型。在图2中还可以观察到子网拓扑可以具有多个网关，使其成为混合拓扑而不是纯粹的中心辐射型拓扑(或者不是严格的中心辐射型拓扑)。

[0065] 网络拓扑200可以包括任何数量类型的IoT网络，诸如使用蓝牙低功耗(BLE)链路122的网状网络206。可能存在的其他IoT网络包括WLAN网络208、蜂窝网210和LPWA网络212。如本文所述，这些IoT网络中的每一个都可以为新开发提供机会。

[0066] 例如，诸如通过骨干链路202在IoT装置104之间的通信可以由用于认证、授权和计费(AAA)的分散式系统保护。在分散式AAA系统中，可以跨互连的异构基础设施实施分布式支付、信贷、审计、授权、代理、仲裁和认证系统。这允许系统和网络走向自主操作。

[0067] 在这些类型的自主操作中，机器可以签订人力资源合约并与其他机器网络协商合作伙伴关系。这可以允许实现共同目标和平衡的服务交付，而不是概述的、计划的服务级别协议，以及实现提供计量、测量和可追溯性和可跟踪性的解决方案。创建新的供应链结构和方法可以实现创建大量服务、挖掘其价值并在没有任何人为参与的情况下瓦解。

[0068] 通过将诸如声、光、电子交通、面部和模式识别、气味和振动等感测技术集成到自主组织中，可以进一步增强IoT网络。感知系统的集成可以允许服务交付的系统性的且自主的通信和协调，而不是基于合约性服务目标、编制和服务质量(QoS)的资源的云集和融合。

[0069] 网状网络206可以由执行内联数据到信息变换的系统来增强。例如，包括多链路网络的处理资源的自形成链可以以高效的方式分发原始数据到信息的转换。这可以允许诸如第一阶段执行第一数字操作，在将结果传递到另一阶段之前，下一阶段然后执行另一数字操作，并且将所述结果传递到另一阶段之类的功能。所述系统可以提供区分资产和资源以及每个的相关联管理的能力。此外，可以插入基础设施和基于资源的信任和服务索引的适当组件，以改善数据完整性、质量保证并递送数据置信度量。

[0070] 如本文所述，WLAN网络208可以使用执行标准转换的系统来提供多标准连接，使得IoT装置104能够使用不同协议进行通信。进一步的系统可以在包括可见互联网资源和隐藏互联网资源的多标准基础设施之间提供无缝互连。

[0071] 蜂窝网210中的通信可以通过卸载数据、将通信扩展到更远程装置或两者的系统来增强。LPWA网络212可以包括执行到IP互连的非互联网协议(IP)、寻址和路由的系统。

[0072] 图3是根据一些实施例的与多个物联网(IoT)装置通信的云计算网络或云302的图

300。云302可以表示互联网，或者可以是局域网(LAN)、或广域网(WAN)，诸如公司的专有网络。IoT装置可以包括以各种组合来分组的任何数量的不同类型的装置。例如，交通控制组306可以包括沿着城市中的街道的IoT装置。这些IoT装置可以包括红绿灯、交通流量监控器、相机、天气传感器等。交通控制组306或其他子组可以通过无线链路308(诸如，LPWA链路等)来与云302进行通信。进一步地，有线或无线子网络312可以允许IoT装置彼此通信，诸如通过局域网、无线局域网等。IoT装置可以使用诸如网关310等另一装置来与云302进行通信。

[0073] IoT装置的其他分组可以包括远程气象站314、本地信息终端316、报警系统318、自动柜员机320、报警面板322、或移动车辆，诸如应急车辆324或其他车辆326等。这些IoT装置中的每一个都可以与其他IoT装置、与服务器304、或与两者进行通信。

[0074] 如从图3中可以看出，大量IoT装置可以通过云302进行通信。这可以允许不同的IoT装置自主地向其他装置请求或提供信息。例如，交通控制组306可以从远程气象站组314请求当前天气预报，所述远程气象站组可以在没有人为干预的情况下提供预报。进一步地，可以由自动柜员机320向应急车辆324警告正在发生盗窃。当应急车辆324朝向自动柜员机320前进时，其可以访问交通控制组306以请求准许到达所述位置，例如，通过灯变红以在交叉路口阻止交叉车流足够的时间从而使应急车辆324无阻碍地进入交叉路口。

[0075] 诸如远程气象站314或交通控制组306等IoT装置集群可以被配备成与其他IoT装置以及与云302进行通信。这可以允许IoT装置在装置之间形成自组织(ad-hoc)网络，允许它们用作单个装置，其可以被称为雾装置。关于图4进一步讨论雾装置。

[0076] 图4是根据一些实施例的与IoT装置的网状网络通信的云计算网络或云302的图400，所述IoT装置可以被称为雾装置402、在云302边缘操作。类似编号的项如关于图3所描述的那样。如本文使用的，雾装置402是可以被分组用于执行特定功能，诸如交通控制、天气控制、工厂控制等的装置集群。

[0077] 在这个示例中，雾装置402包括在交通交叉路口的一组IoT装置。雾装置402可以根据由OpenFog联盟(OFC)等发布的规范来建立。这些规范允许在将雾装置402耦合到云302以及耦合到端点装置(诸如在这个示例中的交通灯404和数据聚合器406)的网关310之间形成计算元件的层级结构。雾装置402可以利用IoT装置集合提供的组合的处理和网络资源。因此，雾装置402可以用于任何数量的应用，包括例如金融建模、天气预报、交通分析等。

[0078] 例如，通过交叉路口的交通流量可以由多个交通灯404(例如，三个交通灯404)控制。对交通流量和控制方案的分析可以由通过网状网络与交通灯404和彼此通信的聚合器406实施。可以通过网关310将数据上传到云302，以及从云302接收命令，所述网关通过网状网络与交通灯404和聚合器406通信。

[0079] 可以在雾装置402中使用任何数量的通信链路。例如，与IEEE 802.15.4兼容的短程链路408可以提供靠近交叉路口的IoT装置之间的本地通信。例如，与LPWA标准兼容的较长范围链路410可以提供IoT装置与网关310之间的通信。为了简化所述图，并非每个通信链路408或410都标有附图标记。

[0080] 雾装置402可以被认为是大规模互连网络，其中，多个IoT装置例如通过通信链路408和410彼此通信。可以使用由Open Connectivity Foundation™(OCF)于2015年12月23日发布的开放互连协会(OIC)标准规范1.0来建立网络。这个标准允许装置发现彼此并且建立

互连通信。也可以使用其他互连协议，包括例如，来自AllSeen联盟的AllJoyn协议、优化的链路状态路由(OLSR)协议、或用于移动自组连网的更好方法(B.A.T.M.A.N.)等。

[0081] 在一些方面，来自一个IoT装置的通信可以沿着最方便的路径传递以到达网关310，例如，具有最少数量的中间跳数或最高带宽等的路径。在这些网络中，互连的数量提供了大量的冗余，从而允许即使丢失了许多IoT装置也可以维持通信。

[0082] 在一些方面，雾装置402可包括临时IoT装置。换句话说，并非所有IoT装置都可以是雾装置402的永久成员。例如，在示例性系统400中，三个瞬态IoT装置已经加入雾装置402、第一车辆412、第二车辆414和行人416。在这些情况下，IoT装置可以内置在车辆412和414中，或者可以是由行人416携带的智能电话上的应用。还可以存在其他IoT装置，诸如自行车计算机、摩托车计算机、无人机等中的IoT装置。

[0083] 由IoT装置形成的雾装置402可以被呈现给云302中的客户端，诸如服务器304，作为位于云302的边缘的单个装置。在这个示例中，可以在雾装置402内没有标识任何特定IoT装置的情况下发生到雾装置402中的特定资源的控制通信。因此，如果雾装置402内的一个IoT装置发生故障，则雾装置402中的其他IoT装置可能能够发现和控制资源，所述资源诸如致动器或附接到IoT装置的其他装置。例如，交通灯404可以是有线的，以便允许任何一个交通灯404控制其他交通灯404的灯。聚合器406还可以在交通灯404的控制下以及雾装置402的其他功能中提供冗余。

[0084] 在一些示例中，可以使用命令式编程风格来配置IoT装置，例如，每个IoT装置具有特定功能和通信伙伴。然而，可以以声明性编程风格来配置形成雾装置402的IoT装置，以便允许IoT装置重新配置它们的操作和通信，诸如以响应于条件、查询和装置故障来确定所需的资源。这可以在诸如行人416的瞬态IoT装置加入雾装置402时执行。

[0085] 由于行人416可能比车辆412和414行进得更慢，因此雾装置402可以重新配置自身以确保行人416有足够的时间使其通过交叉路口。这可以通过形成车辆412和414以及行人416的临时组以控制交通灯404来执行。如果车辆412或414中的一个或两个是自主的，则临时组可以指导车辆在交通灯404之前减速。进一步地，如果交叉路口处的所有车辆都是自主的，则可能减少对交通信号的需求，因为自主车辆的防撞系统可能允许高度交叉的交通模式，这对于交通灯来说可能太复杂而无法管理。然而，交通灯404对于行人416、骑车人或非自主车辆仍然可以是重要的。

[0086] 当瞬态装置412、414和416离开雾装置402的交叉路口附近时，雾装置402可以重新配置其自身以从网络中消除那些IoT装置。当其他瞬态IoT装置接近交叉路口时，雾装置402可以将其自身重新配置为包括那些装置。

[0087] 雾装置402可以包括用于多个交叉路口的诸如沿着街道的交通灯404，以及沿着街道的所有瞬态IoT装置。雾装置402然后可以将其自身分成功能性单元，诸如交通灯404和靠近单个交叉路口的其他IoT装置。这种类型的组合可以使得能够在雾装置402中形成更大的IoT构造，例如，执行具体功能的IoT装置组。

[0088] 例如，如果应急车辆加入雾装置402，则可以创建应急构造或虚拟装置，其包括街道的所有交通灯404，从而允许控制整个街道的交通流量模式。应急构造可以指导沿着街道的交通灯404保持红色以用于反向交通，并且绿色用于应急车辆从而加速应急车辆的通过。

[0089] 如雾装置402所示，IoT网络的有机演变是改进或最大化IoT实施方式的效用、可用

性和回弹性的中心。进一步地，所述示例表明了用于提高可信度并因此提高安全性的策略的有用性。装置的本地标识在实施方式中可能是重要的，因为身份的分散化确保不能利用中心机构来允许对可能存在于IoT网络内的对象进行模仿。进一步地，本地标识降低了通信开销和时延。

[0090] 区块链可以用于分散标识，因为它们可以在装置之间提供关于当前使用的名称和身份的协议。如本文使用的，区块链是由数据结构块组成的身份记录的分布式数据库。进一步地，如本文使用的，条款区块链可以包括其他分布式分类账系统中的任何一个或多个。其他分布式分类账方法包括瑞波(Ripple)、超级分类账、多链、无钥签名基础设施等。每个数据结构块基于事务，其中下发装置、复合装置或虚拟装置的新名称是事务的一个示例。

[0091] 使用区块链进行标识，可以通过观察名称和身份的重新下发来检测模仿，而无需相应的终止。公共区块链可能是最有用的，因为它们可以使得不同的观察者团体能够检测错误命名、恶意命名或命名基础设施故障。因此，可信任身份基础设施可以是信任IoT网络的中心。

[0092] 图5是示出根据一些实施例的由多个原子对象504、506和508形成复合对象502的示意图500。对象包括组成分布式系统的节点的功能、状态和接口语义的数据模型表示。如本文使用的，对象或IoT对象可以是组成IoT装置的物理装置、由一组物理装置或虚拟装置形成的虚拟装置、或任何数量的其他配置。

[0093] 对象可以交互以完成更大的功能、目标或工作流程。可以根据其类型(例如，所执行的功能)以及实例(例如，存在的)来标识对象。多个对象实例可以具有相同类型身份，但可以具有唯一实例身份。进一步地，多个对象实例可以被组织成多个组，其中，一个分组实例可以具有一个身份。以给定其类型(例如，功能、状态和接口语义)的具体方式交互的一组对象可以表示复合对象。所述复合自身可以具有类型和实例抽象。因此，复合对象遵循与原子对象相同的身份规则。具有类型和实例性质的复合允许对象通过复合实现可扩展性。

[0094] 对象可以与单个装置(诸如，电冰箱)持续一样长的时间，或仅直到完成当前功能。例如，冰箱可以被视为由多个其他对象(诸如，灯、压缩机、温度传感器、恒温器、水分配器、制冰机等)组成的复合对象502。其他对象可以各自为原子对象504、506、和508，或者他们自身可以是复合对象502。制冰机可以是由原子对象504、506和508(诸如，温度传感器、恒温器、电磁操作水阀、定时器、冰盘等)形成的复合对象502。由多个物理装置组成的虚拟复合对象502的示例是关于图4描述的交叉路口和应急集群。

[0095] 因此，可以在以下三个抽象的情境中理解对象身份：对象实例、对象类型、和元身份。对象实例是占用有限资源(诸如，存储器、CPU、带宽、状态等)的计算元件。对象实例化具有涉及创建、突变和删除的生命周期。对象类型是声明预期或可能行为、状态和复合的逻辑构造。对象类型可以在实例化时对对象如何表现和交互施加约束。对象类型还可以指示对象可以响应的请求的类型，例如接口。

[0096] 元身份是定义对象可以存在于其中的元数据情境的方式。对象可能不知道包封元身份。对象实例可以通过定义具有所期望元数据情境的组然后将所述对象登记到所述组中来动态地应用刻板印象信息。

[0097] 认证和身份是核对问题。对象身份如果没有被认证则不可以被相信。然而，没有身份的认证具有有限的效用。在预期到复制和分发私钥的能力受到限制的情况下，非对称密

钥签名(诸如,ECDSA(椭圆曲线数字签名算法)、RSA等)对认证是有用的。密钥的使用建立了虽然受到限制但委托人或代理访问密钥的证据。因此,委托人或代理必须是真实的。

[0098] 认证的语义当被应用于对象身份时也遵循以下三个抽象:对象实例、对象类型、和元身份。对于对象实例,认证质询-响应建立了当前交互可能仅与对象的具体实例化一起进行。对于对象类型,认证质询-响应证明了当前交互受类型标识的语义约束。对于元身份,认证质询-响应根据所定义的情境来分类当前交互。

[0099] 图6是由原子对象604和复合对象606集形成组对象602的示意图600。组对象602属于为对象类型的子集的对象类。对象类例如可以是热交换器,而类热交换器的对象类型可以是更特定的装置,诸如,冰箱、热泵、空气调节器、蒸发冷却器等。

[0100] 可以使用EPID(增强隐私ID)来促进对对象类的认证,所述EPID是涉及与多个私钥匹配的单个公钥的非对称加密系统。可以使用单个公钥来校验由私钥中的任何一个生成的签名。因此,组对象602可以具有单个公钥,而原子对象604和复合对象606中的每一个下发唯一私密ID。所述系统不限于使用EPID,而且可以使用其他标识技术,诸如,共享访问签名。

[0101] 如果对象类与对应于EPID组ID(gid)的数字相关联并且相同类型的对象实例下发对应于EPID组的私钥,则对象实例可以向校验器认证其类。对象类认证采用允许其他对象基于类型化规则与所述对象交互的证明形式。这在行业中也被称为类型强制执行(type-enforcement)。使用其组件对象的类型标识符来构造复合对象类标识符是对象类型扩展方法。例如,接受作为自变量C=(c1,c2,c3,...cn)的函数f()产生表示复合对象的类型标识符的EPID gid值C2_id,其中,cX是其组件对象中的每一个的对象类型。f()的实施方式可以包括使用C中的每个cx的密码散列。在另一示例中,f()可以使用命名层级结构的OID(对象标识符),其中,每个cx是C的父代OID的OID子树。也可能存在用于计算f()的其他方法。

[0102] 可扩展复合对象类标识符允许在托管对象的装置所有方608的寿命期间的任何时间处组合IoT对象的系统。区块链610可以跟踪复合对象的演进,使得可以通过已有复合来通知程序编写工具。可以使用区块链610通过提供向复合对象定义(例如,C)注册对象类型标识符(例如,gid)的事务612来形成分布式模式库。当前集中式对象存储库模式通常取决于在中央服务器上授权地维持类定义的单个逻辑服务。然而,对中央服务器的修改可能导致未授权模式改变。相比之下,使用区块链610可以确保在可以改变现有对象类定义之前跨例如在雾中的多个IoT装置存在阈值共识。

[0103] 区块链610促进对同构对象分类的标识。当例如在消息614中提出新的对象类时,可以搜索区块链610以查看C是否已经存在。

[0104] 由形成复合对象的子对象复合成组对象602是IoT对象模型的扩展机制。可以使用与子对象(诸如,交叉路口XYZ)相关的函数来命名复合对象。当组中的每个提出成员发送消息616以获得包括标识集合的凭证的消息218时,对象实例集可以形成组对象602。当EPID用作凭证授予机制时,集合中的每一个对象可以彼此交互或者与作为集合代理的其他IoT装置交互。

[0105] 由系统使用区块链610以从名称服务器620移除对信任的需要。如果在当前正在使用具有相同名称的组时重复使用组名称,则区块链610可以对名称服务器620的不法行为实施管制。可以由存储并监测区块链610的IoT装置来确定对组名称的重复使用。可以通过标识当前名称请求与有效的且包括组名称的前一块的重叠来进行这种确定。

[0106] 在一些方面，主要集合组成员(PCGM)或组对象602被配置用于基于集合的具体配置来确定组名称。PCGM将组名称传送622至其他集合成员，例如，执行与PCGM相同的操作以得到相同组名称的复合对象606和原子对象604或其他集合成员。函数F()可以使用设置的成员身份逻辑来计算集合组名称C2_id，以便在不同成员分别计算组名称时避免自检顺序非确定性差异。

[0107] 作为示例，EPID组ID(gid)可以采用32位或128位值。当使用32位值时，函数F()可以截断高阶12字节。名称服务器620可以校验是否重新下发gid而不管gid的长度如何。较短gid长度可能在受约束的环境(例如，使用更有限的IoT装置)中是有用的。尽管来自F()的名称冲突可能很少，但可以通过F()的递归调用再次提供组成员身份值(例如，F’＝F(m1,m2,...,mn,F(m1,m2,...,mn))来实现冲突解决。

[0108] 图7是根据一些实施例的用于使用对象集来创建组的示例方法700的处理流程图。方法700可以使用关于图8所描述的系统802来运行。框702表示例如何时期望新的组对象。这可能在瞬态对象移动接近当前组对象时发生，如关于图4的应急集群所描述的，所述应急集群可能在应急车辆接近街道时形成。在另一示例中，对装置(诸如关于图5和图6描述的冰箱)供电可能发起对组对象的创建。

[0109] 在框704处，通过维持对原子(A)或复合(C)子对象中的每一个的ID的参考来形成复合对象，所述原子或复合子对象将组成复合对象的主要集合组成员(PCGM)中的列表中的组对象。组成复合对象的对象可以由完成如由以下各项确定的功能所需的对象来确定：对象的共识、装置所有方中的先前程序、或任何数量的其他技术(诸如，使用多个IoT装置构造对象)。

[0110] 在框706处，形成了集合组标识符。这可以通过对组成组对象的PCGM中的对象ID列表应用函数来完成。所述函数可以组合并形成对象ID的散列码，例如，C2_ID＝SHA2(C1,C2,C3,…,A1,A2,A3,…,An)。

[0111] 在框708处，子对象(例如，所有子对象)中的一个或多个与例如在装置所有方中的名称服务器进行通信以获得组密钥。这可以通过使用EPID加入协议来执行。在加入协议中，子对象向名称服务器发送加入消息并且接收例如C2_ID组对象的EPID凭证作为回报。

[0112] 在框710处，组名称服务器接受针对来自PCGM中的列表的组计算的名称。然后，名称服务器可以将所述名称提交给区块链。在框712处，名称服务器从区块链得到名称(例如，C2_ID)。如本文使用的，区块链是在多个独立IoT装置处保存的事务的分布式数据库。可以由IoT装置中的每一个来执行对事务有效性的确认，从而提供对真实性和身份的多个确认。

[0113] 在框714处，判定名称是否已被使用，例如所述名称存在于较早事务块中，而对象的名称没有相应到期。如果是，则在框716处，可以通过F()的递归调用再次提供组成员身份值F’＝F(m1,m2,...,mn,F(m1,m2,...,mn))来确定新的名称。

[0114] 如果当前没有使用名称，则在框718处判定组成员身份是否是隐私敏感的。这可以在某个位置存在IoT装置不应该是公知(诸如，车辆存在于一系列交叉路口处)的情况下执行。如果是，则在框720处PCGM充当代理，作为中介来安排来自子对象的加入协议请求。如果否，则在框722处名称服务器从区块链中找出子对象成员名称。

[0115] 在框724处，判定请求方是否是授权组成员。如果是，则在框726处执行加入请求。在框728处，名称服务器将组名称(例如，C2_ID)提交给区块链。

[0116] 在块730处，判定是否存在另一子对象并且因此是否需要组凭证。如果是，则流程图返回到框712，以用于对子对象进行凭证授予。如果否，或如果其确定请求方不是授权组成员，则进程在框732处结束。

[0117] 图8是可以存在于用于卸载数据的IoT装置800中的组件的示例的框图。IoT装置800可以包括示例中示出的组件的任何组合。组件可以实施为IC、其一部分、分立电子器件，或者在IoT装置800中适配的其他模块、逻辑、硬件、软件、固件或其组合，或者作为以其他方式并入较大系统的机箱内的组件。图8的框图旨在示出IoT装置800的组件的高级视图。然而，可以省略所示组件中的一些，可以存在附加的组件，并且在其他实施方式中可以出现所示组件的不同安排。

[0118] IoT装置800可以包括处理器802，所述处理器可以是微处理器、多核处理器、多线程处理器、超低电压处理器、嵌入式处理器或其他已知处理元件。处理器802可以是片上系统(SoC)的一部分，其中处理器802和其他组件形成为单个集成电路或单个封装体，诸如来自Intel的Edison™或Galileo™SoC板。作为示例，处理器802可以包括基于英特尔®架构核心™的处理器，诸如Quark™、Atom™、i3、、i5、i7或MCU级处理器，或者可从加利福尼亚州圣克拉拉市的Intel®公司获得的另一此类处理器。然而，可以使用任何数量的其他处理器，诸如可从加利福尼亚州森尼维耳市的超威半导体公司(Advanced Micro Devices,Inc.,AMD)获得的、来自加利福尼亚州森尼维耳市的MIPS科技公司的基于MIPS的设计、由ARM控股有限公司或其客户或其许可证持有人或采用者许可的基于ARM的设计。处理器可以包括诸如来自Apple®公司的A5-A9处理器，来自Qualcomm®科技公司的Snapdragon™处理器、或来自德州仪器公司的OMAP™处理器之类的单元。

[0119] 处理器802可以通过总线806与系统存储器804通信。可以使用任何数量的存储器装置来提供给定量的系统存储器。作为示例，存储器可以是根据联合电子器件工程委员会(JEDEC)的基于低功率双倍数据速率(LPDDR)的设计的随机存取存储器(RAM)，诸如根据JEDEC JESD 209-2E的当前LPDDR2标准(发布于2009年4月)、或下一代LPDDR标准，诸如将提供LPDDR2的扩展以增加带宽的LPDDR3或LPDDR4。在各实施方式中，各个存储器装置可以是任何数量的不同封装体类型，诸如单管芯封装体(SDP)、双管芯封装体(DDP)或四管芯封装体(Q17P)。在一些实施例中，这些装置可以直接焊接到母板上以提供较低简档的解决方案，而在其他实施例中，这些装置被配置为一个或多个存储器模块，这些存储器模块进而通过给定的连接器耦合到母板。可以使用任何数量的其他存储器实施方式，诸如其他类型的存储器模块，例如，不同种类的双列直插式存储器模块(DIMM)，包括但不限于microDIMM或MiniDIMM。例如，存储器的大小可以在2GB与16GB之间，并且可以配置为DDR3LM封装体或LPDDR2或LPDDR3存储器，其通过球栅阵列(BGA)焊接到母板上。

[0120] 为了提供诸如数据、应用、操作系统等信息的持久存储，大容量存储装置808还可以经由总线806耦合到处理器802。为了实现更薄更轻的系统设计，可以通过固态驱动器(SSD)来实施大容量存储装置808。可以用于大容量存储装置808的其他装置包括闪存卡，诸如SD卡、microSD卡、xD图卡等，以及USB闪存驱动器。

[0121] 在低功率实施方式中，大容量存储装置808可以是管芯上存储器或与处理器802相关联的寄存器。然而，在一些示例中，大容量存储装置808可以使用微硬盘驱动器(HDD)来实

施。进一步地，除了所描述的技术之外或代替所描述的技术，任何数量的新技术可以用于大容量存储装置808，诸如电阻变化存储器、相变存储器、全息存储器或化学存储器等。例如，IoT装置800可以结合来自Intel®和Micron®的3D XPOINT存储器。

[0122] 组件可以通过总线806进行通信。总线806可以包括任何数量的技术，包括工业标准架构(ISA)、扩展ISA(EISA)、外围组件互连(PCI)、外围组件互连扩展(PCIx)、PCI Express(PCIe)或任何数量的其他技术。总线806可以是例如在基于SoC的系统中使用的专有总线。可以包括其他总线系统，诸如I^2C接口、I^3C接口、SPI接口、点对点型接口、和电源总线等。

[0123] 总线806可以将处理器802耦合到网状收发机810，用于与其他网状装置812通信。网状收发机810可以使用任何数量的频率和协议，诸如IEEE 802.15.4标准下的2.4千兆赫(GHz)传输，使用由Bluetooth®特别兴趣小组定义的Bluetooth®低功耗(BLE)标准、或ZigBee®标准等。为具体无线通信协议配置的任何数量的无线电可以用于到网状装置812的连接。例如，WLAN单元可用于根据电气和电子工程师协会(IEEE)802.11标准来实施Wi-Fi™通信。另外，例如，根据蜂窝或其他无线广域协议的无线广域通信可以经由WWAN单元发生。

[0124] 网状收发机810可以使用多个标准或无线电进行通信以用于不同范围的通信。例如，IoT装置800可以使用基于BLE的本地收发机或另一低功率无线电与地理上邻近的装置(例如，在约10米内)通信以节省功率。可以通过ZigBee或其他中间功率无线电到达更远的网状装置812，例如，在约50米内。两种通信技术可以以不同功率水平在单个无线电上发生、或者可以在单独的收发机(例如，使用BLE的本地收发机和使用ZigBee的单独网状收发机)上发生。网状收发机810可以并入MCU中作为可由芯片(诸如可从Intel获得的Curie®单元)直接访问的地址。

[0125] 可以包括上行链路收发机814以与云302中的装置通信。上行链路收发机814可以是遵循IEEE 802.15.4、IEEE 802.15.4g、IEEE 802.15.4e、IEEE 802.15.4k或NB-IoT标准等的LPWA收发机。IoT装置800可以使用由Semtech和LoRa联盟开发的LoRaWAN™(长距离广域网)在广泛区域上进行通信。本文描述的技术不限于这些技术，而是可以与实施长距离、低带宽通信的任何数量的其他云收发机一起使用，诸如Sigfox和其他技术。进一步地，可以使用IEEE 802.15.4e规范中描述的其他通信技术，诸如时隙信道跳变。

[0126] 除了针对网状收发机810和上行链路收发机814所提到的系统之外，还可以使用任何数量的其他无线电通信和协议，如本文所述。例如，无线电收发机810和812可以包括LTE或其他蜂窝收发机，其使用扩频(SPA/SAS)通信来实施高速通信，诸如用于视频传输。进一步地，可以使用任何数量的其他协议，诸如用于中速通信的Wi-Fi®网络，诸如静止图片、传感器读数和网络通信的提供。

[0127] 无线电收发机810和812可以包括与任何数量的3GPP(第三代合作伙伴计划)规范兼容的无线电，特别是长期演进(LTE)、长期演进-高级(LTE-A)、长期演进-高级专业版(LTE-A Pro)、或窄带IoT(NB-IoT)等。可以注意到，可以选择与任何数量的其他固定、移动或卫星通信技术和标准兼容的无线电。这些可以包括例如任何蜂窝广域无线电通信技术，其可以包括例如第五代(5G)通信系统、全球移动通信系统(GSM)无线电通信技术、通用分组

无线电服务(GPRS)无线电通信技术、或GSM演进的增强型数据率(EDGE)无线电通信技术。可以使用的其他第三代合作伙伴计划(3GPP)无线电通信技术包括UMTS(通用移动电信系统)、FOMA(自由移动的多媒体接入)、3GPP LTE(长期演进)、3GPP LTE-高级(长期演进-高级)、3GPP LTE-高级专业版(长期演进-高级专业版)、CDMA2000(码分多址2000)、CDPD(蜂窝数字分组数据)、Mobitex、3G(第三代)、CSD(电路交换数据)、HSCSD(高速电路交换数据)、UMTS(3G)(通用移动电信系统(第三代))、W-CDMA(UMTS)(宽带码分多址(通用移动电信系统))、HSPA(高速分组接入)、HSDPA(高速下行链路分组接入)、HSUPA(高速上行链路分组接入)、HSPA+(高速分组接入Plus)、UMTS-TDD(通用移动电信系统-时分双工)、TD-CDMA(时分-码分多址)、TD-SCDMA(时分-同步码分多址)、3GPP Rel。8(Pre-4G)(第3代合作伙伴计划发布8(第Pre-4代)),3GPP Rel。9(第三代合作伙伴计划发布9),3GPP Rel。10(第三代合作伙伴计划发布10),3GPP Rel。11(第三代合作伙伴计划发布11),3GPP Rel。12(第三代合作伙伴计划发布12),3GPP Rel。13(第三代合作伙伴计划发布13),3GPP Rel。14(第三代合作伙伴计划发布14)、3GPP LTE Extra、LTE授权辅助接入(LAA)、UTRA(UMTS陆地无线电接入)、E-UTRA(演进型UMTS陆地无线电接入)、LTE高级(4G)(长期演进-高级(第4代))、cdmaOne(2G)、CDMA2000(3G)(码分多址2000(第三代))、EV-DO(演进-数据优化或演进-仅数据)、AMPS(1G)(高级移动电话系统(第1代))、TACS/ETACS(总接入通信系统/扩展总接入通信系统)、D-AMPS(2G)(数字AMPS(第2代))、PTT(按键通话)、MTS(移动电话系统)、IMTS(改进型移动电话系统)、AMTS(高级移动电话系统)、OLT(挪威语“Offentlig Landmobil Telefoni”,公共陆地移动电话)、MTD(瑞典语Mobiltelefonisystem D的缩写,或移动电话系统D)、Autotel/PALM(公共自动陆地移动)、ARP(芬兰语“Autoradiopuhelin”,“汽车无线电话”)、NMT(北欧移动电话)、Hicap(NTT(日本电报电话公司)的高容量版本)、CDPD(蜂窝数字分组数据)、Mobitex、DataTAC、iDEN(集成数字增强网络)、PDC(个人数字蜂窝)、CSD(电路交换数据)、PHS(个人手持电话系统)、WiDEN(宽带集成数字增强网络)、iBurst、非授权移动接入(UMA,也称为3GPP通用接入网络,或GAN标准)、无线吉比特联盟(WiGig)标准、一般的mmWave标准(无线系统在10-90GHz及以上运行,诸如WiGig、IEEE 802.11ad、IEEE 802.11ay等)。除了上面列出的标准之外,可以将任何数量的卫星上行链路技术用于上行链路收发机814,包括例如符合ITU(国际电信联盟)或ETSI(欧洲电信标准协会)发布的标准的无线电等等。因此,本文提供的示例被理解为适用于现有的且尚未明确表达的各种其他通信技术。

[0128] 可以包括网络接口控制器(NIC)816以向云302或其他装置(例如网状装置812)提供有线通信。有线通信可提供以太网连接,或者可以基于其他类型的网络,诸如控制器区域网络(CAN)、本地互连网络(LIN)、设备网(DeviceNet)、控制网(ControlNet)、数据高速通道+、过程现场总线(PROFIBUS)或过程现场网(PROFINET)等。可以包括附加的NIC816以允许连接到第二网络,例如,通过以太网提供到云的通信的NIC 816、以及通过另一种类型的网络提供到其他装置的通信的第二NIC 816。

[0129] 总线806可以将处理器802耦合到用于连接外部装置的接口818。外部装置可以包括传感器820,诸如加速计、水平传感器、流量传感器、温度传感器、压力传感器、气压传感器等。接口818可用于将IoT装置800连接到致动器822,诸如电源开关、阀门致动器、可听声音生成器、视觉警告装置等。

[0130] 虽然未示出,但是各种输入/输出(I/O)装置可以存在于IoT装置800内或连接到所

述IoT装置。例如，可以包括显示器以示出诸如传感器读数或致动器位置等信息。可以包括诸如触摸屏或小键盘等输入装置以接受输入。

[0131] 电池824可以为IoT装置800供电，但是在IoT装置800安装在固定位置的示例中，它可以具有耦合到电网的电源。电池824可以是锂离子电池、金属-空气电池，诸如锌-空气电池、铝-空气电池、锂-空气电池、混合型超级电容器等。

[0132] 电池监测器/充电器826可以包括在IoT装置800中以跟踪电池820的充电状态(SoCh)。电池监测器/充电器826可用于监测电池824的其他参数，以提供故障预测，诸如电池824的健康状态(SoH)和功能状态(SoF)。电池监测器/充电器826可以包括电池监测集成电路，诸如来自凌力尔特公司(Linear Technologies)的LTC4020或LTC2990、来自美国亚利桑那州凤凰城的安森美半导体公司(ON Semiconductor)的ADT7488A、或来自德克萨斯州达拉斯市的德州仪器的UCD90xxx族的IC。电池监测器/充电器826可以通过总线806将关于电池824的信息传送到处理器802。电池监测器/充电器826还可以包括模数(ADC)转换器，所述模数转换器允许处理器802直接监测电池826的电压或来自电池824的电流。电池参数可以用于确定IoT装置800可以执行的动作，诸如传输频率、网状网络操作、感测频率等。

[0133] 电源块828或耦合到电网的其他电源可以与电池监测器/充电器826耦合以对电池824充电。在一些示例中，电源块828可以用无线功率接收器代替，以例如通过IoT装置800中的环形天线无线地获得功率。无线电池充电电路(诸如来自加利福尼亚州米尔皮塔斯市的凌力尔特公司的LTC4020芯片等)可以包括在电池监测器/充电器826中。所选择的特定充电电路取决于电池824的尺寸，并且因此取决于所需的电流。可以使用由Airfuel联盟颁布的Airfuel标准、由无线电力联盟(Wireless Power Consortium)颁布的Qi无线充电标准、或者由无线电力联盟颁布的Rezence充电标准等来执行充电。在一些示例中，电源块828可以用太阳能电池板、风力发电机、水发电机或其他自然电力系统来增强或代替。

[0134] 大容量存储装置808可以包括用于实施本文所描述的组创建功能的多个模块。尽管在大容量存储装置808中示出为代码块，但是可以理解，任何模块都可以完全或部分地用例如内置在专用集成电路(ASIC)中的硬连线电路代替。大容量存储装置808可以包括可以用于形成组对象的原子对象和复合对象的子对象列表830。集合组标识符832可以使用子对象列表830(例如，使用在子对象列表830上的散列公式)来生成组id。

[0135] 可以包括名称服务器834以提供名称支持并向区块链836提交名称。名称服务器834可以确认所选名称当前未使用，并且向子对象下发凭证以代表组对象起作用。

[0136] 区块链836包括事务数据库，所述事务数据库包括数据块，所述数据块具有与组对象、形成组对象的子对象的名称相对应的事务，以及组对象的如形成、演进或解散等当前状态。除了标识信息之外，区块链836还可以包括如用于组对象和子对象的公共加密密钥等授权信息。区块链836的副本可以保持在网状网络中的部分或所有IoT装置上。这允许其他IoT装置确认区块链836中的变化并且标记任何在没有适当授权的情况下改变区块链836的尝试。虽然在这个示例中用于组标识事务，但是区块链836可以用于与如本文所描述的安全性、支付、事务等相关的任何数量的其他事务，

[0137] 如果要将组的构成视为私有，则代理中介838可以将来自区块链836的凭证提供给组对象的子对象。这可以用于例如提高定位于如十字路口和街道等公共场所的IoT网络的安全性。

[0138] 可以包括EPID服务器840以提供加密服务，比如使用公钥或私钥来加密和解密数据。进一步地，EPID服务器840可以提供公钥，或提供可以用于授权子对象代表组对象起作用以及充当密钥校验服务器的其他凭证。EPID服务器840还可以用在其他应用中以形成和下发密钥，或生成类型身份，如关于图10至图15所讨论的。

[0139] 图9是根据一些实施例的包括用于引导处理器902形成组对象的代码的示例性非暂态机器可读介质900的框图。处理器902可以通过总线904访问非暂态机器可读介质900。可以如关于图8的处理器802和总线806所描述的来选择处理器902和总线904。非暂态机器可读介质900可以包括针对图8的大容量存储装置808所描述的装置，或者可以包括光盘、拇指驱动器、或任何数量的其他硬件装置。

[0140] 非暂态机器可读介质900可以包括代码906，以引导处理器902从子对象列表中计算组名称，例如，如关于图6和图7所描述的那样。可以包括代码908以引导处理器902访问区块链910，例如，用于判定组对象名称是否在区块链910中，并且如果是，则确定组对象的状态。代码908还可以引导处理器902一旦名称被确认时就向区块链910提交事务。代码908还可以引导处理器902将对区块链910的变化迁移到IoT网络中的其他单元。

[0141] 机器可读介质900可以包括代码912，以引导处理器902将组对象的子对象的身份存储在列表中。代码912还可以引导处理器判定加入组的请求是否来自所授权的子对象。如果是，则代码912还可以引导处理器向请求子对象下发凭证。机器可读介质900可以包括代码914，以引导处理器充当用于向受隐私保护的组对象的子对象提供凭证的代理服务器。

[0142] 机器可读介质900可以包括代码916，以引导处理器902充当组对象的名称服务器。机器可读介质900可以包括代码918，以引导处理器902请求凭证以例如作为子对象加入组。

[0143] 图10是根据一些实施例示出针对对象类型身份使用EPID的示意图1000。装置所有方1002包括类型名称服务器1004，其基于来自复合对象1010或1012的登记请求1006或1008来登记新类型。如本文所使用的，登记类型或对象意味着在数据库中或者在类型列表或对象列表中注册类型或对象。例如，登记可以包括向区块链发送事务来存储类型。新的对象类型Tn+1可以通过来自子对象1014至1018的复合组1010或1012的构成推断出来。子对象1014至1018(例如，1014、1016和1018)的类型名称可以用于形成针对复合对象1010或1012的新类型名称。

[0144] 复合对象1010或1012可以通过检查与其交互的子对象1014至1018来动态地确定类型名称。可以使用两种方法来检查子对象1014至1018的配置。如关于图12的梯形图所描述的，第一种方法使用自检。在自检中，IoT对象或具有资源模型定义的其他装置可以在请求时描述自身。例如，IoT对象可以被配置成在请求时提供由对象实施的结构、接口和语义。在一些方面中，IoT对象可以使用如XML模式、JSON模式和/或YANG等数据模型语言(DML)来描述结构、接口和语义。实际实施方式可能不会直接解释数据模型，因为这可能意味着执行缓慢。但是可以使用测试来示出由自检产生的DM与实施的行为相匹配。

[0145] 如关于图13的梯形图所描述的，第二种方法可以使用证明来验证装置的完整性、凭证或身份。如本文所使用的，证明是用于公开装置或平台的信任性质的安全方法，其中所述装置或平台自报告信任性质。所述信任性质可以包括平台制造商、由供应方实现的反映安全性强化的证书，比如用于加密模块实施方式的FIPS140-2。ISO9000、以及遵循以确保质量的供应方流程也可以是相关的。证明通常会揭示硬件版本、固件版本和软件版本以及补

丁级。其可以揭示关于由如可信执行环境(TEE)等强化环境保护的密钥的信息、以及关于密钥类型的信息。例如，强化环境可以使用可信平台模块(TPM)来定义密钥类型，其中一种类型的密钥无法从TPM迁移到强化程度较低的加密模块。

[0146] 自检和证明两者都可以基于子对象类型产生包含对象成员资格的集合。进一步地，这两种方法可以一起使用，例如，使用证明密钥来确认来自特定单元的自检身份。所有IoT对象都是有类型的，但并非所有对象都具有对所述类型进行认证的凭证。

[0147] 例如，如关于图12的梯形图所描述的，用于导出新对象类型名称的方法支持对象类型的自动生成。自动生成允许有用的对象集合形成对象复制的模式。然后，使用类型名称和模式作为输入参数，可以更容易地在网络的其他地方对有用集合进行实例化。

[0148] 类型名称服务器1004可以使用EPID、通过使用类型名称作为组ID准许相同类型对象的每个实例进入EPID组来对对象类型标识符进行认证。区块链1022可以用于例如通过提交来自类型名称服务器1004的事务1024来记录动态导出的类型的创建，使得可以可靠地对相同类型的对象进行实例化而不存在同构冗余。

[0149] 图11是根据一些实施例的用于动态创建对象类型的示例方法1100的梯形图。图11的方法1100可以由关于图14所描述的IoT装置1400实施。在步骤1104中，复合对象1102可以向类型名称服务器1106发送创建类型组(例如T1)的请求1104。如关于图10所描述的，类型名称服务器1106可以包括在装置所有方1002中，或关于图4所描述的可以包括在如聚合器406等中心或单独的装置中。

[0150] 在步骤1108中，类型名称服务器1106以类型自检的请求来响应复合对象1102。在步骤1110中，所述请求触发向子对象1112递归的发送提供自检或证明信息的请求。子对象1112以所请求的信息进行响应1114。一旦递归完成，复合对象1102就可以从所有子对象1112(例如，如T1＝F(t1、t2、t3、...、tn))的类型中计算类型名称1116。然后，复合对象1102可以使用EPID加入请求1118中的对象实例密钥来向类型名称服务器1106证明所述类型。

[0151] 类型名称服务器1106向区块链1122的管理员发送创建事件的先前实例化的请求1120。可以从区块链1122的管理员接收指示所述类型已经存在的消息1124。这还可以通过类型名称服务器1106确定先前的类型已经使用所述名称创建并且存在于区块链1122中来执行。

[0152] 如果没有创建类型，则类型名称服务器下发1126在区块链1122中创建类型的请求1128。这可以通过将创建事务提交到驻留在托管类型名称服务器1106的IoT装置中的区块链1122的实例化来完成。

[0153] 在一些示例中，存储区块链1122的其他IoT装置可能无法验证例如将所述类型的另一个实例化定位在其已经存储的区块链1122中的新创建。如果大多数装置无法验证创建，则拒绝创建，并且区块链1122恢复到先前链。类型名称服务器1106然后可以重命名1126类型并重试创建1128。

[0154] 如果创建成功，例如，如从区块链1122的管理员接收的消息1130或通过大多数IoT装置确认新的区块链1122所指示的，则类型名称服务器1106然后可以向复合对象1102下发EPID加入请求1132。EPID加入请求1132包括所述类型的EPID凭证。这些可以由复合对象1102直接与子对象1112共享，或者子对象1112可以发送具有新类型名称的加入请求以使类型名称服务器1106提供凭证。

[0155] 图12是根据一些实施例的使用递归进行类型自检的示例方法1200的梯形图。类似编号的项如关于图11所讨论的那样。图12的方法1200可以由关于图14所描述的IoT装置1400实施。自检提供了从复合对象至叶对象的连接图。叶对象另外被称为原子对象，因为其不具有子对象。

[0156] 在步骤1202中，复合对象1102可以将命令1202发送到子对象1204以指导子对象1204执行自检。如果子对象1204是原子对象，则其返回签名作为类型标识。如果子对象1204本身是复合对象，则其向形成子对象1204的每个子子对象1208发送命令1206以执行自检。这从复合对象1102到每个子对象1204并且从每个子对象1204到每个子子对象1208递归地发生，如由发送到较低层的命令1210和从较低层返回的类型图1212或1214所指示的。

[0157] 自检使用递归作为遍历子对象图的方法。递归在以下给定的两种可能条件之一的情况下停止：首先如果遇到原子对象，并且其次如果再次遇到已经遇到的对象。子对象图的递归遍历产生树(直接非循环图)，所述树由至少且至多一种到达图中每个节点的方式组成。类型图可以具有格式G＝(gn)，[G]$K_{n\_实例}$，其中gn是组号，[G]是组名称，并且$K_{n_实例}$是特定组的密钥。从树的递归遍历返回时，当前节点填充清单中的条目，从而形成包含对象类型信息的树结构。如果对象拥有实例密钥，则会对类型信息进行签名。因此，子子对象1208可以将格式G'＝(gn+1|gn)，[G']$K_{n_实例}$的类型图返回到子对象1204。一旦所有子子对象1208已经将其类型或类型图返回给子对象1204，所述子对象就可以将其自己的类型图1216返回到复合对象1102，例如，G"＝(gn+2|gn+1|gn)，[G"]$K_{n\_实例}$。

[0158] 结果清单由复合对象1102用作根对象，以生成1218其自己的类型名称。这还可以包括作为到用于生成类型名称的函数F()的输入的局部范围的性质名称。可以将清单供应给类型名称服务器1106，如关于图11所讨论的，其可以校验类型名称的签名和构造。类型名称服务器1106可以检查区块链中的先前类型名称保留。如果找到原始类型名称并且下发了凭证，则可以更新区块链，从而使得能够独立校验类型名称保留状态。

[0159] 图13是根据一些实施例用于递归式类型证明的示例方法1300的梯形图。图13的方法1300可以由关于图14所描述的IoT装置1400实施，递归对象证明类似于递归对象自检，区别在于类型信息可以使用例如编程到装置中或由编程到装置中的凭证形成的类型名称凭证进行签名。当使用对象类型凭证时，类型名称可以标识先前登记的类型，因此区块链可以包含其类型层级结构的历史记录。因此，使用类型凭证可以停止递归。在递归对象证明的实施例中，作为用于重新校验类型层级结构的方法，可以忽略已认证的类型终止。

[0160] 在步骤1302中，复合对象1102向子对象1204发送命令1302以指导子对象1204发送证明凭证。如果子对象1204是原子对象，其将返回对象凭证作为类型标识。如果子对象1204本身是复合对象，则其向形成子对象1204的每个子子对象1208发送命令1304以发送证明凭证。这从复合对象1102到每个子对象1204并且从每个子对象1204到每个子子对象1208递归地发生，如由发送到较低层的命令1306和从较低层返回的类型图1308所指示的。类似的类型图1310从每个子子对象1208返回到子对象1204。类型图1312然后可以从每个子对象1204返回到复合对象1102。对于自检，复合对象1102然后可以校验1314每个签名。

[0161] 图14是根据一些实施例的可以存在于IoT装置1400中用于当形成复合对象时将类型分配给复合对象的组件的示例的框图。类似编号的项如关于图3和图8所描述的那样。可以注意到，可以选择不同的组件并将其用于关于图8所讨论的IoT装置800以及关于图14所

讨论的IoT装置1400。

[0162] 大容量存储装置808可以包括用于实施本文所描述的类型创建功能的多个模块。尽管在大容量存储装置808中示出为代码块，但是可以理解，任何模块都可以完全或部分地使用例如内置到专用集成电路(ASIC)中的硬连线电路代替。大容量存储装置808可以包括列出了可以用来形成组对象的原子对象类型和复合对象类型的类型名称服务器1402。类型名称服务器1402可以向类型检查器1404下发命令以确定形成复合对象的子对象和子子对象的类型。类型检查器1404可以使用自检或证明来执行网状装置812的递归检查。类型图生成器1406可以使用来自子对象和子子对象的响应、包括由较低级对象生成的类型图来生成类型图。类型名称计算器1408可以用于例如通过计算类型图中条目的散列函数来从所生成的类型图中生成类型名称。可以包括类型凭证1410以标识IoT装置1400的类型。类型凭证1410可以包括由制造商编程到装置中例如用于证明的凭证，或包括由另一个装置提供给IoT装置1400例如用于证明的凭证。可以使用制造到装置中的凭证来创建组合类型凭证，以验证或加密向装置提供的凭证。

[0163] 除了如组名称事务等其他信息之外，区块链836可以包括在IoT装置1400中以记录类型名称事务。如本文所描述的，区块链836事务可以通过还存储区块链836的副本的网状装置812的多数投票来验证。

[0164] 图15是根据一些实施例的包括用于引导处理器902形成组对象的代码的示例性非暂态机器可读介质1500的框图。处理器902可以通过总线904访问非暂态机器可读介质1500。可以如关于图8的处理器802和总线806所描述的来选择处理器902和总线904。非暂态机器可读介质1500可以包括针对图8的大容量存储装置808所描述的装置，或者可以包括光盘、拇指驱动器、或任何数量的其他硬件装置。

[0165] 非暂态机器可读介质1500可以包括代码1502，以引导处理器902执行递归类型自检以确定复合对象中的装置类型。可以包括代码1504以引导处理器902执行顺序证明以确定复合对象中的装置类型。可以包括代码1506以引导处理器902利用从子对象和子子对象返回的信息来构建类型图。可以包括代码1508以引导处理器902计算类型的类型名称，例如，从类型图计算散列函数。可以包括代码1510以引导处理器902判定类型名称是否已经在区块链中，并且如果否，则将类型名称提交给区块链。代码910还可以引导处理器902将变化迁移到存储在网状网络中的其他装置中的区块链。可以包括代码1512以引导处理器902向子对象发送EPID加入请求以创建类型组。如果例如由于区块链记录中的冗余或其他故障而未创建名称，可以包括代码1514以引导处理器902重新生成类型名称并重复提交过程。

[0166] 图16是根据一些实施例的形成联盟小组1600的示意图。IoT网络可以形成可能不定期相互作用的松散的对象联盟，被称为联盟小组1600。然而，将对象标记为组抽象的一部分可以提供语义值。可以通过管理决策形成联盟小组1600，例如，以指示区、位置或通用目的，如定位于单一建筑物中的楼层或公寓中的装置。如装置所有方1602等管理机构可以例如通过联盟小组名称服务器1604来选择分组装置所使用的组标识符。联盟小组成员1606可以通过向装置所有方1602发送加入请求1608来在联盟小组1600中进行登记。可以向组成员提供来自联盟小组名称服务器1604的凭证1610，包括EPID凭证。联盟小组成员1606可以例如通过对象内接口1614将凭证1610进一步提供给子对象1612。联盟小组名称可以从区块链1616访问，或在创建时提交到区块链1616。

[0167] 用于联盟小组1600的凭证允许联盟小组成员1606进行认证而不揭示可能用于跟踪隐私的值。因此，成员资格的标准可能是机密的，其中组大小用于确定与使用凭证相关联的隐私风险的程度。

[0168] 通过IoT装置或对象来在联盟小组1600中进行登记允许对象继承联盟小组1600的性质和属性。联盟小组成员1606的这些性质和属性可能不包含处理组性质和组属性的代码、状态或接口。虽然如此，其他实体可以命名性质和属性以进行排序、分类、路由、管理或执行分析。在这层意义上，联盟分组是用于对象元数据的动态应用的策略。

[0169] 图17是根据一些实施例的用于在联盟小组中登记成员的示例方法1700的处理流程图。图17的方法1700可以由关于图18所描述的IoT装置1800实施。框1702表示例如IoT装置组通电或以其他方式激活时的情况，例如虚拟装置启动时的情况。在块1704处，网络域所有方定义了组(G1、G2、…、Gn)。组可以包括如楼上、楼下等地点指定，或如管理、气候控制等功能指定，并且可以包括如在体育场里的撤离、进入路线等地点和功能的组合。可以使用任何数量的其他指定。一般来说，选择联盟小组名称以向系统提供有用的元数据。

[0170] 在块1706处，判定组(例如，G1)是否是可发现的。如果否，则在框1708处，将所述组发布到区块链。在框1710处，可以接收来自对象(例如O1)的请求以加入组G1。在框1712处，可以接收来自对象O1的EPID加入参数。这些可以响应于来自组装置所有方的请求而被发送。

[0171] 在框1714处，联盟小组名称服务器校验来自O1的加入请求。可以使用任何种类的凭证或技术来认证所述请求。例如，联盟小组名称服务器可以检查实例、机构或类型名称凭证，以判定这些值是否在区块链中。在安全性更高的应用中，在允许装置加入联盟小组之前，可能要求所有凭证都是正确的。同样地，在安全性更低的应用中，联盟小组名称服务器在联盟小组中登记装置时可能不需要凭证。如果在框1716处确定请求有效，则在框1718处可以向对象O1下发如EPID等联盟小组凭证。如果所述请求未被确定为有效，则所述过程在框1720处结束，而不下发凭证。

[0172] 图18是根据一些实施例的可以存在于IoT装置1800中用于创建联盟小组的组件的示例的框图。类似编号的项如关于图3和图8所描述的那样。可以注意到，可以选择不同的组件并将其用于关于图8所讨论的IoT装置800以及关于图18所讨论的IoT装置1800。

[0173] 大容量存储装置808可以包括用于实施如本文所描述的联盟小组的创建的多个模块。尽管在大容量存储装置808中示出为代码块，但是可以理解，任何模块都可以完全或部分地使用例如内置到专用集成电路(ASIC)中的硬连线电路代替。大容量存储装置808可以包括联盟小组名称服务器1802，所述联盟小组名称服务器包括用于对象的方便分组。如本文所讨论的，可以基于位置、功能或组合来形成组。用户可以定义要用于分组的参数。类型名称服务器1802可以构建并维护联盟小组成员列表1804以生成联盟小组的名称。如果所述组不可发现，则发布方1806可以将所述组的包括类型、位置和其他元数据的特征提供给其他IoT装置，以便这些IoT装置可以判定其是否应该加入所述组。例如，这可以通过将组名称和构成发布到区块链836来执行。

[0174] 除了如类型名称事务和复合对象事务等其他信息之外，区块链836可以包括在IoT装置1800中以记录联盟小组名称事务。如本文所描述的，区块链836事务可以通过还存储区块链836的副本的网状装置812的多数投票来验证。

[0175] 可以包括凭证校验器1808以接收来自希望加入联盟的IoT装置和复合对象的凭证。可以针对区块链836中的事务来检查凭证校验器1808以判定凭证是否有效。如果是，则所述凭证校验器1808可以获得来自EPID服务器840的凭证并将其下发到发送加入请求的IoT装置或复合对象。凭证校验器1808可以然后将事务提交给区块链836以记录已经加入联盟小组的IoT装置或复合对象。

[0176] 图19是根据一些实施例的包括用于引导处理器902创建联盟小组的代码的非暂态机器可读介质1900的框图。处理器902可以通过总线904访问非暂态机器可读介质1900。可以如关于图8的处理器802和总线806所描述的来选择处理器902和总线904。非暂态机器可读介质1900可以包括针对图8的大容量存储装置808所描述的装置，或者可以包括光盘、拇指驱动器、或任何数量的其他硬件装置。

[0177] 非暂态机器可读介质1900可以包括代码1902以引导处理器902通过例如位置、功能或两者来定义联盟小组。可以包括代码1904以引导处理器902判定联盟小组是否是可发现的，例如，设置为使用标识联盟小组的元数据来响应发现请求。可以包括代码1906以引导处理器902将联盟小组发布到区块链，或直接发布到周围装置。这可以使联盟小组的存在已知、可发现或两者。

[0178] 可以包括代码1908以引导处理器902接受来自IoT装置、包括原子对象、复合对象或两者的联盟小组加入请求。加入请求可以标识联盟小组，并且包括如位置、类型和其他凭证或元数据等校验信息。可以包括代码1910以引导处理器902验证凭证，例如，判定其是否存在于区块链中。可以包括代码1912以向请求器下发如EPID密钥等凭证。

[0179] 可能需要保护例如在联盟小组、网状网络、雾装置或其他安排中的IoT装置之间的通信，但对于功能有限的装置来说，这可能存在问题。进一步地，IoT装置可能分布在不同的网络上，从而使保护通信更具挑战性。分布式分类账系统可以增强IoT装置的通信安全性。

[0180] 图20是根据一些实施例展示跨公共域2002、私密域2004、和公共-私密域2006的互操作性的示意图2002。网络拓扑可能处于连续的变化状态，使得永久映射的任何尝试都不可能。因此，IoT装置可以使用如域名称服务器(DNS)等骨干资源来在域之间发送分组。分组可以通过如路由器2008所示出的互联网骨干网在域2002、2004和2006之间路由。

[0181] 在一些方面，路由器2008提供将域彼此耦合的边缘连接。如本文所描述的，可以在域2002、2004和2006的边缘处提供任何数量的服务以增强互连性。例如，公共域2002与私密域2004之间的互连可以为域访问、针对域访问的显示许可和跟踪、以及公共和私有通信量的分离等提供小额支付的机会。类似地，公共域2002与公共-私密域2006之间的互连可以为如基于时间的租用、资源市场、以及分布式身份服务器等服务提供机会。私密域2004和公共-私密域2006之间的互连可以为内联服务互连、基于行为的威胁分析、以及证据来源等提供机会。

[0182] 图21是根据一些实施例的跨具有有线网络2102以及无线网络2104和2106的异构2100网络的互操作性的示意图。无线网络2104和2106可以通过有线网络2102中的装置通信地耦合。这为无线网络2104和2106中的装置之间的通信的效率改进、以及无线网络2104或2106中的装置与有线网络2102中的装置之间的通信的改进提供了机会。例如，将第一无线网络2104耦合至有线网络2102的边缘装置2108可以提供用于信息变换的数据以减小有效载荷的大小。进一步地，边缘装置2108可以具有允许来自第一无线网络2104的分组通过同

时阻止未经许可的分组传送的许可系统。许可系统可以包括用于使小额支付允许信息跨有线网络2102移动的系统。作为示例，第一无线网络2104可以是农业现场的地面湿度传感器阵列。报告频率可以取决于变化率，这可能由于需要购买带宽以匹配最高报告率而增加成本。因此，小额支付系统可以通过允许按需支付事务来降低成本。

[0183] 图22是根据一些实施例的用于任务定义和委托的示例方法2200的示意图。图22的方法2200可以由关于图24所描述的IoT装置2400来实施。所示出的示意图可以表示自组织许可指南和许可指南功能2202的任务定义和委托。然而，交互过程可以在2204处开始。

[0184] 在框2204处，装置可以标识其用于执行任务的对等机。虽然装置可以执行这种发现，但此情境下的术语装置还可以指通过单个装置或多个装置采取动作的代理或服务。在框2204处发现对等机及其能力可以通过装置的发现程序、请求的系统、所定义协议或通过以上所描述的资源发现的布隆过滤器跳转方法来进行。

[0185] 在框2206处，装置可以生成许可指南和许可指南功能2202。许可指南和功能可以是机器可读的。许可指南可以存储在区块链上或区块链外。在示例中，许可指南可以是可发现的并且可以广告至由装置发现的对等机。在框2206处，装置可以将待执行的功能编写为待写入许可指南中的离散功能。在示例中，所述功能可以是固定功能、通用代码段或专用代码段。所述功能可以由人类开发者、通过用于生成代码的人工智能(AI)方法或任何组合编写。在示例中，所述功能可以通过遗传算法生成。

[0186] 在框2208处，可以由装置、对等机或装置和对等机的自组织网络中的任何其他方协商或编辑许可指南。可以编辑许可指南的许多不同方面。例如，许可指南可以具有以上所描述的包含用于加入和退出许可指南的方法的格式。作为协商许可指南的一部分，可以在许可指南广告许可指南的属性和功能之后进行编辑。响应于广告属性或功能，装置的对等机可以通过同意许可指南或插入或编辑许可指南来同意供应这些属性或功能。在示例中，如果提供了装置或对等机进行的授权以尝试访问对等机资源和其他功能当中的任何服务，则装置可以通过许可指南请求生成令牌。在示例中，许可指南可以包括具有限制的功能，所述限制具有包括时间约束、服务质量或数据质量在内的附加信息。在示例中，许可指南可以包括许可指南所有方可以从参与对等机处请求的其他条件。许可指南可以概述对源对等机的受限使用。在示例中，许可指南可以移动以允许多租户。

[0187] 如上所讨论的，条款可以由对等机协商。例如，数据消费者和数据提供商可以具有用于在达成许可指南之前对条款进行协商的机制。在示例中，各方可以广告条款和费用。在示例中，条款和费用是可协商的。以此方式，参与许可指南的实体可以保留用于确保其不会受约束于无利可图的许可指南的立场。这些条件的示例可以包括数据供应商可能想要强加的最小订阅费用和期限。

[0188] 在框2210处，可以执行许可指南。许可指南的执行可以无限期地运行。在示例中，许可指南的执行可以持续固定且指定的时间。响应于与服务提供商或数据提供对等机与许可指南的通信失败，许可指南可以终止。同样，如果新的对等机对来自装置或服务的功能性能进行了改进，则所述对等机可以接管许可指南的功能。许可指南功能的改进可以包括以较低费用、较高数据质量或其他可测量度量执行许可指南中使用的服务。在示例中，可以在许可指南开始之前将许可指南执行期间执行的机制列表记录到许可指南中。

[0189] 在框2212处，可以监测许可指南的执行。监测许可指南的执行可以包括搜索新对

等机和新节点。在框2214处，可以响应于满足许可指南的一致的条件而在参与各方之间发生支付。在示例中，可以在许可指南中指定支付。在框2216处，一旦许可指南的期限到期，就可以终止许可指南。在示例中，可以响应于确定参与各方中的任何参与方退出许可指南并且未定位到替换方而终止许可指南。在示例中，可以响应于检测到已经实现了创建许可指南的目的而终止许可指南。

[0190] 在自组织许可指南2202内，可以描述许可指南功能。例如，自组织许可指南2202内的功能可以包括加入许可指南功能2218。可以像以上已经描述的那样实施加入许可指南功能。自组织许可指南2202还可以包括如以上所描述的退出许可指南功能2220。自组织许可指南2202可以包括可以类似于以上所描述的其他列表装置功能的参与装置列表功能2222。自组织许可指南2202可以包括如以上所描述的装置属性列表功能2224。

[0191] 在示例中，自组织许可指南2202可以包括用于解释添加到自组织许可指南2202的装置的条款和条件的功能。装置条款和条件列表功能2226可以允许加入许可指南的装置将对其服务条款的条件作为参数或功能包括在自组织许可指南2202内。在示例中，装置条款和条件列表功能还可以包括用于强制执行可能作为许可指南的部分而一致的将由许可指南的参与方强加或同意的罚款的功能。

[0192] 在示例中，自组织许可指南2202可以包括用于解释服务质量(QoS)条款和条件(T&C)列表2228的功能。QoS T&C列表2228可以包括允许来自许可指南的服务数据的消费者规定关于服务和数据供应的QoS规则。这些规则可以包括例如数据可用性规范、服务可用性、数据供应频率、所供应数据的准确性和数据粒度。QoS T&C列表2228还可以包括数据是否来自可信传感器的规则，其中，当可以表明数据的提供来自例如传感器的测量结果而不是处理器中的一段代码生成的值时，数据可能来自可信传感器。如以上所描述的，自组织许可指南2202可以包括请求令牌功能2230和撤销令牌功能2232。

[0193] 在示例中，自组织许可指南2202可以包括用于解释支付条款和条件的功能。因此，自组织许可指南2202可以包括用于示出触发各方之间的支付的事件的支付T&C功能2234。在示例中，触发各方之间的支付的这些事件可以包括完成订阅服务供应、完成订阅数据供应。T&C功能2234可以写入按每次使用付费模型或其他模型的框架内的功能中，在所述其他模型中，还可以存在用于由于未能满足之前同意的条款而对许可指南的一方强加罚款的功能。

[0194] 在示例中，自组织许可指南2202可以包括数据平面功能2236。数据平面功能2236可以允许许可指南的各方同意将如何供应和消费数据或服务。数据平面功能2236可以规定可以在链外机制中共享数据，并且数据平面功能2236可以指定可以使数据对其可用的特定端点和端点技术。在一个示例中，可以通过使端点订阅来源的功能或通过发布数据以供消费的功能使数据可用。在示例中，参与许可指南2202的各方的数据消费和服务消费方式可以包括认证和授权信息。自组织许可指南2202的各方可以供应服务或数据，并且可以指定各方可以如何使消费偏好可用。消费数据和服务的各方还可以指定消费各方可以如何消费认证和授权的偏好。

[0195] 针对供应和消费技术所示出的重叠可以允许各方在无人工参与的情况下就共享服务和数据的方法达成一致。在示例中，可以引入协议转换中介，作为可以加入许可指南2202以提供服务和数据的自动转换或自动代理为消费者和消费方所期望的端点类型或数

据格式的一方。

[0196] 图23是根据一些实施例的用于由协议转换中介进行的协议转换代理的示例方法2300的处理流程图。图23的方法2300可以由关于图24所描述的IoT装置2400来实施。例如，协议转换中介的概念可以是例如可以加入许可指南以提供服务或数据自动转换或自动代理为消费者所期望的端点类型或数据格式的一方。处理流程可以在框2302处开始。

[0197] 在框2302处，可以发现对等机。可以通过协议转换中介、通过参与方或通过许可指南2202计算来完成这一点。在示例中，发现对等机可以是初始阶段或可以在整个过程中重复以确保对等机是已知的。

[0198] 在框2304处，可以起草潜在参与者之间的许可指南2202。起草自组织许可指南2202可以包括定义将在起草自组织许可指南2202阶段期间进行的一个或多个任务。在示例中，任务可以指服务供应。在示例中，供应服务可以利用供应商提供的有关服务的信息。服务供应商可以通过查找服务来广告其服务。查找服务可以是集中式的或分散式的。本文描述了一种查找服务的方法。在示例中，这种起草自组织许可指南2202可以包括交换阶段，其中，许可指南2202中的对等机可能已经指定了具体参数的范围。参数可由一方标记为优选。参数可以提供所述偏好相比其他方偏好的有序权重。

[0199] 在框2306处，可以加入许可指南2202。协议转换中介可以加入许可指南2202。协议转换中介可以监视一方或多方加入许可指南2202。在示例中，许可指南2202可以包括稍后可以用来判定许可指南2202是否结束或服务的消费者是否希望继续并尝试寻找可替代供应商的生存时间(TTL)参数。暴露于许可指南2202的装置还可以具有最小数量的各方以满足许可指南2202的参数。在示例中，这些所列参数可以在服务、参与装置的属性、T&C以及QoS参数方面进行概述。在加入许可指南阶段期间，各方可以响应于标识用于执行任务或协议的较低成本实体而加入、退出或被逐出所述过程。同样，各方可以响应于标识用于执行任务或协议的具有较高净值实体的实体而加入、退出或被逐出。

[0200] 在示例中，如果存在任务消费者倾向于呈现的三种具体特征和属性，则这些特征和属性可能最初由三个不同的各方以不同的成本供应。在这个示例中，在此阶段期间，响应于标识可以以更好的费用点供应服务的单方，则使用这个所找到的单方可能是更优的解决方案。

[0201] 在框2308处，协议转换中介可以请求对服务提供节点的自动委托。服务提供节点可以指提供自组织许可指南2202中所概述的服务的节点。自动委托可以包括向现场的IoT装置部署微服务，所述IoT装置包含以任务消费者指定的方式处理数据和服务的功能。在示例中，自动委托可以涉及可以在没有人工干预的情况下在合理时间段内自动或远程完成的任务。如果指定，则自动委托还可以使用对现场装置的手动部署。手动部署可以包括由人类、经过训练的动物、无人机或机器人进行的部署。在示例中，如果包括供应商的部署时间的QoS设置满足各方对许可指南2202的请求，则可以在此过程的某个版本中使用手动部署。

[0202] 在示例中，可以向许可指南2202内的各方提供用于描述功能的令牌或对象，包括常量、标识符、操作符、保留字、和分隔符以及前言。如先前所描述的，前言可以涉及对等机之间可以用于进一步处理的任何信息的配置、初始化和交换。前言可以包括服务的位置、机器可读应用协议接口(API)描述符、访问凭证以及对密钥的访问。在示例中，失败的前言可以包括失去相当多的供应商、失去消费者、退出过程。如果一方退出，则过程可以返回至起

草自组织许可指南2202。

[0203] 在框2310处，如果前言和前面的步骤执存在并且成功，则开始执行许可指南2202。基于前言和许可指南2202的条件和参数以及各方的同意条款，如果满足条款，则可以解锁支付。在示例中，在起草许可指南2202时已经交换并同意了所述条款。

[0204] 在框2312处，可以响应于检测到对等机终止参与许可指南2202而通过协议转换中介进行最终支付。在许可指南2202可以继续在现有成员的情况下运行的情况下，如果确定TTL尚未到期，则许可指南2202可以继续运行。然而，如果TTL在过程完成之前到期，则许可指南2202可以结束。在示例中，如果许可指南2202在没有找到可替代供应商或消费者的情况下可能无法继续，则所述过程可以返回至发现对等机阶段2302。

[0205] 图24是根据一些实施例的可以存在于IoT装置2400中的用于定义任务和委托节点的组件的示例的框图。类似编号的项如图8所描述的那样。

[0206] 同样如以上所描述的，参照图8，大容量存储装置808可以包括用于实施本文所描述的组创建功能的多个模块。尽管在大容量存储装置808中示出为代码块，但是可以理解，任何模块都可以完全或部分地用例如内置在专用集成电路(ASIC)中的硬连线电路替换。大容量存储装置808可以包括用于为多个已发现的对等机起草许可指南2202的许可指南起草器2402，其中，所述多个已发现对等机各自可以具有参数，并且其中，可以响应于许可指南2202的条款可由所述多个已发现对等机中的至少两个允许而生成所述条款。所述多个已发现对等机中的每个可发现对等机的参数可以包括相关联对等机的可允许条款的范围。许可指南起草器2402可以包括用于列出所述多个已发现对等机的条款和条件的功能。例如，许可指南起草器2402可以包括所述多个已发现对等机的服务质量条款和条件的列表。许可指南起草器2402包括所述多个已发现对等机的数据平面条款和条件的列表。在示例中，数据平面可以指示对等机将如何供应和消费数据的过程。许可指南2202还可以包括如以上所描述的生存时间。在示例中，许可指南2202可以包括用于管理对等机加入和退出许可指南2202的协议转换中介。许可指南2202可以包括用于管理所述多个已发现对等机之间的配置的交换的前言。

[0207] 大容量存储装置808可以包括用于响应于检测到满足条款的条件而执行许可指南2202的动作的动作执行器2404。动作执行器2404可以包括用于向对等机自动委托指导所述对等机处理数据的服务的功能。在示例中，所述条款是指在所述多个已发现对等机之间要支付的支付费用，并且可以在检测到所述多个已发现对等机中的对等机终止参与许可指南2202时在对等机之间进行最终支付。

[0208] 图25是根据一些实施例的包括用于定义任务和委托节点的代码的非暂态机器可读介质2500的框图。类似编号的项如关于图9所描述的项那样。

[0209] 非暂态机器可读介质2500可以包括用于引导处理器902为多个已发现对等机起草许可指南2202的代码2502，其中，所述多个已发现对等机各自可以具有参数，并且其中，响应于许可指南2202的条款可由所述多个已发现对等机中的至少两个允许而生成所述条款。起草许可指南2202可以包括用于列出所述多个已发现对等机的条款和条件的功能。起草许可指南2202可以包括列出所述多个已发现对等机的服务质量条款和条件。起草许可指南2202可以包括列出所述多个已发现对等机的数据平面条款和条件。数据平面可以指示对等机将如何供应和消费数据的过程。许可指南2202可以包括生存时间。许可指南2202可以包

括用于管理对等机加入和退出许可指南2202的协议转换中介。许可指南2202可以包括用于管理所述多个已发现对等机之间的配置的交换的前言。

[0210] 非暂态机器可读介质2500可以包括用于引导处理器902响应于检测到满足条款的条件而执行许可指南2202的动作的代码2504。执行许可指南2202的动作可以包括例如向对等机自动委托指导所述对等机处理数据的服务。如本文所使用的，条款是指将在所述多个已发现对等机之间支付的支付费用。在示例中，可以在检测到所述多个已发现对等机中的对等机终止参与许可指南2202时在对等机之间进行最终支付。

[0211] 跨IOT网络的消息流可以随着时间的推移建立可识别模式，但是如果未授权的代理获得对网络的访问，则未授权的代理可以能够出于其自己的目的而更改操作。因此，如果事务在区块链中可见，则有可能在网络上检测此类非法活动并且采取行动来解决、或甚至防止发生有效的未授权事务。

[0212] 在示例中，区块链可以用于保存网络上的事务记录以及网络代理执行操作的预授权。此预授权功能可以称为分散式网络访问代理(DNAP)协议。

[0213] 图26是根据一些实施例的分散式网络访问代理使用功能的示例组织2600的示意图。类似编号的项如参考图22所公开的那样。针对DNPA协议的功能及其与许可指南2602交互的过程可以在2604处开始。

[0214] 在框2604处，装置可以引导。引导过程可以是在预执行环境(PXE)中的网络接口装置上的网络栈的初始化，并且可以不暗示存在更高级别的软件栈或操作系统。

[0215] 在框2606处，网络接口适配器可以生成用于作为区块链感知装置操作的密钥。使用所生成密钥的装置也可以使用或操作来自硬件启用的安全飞地。生成的密钥可以用于对离开装置的通信量进行签名，使得可以确定每个分组的通信量的起源和每个分组的内容。在示例中，此装置的基于密钥的加密可以是在装置上启用的硬件，并且可以协助防止中间人攻击。如果未使用来自有效代理的私钥对通信量签名，则网络可以丢弃到达装置的通信量。在示例中，为了使用网络交换机和路由器，可以对网络交换机进行修改，使得通信量的硬件加密和解密可以发生。

[0216] 在框2608处，网络接口适配器可以在区块链上创建访问请求事务。在示例中，可以将在网络上运行的分组强制路由到DNAP。在此情境中，DNAP可以被认为是第2层数据链路层的功能，因为其可以作为网络的物理交换机和路由器上的服务起作用。一旦网络装置尝试使用核心网络基础设施，那么如果网络装置尝试使用核心网络基础设施或除通过专用介质的私有对等连接之外的连接，则所述网络装置可能不能避免将网络装置通信量路由到分散式网络访问代理。在示例中，通过专用介质的对等连接可以包括通过蓝牙或以太网交叉电缆的通信。

[0217] 在框2610处，DNAP协议可以授予装置某些网络访问功能。在示例中，DNAP协议可以利用许可指南的先前讨论的功能。运行DNAP协议的网络上的类似交换机和路由器的节点可以成为区块链的挖掘器。在示例中，网络的节点可以运行一致性算法，所述一致性算法不使用大的计算开销或基于直接参与事务。消逝时间算法的证据可以是此协议中使用的技术的一个示例。DNAP协议的使用还可以防止流氓交换机和路由器的引入，因为恶意行为者将必须能够例如部署或损害51％的网络基础设施以执行成功的攻击。DNAP装置尝试使用访问请求事务功能可以导致网络接口适配器通过许可指南的机制向网络标识自己。网络接口适配

器可以运行硬件启用的安全飞地以协助此过程。

[0218] 在框2612处，如果DNAP使用装置被许可指南中的加入功能接受，则可以将DNAP使用装置添加到网络上创建的或授权的装置的许可指南列表中。在框2610处，可以发生初始化过程，并且装置可以向许可指南描述其属性和特征。在示例中，DNAP描述的属性可以通过DNAP装置上硬件启用的安全飞地来证明，以建立信任级别。在示例中，可以在人机接口装置(HID)的扩展中定义对DNAP装置属性的描述。对属性的描述或存储在许可指南中的数据可以存储在链外。在示例中，启用了DNAP协议的交换机或路由器、链外数据的存储可以涉及交换机内的一些存储的集成。DNAP网络中的交换机和路由器可以是边缘节点或雾节点。存储可以在网络上的路由器和交换机之上成为DHT类型的分布式存储机制。

[0219] 在框2614处，可以向装置下发令牌以许可装置以协调的方式执行动作。将令牌用于装置可以允许DNAP网络上的实体有单独装置防火墙。在示例中，如果装置持有互联网控制消息协议(IMCP)令牌，则所述装置可以发送和接收ping通信量。令牌的使用可以通过允许具有相同令牌的装置不通过路由器彼此对话而允许形成虚拟局域网(VLAN)。令牌也可用于创建未连接到更大企业网络的私密网络。

[0220] 令牌分配可以具有用于将默认令牌类型分配给满足一定标准的装置的规则。这些规则可以管控装置的类型并且装置是否符合最低安全标准。在示例中，装置的类型可以是公司所有的和支持的装置，或者是“自带”风格计划中的雇员所有的装置。在一些环境中，诸如个人从个人装置访问金融数据库，本文所描述的令牌分配可以在公司环境之外应用。在示例中，未被授权或者不拥有用于某些动作的令牌的DNAP装置可以接收装置请求功能已经失败的通知，因为所述装置未被网络授权。使用基于令牌的批准方法可以分散网络上的安全性执行。在示例中，网络管理员可以手动创建令牌以表示网络管理员在网络上许可或拒绝的动作。在示例中，可以由网络设备制造商提供预先填充的令牌集。

[0221] 在框2616处，可以在网络上授权DNAP装置以执行某些功能。DNAP装置可以被授予附加的令牌或者使令牌被撤销。此操作的控制平面可以是区块链支持的。区块链支持可以指在装置下发令牌之后在装置所连接到的端口或接入点上执行的规则，其中，针对连接装置所提供的规则通常不会改变并且基于装置的经确认身份而强制执行所述规则。在示例中，网络中的交换机和路由器可以是挖掘器并且可以将事务同步到共同分享的分类账。

[0222] 在框2618处，可以阻止装置可以尝试执行的功能，并且装置可以接收指示网络已阻止通信的消息。

[0223] 图27是根据一些实施例的用于分散式网络访问代理来使用功能的示例方法2700的处理流程图。图27的方法2700可以由关于图28所描述的IoT装置2800来实施。处理流程可以在框2702处开始。

[0224] 在框2702处，可以初始化网络装置。在示例中，网络装置可以是客户端、服务器、网络基础设施的一部分、或网络接口。在框2704处，装置上的固件和硬件生成身份并且允许装置以区块链客户端的能力起作用。在示例中，节点可以具有网络交换机角色或路由器角色，并且装置可以以DNAP区块链的验证器的能力起作用。DNAP区块链可以分布在所有网络基础设施节点上。

[0225] 在框2706处，装置可以发布发现广播消息，类似于预引导执行环境(PXE)或动态主机配置协议(DHCP)。在示例中，可以使用PXE和DHCP协议来实施装置和DNAP协议。在示例中，

如果发现广播没有返回任何DNAP感知系统的位置，则网络装置可以延迟并且重试。如果发现广播没有返回任何DNAP感知系统的位置，则装置可以执行遗留操作，其允许装置在非DNAP网络上操作。延迟和重试的过程或切换到另一网络的过程可以通过预设策略、BIOS设置、固件设置、装置上的物理跳线设置、或以其他方式手动调整来控制。

[0226] 在框2708处，响应于在操作中发现DNAP网络，DNAP装置申请加入DNAP网络。如上所讨论的，加入DNAP网络可以包括加入网络中遵循的许可指南。

[0227] 在框2710处，DNAP装置可以发布其属性和特征，并且可以基于装置的属性或身份来请求分配给DNAP装置的令牌。分配令牌的决策可以由网络管理员通过使用策略或者基于例如装置的网络、地址、身份、装置类型、装置能力、装置特征、或者基于在装置和许可指南上策略的有效性测量来控制。如上所讨论的，构造许可指南可以由可以使用用户界面或应用界面的网络工程师完成。许可指南和令牌的实施方式可以基于每个装置实现网络通信量的详细控制。在示例中，企业系统可以允许超文本传输协议(HTTP)通信量或其他特定类型的通信量作为装置的默认值。使用DNAP协议的企业系统还可以为装置提供指定的业务功能附加令牌，以在这些装置可以希望使用其他网络服务时许可其他通信量类型。

[0228] 在框2712处，装置可以在网络上发送分组。操作系统和开放系统互连(OSI)栈的更高层可以不知道此过程。在示例中，发送装置分组可以在网络层运行。网络可以以若干方式认证分组。例如，令牌可被附带至分组的报头，或者分组可以利用发送分组的身份的私钥被签名。如果发送分组的身份可以通过校验并且他们拥有发送那个类型通信量的令牌，则可以许可到达网络的分组。如果通信量不被许可，则网络运营商可以决定将否定确认(NACK)发送回至客户端，否则分组通过网络路由到其目的地。

[0229] 在DNAP中，网络基础设施本身可以充当区块链中的验证器节点，作为存储关于系统状态的共识的地方。例如，对于恶意实体来破坏这种方法，恶意实体将需要破坏51％的网络基础设施。破坏大多数网络基础设施可以导致恶意实体更多的负担，因为有许多位置需要受到破坏，而不是单一的集中式防火墙服务。网络基础设施的共识可以是访问控制列表(ACL)命令列表(C-List)。在示例中，一旦利用分散式协议建立了网络基础设施的共识，就可以在存储在区块链中的ACL或C-LIST的管理上重写或映射上述方法。在示例中，DNAP协议可以基于由具有协议中的有效地址的代理签名的事务的触发来更新状态改变。

[0230] 如本文关于安全性和与DNAP通信所使用的，资源的创建者可以下发令牌，令牌本身可以是可转移的或不可转移的，并且令牌可以基于来自网络运营商的指令像一次性凭证一样被使用。使用DNAP功能令牌，一旦使用令牌，令牌可以不再被使用，并且因此DNAP和类似系统中使用的令牌可以像配额一样用于控制装置对网络的访问量。可以将令牌设置为针对X个分组、或X个数据量、或X个时间段起作用，或者其可以针对某些类型的通信量和其他的配额具有无限租期。

[0231] 图28是根据一些实施例的可以存在于IoT装置2800中用于与有价值数据单元协商的组件的示例的框图。类似编号的项如图8所描述的那样。

[0232] 同样如以上所描述的，参照图8，大容量存储装置808可以包括用于实施本文所描述的组创建功能的多个模块。尽管在大容量存储装置808中示出为代码块，但是可以理解，任何模块都可以完全或部分地用例如内置在专用集成电路(ASIC)中的硬连线电路替换。大容量存储装置808可以包括装置身份生成器2802，用于为作为区块链客户端的装置生成装

置身份。装置可以从DNAP请求令牌。令牌可以授予装置除了对等之外发送和接收网络数据的能力。在示例中，令牌可以授予装置在网络的开放系统互连层的层上发送和接收数据的能力。在示例中，装置可以存储由装置接收和发送的事务的事务记录，所述事务记录将与DNAP共享。装置可以生成密钥以指示从装置发送的分组的起源。装置可以是区块链启用的装置，并且装置可以在区块链上存储由装置发送并由装置接收的事务。对装置属性的描述可以存储在区块链之外。

[0233] 大容量存储装置808可以包括消息发布方2804，用于从装置发布发现广播消息。大容量存储装置808可以包括网络申请器2806，用于响应于装置基于发布的发现广播消息从DNAP接收响应而从装置申请加入分散式网络访问代理(DNAP)网络。大容量存储装置808可以包括装置描述器2808，用于向DNAP描述装置的身份和属性。

[0234] 大容量存储装置808可以包括分组发送器2810，用于响应于网络基于装置的身份和属性向装置授予访问权而通过网络从装置发送分组。在示例中，分组可以附带令牌，并且可以将分组和令牌的组合发送为DNAP以进行校验，其中，响应于检测到令牌未被DNAP接受，DNAP拒绝分组和令牌两者。在示例中，令牌可以针对与阈值分组数量、阈值数据量、或阈值时间段中的至少一个的使用为有效的。

[0235] 图29是根据一些实施例的包括用于定义任务和委托节点的代码的非暂态机器可读介质2900的框图。类似编号的项如关于图9所描述的项那样。

[0236] 非暂态机器可读介质2900可以包括代码2902，用于引导处理器902为作为区块链客户端的装置生成装置身份。装置可以从DNAP请求令牌。令牌可以授予装置除了对等之外发送和接收网络数据的能力。在示例中，令牌可以授予装置在网络的开放系统互连层的层上发送和接收数据的能力。在示例中，装置可以存储由装置接收和发送的事务的事务记录，所述事务记录将与DNAP共享。装置可以生成密钥以指示从装置发送的分组的起源。装置可以是区块链启用的装置，并且装置在区块链上存储由装置发送并由装置接收的事务。对装置属性的描述可以存储在区块链之外。

[0237] 非暂态机器可读介质2900可以包括代码2904，用于引导处理器902从装置发布发现广播消息。非暂态机器可读介质2900可以包括代码2906，用于引导处理器902响应于装置基于所发布的发现广播消息接收来自DNAP的响应而从装置申请加入分散式网络访问代理(DNAP)网络。非暂态机器可读介质2900可以包括代码2908，用于引导处理器902将装置的身份和属性描述到DNAP。

[0238] 非暂态机器可读介质2900可以包括代码2910，用于引导处理器902响应于网络基于装置的身份和属性向装置授予访问权而通过网络从装置发送分组。在示例中，分组可以附带令牌，并且可以将分组和令牌的组合发送为DNAP以进行校验，其中，响应于检测到令牌未被DNAP接受，DNAP拒绝分组和令牌两者。在示例中，令牌可以针对与阈值分组数量、阈值数据量、或阈值时间段中的至少一个的使用为有效的。

[0239] 许可指南可以用于为装置提供分散式授权、认证、和计费。本公开公开了用于对远程认证拨入用户服务(RADIUS)和相关DIAMETER协议的扩展的构建块。在示例中，所公开的技术解决了由集中管控的系统导致的可扩展性问题。这些技术可以应用于更大的分布式半径网络。在示例中，大型网络的成员可以在其校园中运行其自己的RADIUS服务器、维护其自己的用户账户。在示例中，认证可以通过将成员的网络访问请求路由回至成员的网络的

RADIUS代理来进行，而不管请求的位置如何。如果在成员网络上接受加入网络的请求，则大型网络的其余部分接受来自所述起源的通信量作为认证的。此技术允许网络避免在这样大的分布式动态网络中同步用户账户。可以添加此技术以便在新实体加入网络时提供审查过程。可以添加此技术以便提供实体安全地运行其RADIUS服务器并且符合设置策略设置的标准的确认。

[0240] 图30是根据一些实施例的用于利用许可指南3002提供认证、授权、和计费的分散式版本的示例组织3000的示意图。类似编号的项如参考图22所公开的那样。功能的过程可以在3004处开始。

[0241] 组织3000和方法可以是完整系统，并且还可以是现有授权、认证、和计费协议的扩展。在框3004处，用户可以登录到其已经是用户的集中式机构。在示例中，用户可以是大学的学生或教职成员，并且集中式机构可以是大学网络。登录后，用户可以创建其简档。此时可以使用用户简档、密码、或网络一起用于来向系统验证用户身份。如果用户是装置，则所述装置可以通过系统模块引导和委托装置认证，而不是登录用户账户。

[0242] 在框3006处，用户的装置可以在使用的指令处交换支付。在示例中，用户的装置可以访问按每次使用付费的网络，并且可能需要支付来访问所述网络。通过用户装置的用户可以通过网络与网络运营商协商支付。这种支付可以是可选的，例如，网络提供商可以提供免费访问。网络提供商可以选择收费，并且在收费时网络提供商可以指定网络提供商可以接受的支付形式。在示例中，网络可以接受加密货币或信息币。如关于3006所描述的交换支付可以如所列出的那样执行，或者在加入实体已经接受条款并且提供商允许加入实体加入条目访问的过程结束时执行。

[0243] 在框3008处，可以为用户创建私钥，并且私钥可以与地址相关联。在框3010处，用户装置可以请求加入许可指南。如上面在框2218所描述的，加入许可指南可以是在用户装置可以成为网络的永久成员的情况下发生一次的事件。在示例中，加入许可指南可以是有时间限制的、或者受其他条件限制。如上所描述的，加入许可指南功能可以在接受申请者之前确保满足某些条件。在示例中，如果进行了支付，则在完成加入许可指南的整个过程之前，可以或可以不结束支付。

[0244] 如上所描述的，在框2222处，可以存储参与身份列表。参与身份的存储可以在链外完成。存储也可能以散列形式发生。进一步地，关于参与身份的存储，指针可用于标识可以存储身份信息的位置。存储的数据也可以被加密并限制授权实体查看。

[0245] 在框3012处，可以使用属性过滤器来验证属性。在示例中，可以使用零知识证据机制来完成验证。属性验证可以使用证明。在示例中，属性过滤器可以验证在网络上操作的条件，例如标识个人是否超过18岁。属性过滤器可以允许个人的属性证明，而个人不必公开其完全身份。

[0246] 在框2230处，像上面一样，申请者装置可以请求令牌。如前，令牌可以是无限制的或者令牌可以是有限制的。令牌可以或可以不被加密货币支持。令牌的使用可以允许混合，其中一些令牌可以使用支付来获取而其他令牌是免费的，这由网络运营商决定。对令牌的请求可以涉及通过执行计费功能的区块链3014和区块链3014的侧链3016的附加步骤。在框3018处，在区块链3014内，来自许可指南3002的支付或功能调用在区块链上保留硬币。在框3020处，在侧链3016内，保留的令牌可以与创建令牌的侧链3016相关联。在侧链3016中保留

硬币或创建令牌的动作(其中,令牌可以被添加到区块链中)构成计费形式,其中,可以标识和构造哪些身份已经请求了哪种令牌。

[0247] 在框2232处,像上面一样,可以通过制定许可指南3002的策略来撤销令牌。在示例中,如果实体希望离开许可指南3002,则可以请求由实体退还令牌。响应于来自许可指南3002的请求,在框3022处,可以从侧链3016删除令牌。在框3024处,在区块链3014内,与侧链3016中所删除令牌相关联的任何硬币可以被释放给网络提供商或者根据事务的原因退还给实体。

[0248] 在框2234处,像上面一样,网络提供商宣称的支付T&C可以被编码到许可指南3002中。在框3026处,可以发送认证请求。在示例中,认证通过装置向网络发送请求来工作。装置可以向校验方提供公钥。在示例中,发送公钥的一方可以在区块链3014中检查以判定是否将令牌记入这种公钥。访问网络上的不同服务可以请求持有者拥有不同类型的令牌。

[0249] 在框3028处,可以消费令牌。在示例中,可以基于每次使用来消费令牌。在每次使用的基础上使用令牌可以是一种授权形式,所述授权形式向网络提供商给出一种用于基于每个服务、在实体的网络上将预算分配给所述实体的方法。提供商可以替代地指示令牌不是每次使用并且可以在没有使用限制的情况下被使用。在框3030处,可以将通过侧链3016的令牌的消费或呈现记录为侧链上的事务。此记录可以被视为另一种计费服务。在框3016处,侧链可以指示是否消费了令牌。令牌是否被消费,并且在侧链3016上是否可能存在这种消费记录。在示例中,在侧链3016上消费的令牌可以由主区块链3014上的硬币支持。在框3032处,在区块链3014上,可以将硬币释放回或者支付返回至网络运营商并且至提供商的钱包。

[0250] 图31是根据一些实施例的用于利用许可指南提供认证、授权、和计费的分散式版本的示例方法3100的处理流程图。图31的方法3100可以由关于图32所描述的IoT装置3200来实施。处理流程可以在框3102处开始。

[0251] 在框3102处,请求使用网络的实体可以例如通过门户或API进行注册。在示例中,可以由各个大学提供门户以供学生注册和支付费用。在示例中,对于寻求加入面向机器网络的实体,这样的实体可以使用来自任何钱包或信用卡提供商的资金自动加入。

[0252] 在框3104处,如果加入实体在其希望加入的网络上没有信用,则可以使用支付交换。在框3106处,加入实体可以通过参与支付交换来加入智能合约。在示例中,可以注册加入实体的属性。在示例中,使用的属性可以包括出生日期和其他个人数据。在示例中,机器的属性可以包括装置类型或软件的类型和版本。如果使用支持文档报告属性数据,则可以证明属性数据。在机器属性的情况下,这些机器属性可以通过技术方法证明,包括可信任感测或硬件信任根(HWROT)。响应于此证明,可以在许可指南中维护参与实体列表,并且实体现在可以从许可指南请求令牌。

[0253] 在框3108处,响应于由共识网络确定的有效身份请求的确认,令牌可被下发至实体。响应于网络上的身份余额大于零,令牌可被下发至实体。在示例中,可以为实体的证明设置TTL。在示例中,可以通过时间、使用、和地理上限制实体的证明。在示例中,限制可以由令牌强制执行,因为如果实体是移动的,则令牌可以在一些区中工作而在其他区中不工作。

[0254] 在框3110处,可以保留硬币以抵抗令牌。在示例中,硬币可以保留在侧链中。响应于不成功的尝试,可以重试保留硬币的过程。在示例中,所述过程还可以包括退出事务,从

而在过程中退还交换的信用。如果尝试保留硬币成功，则可以创建令牌并将其下发至实体，然后所述实体可以发送认证请求。如先前所描述的，认证请求可以经属性过滤。当令牌被消费时，在侧链中与其相关联的硬币可以被解锁或释放，并且这些令牌可以传给网络提供商。

[0255] 在框3112处，实体可以离开许可指南。为了避免离开许可指南，如果实体的令牌已经被消费，则实体可以请求附加的令牌。在示例中，如果实体身份在网络上不再有效，则许可指南可以结束。在示例中，网络实体或网络提供商还可以发起此过程以驱逐所述实体。可以撤销或销毁未用完的令牌，并且可以根据许可指南的条款退还实体的剩余资金余额。

[0256] 图32是根据一些实施例的可以存在于IoT装置3200中用于利用IoT装置进行分散式授权、认证、和计费的组件的示例的框图。类似编号的项如图8所描述的那样。

[0257] 同样如以上所描述的，参照图8，大容量存储装置808可以包括用于实施本文所描述的组创建功能的多个模块。尽管在大容量存储装置808中示出为代码块，但是可以理解，任何模块都可以完全或部分地用例如内置在专用集成电路(ASIC)中的硬连线电路替换。大容量存储装置808可以包括装置注册器3202，用于通过到第二网络的门户将装置注册到第一网络，其中，第二网络被授权访问第一网络。装置可以执行到第二网络中的钱包的支付交换。

[0258] 大容量存储装置808可以包括装置加入器3204，用于通过同意许可指南的义务将装置加入到许可指南。大容量存储装置808可以包括令牌请求器3206，用于使用许可指南的功能来请求令牌，所述令牌将装置标识为经认证的以访问第二网络。在示例中，对令牌的请求可以导致在计费区块链上预留硬币以对应于在侧链上生成的令牌。响应于检测到令牌是由侧链撤销和消费的至少一个，可以释放区块链的硬币。在示例中，加入许可指南可以包括针对属性过滤器从装置提供装置的属性给许可指南，以验证在第一网络中允许所述装置的属性。属性可以包括在装置加入许可指南时有效用户简档的属性。响应于被用作装置的授权形式，令牌可以自行销毁。

[0259] 大容量存储装置808可以包括请求发送器3208，用于从装置向第一网络发送认证请求，其中，响应于检测到令牌，第一网络确认所述认证。响应于通过装置将令牌呈现给第一网络来对装置进行认证，可以在侧链上消费令牌。基于向第一网络认证装置具有用于访问第二网络的凭证，所述装置可以被授权访问第一网络。在示例中，基于访问次数、通过第一网络访问的数据量、和授予访问时间中的至少一个，装置使用第一网络的授权可能到期。

[0260] 图33是根据一些实施例的包括用于利用IoT装置进行分散式授权、认证、和计费的代码的非暂态机器可读介质3300的框图。类似编号的项如关于图9所描述的项那样。

[0261] 非暂态机器可读介质3300可以包括代码3302，用于引导处理器902通过到第二网络的门户将装置注册到第一网络，其中，第二网络被授权访问第一网络。装置可以执行到第二网络中的钱包的支付交换。

[0262] 非暂态机器可读介质3300可以包括代码3304，用于引导处理器902通过同意许可指南的义务来将装置加入到许可指南。非暂态机器可读介质3300可以包括代码3306，用于引导处理器902使用许可指南的功能来请求令牌，所述令牌将装置标识为经认证的以访问第二网络。在示例中，对令牌的请求可以导致在计费区块链上预留硬币以对应于在侧链上生成的令牌。响应于检测到令牌是由侧链撤销和消费的至少一个，可以释放区块链的硬币。在示例中，加入许可指南可以包括针对属性过滤器从装置提供装置的属性给许可指南，以

验证在第一网络中允许所述装置的属性。属性可以包括在装置加入许可指南时有效用户简档的属性。响应于被用作装置的授权形式，令牌可以自行销毁。

[0263] 非暂态机器可读介质3300可以包括代码3308，用于引导处理器902从装置向第一网络发送认证请求，其中，响应于检测到令牌，第一网络确认所述认证。响应于通过装置将令牌呈现给第一网络来对装置进行认证，可以在侧链上消费令牌。基于向第一网络认证装置具有用于访问第二网络的凭证，所述装置可以被授权访问第一网络。在示例中，基于访问次数、通过第一网络访问的数据量、和授予访问时间中的至少一个，装置使用第一网络的授权可能到期。

[0264] 本技术的一些实施例公开了使用例如远程认证拨入用户服务(RADIUS)和/或DIAMETER协议等在IoT装置上进行分散式授权、认证、和计费。分散式代理可以位于RADIUS服务器、DIAMETER服务器、或运行DIAMETER协议的RADIUS服务器前方。分散式API可以内置在RADIUS服务和/或DIAMETER服务中。在区块链类型加密机制中可以将现有调用包装到RADIUS服务和/或DIAMETER服务中。区块链类型加密机制可以用作请求源的证据层，以例如使请求能够通过以供RADIUS服务器和/或DIAMETER服务器进行处理。

[0265] 图34是根据一些实施例的用于使用远程认证拨入用户服务(RADIUS)和/或DIAMETER协议在IoT装置上进行分散式授权、认证、和计费的技术3400的示意图。可以锁定RADIUS服务器3402以防止修改，而分散式RADIUS代理3404可以是增强功能。分散式RADIUS代理3404可以在消息到达传统RADIUS服务器之前采取动作。分散式API 3406可被插入在RADIUS服务器3402与后端数据库3408之间并且可以包括对RADIUS服务操作的修改。

[0266] 当RADIUS服务器3402实施后端数据库3408时，分散式RADIUS代理3404可以起作用。在示例中，数据库3408可以是文件，或者其可以使用多个支持的数据存储装置中的任何一个。在分散式RADIUS代理3404中，服务可以位于RADIUS服务器3402的前方并且充当分散式过滤器。分散式RADIUS代理3404可以通过使用分散式机制确认请求方的身份来提供安全检查。

[0267] 可以修改RADIUS服务器3402使用的调用以通过分散式API3406路由所述调用。分散式API 3406可以作为一组类并入RADIUS服务器代码库中，所述一组类支持将RADIUS功能路由到区块链。RADIUS服务器3406可以成为区块链客户端并执行身份和事务有效性检查。替代性地或另外地，可以将身份和有效性检查实施为RADIUS服务器被修改以支持的外部服务。利用分散式API，可以修改RADIUS服务器代码，使得操作可以启用身份和有效性检查功能。以下描述用于执行有效性检查的示例性机制。

[0268] 图35是根据一些实施例的图34的组件通过分散式RADIUS代理3404起作用以用于在IoT装置上进行授权、认证、和计费的示例方法3500的梯形图。图35的方法3500可以由关于图38所描述的IoT装置3800来实施。类似编号的项如关于图34所公开的那样。

[0269] 分散式RADIUS代理3404可以处理来自RADIUS客户端3504的RADIUS认证请求3502。可以修改RADIUS客户端3504以使用来自RADIUS客户端区块链的私钥或来自分布式分类账3506身份的私钥来对RADIUS请求进行签名。身份可以用于校验请求源的身份3508，以及所述请求是否可以实际上是对应于区块链或分布式分类账3506上的身份的私钥持有者。在区块链或分布式分类账3506上的身份可以是先前使用许可指南已经建立的，如先前部分所描述的那样。例如，身份可以已经注册了服务、加入了许可指南、并且可以被列为所述合约中

的参与实体，或者所述身份也可以是令牌持有者。身份校验可以在运行时完成，其中，区块链或分布式分类账3506可以在第一次看到由新身份签名的认证请求时接受请求的身份。身份校验响应3510可以返回到分散式代理3404。响应于身份被校验为可接受，分散式代理3404可以请求3512适当的RADIUS服务器。作为响应，RADIUS服务器3402可以响应3514所述请求被批准为成功或被拒绝为失败。

[0270] 成功的身份校验可以链接多个身份，使得来自同一用户的未来RADIUS请求可以被正确的私钥签名，其中，可以拒绝不包括私钥的请求。身份可以呈现具有RADIUS请求的令牌，并通过将对区块链或分类账的校验与所述身份的验证进行比较来响应。如前，验证可以指示作为有效令牌持有者的请求，并且不成功的验证仍然可以通过被列为具体许可指南的成员来校验身份。验证可以指示针对RADIUS请求区块链上的货币何时被花费。例如，为了发出RADIUS请求，身份可以在区块链上具有一些信用和硬币用于花费。

[0271] 图36是根据一些实施例的图34的组件通过分散式API 3406起作用以用于IoT装置上进行授权、认证、和计费的示例方法3600的梯形图。图36的方法3600可以由关于图38所描述的IoT装置3800来实施。类似编号的项如关于图34和图35所公开的那样。

[0272] 调用序列与关于图35的调用序列不同，因为所述调用尽管实质上类似但可以寻址不同的行为者。例如，在图36中，经签名授权请求3602可以是从RADIUS客户端3504到RADIUS服务器3402。身份校验3604可以是从RADIUS服务器3402到分散式API 3406。身份请求3606的第二校验可以从分散式API 3406发送到分布式分类账3506。作为响应，分布式分类账3506可以向分散式API 3406返回身份响应3608，指示身份校验是成功还是失败。作为响应，分散式API 3406可以向RADIUS服务器3402返回第二身份响应3610，指示身份校验是成功还是失败。RADIUS服务器3402可以向RADIUS客户端3504返回RADIUS服务器请求-响应。这些动作的结果可以是验证RADIUS请求源的身份，其中，验证可以例如在可以处理验证请求之前通过区块链或分散式分类账而得以通过。

[0273] 图37是根据一些实施例的用于在IoT装置上进行分散式授权、认证、和计费的动作图3700的示意图。授权请求3702与利用区块链3706的事务验证检查器3704交互。

[0274] 在授权请求3702内，在框3708处，可以将事务内容添加到消息中。在图37示出的示例中，事务内容可以是用户名和密码，例如，“Mike”的用户名和凭证。如下所描述的，敏感信息不会通过此方法暴露给第三方。事务可以包括元数据。元数据可以存储在公共分类账中。如果钱币或加密货币面额是事务的一部分，那么事务内容可以包括事务多少价值的细节。事务的有效性可以取决于满足事务的条件。例如，满足事务的条件可以包括以上所描述示例中的支付动作和认证动作。

[0275] 在授权请求3702内，在框3710处，被请求的网络地址可以包括在事务内容中。代替网络地址，所请求的资源可以包括在事务内容中。例如，网络地址可以是RADIUS服务器的完全限定域名(FDQN)或互联网协议(IP)地址。网络地址可以是网络上的资源。网络地址可以包括基于RADIUS服务器或网络资源所有方的私钥的钱包地址。响应于为了使用服务而请求的支付可以被执行，网络地址可以包括钱包。

[0276] 在授权请求3702内，在框3712处，可以通过所述方的私钥对事务内容进行签名。对事务内容进行签名的过程可以包括形成签名3714，可以包括对公钥的位置3716的引用，或者事务可以包含公钥本身并且将公钥3718提供给授权请求3702本身。

[0277] 在事务验证检查器3704内，可以进行校验公钥3720的请求。公钥的位置可以被查找3722、或者从区块链3706被请求。网络所有方可以创建区块链3706，并且实体可以通过将实体的公钥发布到区块链3706来在区块链3706上购买或获取身份。在协商期间将实体的公钥发布到区块链3706可以交换加密货币、令牌、或其他支付。支付金额可以确定密钥可以在区块链3706中保持多长时间。密钥可以由区块链3706无限期地保持或持续指定的时间段。可以由网络管理员调整建立或确认身份的条件。

[0278] 区块链3706可包括多个块3724。用于存储身份的区块链3706可以是位于具有相当多挖掘器的更大区块链顶部的虚拟区块链。例如，区块链可以并入双重挖掘的概念，其中，在一个区块链3706中为证据所做的工作也用作另一个区块链中的证据。例如，可以使用以上公开的布隆过滤器跳转方法(hop method)来执行查找3722。查找3722的结果可以是公钥已知。查找3722的结果可以是密钥被包括在要开始的事务中。

[0279] 在事务验证检查器3704内，在框3726处，密钥可以解密事务并且可以确认所标识的实体。在非对称密钥的情况下，密钥可以是公共的，或者在对称密钥的情况下，密钥可以是私有的。消息通信将通常使用私有对称密钥进行加密/解密。可以将事务提交给区块链3706。事务可以是对链外存储机制的引用。可在框3726处使用链外存储机制来记录标识校验步骤的结果。记录标识校验步骤的结果可以提供计费。例如，记录可以提交给网络提供商的区块链3706和/或给虚拟区块链。在某些情况下，区块链3706上的记录可以限于关于事务的元数据。在某些情况下，与用户名和密码有关的信息可能被禁止包含在区块链3706中。如果所述信息包括在区块链3706中，则所述信息可以是RADIUS代理和/或修改的RADIUS服务器之间的事务的一部分。

[0280] 在事务验证检查器3704内，可以在框3728处发生链外事件，其中，如果事务身份有效，则可以将事务的内容传递到RADIUS服务器以进行正常处理。在认证请求的情况下，内容可以例如包括用户名和密码。内容到服务器的传递可能发生在RADIUS服务器与其代理或在RADIUS代理中修改的分散式代码之间。

[0281] 在事务验证检查器3704内，可以在框3730处发生链外事件，其中，来自RADIUS服务器的响应可以被直接路由回至客户端。响应的路由可以通过代理和/或RADIUS服务器，部分取决于实施架构选择。RADIUS服务器可以对RADIUS服务器接收的请求执行记录和计费。

[0282] 在事务验证检查器3704内，在框3732处，响应可以被路由返回。响应可以是肯定的或否定的。响应可以作为不可变记录存储到区块链3706中。在区块链3706上存储响应可以增加恶意行为者隐藏其动作的难度。

[0283] 图38是根据一些实施例的可以存在于IoT装置3800中用于利用IoT装置进行分散式授权、认证、和计费的组件的示例的框图。类似编号的项如关于图3和图8所描述的那样。可以注意到，可以选择不同的组件并将其用于IoT装置3800，而不是被选择用于关于图8所讨论的IoT装置800以及本文所讨论的其他IoT装置的那些组件。

[0284] 大容量存储装置808可以包括多个模块，以利用IoT装置实施分散式授权、认证、和计费。尽管在大容量存储装置808中示出为代码块，但是可以理解，任何模块都可以完全或部分地使用例如内置到专用集成电路(ASIC)中的硬连线电路代替。

[0285] 大容量存储装置808可以包括身份校验器3802，用于使用分散式API来校验认证请求的身份，所述认证请求是从RADIUS客户端接收的，所述分散式API用于响应从分布式分类

账接收身份校验响应而通过向分布式分类账发送请求并返回响应到RADIUS服务器来校验身份。响应于经认证身份的响应,RADIUS客户端可以进行事务。所述事务可以包括用户名、密码、和元数据中的至少一个。所述事务可以包括价值事务。所述事务可以是加密货币事务。认证请求可以包括对网络地址的请求。网络地址可以包括RADIUS服务器的完全限定域名或RADIUS服务器的互联网协议地址中的至少一个。RADIUS服务器可以通过从区块链请求公钥的位置来校验公钥。响应于RADIUS客户端接收到对经认证身份的确认,对RADIUS服务器的请求可以发生在链外。RADIUS服务器可以对RADIUS服务器接收的请求执行记录和计费。对认证请求的响应可以作为不可变记录存储在区块链中。

[0286] 响应于从分散式API接收响应,大容量存储装置808可以包括响应返回器3804,用于向RADIUS客户端返回对认证请求的响应。响应于从分布式分类账接收到肯定身份校验响应,大容量存储装置808可以包括请求发送器3806,用于向RADIUS服务器发送请求。

[0287] 图39是根据一些实施例的包括用于引导处理器902利用IoT装置进行分散式授权、认证、和计费的代码的非暂态机器可读介质3900的框图。处理器902可以通过总线904访问非暂态机器可读介质3900。处理器902和总线904可以以与关于图9所描述的处理器902和总线904类似的方式来实施。非暂态机器可读介质3900可以包括针对图8的大容量存储装置808描述的装置,或者可以包括光盘、拇指驱动器、或任何数量的其他硬件装置。

[0288] 非暂态机器可读介质3900可以包括代码3902,用于引导处理器902利用分布式分类账校验认证请求的身份,所述认证请求是从远程认证拨入用户服务(RADIUS)客户端接收的。响应于经认证身份的响应,RADIUS客户端可以进行事务。所述事务可以包括用户名、密码、和元数据中的至少一个。所述事务可以包括价值事务。所述事务可以是加密货币事务。认证请求可以包括对网络地址的请求。网络地址可以包括RADIUS服务器的完全限定域名或RADIUS服务器的互联网协议地址中的至少一个。RADIUS服务器可以通过从区块链请求公钥的位置来校验公钥。响应于RADIUS客户端接收到对经认证身份的确认,对RADIUS服务器的请求可以发生在链外。RADIUS服务器可以对RADIUS服务器接收的请求执行记录和计费。对认证请求的响应可以作为不可变记录存储在区块链中。

[0289] 非暂态机器可读介质3900可以包括代码3904,用于引导处理器902响应于从分布式分类账接收到肯定身份校验响应而向RADIUS服务器发送请求。非暂态机器可读介质3900可以包括代码3906,用于引导处理器902响应于从RADIUS服务器接收响应而向RADIUS客户端返回对认证请求的响应。

[0290] 在一些实施例中,本文的技术公开了IoT对象中的访问控制。在IoT系统中,由于所涉及装置的受限性质,安全性变得复杂,这可能无法实施在诸如台式机、膝上型计算机或智能电话等受限较少装置中使用的安全系统。实施使用较不复杂参数的访问控制可以增强安全环境中IoT应用的安全实施,并改善IoT系统的操作和采用。

[0291] 在IoT系统设计中,对象可以指操作单元的数据模型描述和物理实例化。可以在交互以实现目标或结果的多个对象方面来描述IoT系统。对象可以由多个操作层组成,在这个意义上,对象的定义可以是递归的。对象分解方法(诸如自检)可以解析其叶节点属性的递归。在一些情况下,可以根据具有至少六个层的分层分解来理解IoT对象访问,并且在其他情况下,可以使用更多或更少的层。

[0292] 图40是根据一些实施例的用于IoT对象中的访问控制的逻辑划分4000的示意图。

在示例中，用于访问控制的逻辑划分可以示出调用程序的授权可以伴随访问请求。可以在访问控制列表(ACL)结构4002内限定调用程序授权，其标识调用程序对象4004和目标对象4006。ACL结构4002可以示出创建、读取、更新、删除和通知(CRUDN)许可4008可以应用于分层分解中的任何层。ACL调用程序对象4004和ACL目标对象4006可以是具有相同对象引用类型的结构，因此在分别根据分层模型指定调用程序对象4004和目标对象4006粒度的范围时可以具有完全的灵活性。在每个粒度层，CRUDN策略4008可能是有意义的。

[0293] 可以向调用程序对象4004下发具有授权结构的凭证，所述授权结构定义调用程序正进行请求的特权。可以根据以上的分层结构来定义特权。可以在授权部分中指定发起请求的平台、装置、集合、资源、记录或性质。

[0294] 图41是根据一些实施例的用于IoT对象中的访问控制的调用程序凭证4102与请求4104之间的逻辑划分4100的示意图。调用程序的授权4106可伴随访问请求和产生的许可4108。要访问的对象可能受到对象物理性对对象的固有限制的约束。例如，只读存储装置(ROM)可能没有许可写操作的物理性。可以使用CRUDN来表达物理性。预期的访问可能受到对象物理性的限制，因此访问请求可能期望所请求的许可由物理性支配。预期访问可以是请求4104，包括对象4110和许可4112。如果不受对象物理性的限制，则对象的访问请求(如果已承兑)可以在某些情况下导致装置以未定义或不安全的方式运行。

[0295] 图42是根据一些实施例的在IoT对象中使用层4204进行访问控制的对象能力4202之间的逻辑划分4200的示意图。IoT对象访问的第一层可以是平台层4206。平台层可以包括计算机的物理实例，所述计算机包含计算、连网、存储、感测或致动能力。可以在平台标识符和凭证方面来理解平台访问控制。凭证可以例如在配置或实施期间由制造商嵌入、或存储在单元中，使得凭证可以用作证明凭证。如果访问请求可以是装置凭证发布的条件，则平台凭证可以在没有凭证的情况下在访问请求处进行校验。平台凭证可以用于重新证明平台性质，包括其物理性。

[0296] IoT对象访问的第二层可以是装置层4208。装置层可以包括计算机的逻辑实例，所述计算机包含计算、连网、存储、感测或致动能力。可以在装置标识符和凭证方面来理解装置访问控制。

[0297] IoT对象访问的第三层可以是集合层4210。集合层可以包括如下所公开的一个或多个资源的逻辑结构。可以在命名结构的类型标识符、接口定义和授权标识符方面来理解访问控制。

[0298] IoT对象访问的第四层可以是资源层4212。资源层可以包括如下所公开的一个或多个记录的逻辑结构。可以在命名结构的类型标识符、接口定义和授权标识符方面来理解访问控制。

[0299] IoT对象访问的第五层可以是记录层4214。记录层可以包括如下所公开的一个或多个性质的逻辑结构。可以在资源加上记录索引偏移方面来理解访问控制。

[0300] IoT对象访问的第六层可以是性质层4216。例如，性质层可以包括使用数据建模语言(DML)可定义的任何结构的原子数据结构和/或复杂数据结构。例如，原子数据结构可以包括字符串、数字和/或日期。DML可以提供元数据结构以捕获例如对可接受的数据格式、结构和数据值约束(诸如JSON模式)的限制。访问控制策略可以在创建、读取、更新、删除和通知(CRUDN)的数据结构生命周期方面来表达。“通知”可以进一步分为“观察”和“通知”，其

中，“观察”假定对结构改变事件具有读许可，并且“通知”假定对另一个对象具有写许可。

[0301] 访问控制列表(ACL)评估可以是校验支配调用程序部分和/或与调用程序部分重叠的调用程序对象的授权的过程。ACL评估可以是被访问的结构可以由目标部分支配和/或重叠的过程。除非目标部分中的完整层集与要访问的结构匹配，否则ACL可能在应用中受到限制。除非发现ACL匹配，否则可能会拒绝访问。

[0302] 图43是根据一些实施例的用于IoT对象中的访问控制的示例方法4300的处理流程图。图43的方法4300可以由关于图44所描述的IoT装置4400来实施。处理流程可以在框4302处开始。在框4302处，可以向调用程序实体下发凭证。例如，凭证可以包含六层授权结构，但是也可以取决于安全需求使用诸如四层等其他授权结构。在框4304处，可以向对象实体提供ACL。ACL可以指定对目标对象的六层引用以及CRUDN或CRUDON许可。在框4306处，调用程序可以通过合适的连接接口向对象呈现授权凭证。在框4308处，给定供应商凭证，访问执行引擎(AEE)可以应用ACL策略。

[0303] 在框4310处，可以判定凭证授权是否与调用程序重叠。如果否(即凭证授权不与调用程序重叠)，则处理流程行进至框4312，在此处可以拒绝访问。

[0304] 在框4314处，可以判定目标是否与请求重叠。如果否(即目标不与请求重叠)，则处理流程行进至框4312，在此处可以拒绝访问。

[0305] 在框4316处，可以将调用程序对象层标识的层与凭证对象层标识进行比较，以判定是否存在匹配。如果否(即调用程序对象层标识与凭证对象层标识不匹配)，则处理流程行进至框4312，在此处可以拒绝访问。调用程序对象层标识可以包括平台层、装置层、集合层、资源层、记录层和性质层。

[0306] 在框4318处，可以将目标对象层标识的层与请求对象层标识进行比较，以判定是否存在匹配。如果否(即目标对象层标识与请求对象层标识不匹配)，则处理流程行进至框4312，在此处可以拒绝访问。目标对象层标识可以包括平台层、装置层、集合层、资源层、记录层和性质层。如果以上判定是肯定的，则在框4320处，可以允许对IoT对象进行访问。

[0307] 图44是根据一些实施例的可以存在于IoT装置4400中用于IoT对象中的访问控制的组件的示例的框图。类似编号的项如关于图3和图8所描述的那样。可以注意到，可以选择不同的组件并将其用于IoT装置4400，而不是被选择用于关于图8所讨论的IoT装置800以及本文所讨论的其他IoT装置的那些组件。

[0308] 大容量存储装置808可以包括用于IoT对象中的访问控制的多个模块。尽管在大容量存储装置808中示出为代码块，但是可以理解，任何模块都可以完全或部分地使用例如内置到专用集成电路(ASIC)中的硬连线电路代替。

[0309] 大容量存储装置808可以包括用于将凭证下发至调用程序实体的凭证下发器4402，所述凭证包括多个授权结构层。凭证可以是六层许可。六层许可可以包括平台层、装置层、集合层、资源层、记录层和性质层。所述多个层可以包括平台层以反映计算机的物理实例，所述计算机包括计算、连网、存储、感测或致动能力中的至少一个。所述多个层可以包括装置层以反映计算机的逻辑实例，所述计算机包括计算、连网、存储、感测或致动能力中的至少一个。所述多个层可以包括资源的逻辑结构的集合层，其中，所述资源包括用于记录的逻辑结构，其中，所述记录包括性质的逻辑结构，并且其中，所述性质包括原子数据结构和复杂数据结构中的至少一个。所述性质可以是复杂数据结构，并且复杂数据结构用于使

用数据建模语言可定义的结构。所述性质可以包括原子数据结构，并且原子数据结构可以是字符串、数字或日期中的至少一个。凭证可以指示制造商的安装。

[0310] 大容量存储装置808可以包括对象实体提供器4404，用于向对象实体提供指定对目标对象的引用和许可的访问控制列表。大容量存储装置808可以包括凭证呈现器4406，用于向对象实体呈现授权凭证。对象实体的授权凭证可能受到基于创建、读取、更新、删除和通知(CRUDN)生命周期通知通过对象数据的物理性对对象施加的限制所限制。大容量存储装置808可以包括访问控制列表策略申请器4408，用于申请访问控制列表策略以基于对凭证是否与调用程序实体重叠、目标对象是否与请求重叠、多个装置层标识是否与多个凭证层标识匹配、并且多个目标层标识是否与多个请求层标识匹配的比较来判定是否允许对IoT装置进行访问。

[0311] 图45是根据一些实施例的包括用于引导处理器902在IoT对象中进行访问控制的代码的非暂态机器可读介质4500的框图。处理器902可以通过总线904访问非暂态机器可读介质4500。处理器902和总线904可以以与关于图9所描述的处理器902和总线904类似的方式来实施。非暂态机器可读介质19600可以包括针对图8的大容量存储装置808所描述的装置或者可以包括光盘、拇指驱动器或任何数量的其他硬件装置。

[0312] 非暂态机器可读介质4500可以包括代码4502，用于引导处理器902向调用程序实体下发凭证，所述凭证包括多个授权结构层。凭证可以是六层许可。六层许可可以包括平台层、装置层、集合层、资源层、记录层和性质层。所述多个层可以包括平台层以反映计算机的物理实例，所述计算机包括计算、连网、存储、感测或致动能力中的至少一个。所述多个层可以包括装置层以反映计算机的逻辑实例，所述计算机包括计算、连网、存储、感测或致动能力中的至少一个。所述多个层可以包括资源的逻辑结构的集合层，其中，所述资源包括用于记录的逻辑结构，其中，所述记录包括性质的逻辑结构，并且其中，所述性质包括原子数据结构和复杂数据结构中的至少一个。所述性质可以是复杂的数据结构，并且复杂数据结构可以用于使用数据建模语言可定义的结构。所述性质可以包括原子数据结构，并且原子数据结构可以是字符串、数字或日期中的至少一个。凭证可以指示制造商的安装。

[0313] 非暂态机器可读介质4500可以包括代码4504，用于引导处理器902向对象实体提供指定对目标对象的引用和许可的访问控制列表。非暂态机器可读介质4500可以包括代码4506，用于引导处理器902向对象实体呈现授权凭证。在某些情况下，对象实体的授权凭证可能受到基于创建、读取、更新、删除和通知(CRUDN)生命周期通知通过对象数据的物理性对对象施加的限制所限制。非暂态机器可读介质4500可以包括代码4508，用于引导处理器902申请访问控制列表策略以基于对凭证是否与调用程序实体重叠、目标对象是否与请求重叠、多个装置层标识是否与多个凭证层标识匹配、并且多个目标层标识是否与多个请求层标识匹配的比较来判定是否允许对IoT装置进行访问。

[0314] 示例1包括一种设备。所述设备包括复合对象，所述设备包括装置所有方、形成所述复合对象的多个子对象、以及记录形成所述复合对象的所述子对象的区块链，所述装置所有方还包括向形成所述复合对象的子对象提供名称的名称服务器、和形成所述复合对象的所述子对象的子对象列表。

[0315] 示例2包括如示例1所述的主题。在示例2中，子对象包括由较低级别子对象形成的复合对象。

[0316] 示例3包括如示例1或2中任一项所述的主题。在示例3中，子对象包括原子对象。

[0317] 示例4包括如示例1至3中任一项所述的主题。在示例4中，所述复合对象的名称包括根据所述多个子对象的名称计算的散列。

[0318] 示例5包括如示例1至4中任一项所述的主题。在示例5中，每个子对象包括组密钥，所述组密钥允许所述子对象代表所述组来起作用。

[0319] 示例6包括如示例1至5中任一项所述的主题。在示例6中，所述装置所有方包括EPID服务器。

[0320] 示例7包括如示例1至6中任一项所述的主题。在示例7中，所述装置所有方包括代理中介。

[0321] 示例8包括如示例1至7中任一项所述的主题。在示例8中，所述装置所有方包括区块链。

[0322] 示例9包括如示例1至8中任一项所述的主题。在示例9中，所述区块链包括对所述复合对象的记录。

[0323] 示例10包括一种用于在IoT网络中形成复合对象的方法。所述用于在IoT网络中形成复合对象的方法包括：在装置所有方中构建子对象列表；创建集合组标识符；在区块链事务中将所述集合组标识符提交给区块链；并且从所述名称服务器中的所述区块链获得组名称。

[0324] 示例11包括如示例10所述的主题。在示例11中，所述方法包括从所述区块链判定所述集合组标识符是否已经在使用中，并且如果是，则生成新的集合组标识符。

[0325] 示例12包括如示例10或11中任一项所述的主题。在示例12中，所述方法包括：从子对象接受加入请求；确认所述子对象是组成员；在所述区块链中查找所述子对象的名称；并且从所述名称服务器向所述子对象提供组密钥。

[0326] 示例13包括如示例10至12中任一项所述的主题。在示例13中，所述方法包括判定组成员身份是否是私密的，并且如果是，则从充当所述名称服务器的代理的所述装置所有方向所述子对象提供组密钥。

[0327] 示例14包括如示例10至13中任一项所述的主题。在示例14中，所述方法包括：通过组合所述子对象的名称以形成组合并且计算所述组合的散列码来创建所述集合组标识符。

[0328] 示例15包括如示例10至14中任一项所述的主题。在示例15中，所述方法包括：通过组合形成所述子对象的所有子子对象的名称以形成组合并且计算所述组合的散列码来为子代码创建名称。

[0329] 示例16包括如示例10至15中任一项所述的主题。在示例16中，所述方法包括：确认区块链事务在网状网络中的一组装置中是有效的；并且如果无效，则反转所述区块链事务。

[0330] 示例17包括一种非暂态机器可读介质。所述非暂态机器可读介质包括用于引导处理器进行以下操作的指令：存储组的子对象列表；计算所述组的集合组身份；并且向所述组中的子对象提供组身份凭证。

[0331] 示例18包括如示例17中任一项所述的主题。在示例18中，所述非暂态机器可读介质包括用于引导所述处理器充当子对象的代理服务器的指令。

[0332] 示例19包括如示例17或18中任一项所述的主题。在示例19中，所述非暂态机器可读介质包括用于引导所述处理器进行以下操作的指令：将包括集合组身份的事务提交给区

块链;并且将所述区块链迁移到网中的其他装置。

[0333] 示例20包括如示例17至19中任一项所述的主题,包括包含20的事务块的区块链。在示例20中,事务块包括集合组身份。

[0334] 示例21包括一种包括复合对象的设备。所述设备包括:装置所有方,所述装置所有方包括类型名称服务器,用于为所述复合对象创建类型名称;以及区块链,所述区块链包括包含形成所述复合对象的子对象类型的事务。

[0335] 示例22包括如示例21所述的主题。在示例22中,所述设备包括用于确定包括所述复合对象的子对象的类型的类型检查器。

[0336] 示例23包括如示例21和22中任一项所述的主题。在示例23中,所述类型检查器包括类型自检系统。

[0337] 示例24包括如示例21至23中任一项所述的主题。在示例24中,所述类型检查器包括类型证明系统。

[0338] 示例25包括如示例21至24中任一项所述的主题。在示例25中,所述设备包括用于生成形成所述子对象的子子对象的类型的类型图的类型图生成器。

[0339] 示例26包括如示例21至25中任一项所述的主题。在示例26中,所述设备包括用于根据类型图来生成类型名称的类型名称计算器。

[0340] 示例27包括如示例21至26中任一项所述的主题。在示例27中,所述事务包括类型图。

[0341] 示例28包括如示例21至27中任一项所述的主题。在示例28中,对象包括类型凭证。

[0342] 示例29包括如示例21至28中任一项所述的主题。在示例29中,类型凭证包括制造商密钥。

[0343] 示例30包括如示例21至29中任一项所述的主题。在示例30中,所述类型凭证由名称服务器提供。

[0344] 示例31包括如示例21至30中任一项所述的主题。在示例31中,子对象包括子子对象,并且所述子对象的类型名称根据所述子子对象的类型确定。

[0345] 示例32包括如示例21至31中任一项所述的主题。在示例32中,所述设备包括由子对象生成的类型图,所述类型图包括所述子子对象的类型。

[0346] 示例33包括一种用于在IoT网络中创建对象类型的方法。所述用于在IoT网络中创建对象类型的方法包括:请求通过名称服务器来创建类型组;执行组成复合对象的子对象的类型检查以构建形成所述复合对象的对象的类型图;根据所述类型图来计算类型组名称;并且访问区块链以判定类型组名称是否已经被创建。

[0347] 示例34包括如示例33所述的主题。在示例34中,所述方法包括通过将包括所述类型图的事务写入所述区块链来创建所述类型组名称。

[0348] 示例35包括如示例33或34中任一项所述的主题。在示例35中,所述方法包括从所述名称服务器向所述复合对象下发EPID加入请求。

[0349] 示例36包括如示例33至35中任一项所述的主题。在示例36中,所述方法包括向形成所述复合对象的所述子对象下发类型凭证。

[0350] 示例37包括如示例33至36中任一项所述的主题。在示例37中,所述名称服务器请求所述复合对象执行所述类型检查。

[0351] 示例38包括如示例33至37中任一项所述的主题。在示例38中，所述类型检查包括对形成所述复合对象的所述子对象进行的递归自检。

[0352] 示例39包括如示例33至38中任一项所述的主题。在示例39中，所述递归自检包括：向形成所述复合对象的所述子对象中的每一个发送类型自检请求；执行类型自检以确定形成所述子对象的每个子子对象的类型；在由子子对象形成的所述子对象中的每一个上构建类型图；将所述类型图返回至所述复合对象；并且校验所述类型图上的签名。

[0353] 示例40包括如示例33至39中任一项所述的主题。在示例40中，所述方法包括：从每个子子对象到层级结构中的更低级别的对象执行递归类型自检；为所述层级结构的每一个级别处的对象构建类型图；并且将所述类型图返回到所述层级结构的下一个更高级别。

[0354] 示例41包括如示例33至40中任一项所述的主题。在示例41中，所述类型检查包括对形成所述复合对象的所述子对象执行递归证明。

[0355] 示例42包括如示例33至41中任一项所述的主题。在示例42中，所述递归证明包括：从每一级别向在下一更低级别处的对象发送类型证明请求；将在层级结构的具体级别处组成所述对象的所有对象的类型图返回到下一更高级别；并且在所述复合对象中构建整体类型图。

[0356] 示例43包括一种非暂态机器可读介质。所述非暂态机器可读介质包括用于引导处理器进行以下操作的指令：构建形成复合对象的对象的类型图；计算所述复合对象的类型名称；并且将所述类型名称和类型图记录在区块链中。

[0357] 示例44包括如示例43所述的主题。在示例44中，所述非暂态机器可读介质包括用于引导所述处理器对形成所述复合对象的所述对象执行递归类型自检的指令。

[0358] 示例45包括如示例43或44中任一项所述的主题。在示例45中，所述非暂态机器可读介质包括用于引导所述处理器对形成所述复合对象的所述对象执行递归类型证明的指令。

[0359] 示例46包括如示例43至45中任一项所述的主题。在示例46中，所述非暂态机器可读介质包括用于引导所述处理器在所述类型名称不存在于所述区块链中的情况下创建所述类型名称的指令。

[0360] 示例47包括如示例43至46中任一项所述的主题。在示例47中，所述非暂态机器可读介质包括向具有类型凭证的子对象发送EPID加入请求。

[0361] 示例48包括一种设备。所述设备包括联盟小组，包括：用于向形成所述联盟小组的对象提供名称的联盟小组名称服务器、属于所述联盟小组的所述对象的联盟小组成员列表、以及记录形成所述联盟小组的所述对象的名称的区块链。

[0362] 示例49包括如示例48所述的主题。在示例49中，所述设备包括用于广播联盟小组存在的发布方。

[0363] 示例50包括如示例48或49中任一项所述的主题。在示例50中，所述设备包括用于确认从对象接收的身份凭证的凭证校验器。

[0364] 示例51包括如示例48至50中任一项所述的主题。在示例51中，所述设备包括用于向对象提供加入所述联盟小组的凭证的EPID服务器。

[0365] 示例52包括如示例48至51中任一项所述的主题。在示例52中，所述设备包括：装置所有方，所述装置所有方用于校验来自对象的身份凭证并且将联盟小组凭证提供给所述对

象;以及多个对象,所述多个对象各自具有指示所述联盟小组中的成员身份的联盟小组凭证。

[0366] 示例53包括如示例48至52中任一项所述的主题。在示例53中,在所述联盟小组中的对象通过位置来分组。

[0367] 示例54包括如示例48至53中任一项所述的主题。在示例54中,在所述联盟小组中的对象通过功能来分组。

[0368] 示例55包括一种用于在IoT网络中形成联盟小组的方法。所述用于在IoT网络中形成联盟小组的方法包括:定义联盟小组;接收来自对象的加入所述联盟小组的请求;并且向所述对象下发联盟小组凭证。

[0369] 示例56包括如示例55所述的主题。在示例56中,定义所述联盟小组包括通过位置对装置进行分组。

[0370] 示例57包括如示例55或56中任一项所述的主题。在示例57中,定义所述联盟小组包括通过功能对装置进行分组。

[0371] 示例58包括如示例55至57中任一项所述的主题。在示例58中,所述方法包括如果所述联盟小组是不可发现的则向区块链发布所述联盟小组。

[0372] 示例59包括如示例55至58中任一项所述的主题。在示例59中,所述方法包括在下发所述联盟小组凭证之前校验所述请求。

[0373] 示例60包括如示例59至59中任一项所述的主题。在示例60中,所述方法包括通过确认所述请求包括有效的身份凭证来校验所述请求。

[0374] 示例61包括如示例59至60中任一项所述的主题。在示例61中,所述方法包括通过确认所述请求包括有效的实例凭证来校验所述请求。

[0375] 示例62包括如示例59至61中任一项所述的主题。在示例62中,所述方法包括通过确认所述请求包括有效的类型凭证来校验所述请求。

[0376] 示例63包括一种非暂态机器可读介质。所述非暂态机器可读介质包括用于引导处理器进行以下操作的指令:定义联盟小组;向区块链发布所述联盟小组;并且从对象接受加入请求。

[0377] 示例64包括如示例63所述的主题。在示例64中,所述非暂态机器可读介质包括用于引导所述处理器确认所述联盟小组是可发现的指令。

[0378] 示例65包括如示例63或64中任一项所述的主题。在示例65中,所述非暂态机器可读介质包括用于引导所述处理器确认来自所述对象的所述加入请求是否有效的指令。

[0379] 示例66包括如示例63至65中任一项所述的主题。在示例66中,所述非暂态机器可读介质包括用于引导所述处理器响应于有效加入请求来下发凭证的指令。

[0380] 示例67包括如示例63至66中任一项所述的主题。在示例67中,所述非暂态机器可读介质包括用于引导所述处理器生成EPID凭证的指令。

[0381] 示例68包括一种用于在物联网(IoT)网络中使用的设备。所述用于在物联网(IoT)网络中使用的设备包括为多个已发现对等机起草许可指南的许可指南起草器,其中,所述多个已发现对等机各自具有参数,并且其中,响应于可由所述多个已发现对等机中的至少两个允许的条款而生成所述许可指南的条款。所述多个已发现对等机中的每个可发现对等机的所述参数包括相关联对等机的可允许条款范围的范围,并且所述动作执行器用于响应

于检测到满足所述条款的条件而执行所述许可指南的动作。

[0382] 示例69包括如示例68所述的主题。在示例69中，所述许可指南起草器包括用于列出所述多个已发现对等机的所述条款和条件的功能。

[0383] 示例70包括如示例68或69中任一项所述的主题。在示例70中，所述许可指南起草器包括所述多个已发现对等机的所述服务质量条款和条件的列表。

[0384] 示例71包括如示例68至70中任一项所述的主题。在示例71中，所述许可指南起草器包括所述多个已发现对等机的数据平面条款和条件的列表。

[0385] 示例72包括如示例68至71中任一项所述的主题。在示例72中，所述数据平面用于指示对等机如何提供和消耗所述数据的过程。

[0386] 示例73包括如示例68至72中任一项所述的主题。在示例73中，所述许可指南包括生存时间。

[0387] 示例74包括如示例68至73中任一项所述的主题。在示例74中，所述许可指南包括用于管理对等机加入和退出所述许可指南的协议转换中介。

[0388] 示例75包括如示例68至74中任一项所述的主题。在示例75中，执行所述许可指南的动作包括向对等机自动委托服务从而指导所述对等机处理数据。

[0389] 示例76包括如示例68至75中任一项所述的主题。在示例76中，所述许可指南包括用于管理所述多个已发现对等机之间的配置的所述交换的前导码。

[0390] 示例77包括如示例68至76中任一项所述的主题。在示例77中，所述条款是指在所述多个已发现对等机之间要支付的支付率，并且在检测到所述多个已发现对等机中的一个对等机正在终止参与许可指南时，在对等机之间进行最终支付。

[0391] 示例78包括一种用于在物联网(IoT)装置中进行任务定义和委托的方法。所述用于在物联网(IoT)装置中进行任务定义和委托的方法包括：为多个已发现对等机起草许可指南，其中，所述多个已发现对等机各自具有参数，并且其中，响应于可由所述多个已发现对等机中的至少两个允许的条款而生成所述许可指南的条款；并且响应于检测到满足所述条款的条件而执行所述许可指南的动作。

[0392] 示例79包括如示例78所述的主题。在示例79中，所述起草所述许可指南包括用于列出所述多个已发现对等机的所述条款和条件的功能。

[0393] 示例80包括如示例78至79中任一项所述的主题。在示例80中，所述起草所述许可指南包括列出所述多个已发现对等机的所述服务质量条款和条件。

[0394] 示例81包括如示例78至80中任一项所述的主题。在示例81中，所述起草所述许可指南包括列出所述多个已发现对等机的数据平面条款和条件。

[0395] 示例82包括如示例78至81中任一项所述的主题。在示例82中，所述数据平面用于指示对等机如何提供和消耗所述数据的过程。

[0396] 示例83包括如示例78至82中任一项所述的主题。在示例83中，所述许可指南包括生存时间。

[0397] 示例84包括如示例78至83中任一项所述的主题。在示例84中，所述许可指南包括用于管理对等机加入和退出所述许可指南的协议转换中介。

[0398] 示例85包括如示例78至84中任一项所述的主题。在示例85中，执行所述许可指南的动作包括向对等机自动委托服务从而指导所述对等机处理数据。

[0399] 示例86包括如示例78至85中任一项所述的主题。在示例86中，所述许可指南包括用于管理所述多个已发现对等机之间的配置的所述交换的前导码。

[0400] 示例87包括如示例78至86中任一项所述的主题。在示例87中，所述条款是指在所述多个已发现对等机之间要支付的支付率，并且在检测到所述多个已发现对等机中的一个对等机正在终止参与许可指南时，在对等机之间进行最终支付。

[0401] 示例88包括一种非暂态机器可读介质。所述非暂态机器可读介质包括指令，所述指令当被执行时引导处理器：为多个已发现对等机起草许可指南，其中，所述多个已发现对等机各自具有参数，并且其中，响应于可由所述多个已发现对等机中的至少两个允许的条款而生成所述许可指南的条款；并且响应于检测到满足所述条款的条件而执行所述许可指南的动作。

[0402] 示例89包括如示例88所述的主题。在示例89中，所述起草所述许可指南包括用于列出所述多个已发现对等机的所述条款和条件的功能。

[0403] 示例90包括如示例88或89中任一项所述的主题。在示例90中，所述起草所述许可指南包括列出所述多个已发现对等机的所述服务质量条款和条件。

[0404] 示例91包括如示例88至90中任一项所述的主题。在示例91中，所述起草所述许可指南包括列出所述多个已发现对等机的数据平面条款和条件。

[0405] 示例92包括如示例88至91中任一项所述的主题。在示例92中，所述数据平面用于指示对等机如何提供和消耗所述数据的过程。

[0406] 示例93包括如示例88至92中任一项所述的主题。在示例93中，所述许可指南包括生存时间。

[0407] 示例94包括如示例88至93中任一项所述的主题。在示例94中，所述许可指南包括用于管理对等机加入和退出所述许可指南的协议转换中介。

[0408] 示例95包括如示例88至94中任一项所述的主题。在示例95中，执行所述许可指南的动作包括向对等机自动委托服务从而指导所述对等机处理数据。

[0409] 示例96包括如示例88至95中任一项所述的主题。在示例96中，所述许可指南包括用于管理所述多个已发现对等机之间的配置的所述交换的前导码。

[0410] 示例97包括如示例88至96中任一项所述的主题。在示例97中，所述条款是指在所述多个已发现对等机之间要支付的支付率，并且在检测到所述多个已发现对等机中的一个对等机正在终止参与许可指南时，在对等机之间进行最终支付。

[0411] 示例98包括一种用于在物联网(IoT)网络中使用的设备。所述用于在物联网(IoT)网络中使用的设备包括：设备身份生成器，用于为作为区块链客户端的装置生成装置身份；消息发布方，用于从所述装置发布发现广播消息；网络申请器，用于响应于所述装置基于所述所发布的发现广播消息从分散式网络访问代理(DNAP)中接收响应而从所述装置申请加入DNAP网络；装置描述器，用于向所述DNAP描述所述装置的所述身份和属性；以及分组发送器，用于响应于由所述网络基于所述装置的所述身份和属性而授予所述装置的访问权来通过所述网络从所述装置发送分组。

[0412] 示例99包括如示例98所述的主题。在示例99中，所述装置从所述DNAP中请求令牌。

[0413] 示例100包括如示例98或99中任一项所述的主题。在示例100中，令牌授予所述装置除了对等之外发送和接收网络数据的能力。

[0414] 示例101包括如示例98至100中任一项所述的主题。在示例101中，令牌授予所述装置在网络的开放系统互连层中的层上发送和接收数据的能力。

[0415] 示例102包括如示例98至101中任一项所述的主题。在示例102中，所述分组附带令牌，并且将所述分组和所述令牌的所述组合发送至DNAP以进行校验，其中，响应于检测到所述令牌未被所述DNAP接受，所述DNAP拒绝所述分组和所述令牌两者。

[0416] 示例103包括如示例98至102中任一项所述的主题。在示例103中，所述令牌可以针对与阈值分组数量、阈值数据量、或阈值时间段中的至少一个的使用为有效的。

[0417] 示例104包括如示例98至103中任一项所述的主题。在示例104中，所述装置存储由所述装置接收和发送的事务的事务记录，所述事务记录将与所述DNAP共享。

[0418] 示例105包括如示例98至104中任一项所述的主题。在示例105中，所述装置生成密钥，以指示从所述装置发送的分组的起源。

[0419] 示例106包括如示例98至105中任一项所述的主题。在示例106中，所述装置是区块链启用装置，并且所述装置将由所述装置发送以及由所述装置接收的所有事务存储在所述区块链上。

[0420] 示例107包括如示例98至106中任一项所述的主题。在示例107中，对所述装置属性的描述被存储在区块链外。

[0421] 示例108包括一种用于与物联网(IoT)装置进行安全通信的方法。所述用于与物联网(IoT)装置进行安全通信的方法包括：为作为区块链客户端的装置生成装置身份；从所述装置发布发现广播消息；响应于所述装置基于所述所发布的发现广播消息从分散式网络访问代理(DNAP)中接收到响应来从所述装置申请加入DNAP网络；向所述DNAP描述所述装置的所述身份和属性；并且响应于由所述网络基于所述装置的所述身份和属性而授予所述装置的访问权限来通过所述网络从所述装置发送分组。

[0422] 示例109包括如示例108所述的主题。在示例109中，所述装置从所述DNAP中请求令牌。

[0423] 示例110包括如示例108或109中任一项所述的主题。在示例110中，令牌授予所述装置除了对等之外发送和接收网络数据的能力。

[0424] 示例111包括如示例108至110中任一项所述的主题。在示例111中，令牌授予所述装置在网络的开放系统互连层中的层上发送和接收数据的能力。

[0425] 示例112包括如示例108至111中任一项所述的主题。在示例112中，所述分组附带令牌，并且将所述分组和所述令牌的所述组合发送至DNAP以进行校验，其中，响应于检测到所述令牌未被所述DNAP接受，所述DNAP拒绝所述分组和所述令牌两者。

[0426] 示例113包括如示例108至853中任一项所述的主题。在示例113中，所述令牌可以针对与阈值分组数量、阈值数据量、或阈值时间段中的至少一个的使用为有效的。

[0427] 示例114包括如示例108至113中任一项所述的主题。在示例114中，所述装置存储由所述装置接收和发送的事务的事务记录，所述事务记录将与所述DNAP共享。

[0428] 示例115包括如示例108至114中任一项所述的主题。在示例115中，所述装置生成密钥，以指示从所述装置发送的分组的起源。

[0429] 示例116包括如示例108至115中任一项所述的主题。在示例116中，所述装置是区块链启用装置，并且所述装置将由所述装置发送以及由所述装置接收的所有事务存储在所

述区块链上。

[0430] 示例117包括如示例108至116中任一项所述的主题。在示例117中，对所述装置属性的描述被存储在区块链外。

[0431] 示例118包括一种非暂态机器可读介质。所述非暂态机器可读介质包括指令，所述指令当被执行时引导处理器：为作为区块链客户端的装置生成装置身份；从所述装置发布发现广播消息；响应于所述装置基于所述所发布的发现广播消息来从分散式网络访问代理(DNAP)中接收到响应来从所述装置申请加入DNAP网络；向所述DNAP描述所述装置的所述身份和属性；并且响应于由所述网络基于所述装置的所述身份和属性而授予所述装置的访问权限来通过所述网络从所述装置发送分组。

[0432] 示例119包括如示例118所述的主题。在示例119中，所述装置从所述DNAP中请求令牌。

[0433] 示例120包括如示例118或119中任一项所述的主题。在示例120中，令牌授予所述装置除了对等之外发送和接收网络数据的能力。

[0434] 示例121包括如示例118至120中任一项所述的主题。在示例121中，令牌授予所述装置在网络的开放系统互连层中的层上发送和接收数据的能力。

[0435] 示例122包括如示例118至121中任一项所述的主题。在示例122中，所述分组附带令牌，并且将所述分组和所述令牌的所述组合发送至DNAP以进行校验，其中，响应于检测到所述令牌未被所述DNAP接受，所述DNAP拒绝所述分组和所述令牌两者。

[0436] 示例123包括如示例118至122中任一项所述的主题。在示例123中，所述令牌可以针对与阈值分组数量、阈值数据量、或阈值时间段中的至少一个的使用为有效的。

[0437] 示例124包括如示例118至123中任一项所述的主题。在示例124中，所述装置存储由所述装置接收和发送的事务的事务记录，所述事务记录将与所述DNAP共享。

[0438] 示例125包括如示例118至124中任一项所述的主题。在示例125中，所述装置生成密钥，以指示从所述装置发送的分组的起源。

[0439] 示例126包括如示例118至125中任一项所述的主题。在示例126中，所述装置是区块链启用装置，并且所述装置将由所述装置发送以及由所述装置接收的所有事务存储在所述区块链上。

[0440] 示例127包括如示例118至126中任一项所述的主题。在示例127中，对所述装置属性的描述被存储在区块链外。

[0441] 示例128包括一种用于在物联网(IoT)网络中使用的设备。所述用于在物联网(IoT)网络中使用的设备包括：装置注册器，用于通过到第二网络的门户将装置注册到第一网络，其中，所述第二网络被授权访问所述第一网络；装置加入器，用于通过同意所述许可指南的义务将装置加入许可指南；令牌请求器，用于使用所述许可指南的功能来请求令牌，所述令牌将所述装置标识为经认证的以访问所述第二网络；以及请求发送器，用于从所述装置向所述第一网络发送认证请求，其中，所述第一网络响应于检测到所述令牌来确认所述认证。

[0442] 示例129包括如示例128所述的主题。在示例129中，所述装置执行到所述第二网络中的钱包的支付交换。

[0443] 示例130包括如示例128或129中任一项所述的主题。在示例130中，对所述令牌的

所述请求导致在计费区块链上预留硬币以对应于在侧链上生成的令牌。

[0444] 示例131包括如示例128至130中任一项所述的主题。在示例131中，响应于通过所述装置向所述第一网络呈现所述令牌对所述装置进行认证而在侧链上消耗所述令牌。

[0445] 示例132包括如示例128至131中任一项所述的主题。在示例132中，响应于检测到令牌为由测量区块链的撤销和消耗中的至少一个来释放所述区块链的硬币。

[0446] 示例133包括如示例128至132中任一项所述的主题。在示例133中，加入所述许可指南包括针对属性过滤器将所述装置的属性从所述装置提供到所述许可指南，以验证在所述第一网络中允许所述装置的所述属性。

[0447] 示例134包括如示例128至133中任一项所述的主题。在示例134中，所述属性包括在所述装置正在加入所述许可指南时有效用户简档的属性。

[0448] 示例135包括如示例128至134中任一项所述的主题。在示例135中，所述令牌响应于被用作对所述装置授权的形式而自行销毁。

[0449] 示例136包括如示例128至135中任一项所述的主题。在示例136中，基于向所述第一网络认证装置具有用于访问第二网络的凭证，所述装置被授权访问第一网络。

[0450] 示例137包括如示例128至136中任一项所述的主题。在示例137中，所述授权所述装置使用所述第一网络基于访问次数、通过所述第一网络访问的数据量、以及授予访问的时间中的至少一个而到期。

[0451] 示例138包括一种用于使用物联网(IoT)装置进行分散式授权、认证、和计费的方法。所述用于使用物联网(IoT)装置进行分散式授权、认证、和计费的方法包括：通过到第二网络的门户将装置注册到第一网络，其中，所述第二网络被授权访问所述第一网络；通过同意所述许可指南的义务将装置加入许可指南；使用所述许可指南的功能来请求令牌，所述令牌将所述装置标识为经认证的以访问所述第二网络；并且从所述装置向所述第一网络发送认证请求，其中，所述第一网络响应于检测到所述令牌来确认所述认证。

[0452] 示例139包括如示例138所述的方法。在示例138中，所述装置执行到所述第二网络中的钱包的支付交换。

[0453] 示例140包括如示例138或139中任一项所述的主题。在示例140中，对所述令牌的所述请求导致在计费区块链上预留硬币以对应于在侧链上生成的令牌。

[0454] 示例141包括如示例138至140中任一项所述的主题。在示例141中，响应于通过所述装置向所述第一网络呈现所述令牌对所述装置进行认证而在侧链上消耗所述令牌。

[0455] 示例142包括如示例138至141中任一项所述的主题。在示例142中，响应于检测到令牌为由测量区块链的撤销和消耗中的至少一个来释放所述区块链的硬币。

[0456] 示例143包括如示例138至142中任一项所述的主题。在示例143中，加入所述许可指南包括针对属性过滤器将所述装置的属性从所述装置提供到所述许可指南，以验证在所述第一网络中允许所述装置的所述属性。

[0457] 示例144包括如示例138至143中任一项所述的主题。在示例144中，所述属性包括在所述装置正在加入所述许可指南时有效用户简档的属性。

[0458] 示例145包括如示例138至144中任一项所述的主题。在示例145中，所述令牌响应于被用作对所述装置授权的形式而自行销毁。

[0459] 示例146包括如示例138至145中任一项所述的主题。在示例146中，基于向所述第

一网络认证装置具有用于访问第二网络的凭证,所述装置被授权访问第一网络。

[0460] 示例147包括如示例138至146中任一项所述的主题。在示例147中,所述授权所述装置使用所述第一网络具有基于访问次数、通过所述第一网络访问的数据量、以及授予访问的时间中的至少一个的有效期。

[0461] 示例148包括一种非暂态机器可读介质。所述非暂态机器可读介质包括指令,所述指令当被执行时引导处理器:通过到第二网络的门户将装置注册到第一网络,其中,所述第二网络被授权访问所述第一网络;通过同意所述许可指南的义务将装置加入许可指南;使用所述许可指南的功能来请求令牌,所述令牌将所述装置标识为经认证的以访问所述第二网络;并且从所述装置向所述第一网络发送认证请求,其中,所述第一网络响应于检测到所述令牌来确认所述认证。

[0462] 示例149包括如示例148所述的主题。在示例149中,所述装置执行到所述第二网络中的钱包的支付交换。

[0463] 示例150包括如示例148或149中任一项所述的主题。在示例150中,对所述令牌的所述请求导致在计费区块链上预留硬币以对应于在侧链上生成的令牌。

[0464] 示例151包括如示例148至150中任一项所述的主题。在示例151中,响应于通过所述装置向所述第一网络呈现所述令牌对所述装置进行认证而在侧链上消耗所述令牌。

[0465] 示例152包括如示例148至151中任一项所述的主题。在示例152中,响应于检测到令牌为由测量区块链的撤销和消耗中的至少一个来释放所述区块链的硬币。

[0466] 示例153包括如示例148至152中任一项所述的主题。在示例153中,加入所述许可指南包括针对属性过滤器将所述装置的属性从所述装置提供到所述许可指南,以验证在所述第一网络中允许所述装置的所述属性。

[0467] 示例154包括如示例148至153中任一项所述的主题。在示例154中,所述属性包括在所述装置正在加入所述许可指南时有效用户简档的属性。

[0468] 示例155包括如示例148至154中任一项所述的主题。在示例155中,所述令牌响应于被用作对所述装置授权的形式而自行销毁。

[0469] 示例156包括如示例148至155中任一项所述的主题。在示例156中,基于由所述第二网络向所述第一网络认证所述装置具有访问第二网络的凭证,所述装置被授权访问所述第一网络。

[0470] 示例157包括如示例148至156中任一项所述的主题。在示例157中,所述授权所述装置使用所述第一网络具有基于访问次数、通过所述第一网络访问的数据量、以及授予访问的时间中的至少一个的有效期。

[0471] 示例158包括一种用于在物联网(IoT)网络中使用的设备。所述用于在物联网(IoT)网络中使用的设备包括使用分散式应用程序接口(API)校验认证请求的身份的身份校验器。所述设备还包括:从远程认证拨号用户服务(RADIUS)客户端接收的所述认证请求;所述分散式API,用于通过向分布式分类账发送请求并且响应于从所述分布式分类账接收到身份校验响应而将所述身份校验响应返回到RADIUS服务器来校验所述身份;响应返回器,用于响应于从所述分散式API接收到响应而向所述RADIUS返回对所述认证请求的响应,并且其中,所述RADIUS客户端响应于对认证身份的响应来进行事务。

[0472] 示例159包括如示例158所述的主题。在示例159中,所述事务包括用户名称、密码

和元数据中的至少一个。

[0473] 示例160包括如示例158或159中任一项所述的主题。在示例160中,所述事务包括价值事务。

[0474] 示例161包括如示例158至160中任一项所述的主题。在示例161中,所述事务是加密货币事务。

[0475] 示例162包括如示例158至161中任一项所述的主题。在示例162中,所述认证请求包括对网络地址的请求。

[0476] 示例163包括如示例158至162中任一项所述的主题。在示例163中,所述网络地址包括所述RADIUS服务器的完全限定域名以及所述RADIUS服务器的互联网协议地址中的至少一个。

[0477] 示例164包括如示例158至163中任一项所述的主题。在示例164中,所述RADIUS服务器通过从区块链中请求公钥的位置来校验所述公钥。

[0478] 示例165包括如示例158至164中任一项所述的主题。在示例165中,响应于RADIUS客户端接收到对认证身份的确认,对RADIUS服务器的所述请求发生在链外。

[0479] 示例166包括如示例158至165中任一项所述的主题。在示例166中,所述RADIUS服务器对所述RADIUS服务器接收的请求进行记录和计费。

[0480] 示例167包括如示例158至166中任一项所述的主题。在示例167中,对所述认证请求的所述响应作为不可变记录存储到区块链中。

[0481] 示例168包括一种用于使用物联网(IoT)装置进行分散式授权、认证、和计费的方法。所述用于使用物联网(IoT)装置进行分散式授权、认证、和计费的方法包括:使用分布式分类账来校验认证请求的所述身份,所述认证请求是从远程认证拨号用户服务(RADIUS)客户端接收的;响应于从所述分布式分类账接收到肯定的身份校验响应来向RADIUS服务器发送请求;响应于从所述RADIUS服务器接收到响应将对所述认证请求的响应返回至所述RADIUS客户端,并且其中,响应于对认证身份的响应,所述RADIUS客户端与所述RADIUS服务器进行事务。

[0482] 示例169包括如示例168所述的主题。在示例169中,所述事务包括用户名称、密码和元数据中的至少一个。

[0483] 示例170包括如示例168或169中任一项所述的主题。在示例170中,所述事务包括价值事务。

[0484] 示例171包括如示例168至170中任一项所述的主题。在示例171中,所述事务是加密货币事务。

[0485] 示例172包括如示例168至171中任一项所述的主题。在示例172中,所述认证请求包括对网络地址的请求。

[0486] 示例173包括如示例168至172中任一项所述的主题。在示例173中,所述网络地址包括所述RADIUS服务器的完全限定域名以及所述RADIUS服务器的互联网协议地址中的至少一个。

[0487] 示例174包括如示例168至173中任一项所述的主题。在示例174中,所述RADIUS服务器通过从区块链中请求公钥的位置来校验所述公钥。

[0488] 示例175包括如示例168至174中任一项所述的主题。在示例175中,响应于RADIUS

客户端接收到对认证身份的确认，对RADIUS服务器的所述请求发生在链外。

[0489] 示例176包括如示例168至175中任一项所述的主题。在示例176中，所述RADIUS服务器对所述RADIUS服务器接收的请求进行记录和计费。

[0490] 示例177包括如示例176至176中任一项所述的主题。在示例177中，对所述认证请求的所述响应作为不可变记录存储到区块链中。

[0491] 示例178包括一种非暂态机器可读介质。所述非暂态机器可读介质包括指令，所述指令当被执行时引导处理器：使用分布式分类账来校验认证请求的所述身份，所述认证请求是从远程认证拨号用户服务(RADIUS)客户端接收的；响应于从所述分布式分类账接收到肯定的身份校验响应来向RADIUS服务器发送请求；响应于从所述RADIUS服务器接收到响应将对所述认证请求的响应返回至所述RADIUS客户端，并且其中，响应于对认证身份的响应，所述RADIUS客户端与所述RADIUS服务器进行事务。

[0492] 示例179包括如示例178所述的主题。在示例179中，所述事务包括用户名称、密码和元数据中的至少一个。

[0493] 示例180包括如示例178或179中任一项所述的主题。在示例180中，所述事务包括价值事务。

[0494] 示例181包括如示例178至180中任一项所述的主题。在示例181中，所述事务是加密货币事务。

[0495] 示例182包括如示例178至181中任一项所述的主题。在示例182中，所述认证请求包括对网络地址的请求。

[0496] 示例183包括如示例178至182中任一项所述的主题。在示例183中，所述网络地址包括所述RADIUS服务器的完全限定域名以及所述RADIUS服务器的互联网协议地址中的至少一个。

[0497] 示例184包括如示例178至183中任一项所述的主题。在示例184中，所述RADIUS服务器通过从区块链中请求公钥的位置来校验所述公钥。

[0498] 示例185包括如示例178至184中任一项所述的主题。在示例185中，响应于RADIUS客户端接收到对认证身份的确认，对RADIUS服务器的所述请求发生在链外。

[0499] 示例186包括如示例178至185中任一项所述的主题。在示例186中，所述RADIUS服务器对所述RADIUS服务器接收的请求进行记录和计费。

[0500] 示例187包括如示例178至186中任一项所述的主题。在示例187中，对所述认证请求的所述响应作为不可变记录存储到区块链中。

[0501] 示例188包括一种用于在物联网(IoT)网络中使用的设备。所述用于在物联网(IoT)网络中使用的设备包括：凭证下发器，用于将凭证下发至调用程序实体，所述凭证包括授权结构的多个层；以及对象实体提供器，用于向对象实体提供指定对目标对象的引用和许可的访问控制列表。所述设备还包括：凭证呈现器，用于向所述对象实体呈现授权凭证；以及访问控制列表策略申请器，用于申请访问控制列表以基于对所述凭证是否与所述调用程序实体重叠、所述目标对象是否与请求重叠、多个装置层标识是否与多个凭证层标识相匹配、并且多个目标层标识是否与多个请求层标识相匹配的比较来判定是是否允许对IoT装置进行访问。

[0502] 示例189包括如示例188所述的主题。在示例189中，所述凭证是六层许可。

[0503] 示例190包括如示例188或189中任一项所述的主题。在示例190中，所述六层许可包括平台层、装置层、集合层、资源层、记录层、和性质层。

[0504] 示例191包括如示例188至190中任一项所述的主题。在示例191中，所述多个层包括平台层以反映计算机的物理实例，所述计算机包括计算、连网、存储、感测和致动能力中的至少一个。

[0505] 示例192包括如示例188至191中任一项所述的主题。在示例192中，所述多个层包括装置层以反映计算机的逻辑实例，所述计算机包括计算、连网、存储、感测和致动能力中的至少一个。

[0506] 示例193包括如示例188至192中任一项所述的主题。在示例193中，所述多个层包括资源的逻辑结构的集合层，其中，所述资源包括用于记录的逻辑结构，其中，所述记录包括性质的逻辑结构，并且其中，所述性质包括原子数据结构和复杂数据结构中的至少一个。

[0507] 示例194包括如示例188至193中任一项所述的主题。在示例194中，所述性质是复杂数据结构，并且所述复杂数据结构用于使用数据建模语言可定义的结构。

[0508] 示例195包括如示例188至194中任一项所述的主题。在示例195中，所述性质包括原子数据结构，并且所述原子数据结构是字符串、数字和日期中的至少一个。

[0509] 示例196包括如示例188至195中任一项所述的主题。在示例196中，所述对象实体的所述授权凭证受到基于创建、读取、更新、删除和通知(CRUDN)生命周期通知通过对象数据的物理性对对象施加的限制所限制。

[0510] 示例197包括如示例188至196中任一项所述的主题。在示例197中，所述凭证指示制造商的安装。

[0511] 示例198包括一种用于在IoT对象中进行访问控制的方法。所述用于在IoT对象中进行访问控制的方法包括：向调用程序实体下发凭证，所述凭证包括授权结构的多个层；向对象实体提供指定对目标对象的引用和许可的访问控制列表；向所述对象实体呈现授权凭证；并且申请访问控制列表以基于对所述凭证是否与所述调用程序实体重叠、所述目标对象是否与请求重叠、多个装置层标识是否与多个凭证层标识相匹配、并且多个目标层标识是否与多个请求层标识相匹配的比较来判定是是否允许对IoT装置进行访问。

[0512] 示例199包括如示例198所述的主题。在示例199中，所述凭证是六层许可。

[0513] 示例200包括如示例198或199中任一项所述的主题。在示例200中，所述六层许可包括平台层、装置层、集合层、资源层、记录层、和性质层。

[0514] 示例201包括如示例198至200中任一项所述的主题。在示例201中，所述多个层包括平台层以反映计算机的物理实例，所述计算机包括计算、连网、存储、感测和致动能力中的至少一个。

[0515] 示例202包括如示例198至201中任一项所述的主题。在示例202中，所述多个层包括装置层以反映计算机的逻辑实例，所述计算机包括计算、连网、存储、感测和致动能力中的至少一个。

[0516] 示例203包括如示例198至202中任一项所述的主题。在示例203中，所述多个层包括资源的逻辑结构的集合层，其中，所述资源包括用于记录的逻辑结构，其中，所述记录包括性质的逻辑结构，并且其中，所述性质包括原子数据结构和复杂数据结构中的至少一个。

[0517] 示例204包括如示例198至203中任一项所述的主题。在示例204中，所述性质是复

杂数据结构，并且所述复杂数据结构用于使用数据建模语言可定义的结构。

[0518] 示例205包括如示例198至204中任一项所述的主题。在示例205中，所述性质包括原子数据结构，并且所述原子数据结构是字符串、数字和日期中的至少一个。

[0519] 示例206包括如示例198至205中任一项所述的主题。在示例206中，所述对象实体的所述授权凭证受到基于创建、读取、更新、删除和通知(CRUDN)生命周期通知通过对象数据的物理性对对象施加的限制所限制。

[0520] 示例207包括如示例198至206中任一项所述的主题。在示例207中，所述凭证指示制造商的安装。

[0521] 示例208包括一种非暂态机器可读介质。所述非暂态机器可读介质包括指令，所述指令当被执行时引导处理器：向调用程序实体下发凭证，所述凭证包括授权结构的多个层；向对象实体提供指定对目标对象的引用和许可的访问控制列表；向所述对象实体呈现授权凭证；并且申请访问控制列表以基于对所述凭证是否与所述调用程序实体重叠、所述目标对象是否与请求重叠、多个装置层标识是否与多个凭证层标识相匹配、并且多个目标层标识是否与多个请求层标识相匹配的比较来判定是是否允许对IoT装置进行访问。

[0522] 示例209包括如示例208所述的主题。在示例209中，所述凭证是六层许可。

[0523] 示例210包括如示例208或209中任一项所述的主题。在示例210中，所述六层许可包括平台层、装置层、集合层、资源层、记录层、和性质层。

[0524] 示例211包括如示例208至210中任一项所述的主题。在示例211中，所述多个层包括平台层以反映计算机的物理实例，所述计算机包括计算、连网、存储、感测和致动能力中的至少一个。

[0525] 示例212包括如示例208至211中任一项所述的主题。在示例212中，所述多个层包括装置层以反映计算机的逻辑实例，所述计算机包括计算、连网、存储、感测和致动能力中的至少一个。

[0526] 示例213包括如示例208至212中任一项所述的主题。在示例213中，所述多个层包括资源的逻辑结构的集合层，其中，所述资源包括用于记录的逻辑结构，其中，所述记录包括性质的逻辑结构，并且其中，所述性质包括原子数据结构和复杂数据结构中的至少一个。

[0527] 示例214包括如示例208至213中任一项所述的主题。在示例214中，所述性质是复杂数据结构，并且所述复杂数据结构用于使用数据建模语言可定义的结构。

[0528] 示例215包括如示例208至214中任一项所述的主题。在示例215中，所述性质包括原子数据结构，并且所述原子数据结构是字符串、数字和日期中的至少一个。

[0529] 示例216包括如示例208至215中任一项所述的主题。在示例216中，所述对象实体的所述授权凭证受到基于创建、读取、更新、删除和通知(CRUDN)生命周期通知通过对象数据的物理性对对象施加的限制所限制。

[0530] 示例217包括如示例208至216中任一项所述的主题。在示例217中，所述凭证指示制造商的安装。

[0531] 示例218包括一种设备，所述设备包括用于执行如在任一其他示例中的方法的装置。

[0532] 示例219包括一种机器可读存储装置，所述机器可读存储装置包括机器可读指令，所述机器可读指令当被执行时用于实施如任一其他示例中的方法或实现如任一其他示例

中的设备。

[0533] 一些实施例可以在硬件、固件和软件之一或其组合中被实施。一些实施例还可以实施为存储在机器可读介质上的指令，所述指令可以由计算平台读取并执行以便执行在此描述的操作。机器可读介质可以包括用于以可由机器(例如，计算机)读取的形式存储或传输信息的任何机构。例如，机器可读介质可以包括：只读存储器(ROM)；随机存取存储器(RAM)；磁盘存储介质；光学存储介质；闪存装置；或者电气、光学、声学或其他形式的传播信号(例如，载波、红外信号、数字信号)、或传输和/或接收信号的接口等。

[0534] 实施例是实施方式或示例。说明书中对“实施例”、“一个实施例”、“一些实施例”、“各个实施例”或“其他实施例”的引用意味着结合实施例描述的具体特征、结构或特性包括在本技术的至少一些实施例中，但不必是全部实施例。“实施例”、“一个实施例”或“一些实施例”的多处出现不必全部指代相同的实施例。来自一个实施例的元件或方面可与另一实施例的元件或方面组合。

[0535] 并非本文描述和展示的所有组件、特征、结构、特性等都需要包括在一个或多个具体实施例中。例如，如果说明书陈述组件、特征、结构或特性“可以”、“可能”、“可”或“能够”被包括，则那个具体组件、特征、结构或特性不要求被包括。如果说明书或权利要求提及“一(a)”或“一个(an)”要素，则那并非意味着仅存在一个要素。如果说明书或权利要求提及“附加的”要素，则那并不排除存在多于一个的附加要素。

[0536] 应注意的是，尽管已经参考具体实施方式对一些实施例进行了描述，但根据一些实施例其他实施方式是可能的。另外，在附图中展示和/或本文描述的电路元件或其他特征的安排和/或顺序不需要以所展示和描述的具体方式安排。根据一些实施例，许多其他安排是可能的。

[0537] 在附图中示出的每个系统中，一些情况中的元素可以各自都具有相同的附图标记或不同的附图标记以表明所表示的元素可以是不同和/或类似的。然而，元件可以足够灵活到具有不同的实施方式并与本文示出或描述的系统的一些或全部一起工作。图中示出的各种元件可以是相同的或不同的。哪个被称为第一元件和哪个被称为第二元件是任意的。

[0538] 本技术不限于本文列出的具体细节。实际上，受益于此公开的本领域技术人员将理解，许多来自前述描述和附图的其他变型可以在本技术的范围内进行。从而，是包括其任何修改的以下权利要求定义了本发明的范围。

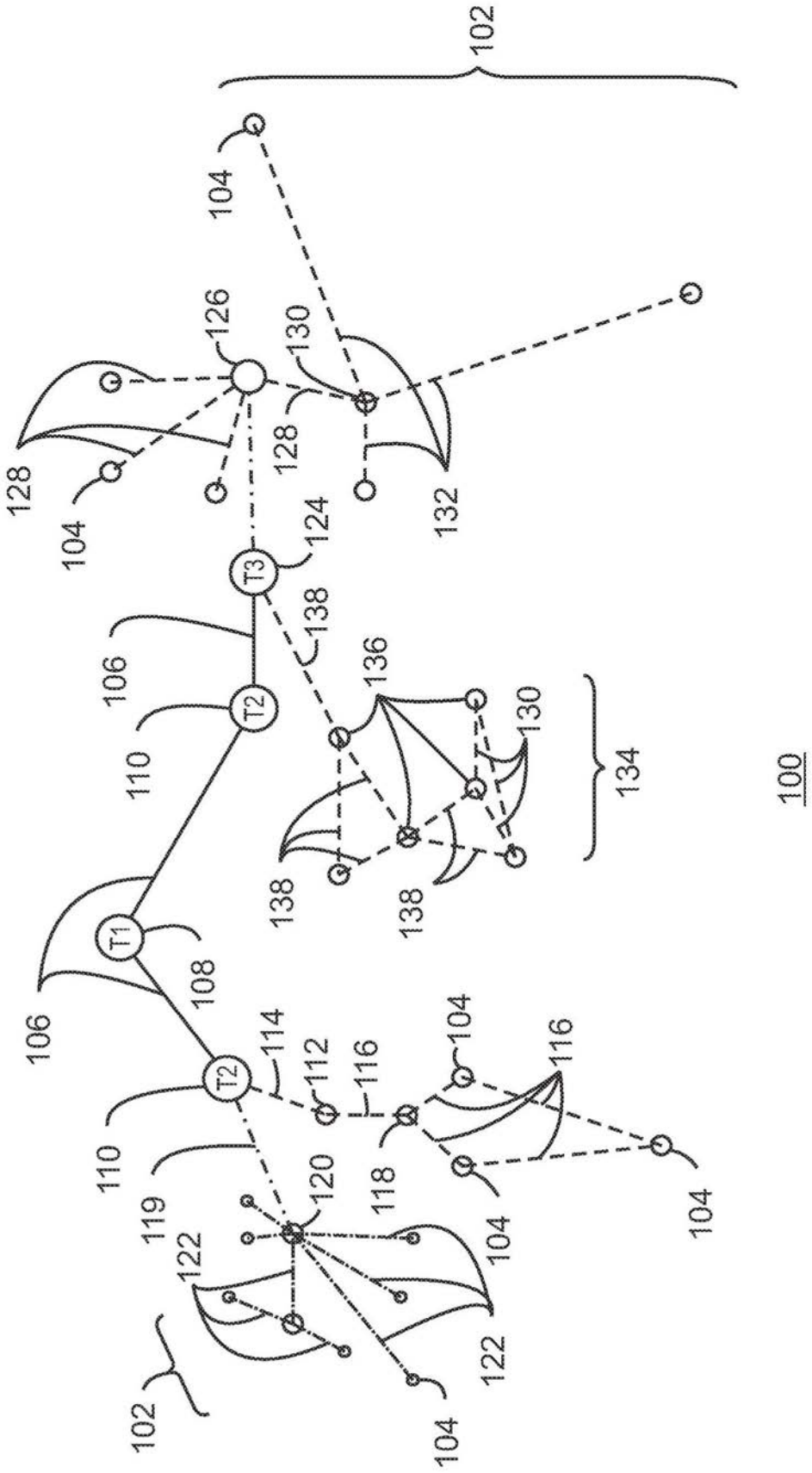

102
104
126
130
128
128
104
132
124
T3
138
106
136
106
T2
110
130
110
134
138
138
T1
108
106
T2
114
112
116
104
116
110
120
118
119
104
122
104
122
102
104
100

图1

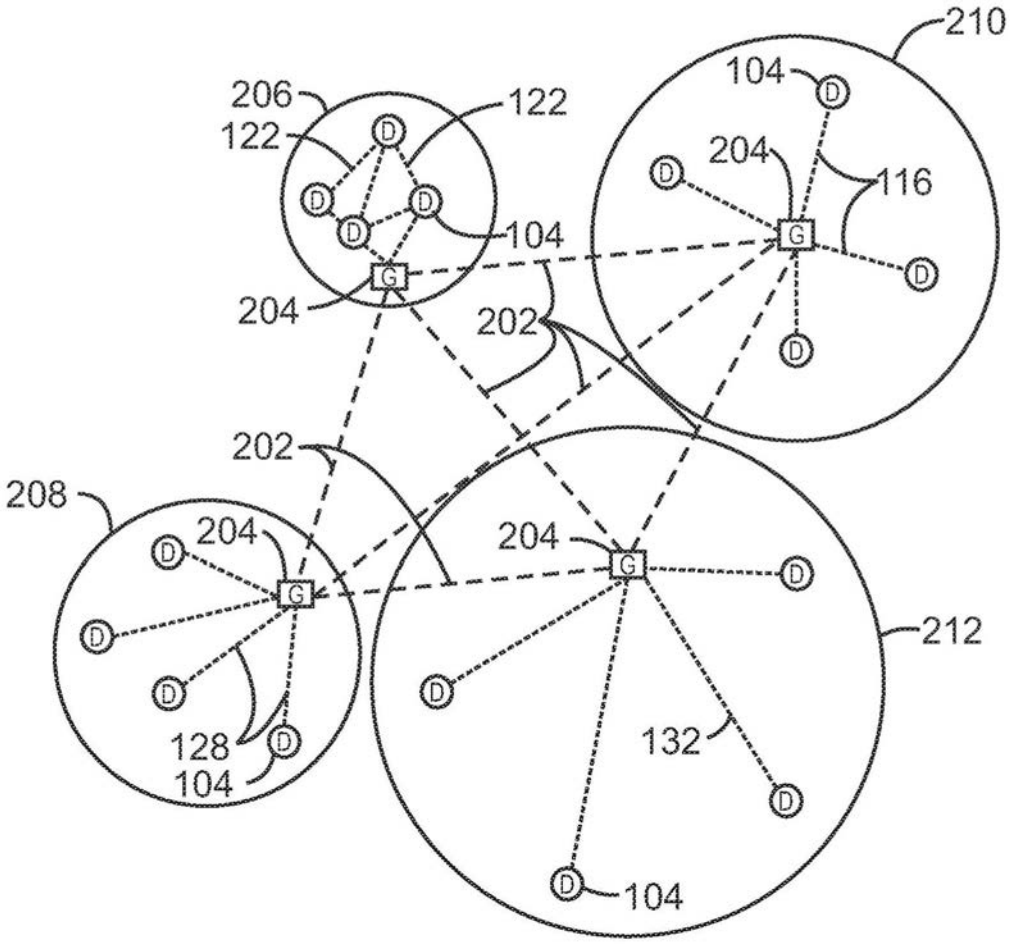
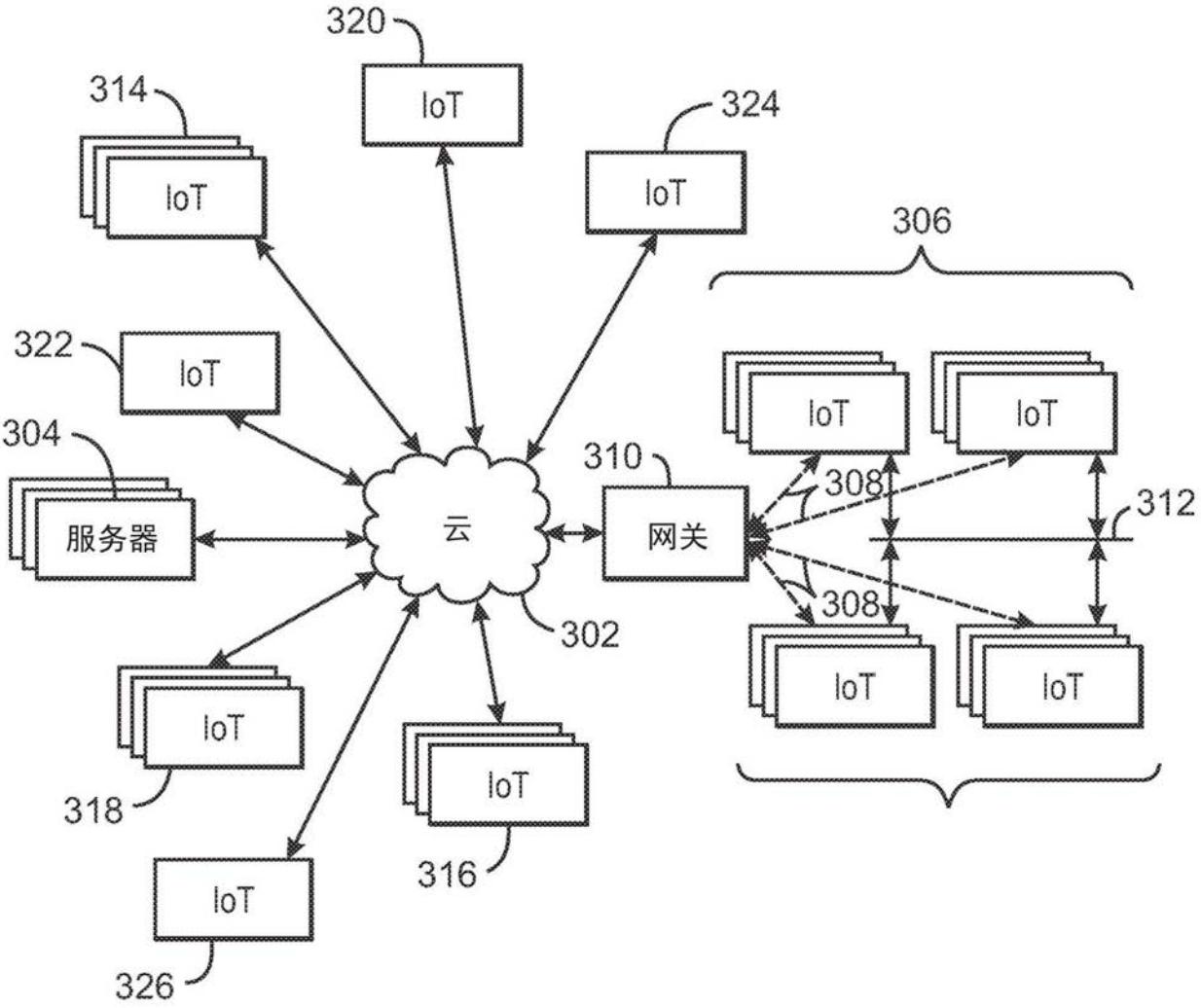

210
104
206
122
122
204
116
104
202
202
208
204
204
212
128
104
132
104
200

图2


320
IoT
314
IoT
324
IoT
306
322
IoT
IoT
IoT
304
服务器
云
310
网关
308
312
308
302
IoT
IoT
IoT
IoT
318
316
IoT
326

300

图3

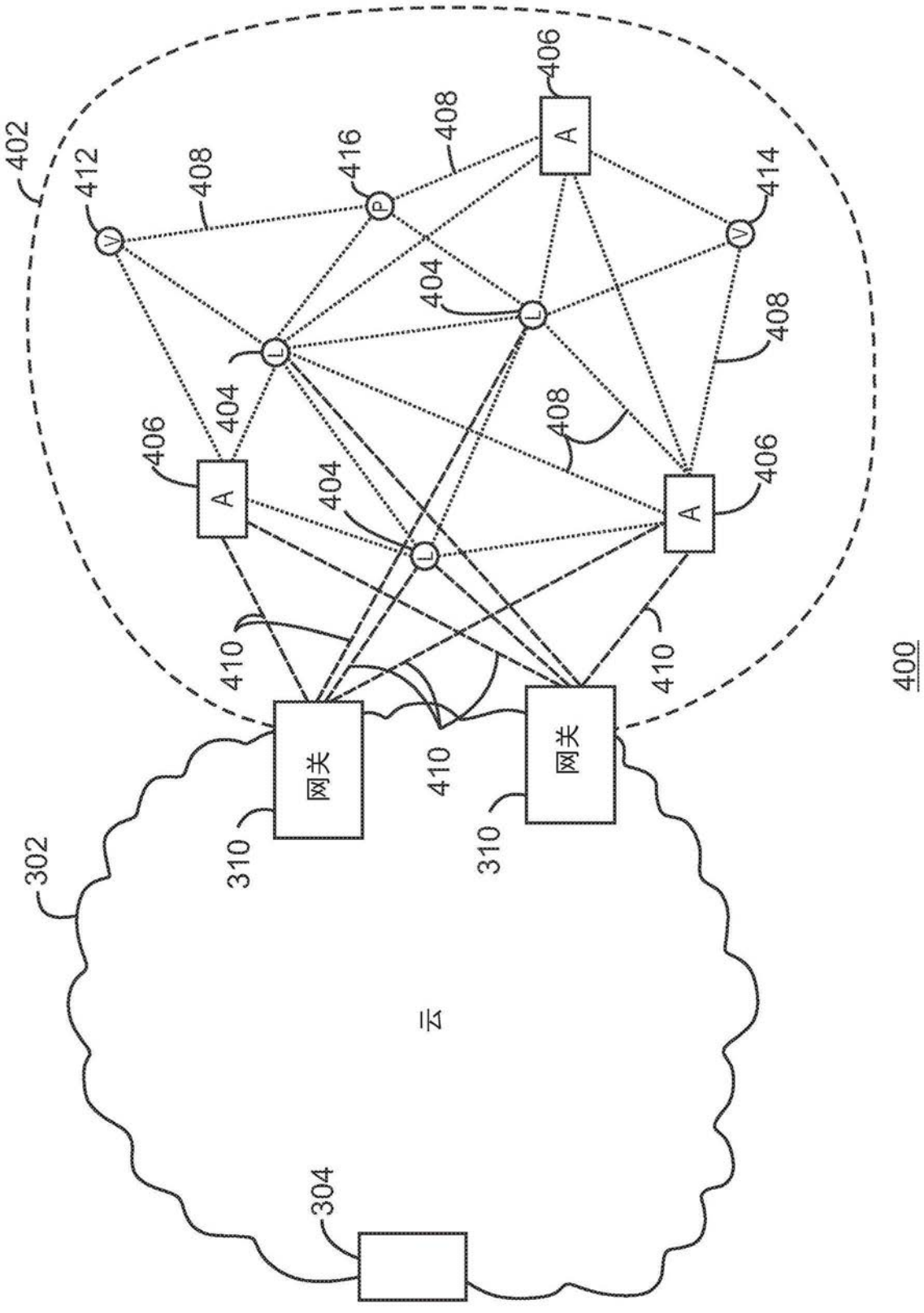
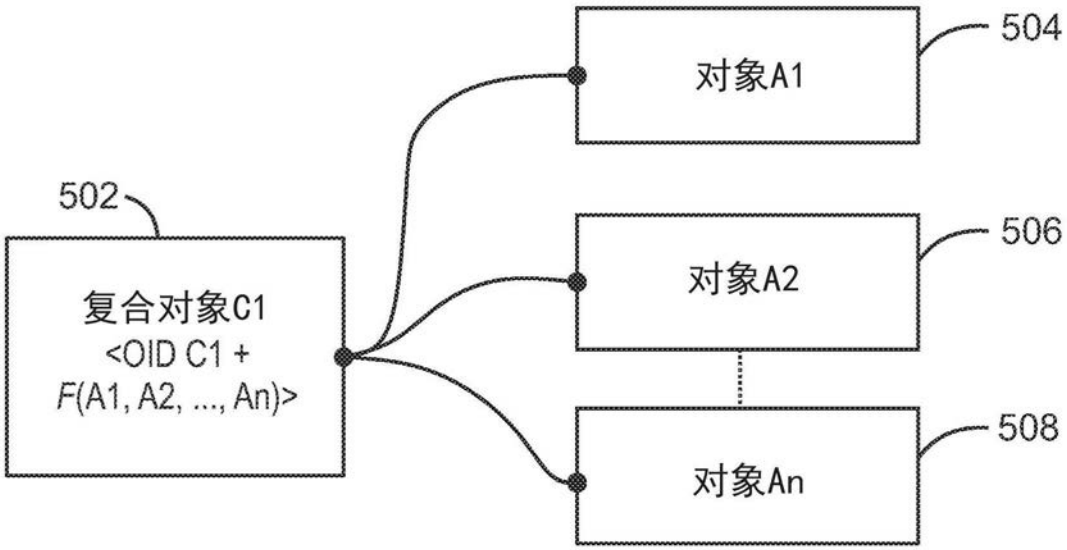

402
412
408
416
408
406
414
404
408
406
404
408
406
404
410
410
410
网关
网关
310
310
302
云
304
400

图4



500

图5

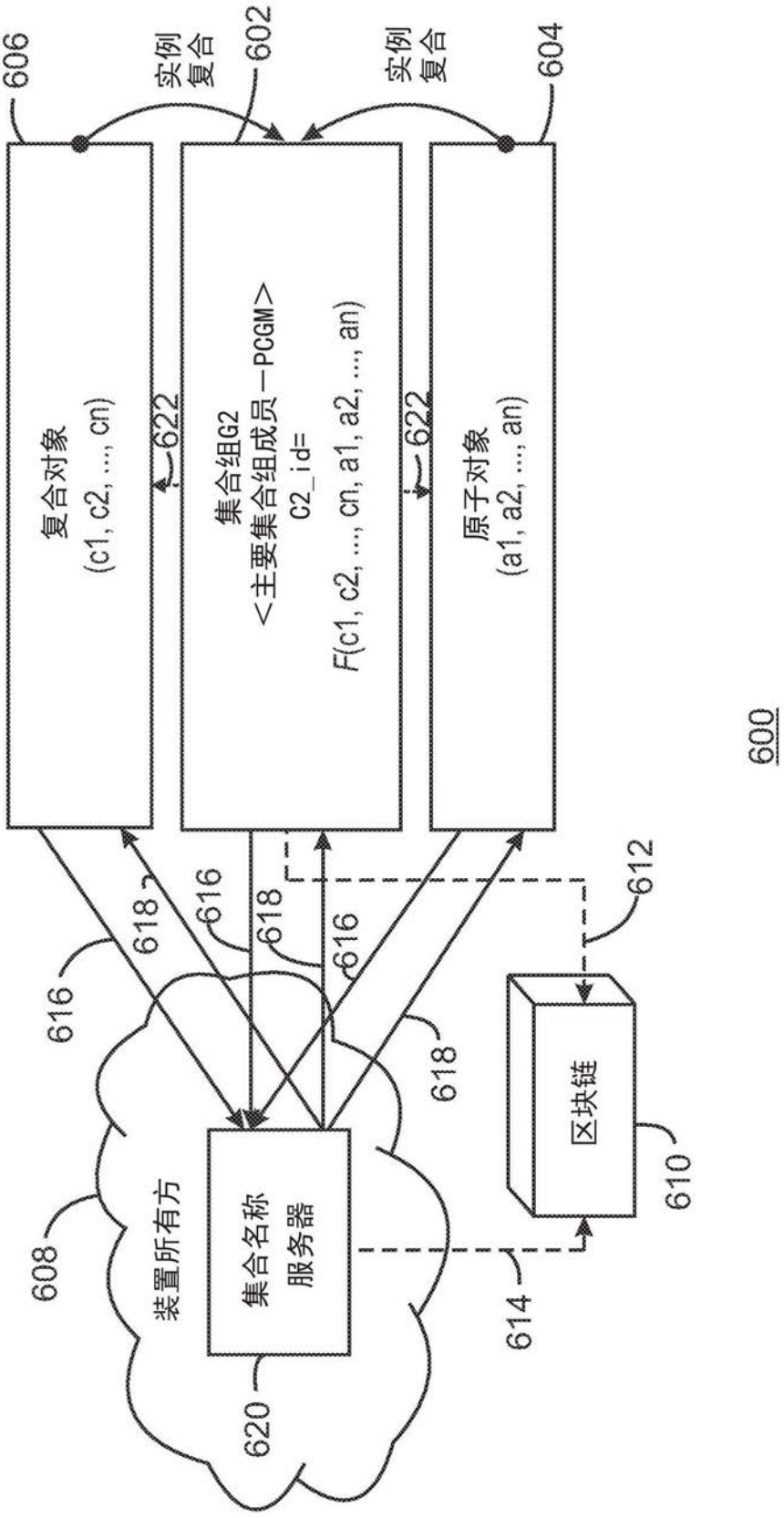

606
实例复合
602
实例复合
604
复合对象
(c1, c2, ..., cn)
622
集合组G2
<主要集合组成员—PCGM>
c2_id=
F(c1, c2, ..., cn, a1, a2, ..., an)
622
原子对象
(a1, a2, ..., an)
600
616
618
616
618
616
618
612
区块链
610
608
装置所有方
集合名称服务器
620
614

图6

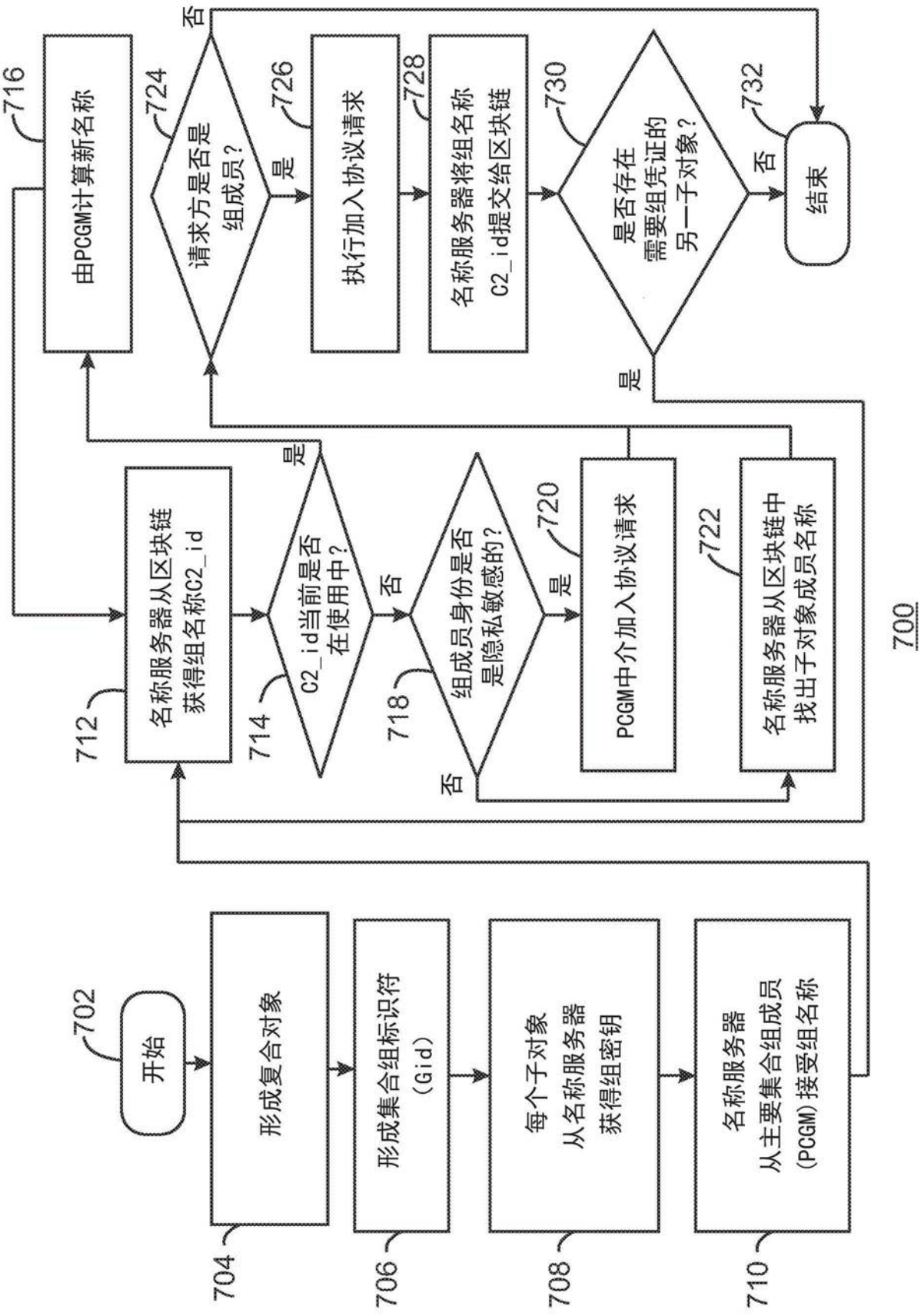

开始
形成复合对象
形成集合组标识符（Gid）
每个子对象从名称服务器获得组密钥
名称服务器从主要集合组成员（PCGM）接受组名称
由PCGM计算新名称
请求方是否是组成员？
执行加入协议请求
名称服务器将组名称C2_id提交给区块链
是否存在需要组凭证的另一子对象？
结束
名称服务器从区块链获得组名称C2_id
C2_id当前是否在使用中？
组成员身份是否是隐私敏感的？
PCGM中介加入协议请求
名称服务器从区块链中找出子对象成员名称
是
否
700

图7

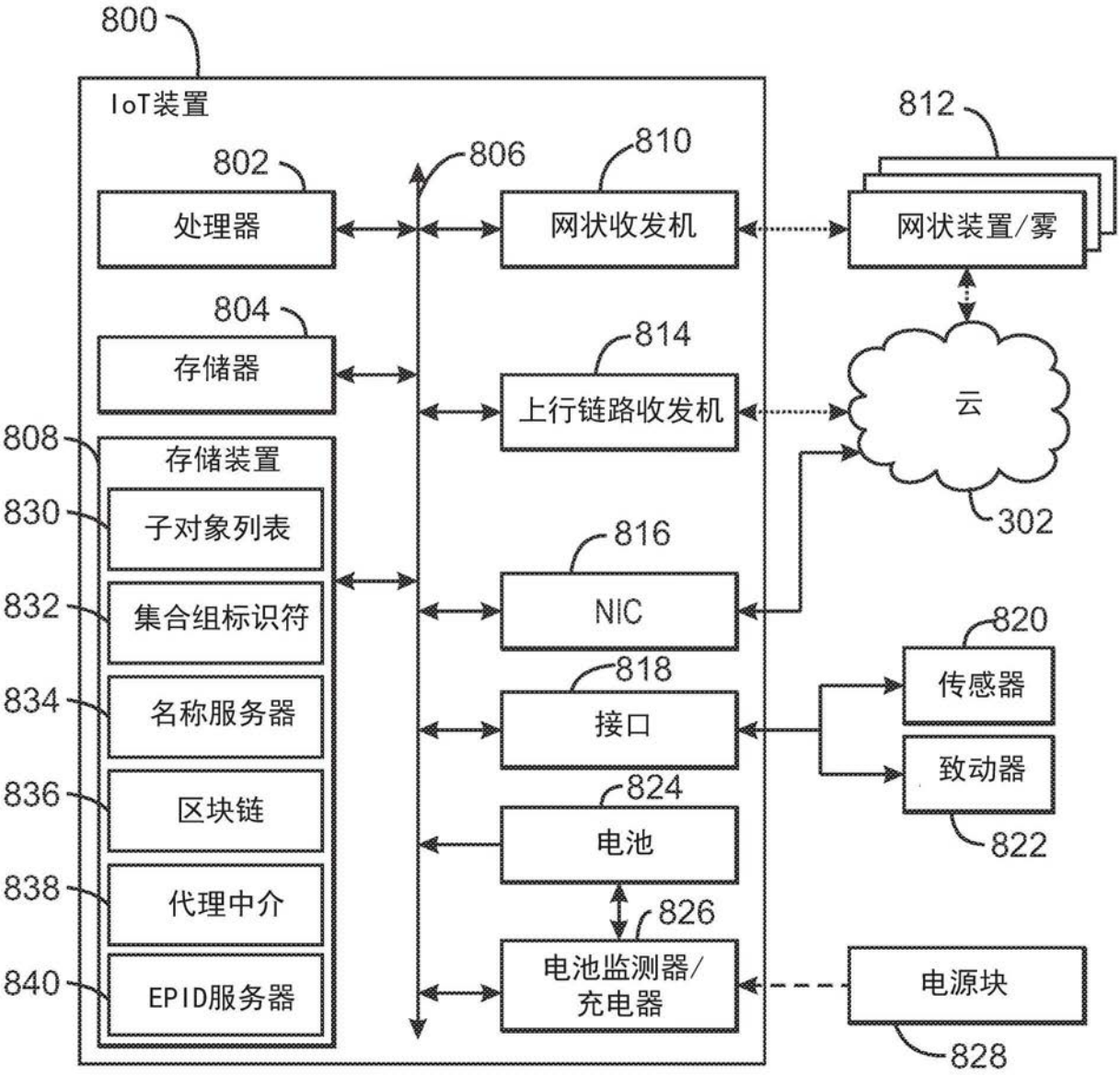

800
IoT装置
802
处理器
804
存储器
808
存储装置
830
子对象列表
832
集合组标识符
834
名称服务器
836
区块链
838
代理中介
840
EPID服务器
806
810
网状收发机
814
上行链路收发机
816
NIC
818
接口
824
电池
826
电池监测器/
充电器
812
网状装置/雾
云
302
820
传感器
致动器
822
电源块
828

图8

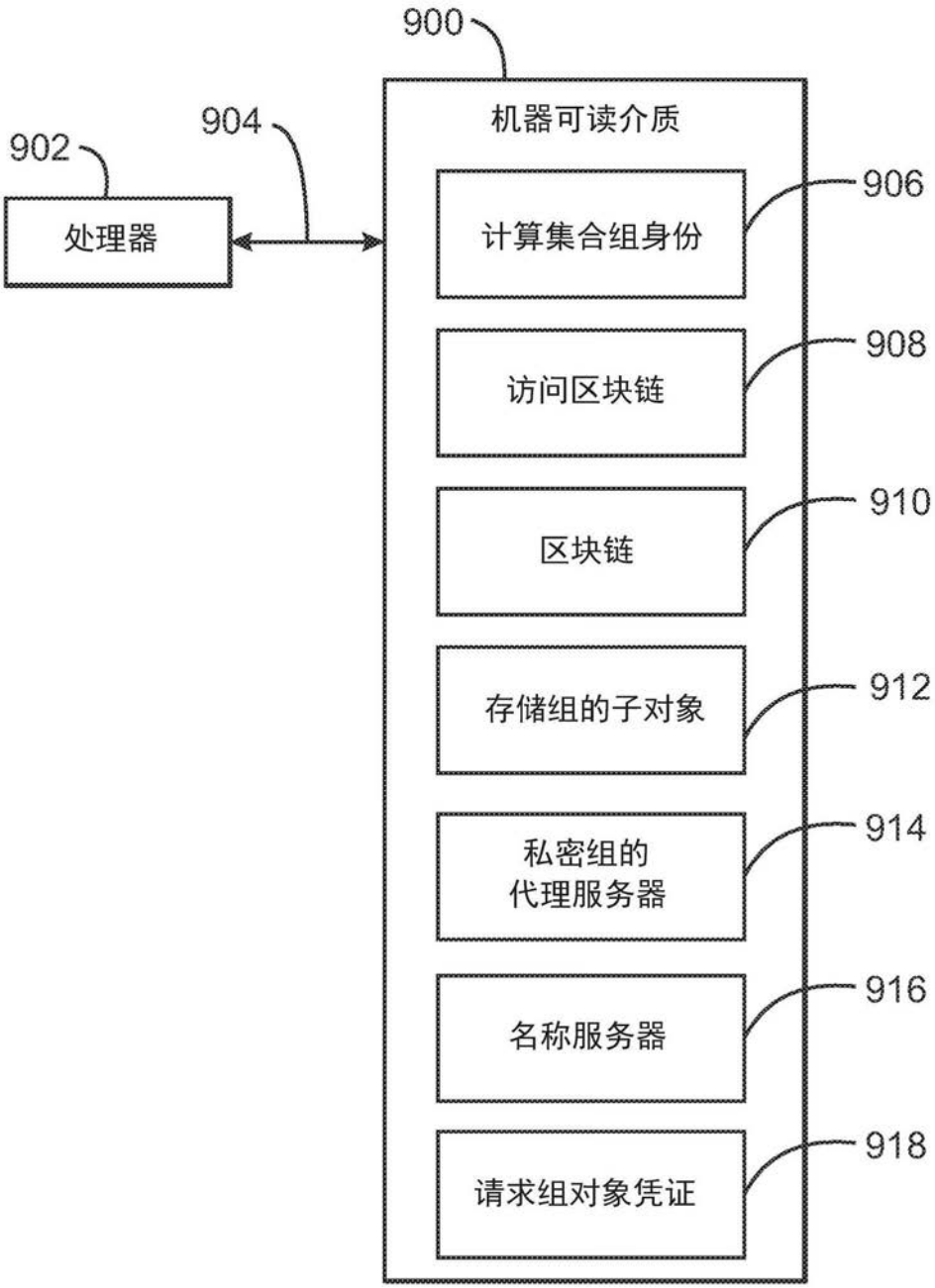

900
机器可读介质
902
处理器
904
计算集合组身份
906
访问区块链
908
区块链
910
存储组的子对象
912
私密组的
代理服务器
914
名称服务器
916
请求组对象凭证
918

图9

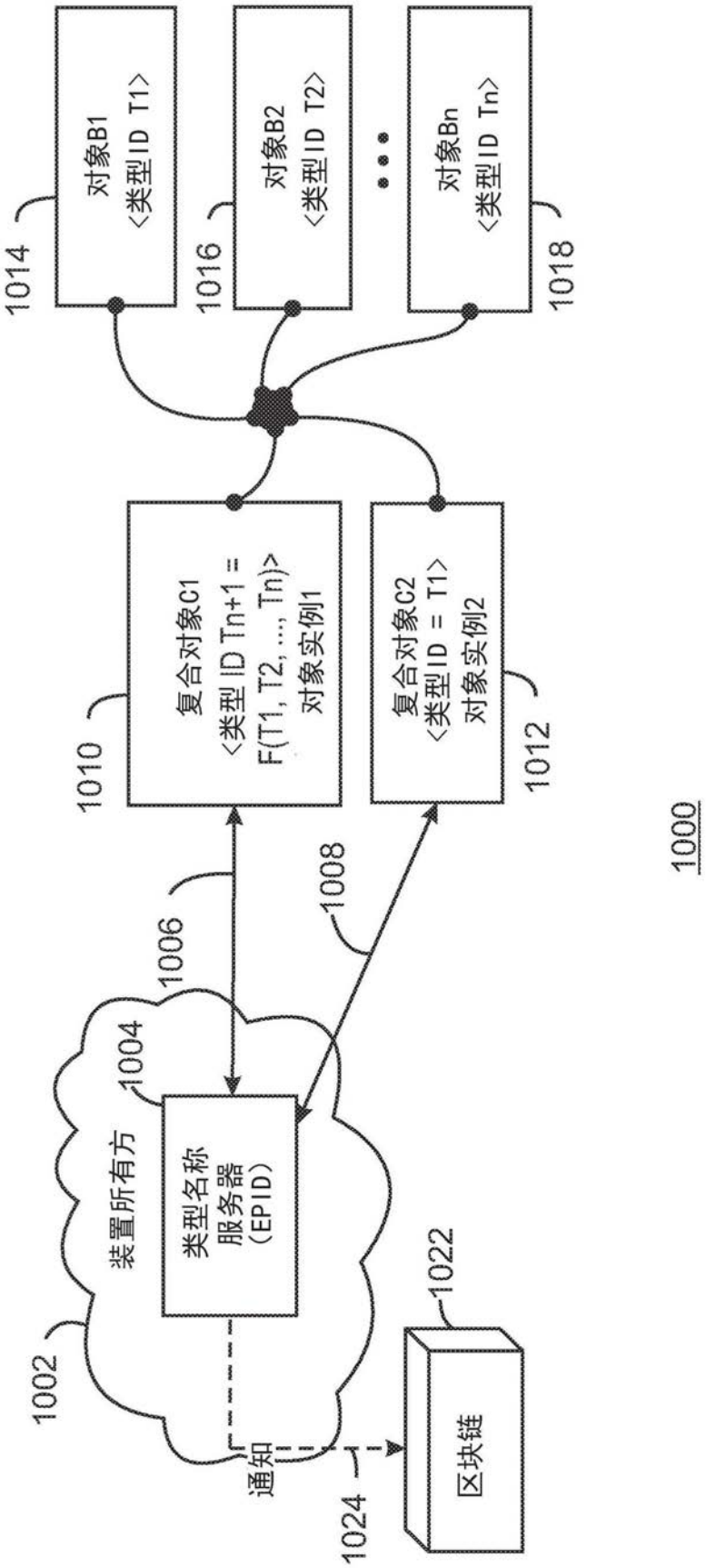

对象B1
<类型ID T1>
对象B2
<类型ID T2>
对象Bn
<类型ID Tn>
1014
1016
1018
复合对象C1
<类型 ID Tn+1 =
F(T1, T2, ..., Tn)>
对象实例1
复合对象C2
<类型ID = T1>
对象实例2
1010
1012
1008
1006
1004
装置所有方
类型名称
服务器
(EPID)
1002
1022
区块链
通知
1024
1000

图10

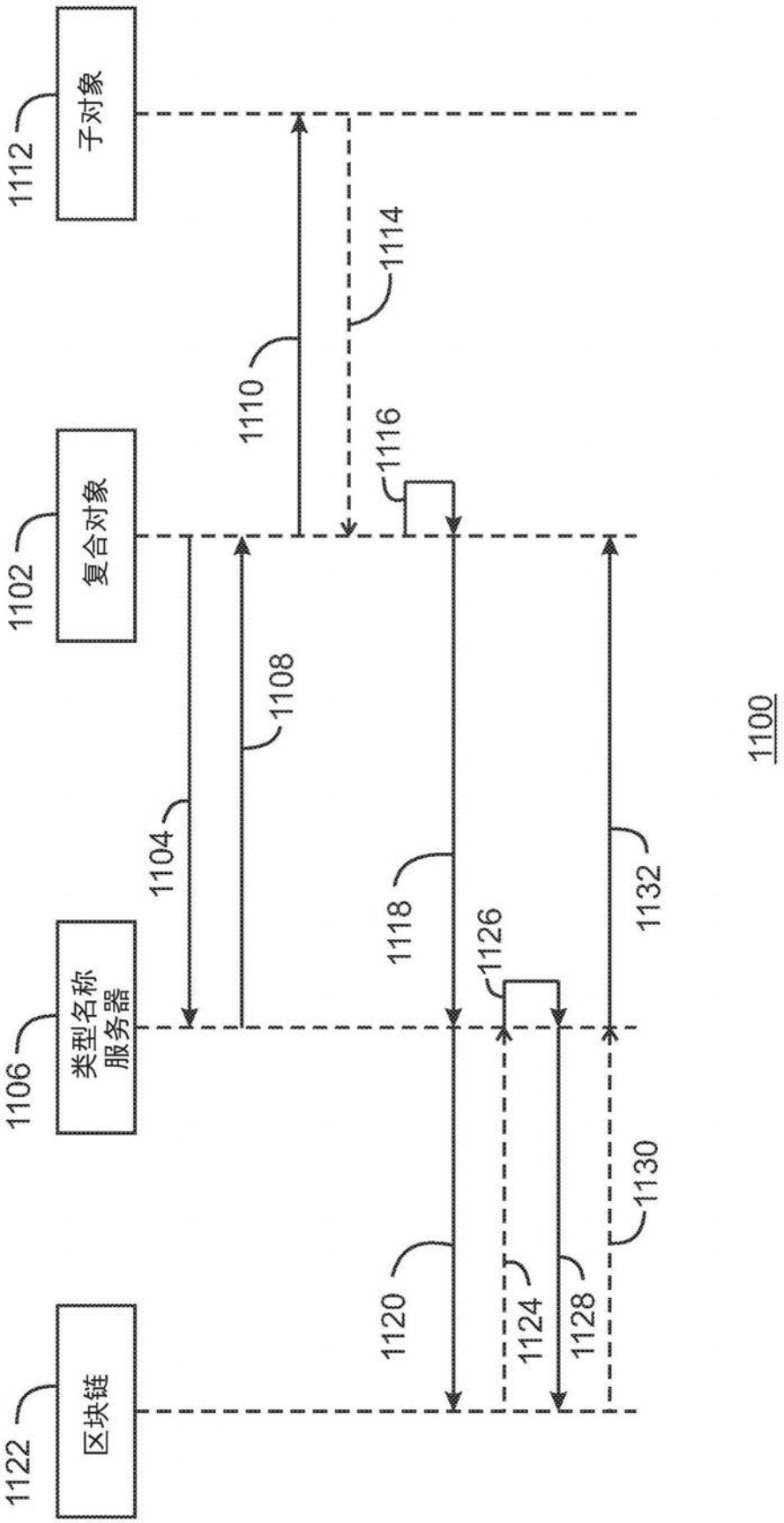

1112
子对象
1114
1110
1116
1102
复合对象
1108
1100
1104
1118
1126
1132
1106
类型名称
服务器
1130
1120
1124
1128
1122
区块链

图11

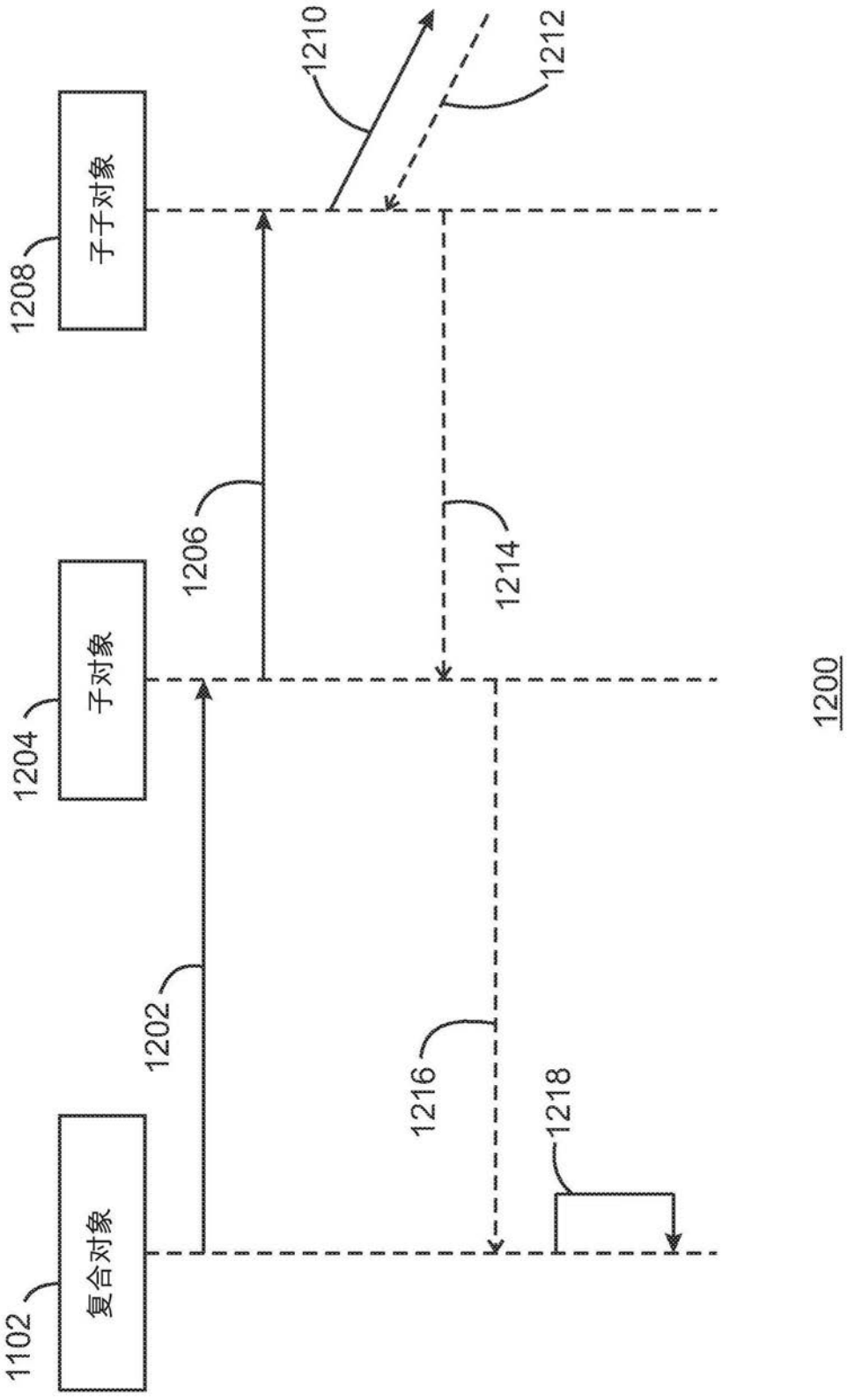

1210
1212
子子对象
1208
1206
1214
子对象
1204
1200
1202
1216
1218
复合对象
1102

图12

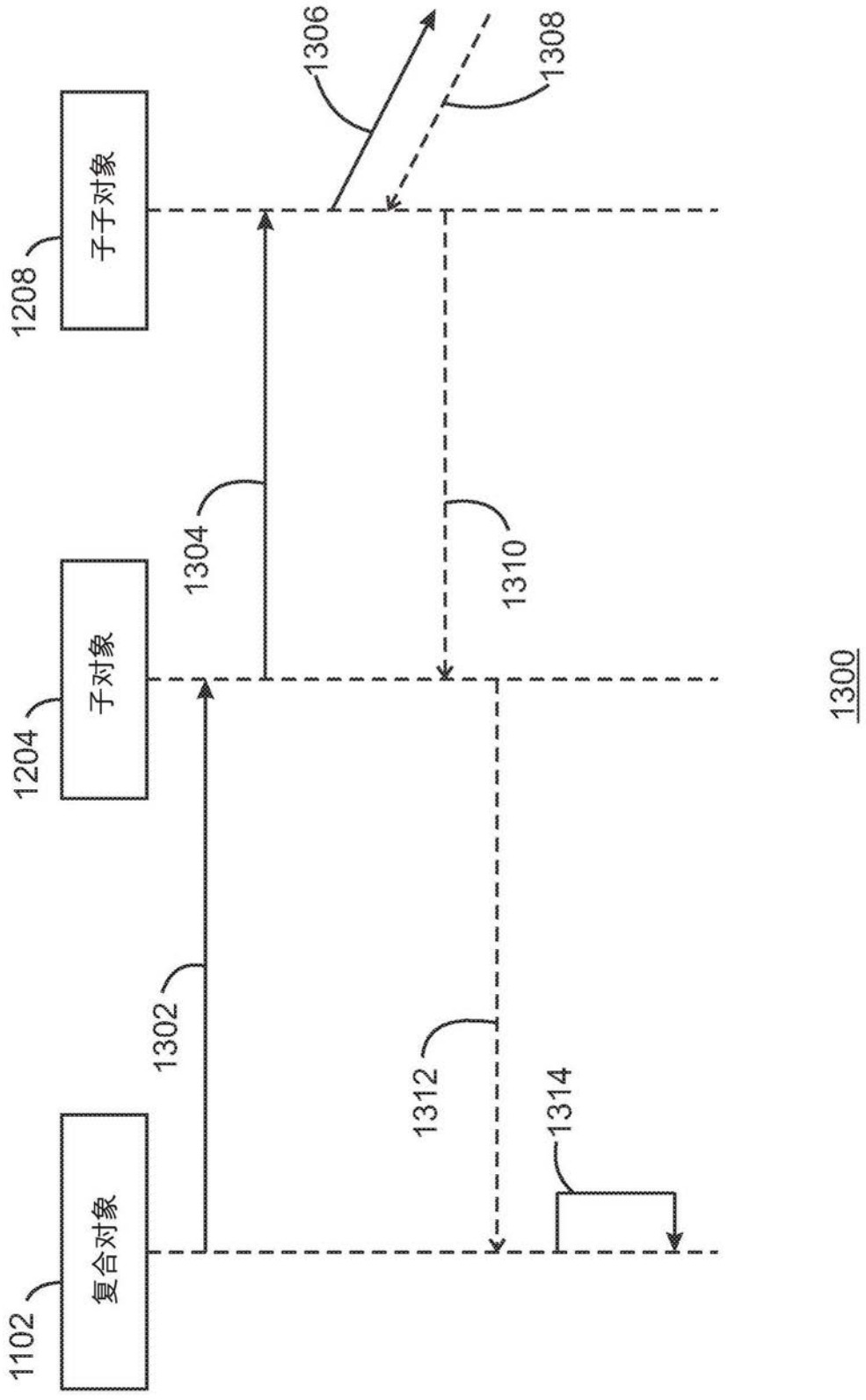

1306
1308
子子对象
1208
1304
1310
子对象
1204
1300
1302
1312
1314
复合对象
1102

图13

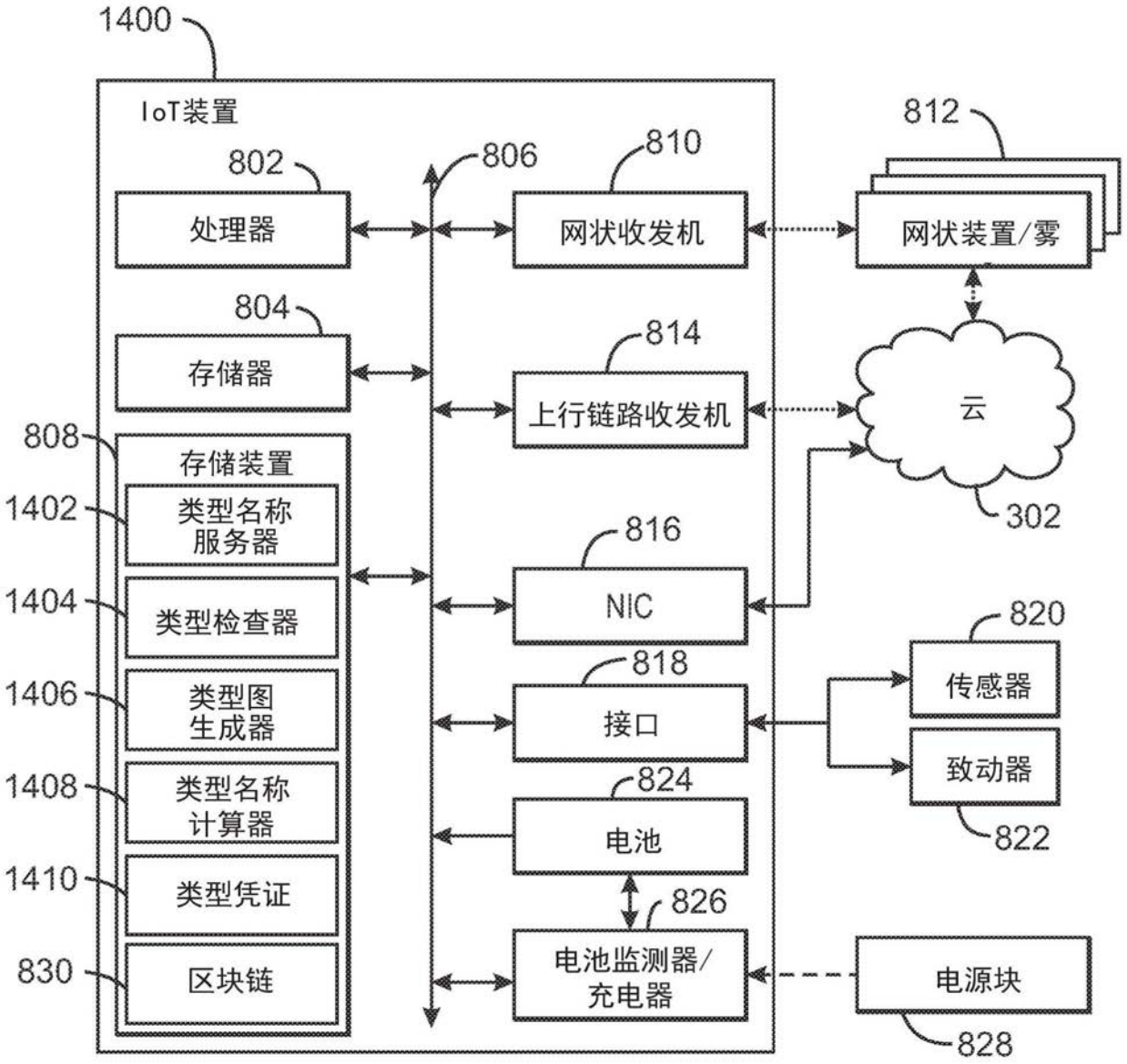

1400
IoT装置
802
处理器
806
810
网状收发机
812
网状装置/雾
804
存储器
814
上行链路收发机
云
302
808
存储装置
1402
类型名称服务器
1404
类型检查器
1406
类型图生成器
1408
类型名称计算器
1410
类型凭证
830
区块链
816
NIC
818
接口
820
传感器
致动器
822
824
电池
826
电池监测器/充电器
电源块
828

图14

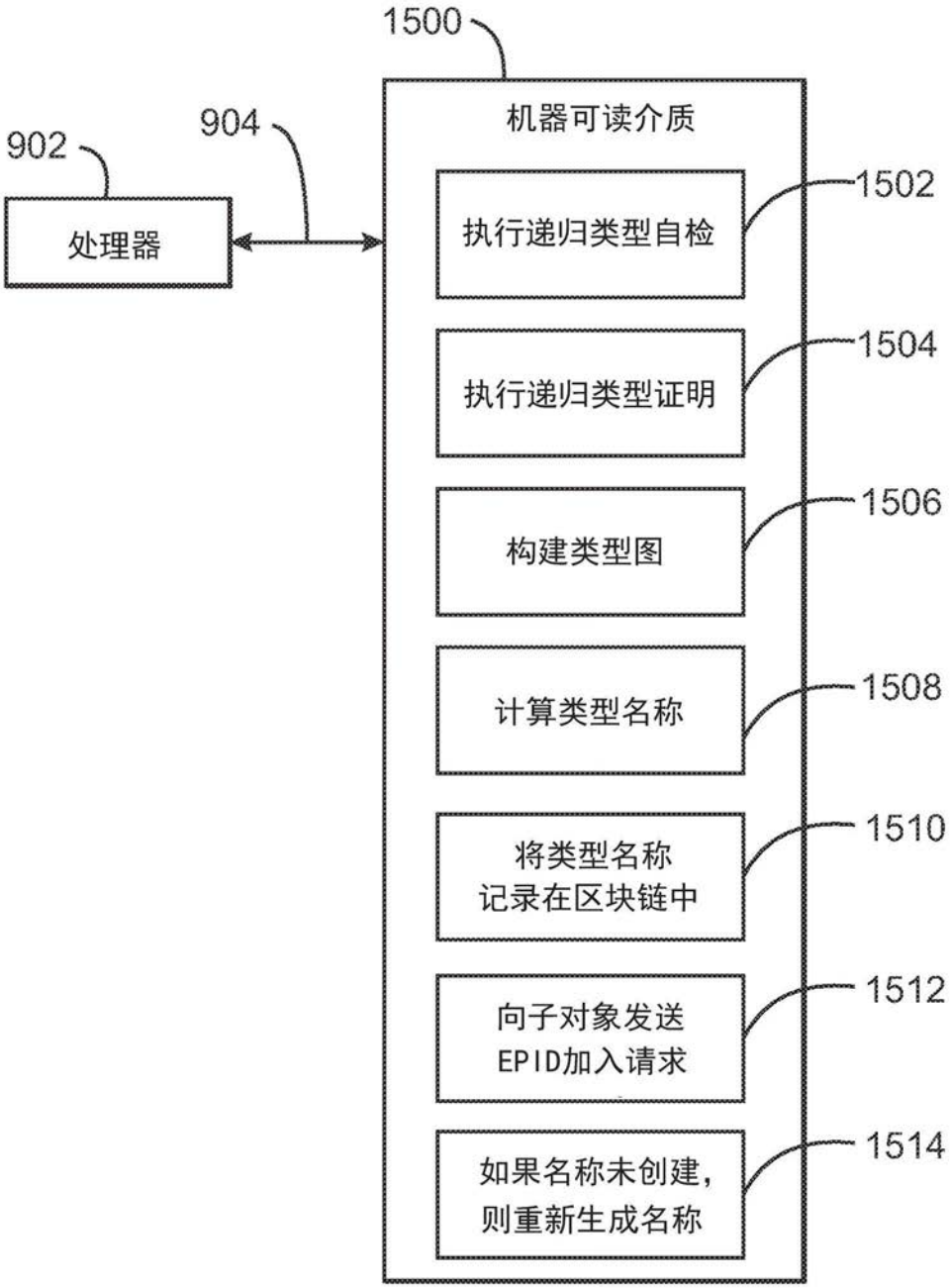

1500
机器可读介质
902
处理器
904
执行递归类型自检
1502
执行递归类型证明
1504
构建类型图
1506
计算类型名称
1508
将类型名称
记录在区块链中
1510
向子对象发送
EPID加入请求
1512
如果名称未创建，
则重新生成名称
1514

图15

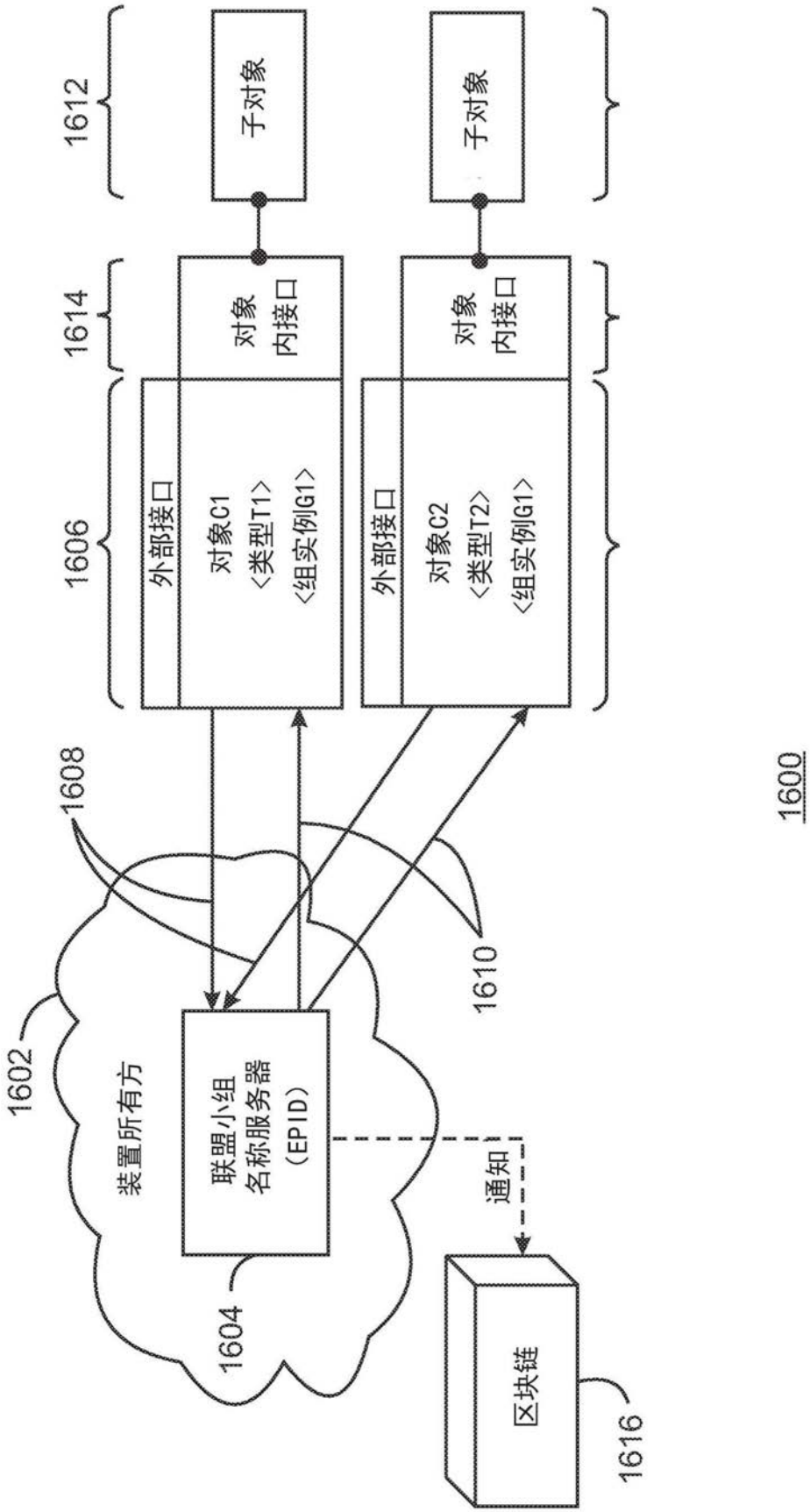

1612
子对象
子对象
1614
对象
内接口
对象
内接口
1606
外部接口
对象C1
<类型T1>
<组实例G1>
外部接口
对象C2
<类型T2>
<组实例G1>
1608
1610
1600
1602
装置所有方
联盟小组
名称服务器
(EPID)
通知
1604
区块链
1616

图16

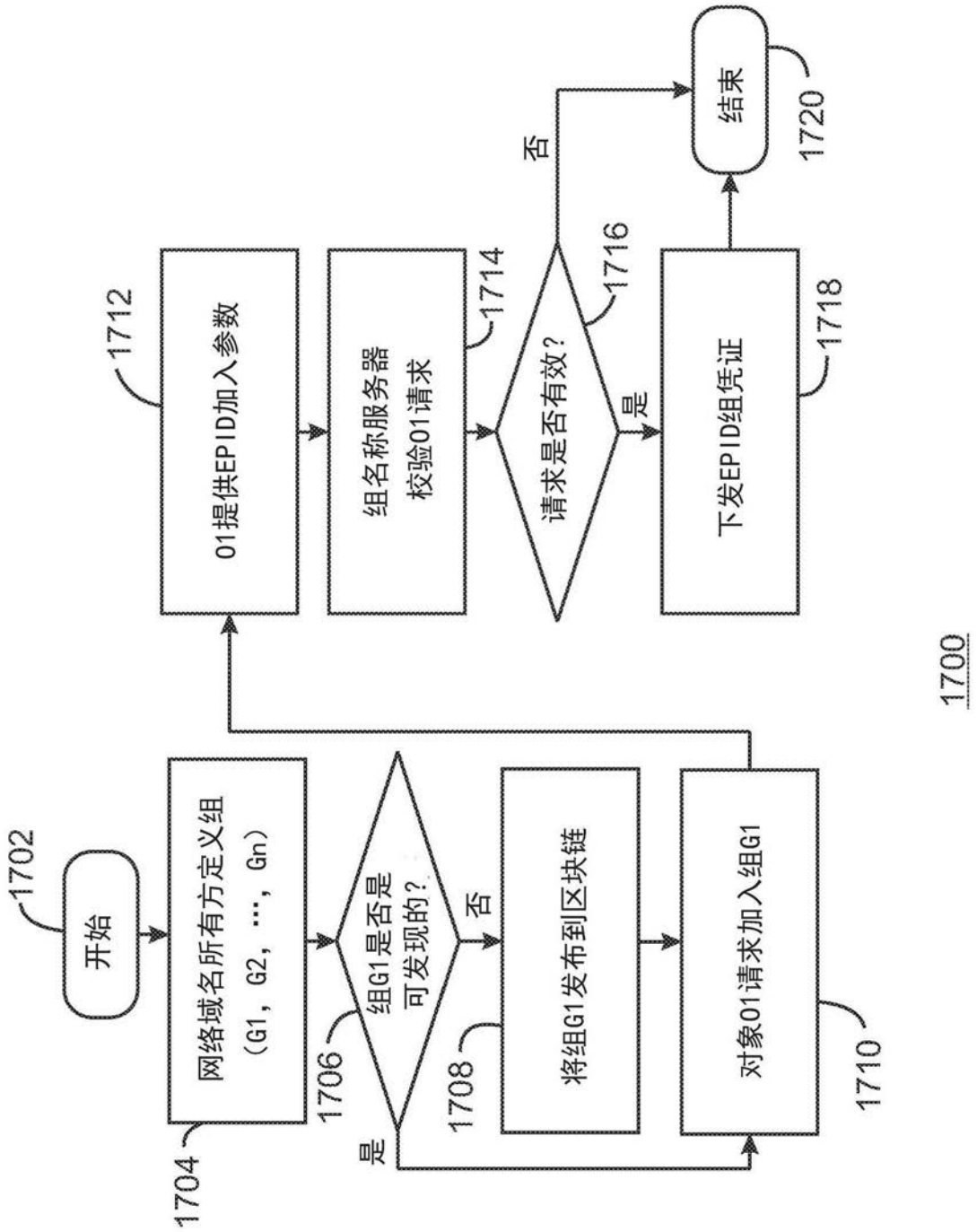

开始
1702
网络域名所有方定义组
（G1，G2，…，Gn）
1704
组G1是否是
可发现的?
1706
是
否
将组G1发布到区块链
1708
对象01请求加入组G1
1710
01提供EPID加入参数
1712
组名称服务器
校验01请求
1714
请求是否有效?
1716
否
是
下发EPID组凭证
1718
结束
1720
1700

图17

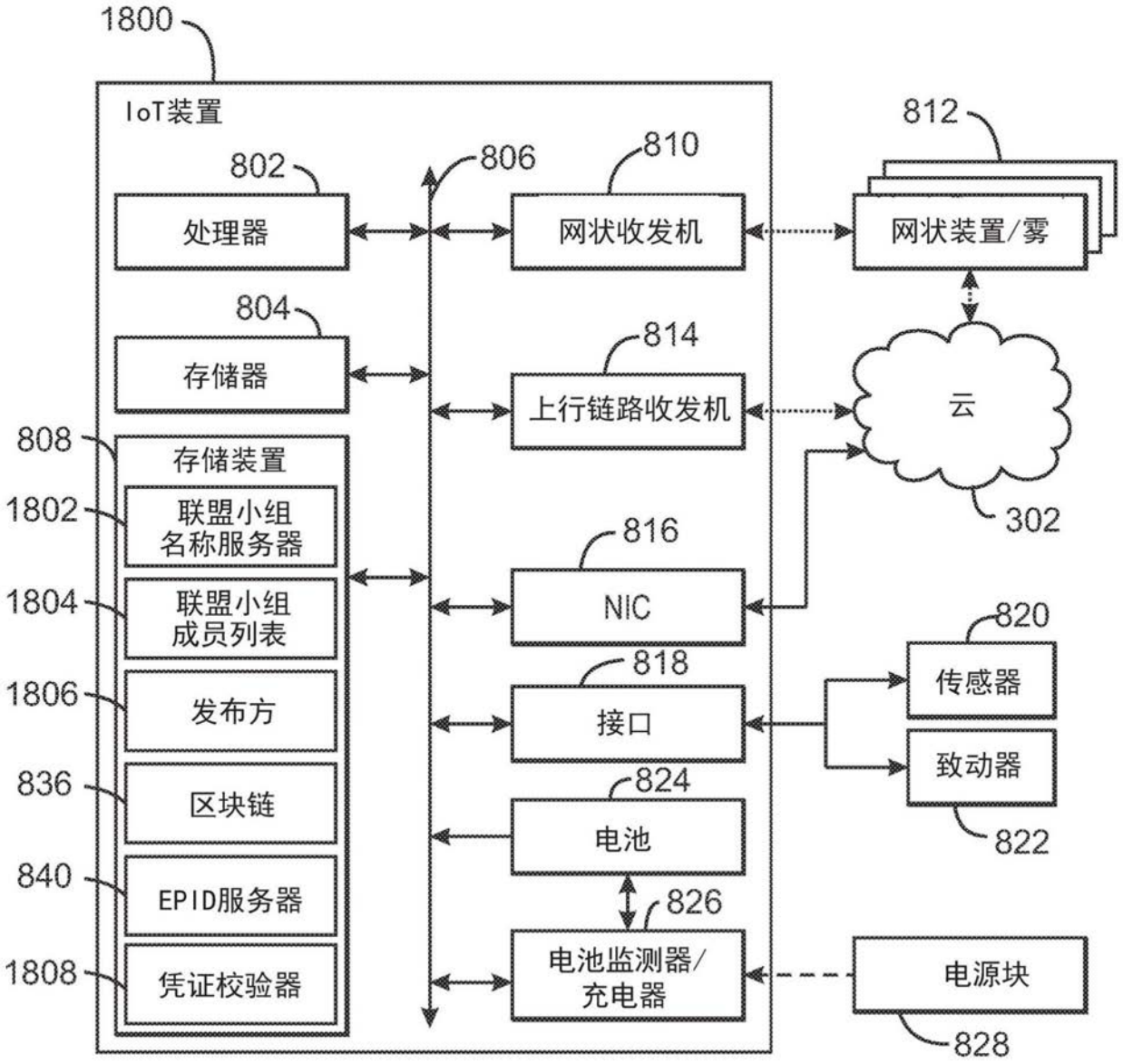

1800
IoT装置
802
处理器
804
存储器
808
存储装置
1802
联盟小组
名称服务器
1804
联盟小组
成员列表
1806
发布方
836
区块链
840
EPID服务器
1808
凭证校验器
806
810
网状收发机
814
上行链路收发机
816
NIC
818
接口
824
电池
826
电池监测器/
充电器
812
网状装置/雾
云
302
820
传感器
致动器
822
电源块
828

图18

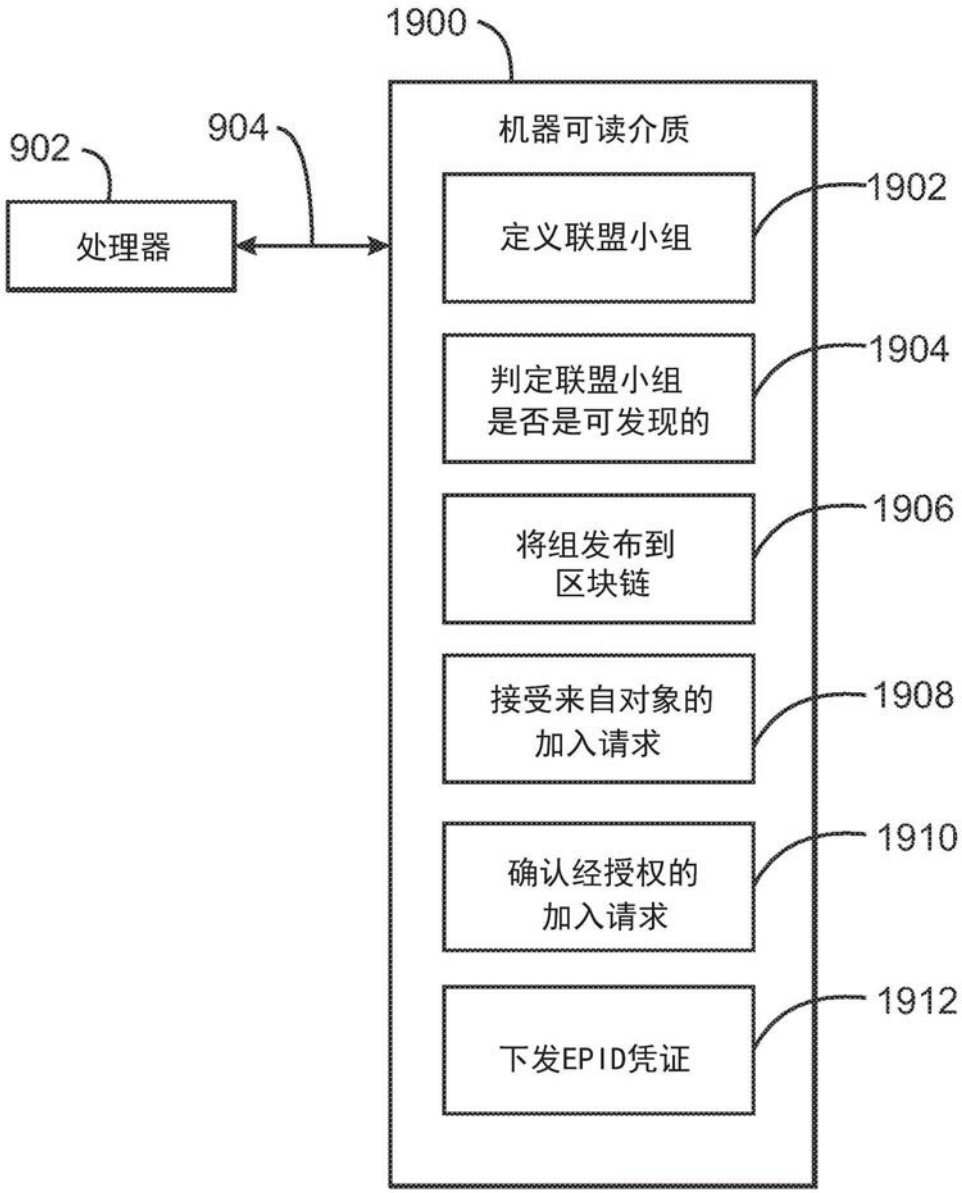

1900
机器可读介质
902
处理器
904
定义联盟小组
1902
判定联盟小组
是否是可发现的
1904
将组发布到
区块链
1906
接受来自对象的
加入请求
1908
确认经授权的
加入请求
1910
下发EPID凭证
1912

图19

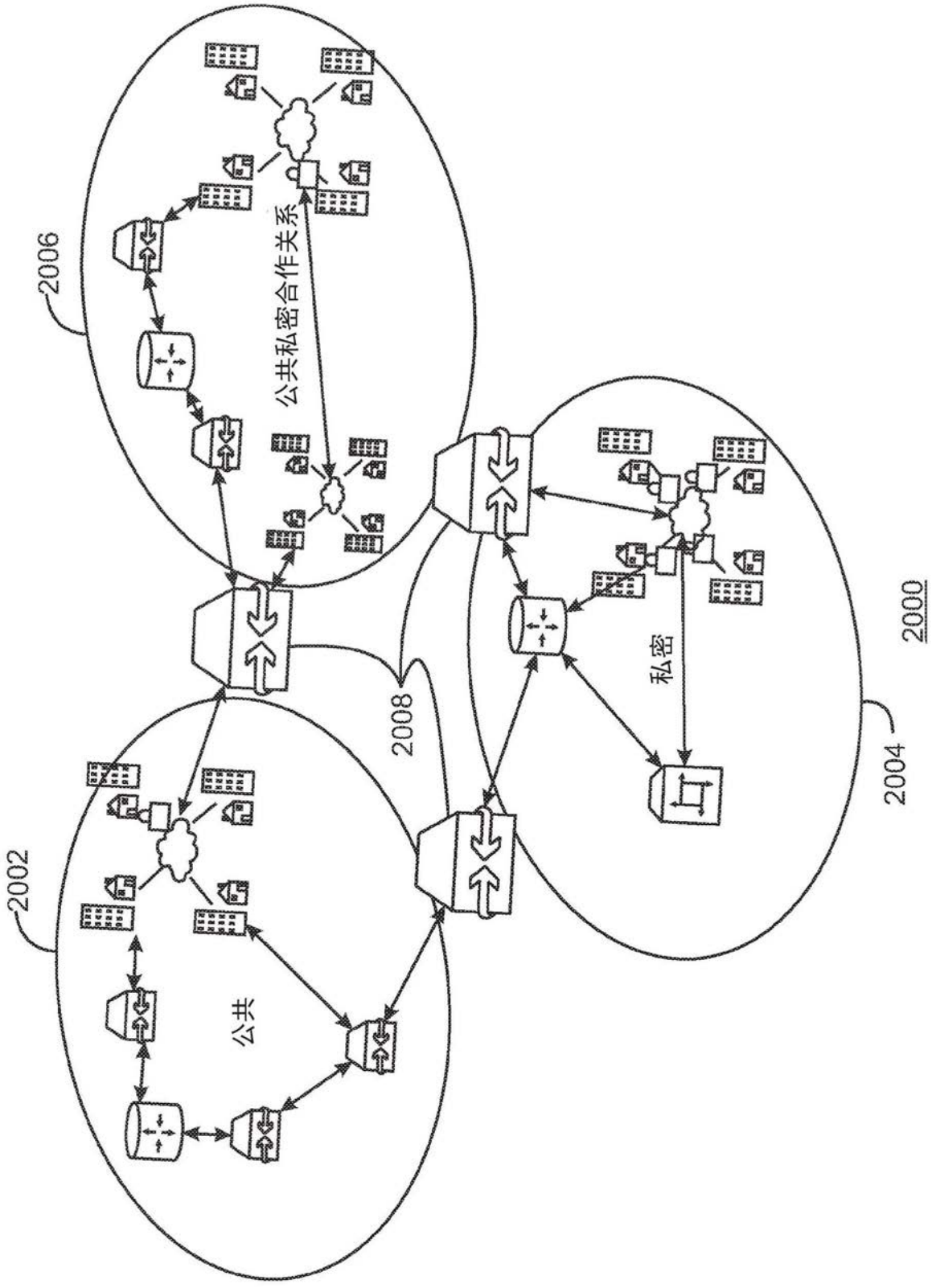


图20

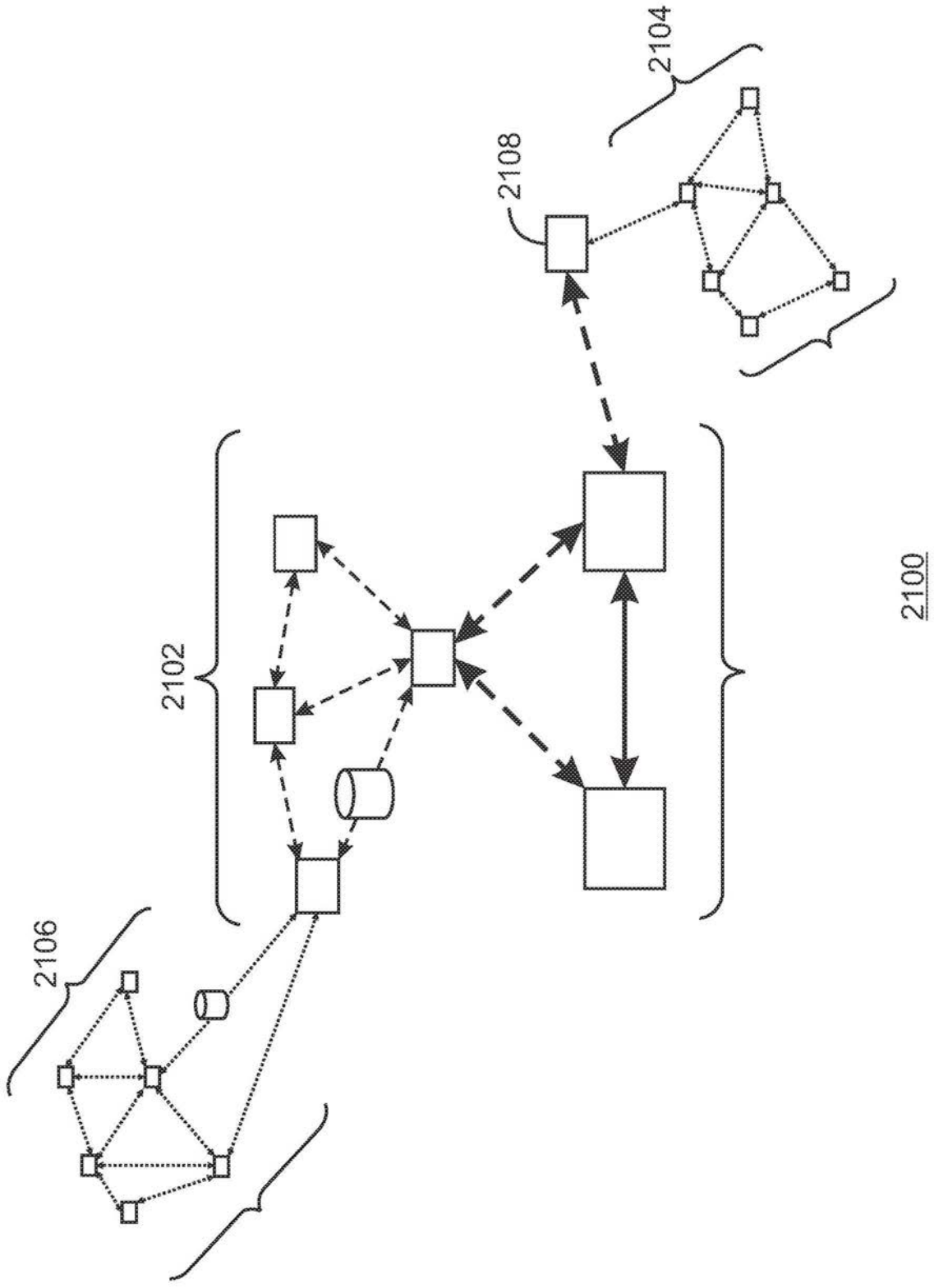
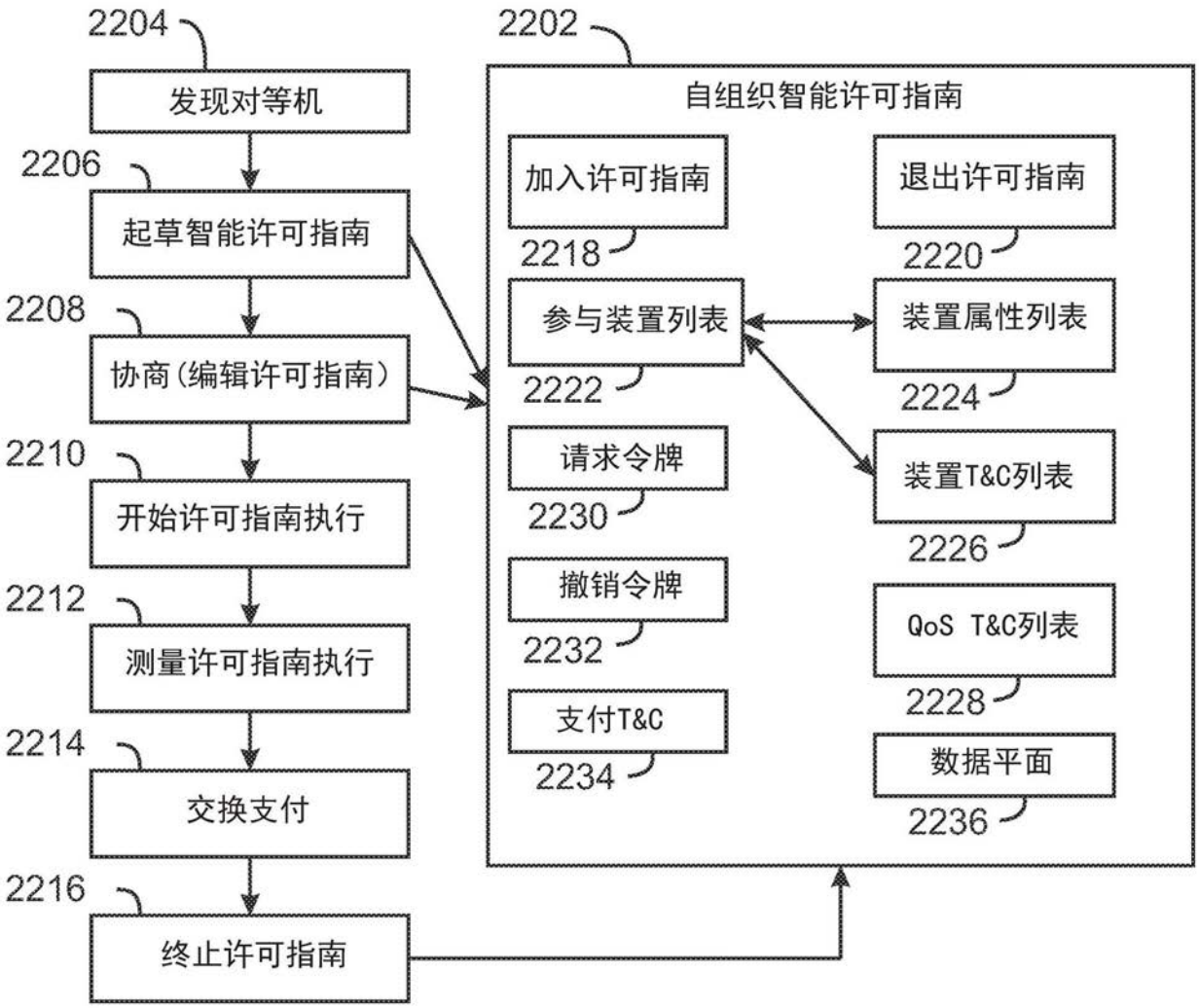


图21


2204
发现对等机
2206
起草智能许可指南
2208
协商(编辑许可指南)
2210
开始许可指南执行
2212
测量许可指南执行
2214
交换支付
2216
终止许可指南
2202
自组织智能许可指南
加入许可指南
2218
退出许可指南
2220
参与装置列表
2222
装置属性列表
2224
请求令牌
2230
装置T&C列表
2226
撤销令牌
2232
QoS T&C列表
2228
支付T&C
2234
数据平面
2236

2200

图22

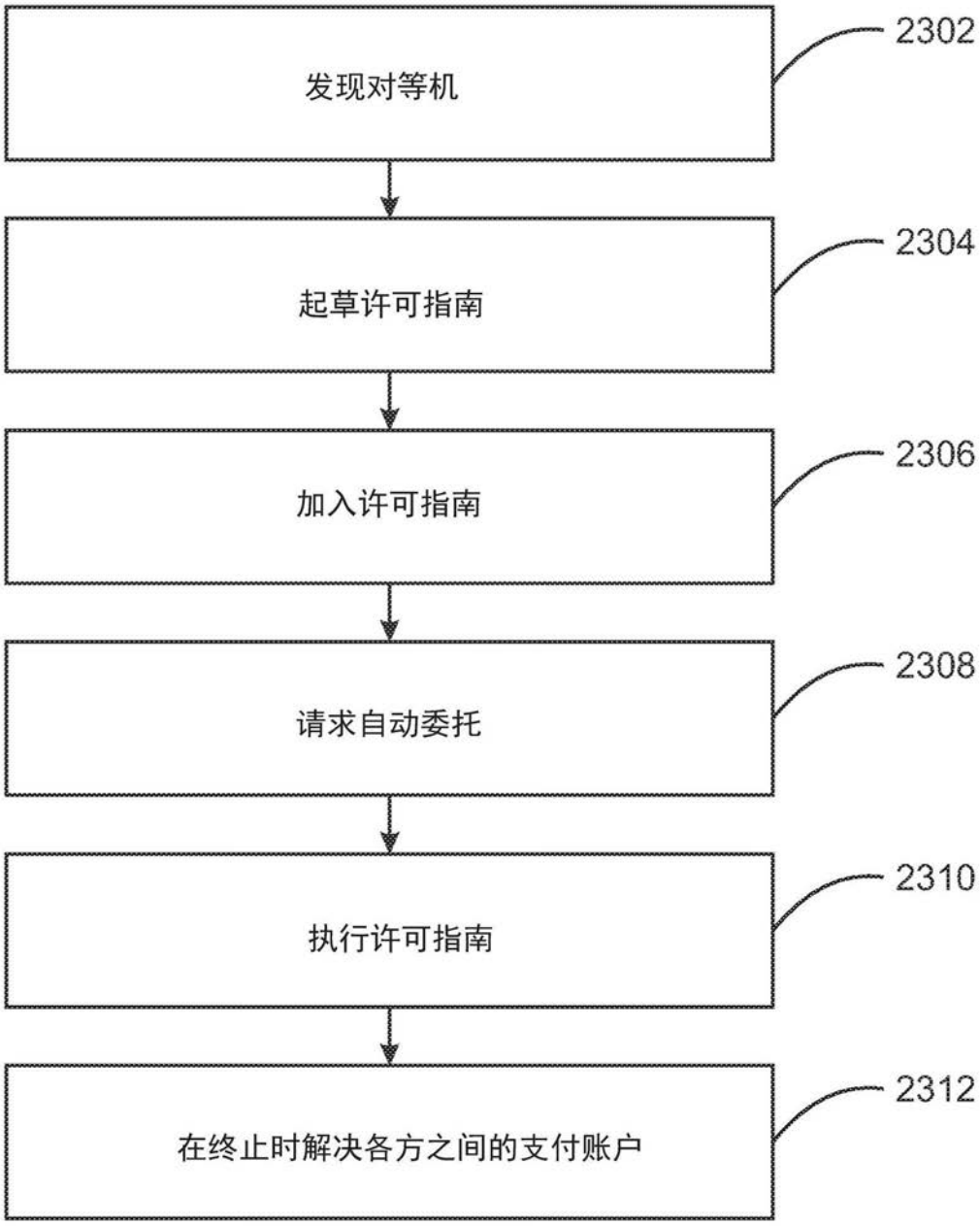

发现对等机
2302
起草许可指南
2304
加入许可指南
2306
请求自动委托
2308
执行许可指南
2310
在终止时解决各方之间的支付账户
2312
2300

图23

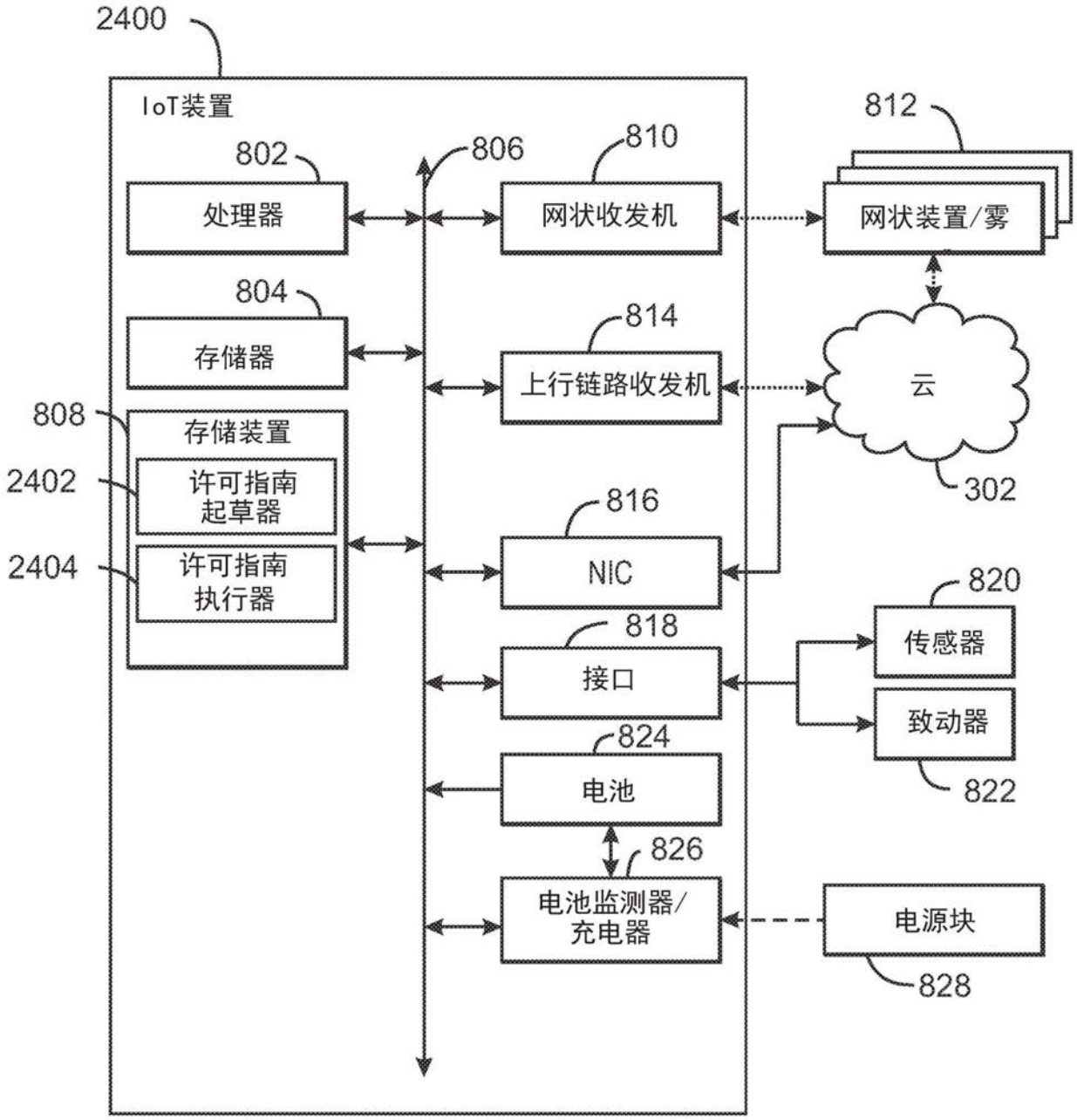

2400
IoT装置
802
处理器
804
存储器
808
存储装置
2402
许可指南
起草器
2404
许可指南
执行器
806
810
网状收发机
814
上行链路收发机
816
NIC
818
接口
824
电池
826
电池监测器/
充电器
812
网状装置/雾
云
302
820
传感器
致动器
822
电源块
828

图24

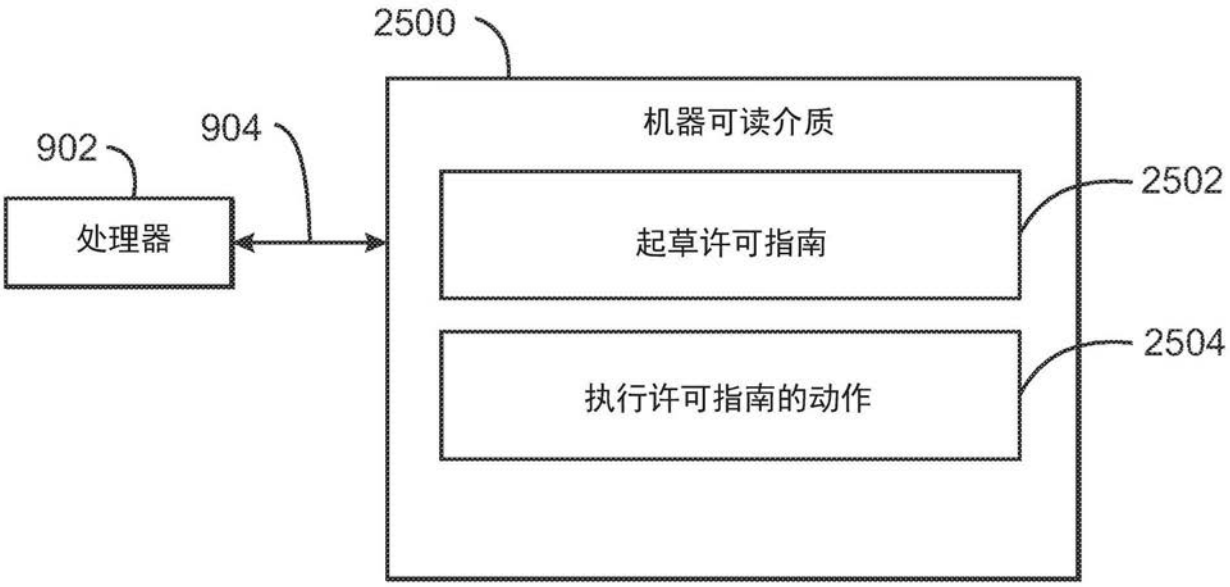

2500
机器可读介质
902
处理器
904
2502
起草许可指南
2504
执行许可指南的动作

图25

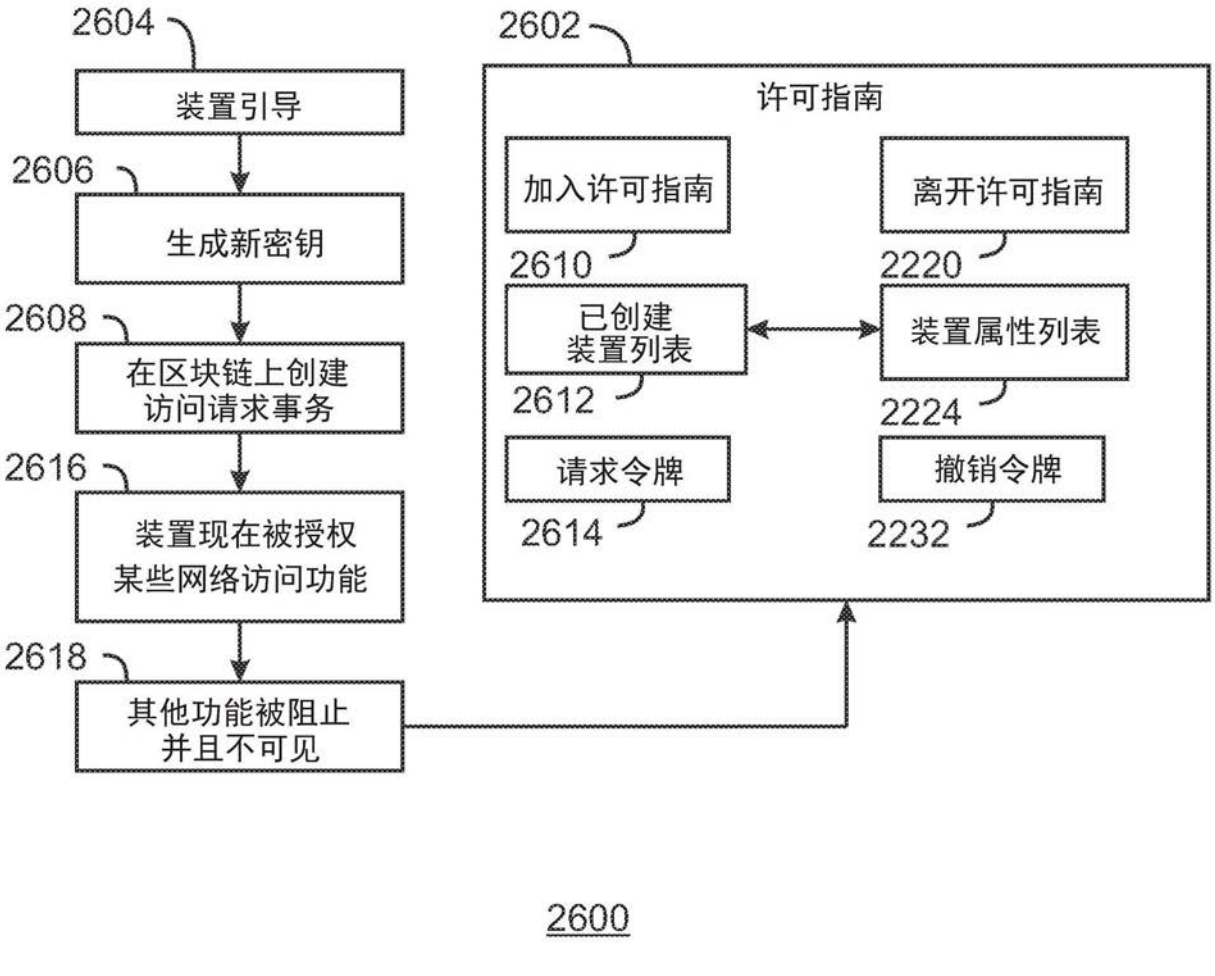

2604
装置引导
2606
生成新密钥
2608
在区块链上创建
访问请求事务
2616
装置现在被授权
某些网络访问功能
2618
其他功能被阻止
并且不可见
2602
许可指南
加入许可指南
2610
离开许可指南
2220
已创建
装置列表
2612
装置属性列表
2224
请求令牌
2614
撤销令牌
2232
2600

图26

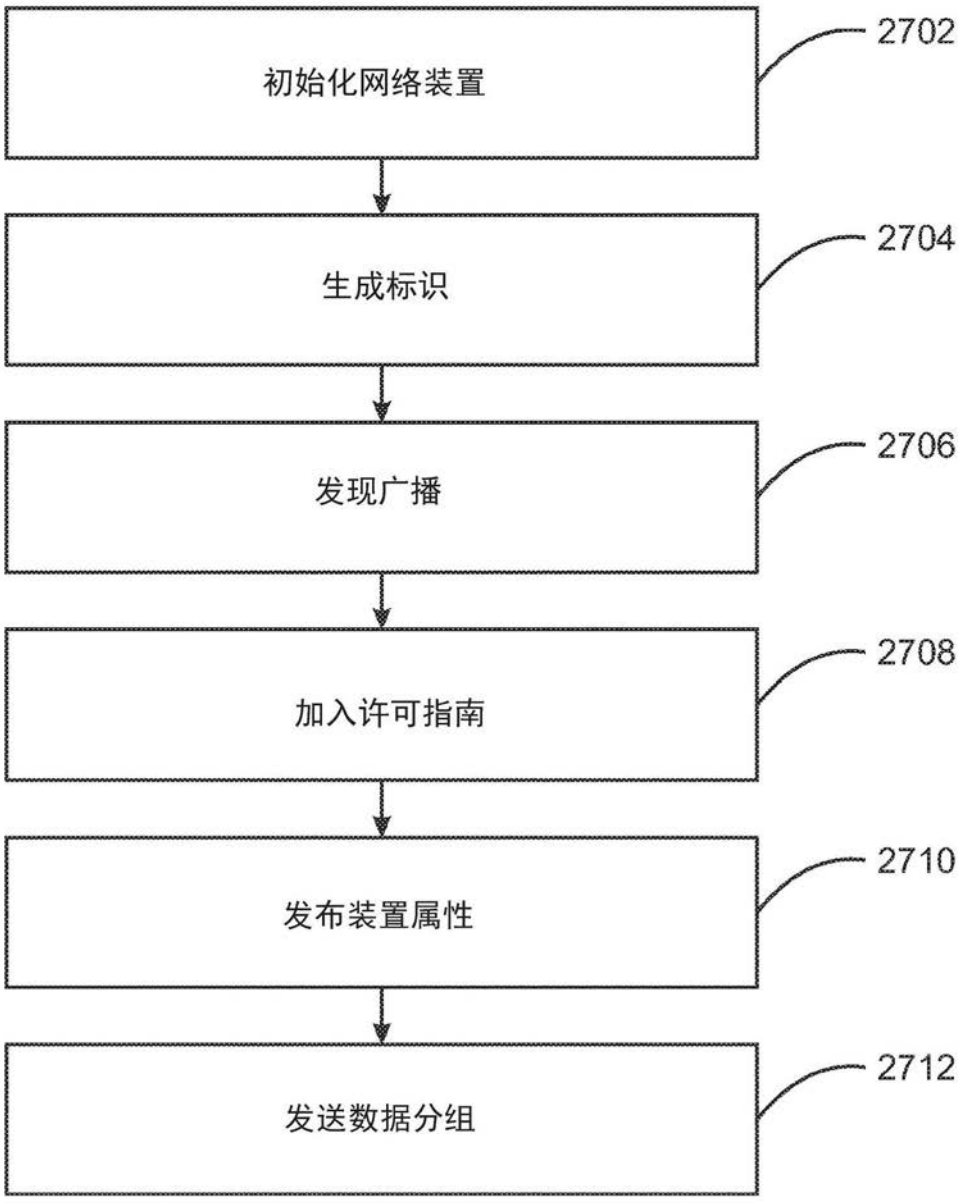

初始化网络装置
2702
生成标识
2704
发现广播
2706
加入许可指南
2708
发布装置属性
2710
发送数据分组
2712
2700

图27

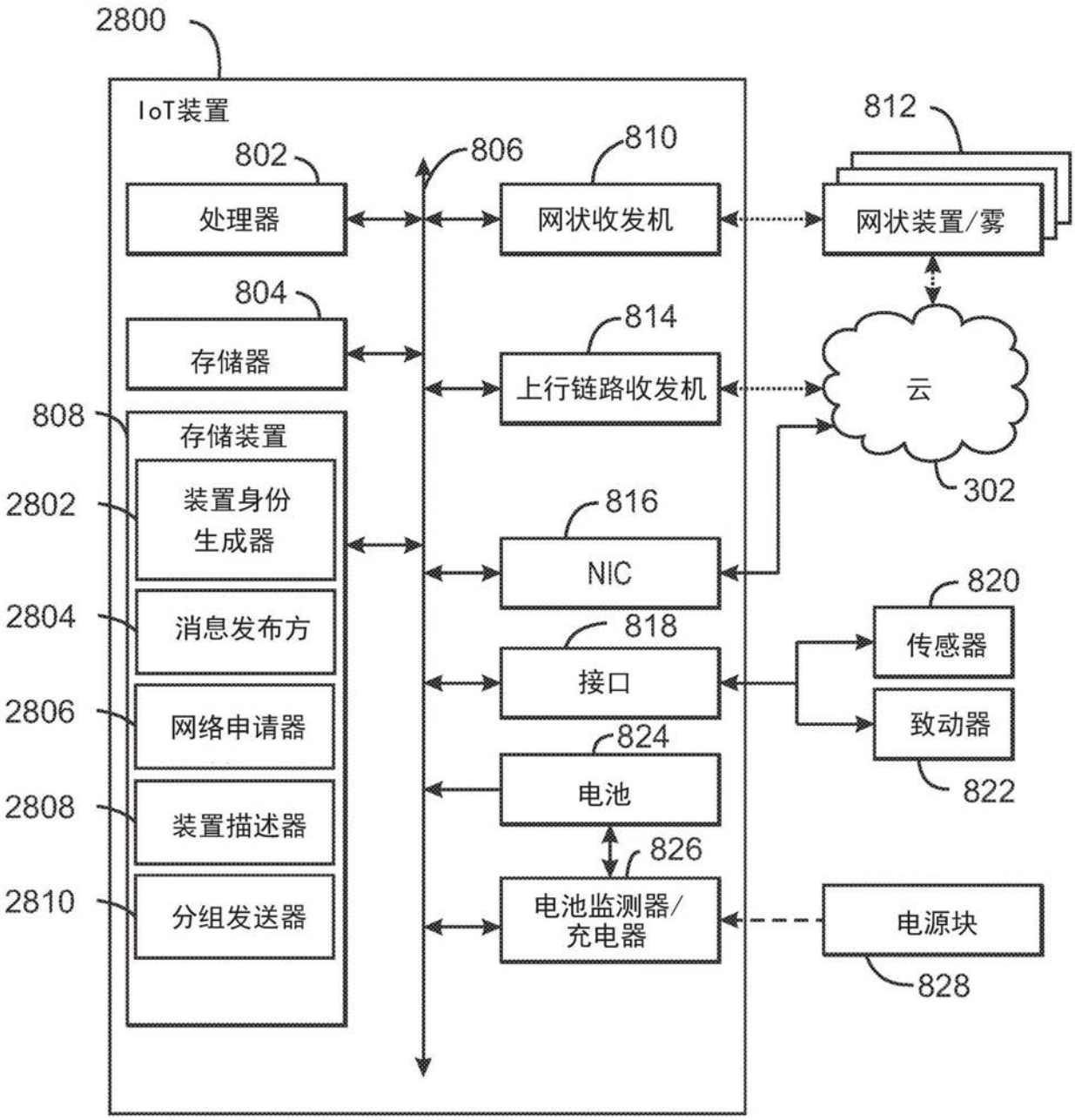

2800
IoT装置
802
处理器
804
存储器
808
存储装置
2802
装置身份
生成器
2804
消息发布方
2806
网络申请器
2808
装置描述器
2810
分组发送器
806
810
网状收发机
814
上行链路收发机
816
NIC
818
接口
824
电池
826
电池监测器/
充电器
812
网状装置/雾
云
302
820
传感器
致动器
822
电源块
828

图28

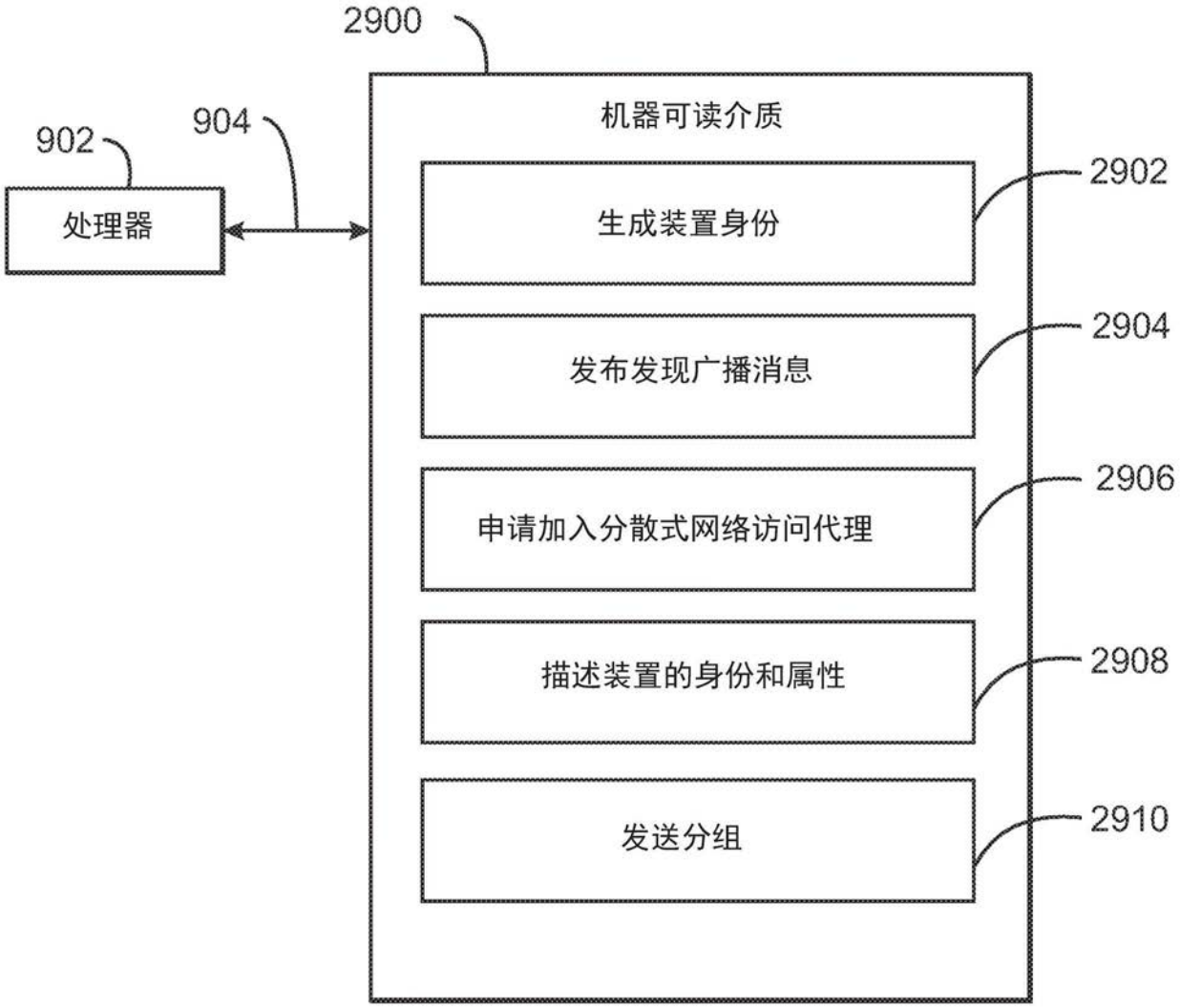

2900
机器可读介质
902
904
处理器
生成装置身份
2902
发布发现广播消息
2904
申请加入分散式网络访问代理
2906
描述装置的身份和属性
2908
发送分组
2910

图29

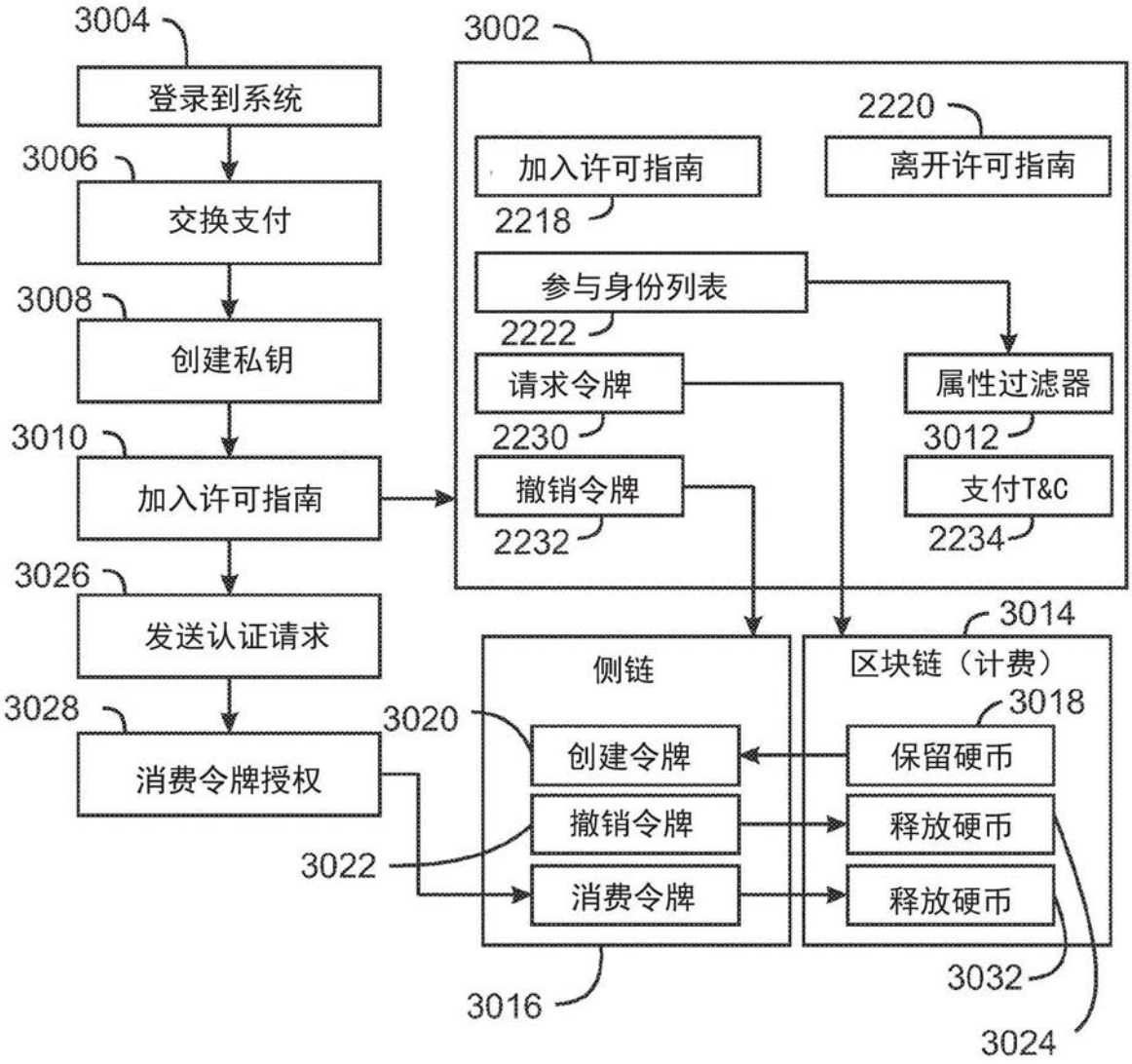

3004
登录到系统
3006
交换支付
3008
创建私钥
3010
加入许可指南
3026
发送认证请求
3028
消费令牌授权
3002
2220
加入许可指南
离开许可指南
2218
参与身份列表
2222
请求令牌
属性过滤器
2230
3012
撤销令牌
支付T&C
2232
2234
3014
侧链
区块链（计费）
3018
3020
创建令牌
保留硬币
撤销令牌
释放硬币
3022
消费令牌
释放硬币
3016
3032
3024
3000

图30

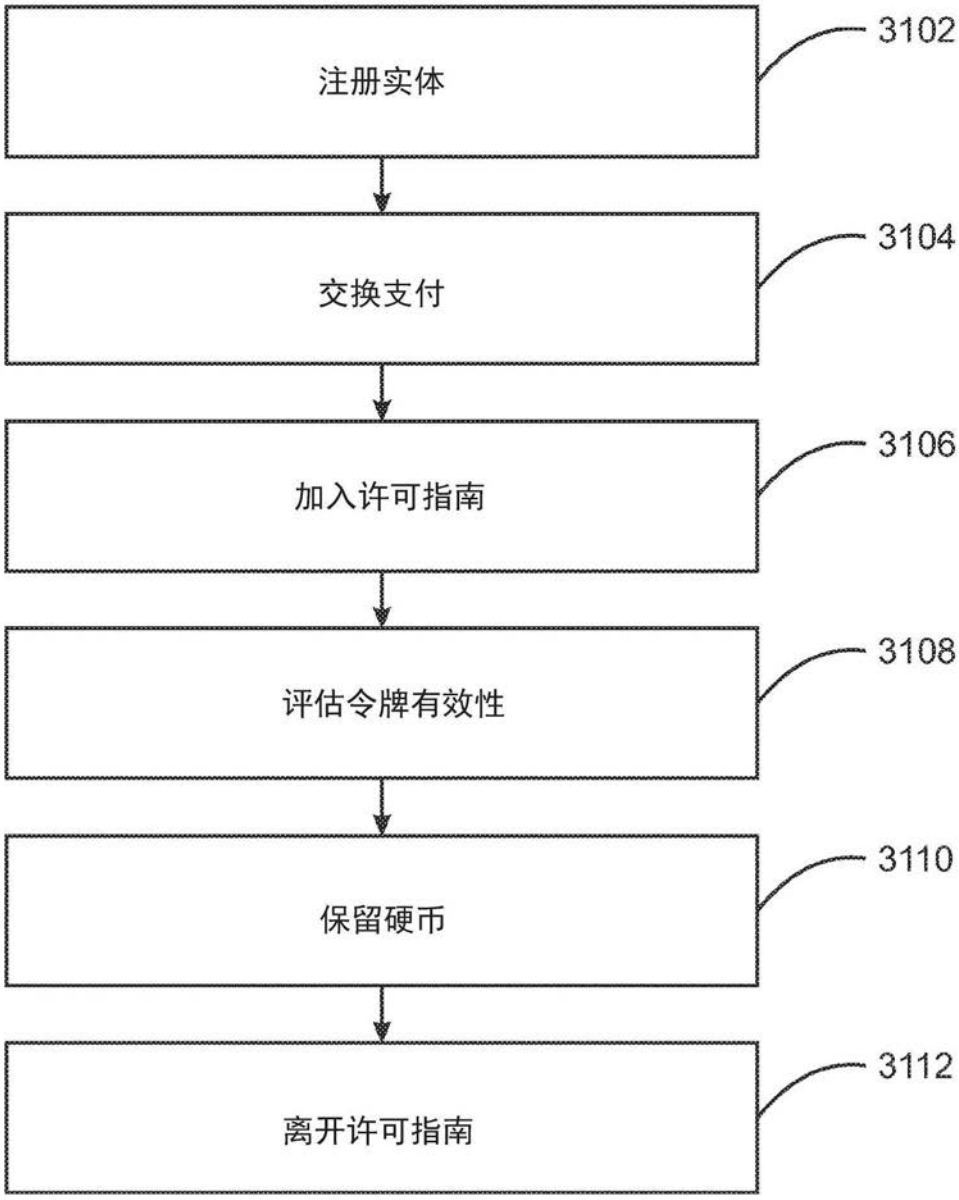

注册实体
3102
交换支付
3104
加入许可指南
3106
评估令牌有效性
3108
保留硬币
3110
离开许可指南
3112
3100

图31

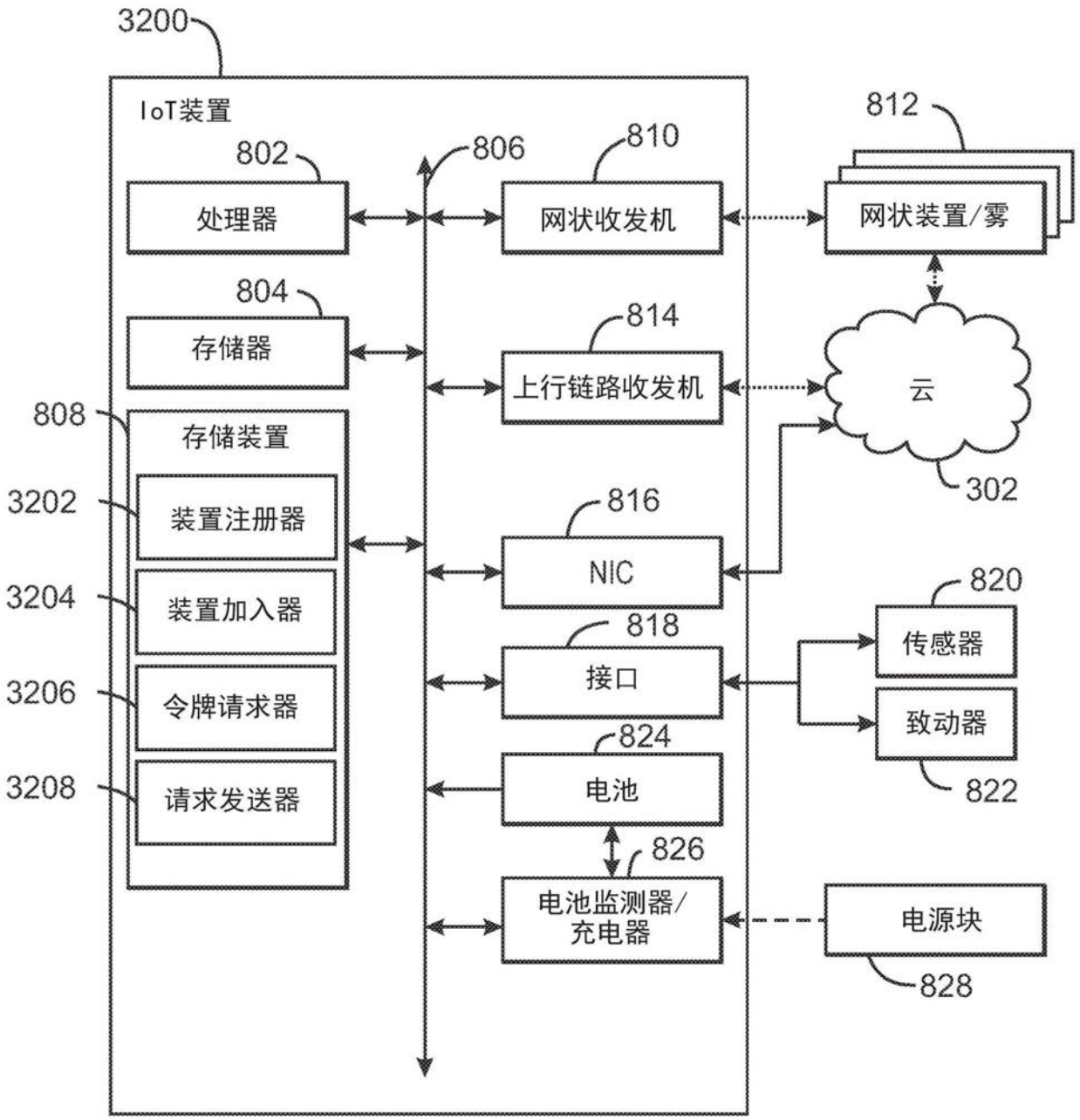

3200
IoT装置
802
处理器
804
存储器
808
存储装置
3202
装置注册器
3204
装置加入器
3206
令牌请求器
3208
请求发送器
806
810
网状收发机
814
上行链路收发机
816
NIC
818
接口
824
电池
826
电池监测器/
充电器
812
网状装置/雾
云
302
820
传感器
致动器
822
电源块
828

图32

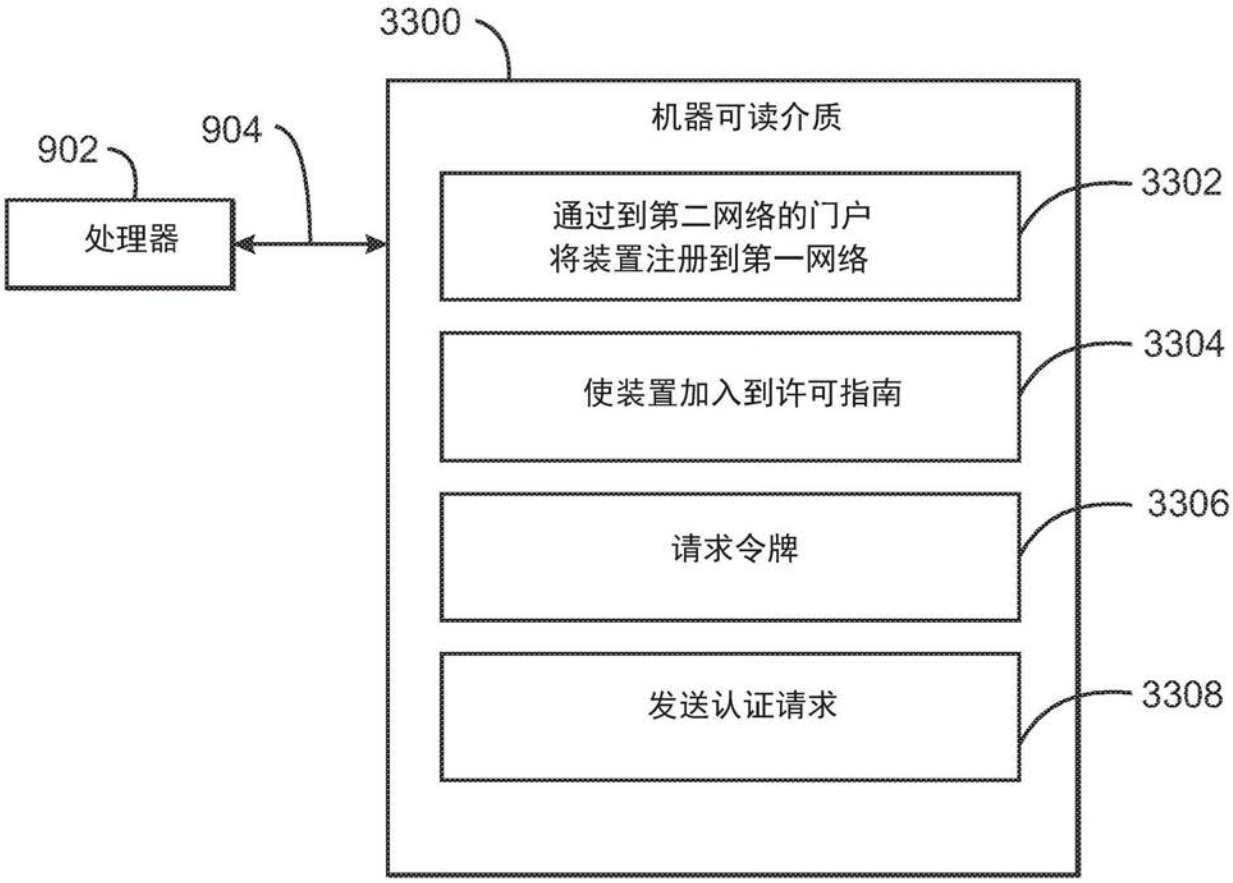

3300
机器可读介质
902
904
处理器
通过到第二网络的门户
将装置注册到第一网络
3302
使装置加入到许可指南
3304
请求令牌
3306
发送认证请求
3308

图33

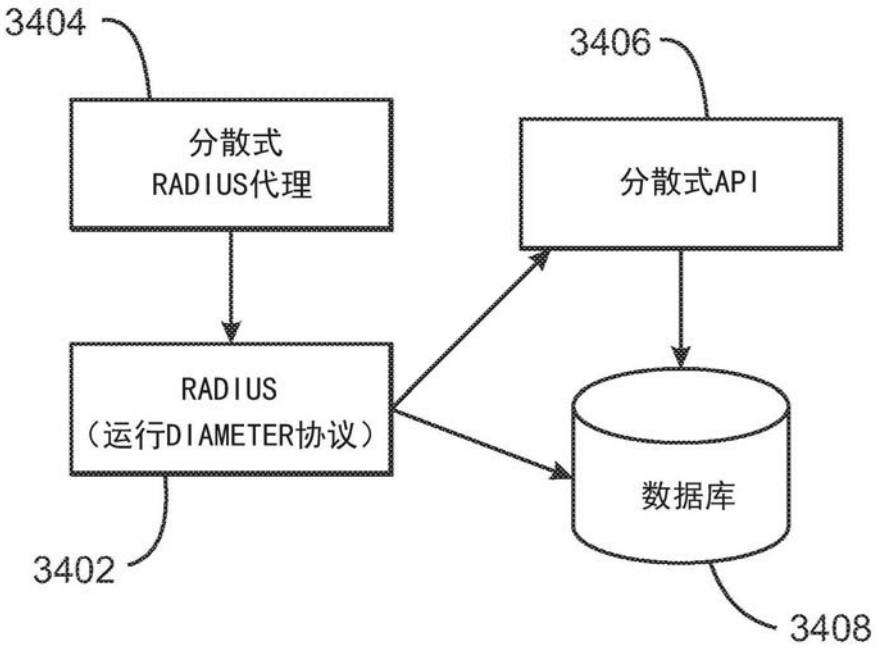
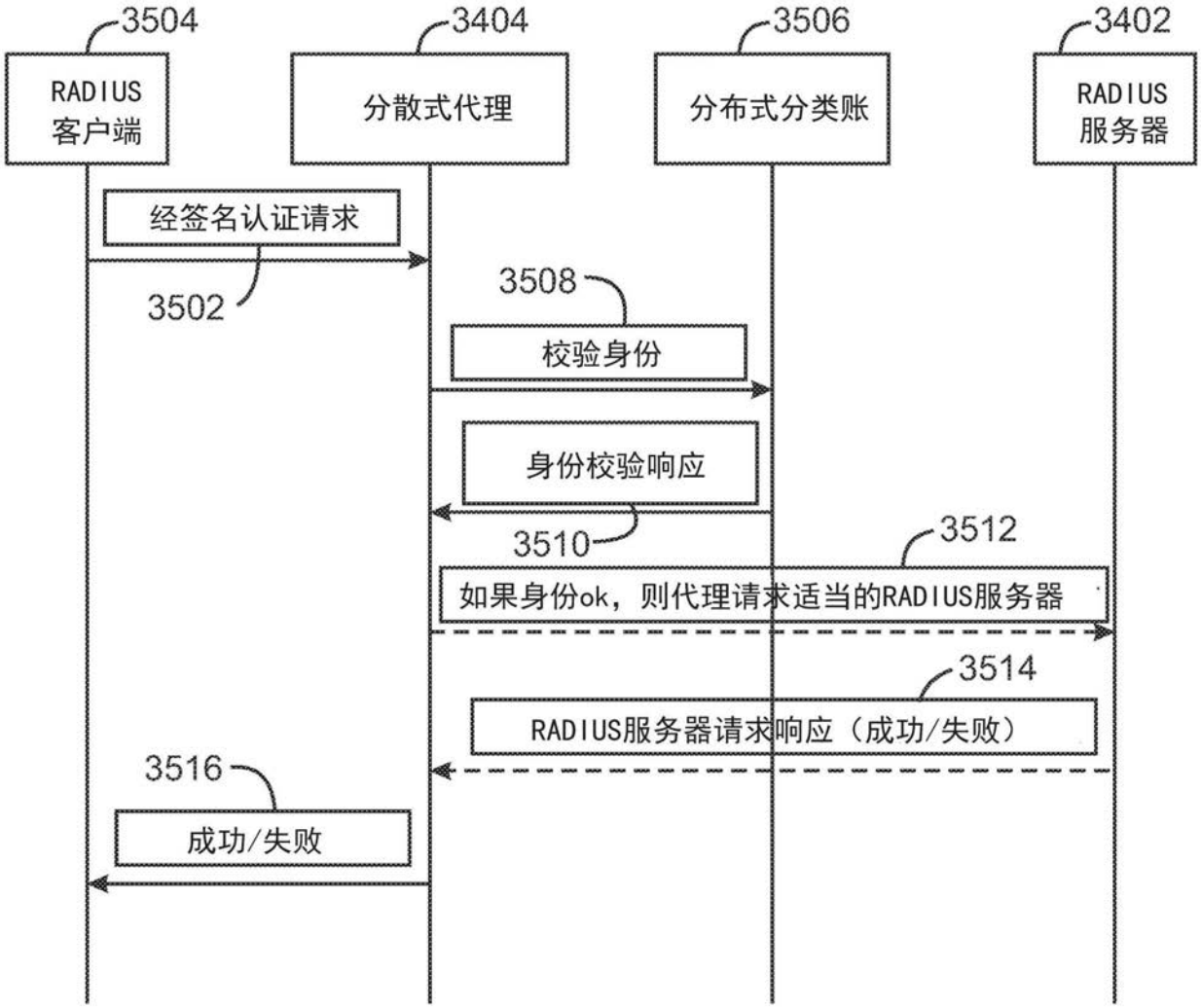
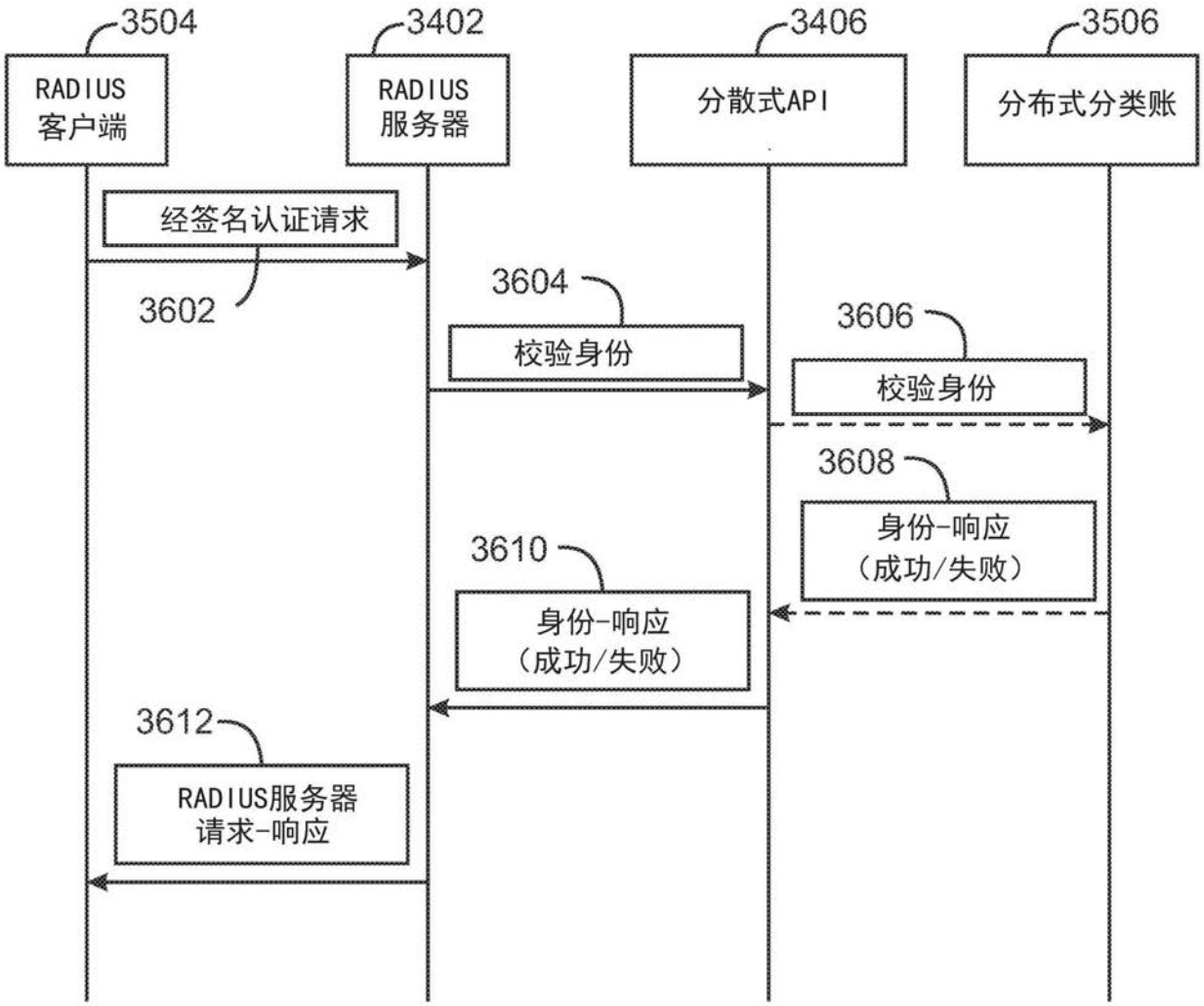

3404
分散式
RADIUS代理
3406
分散式API
RADIUS
（运行DIAMETER协议）
数据库
3402
3408
3400

图34


3504
RADIUS
客户端
3404
分散式代理
3506
分布式分类账
3402
RADIUS
服务器
经签名认证请求
3502
3508
校验身份
身份校验响应
3510
3512
如果身份ok，则代理请求适当的RADIUS服务器
3514
RADIUS服务器请求响应（成功/失败）
3516
成功/失败

3500

图35


3504
RADIUS
客户端
3402
RADIUS
服务器
3406
分散式API
3506
分布式分类账
经签名认证请求
3602
3604
校验身份
3606
校验身份
3608
身份-响应
（成功/失败）
3610
身份-响应
（成功/失败）
3612
RADIUS服务器
请求-响应

3600

图36

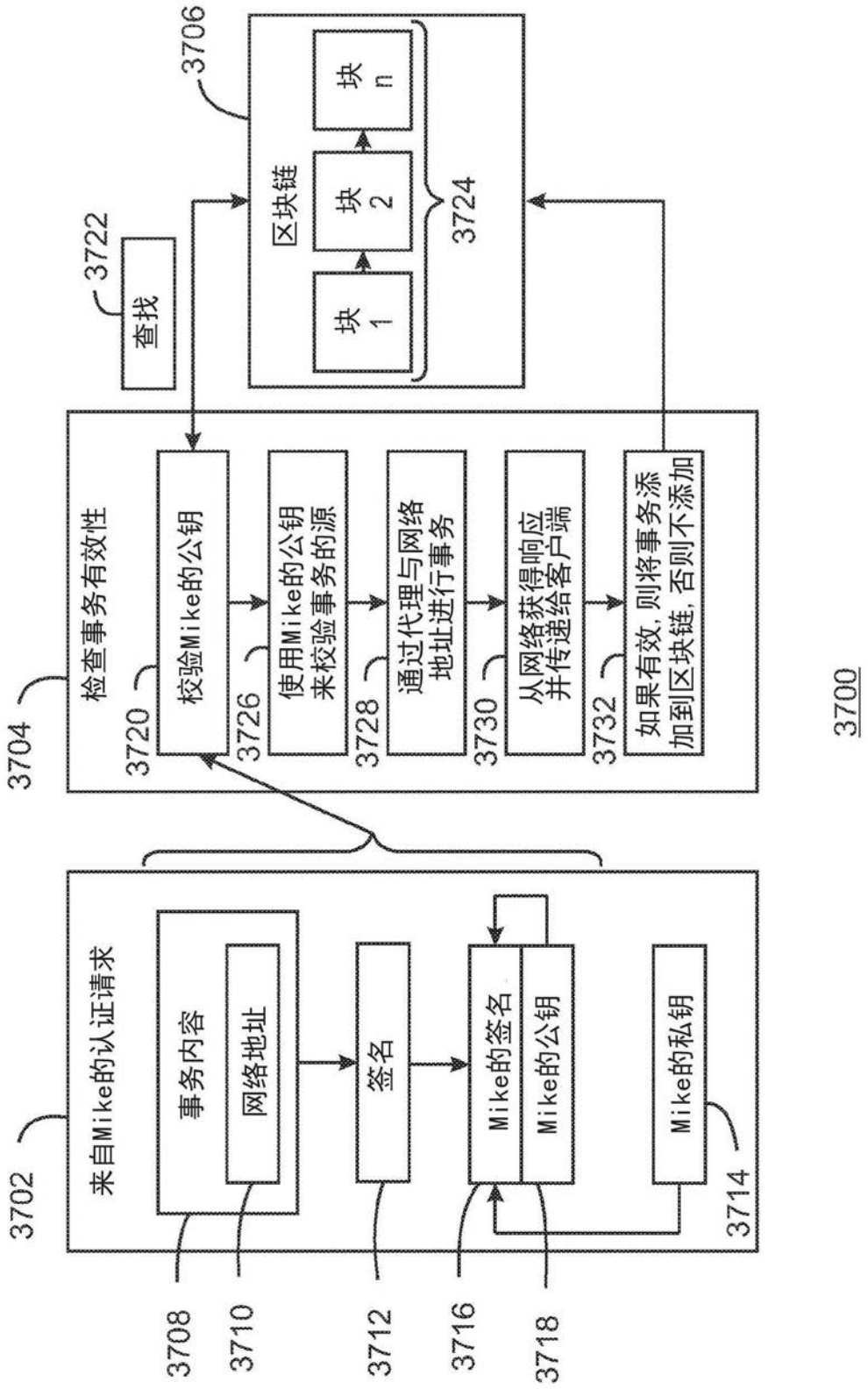

3706
区块链
块 1
块 2
块 n
3724
3722
查找
3704
检查事务有效性
3720
校验Mike的公钥
3726
使用Mike的公钥来校验事务的源
3728
通过代理与网络地址进行事务
3730
从网络获得响应并传递给客户端
3732
如果有效，则将事务添加到区块链，否则不添加
3700
3702
来自Mike的认证请求
事务内容
网络地址
签名
Mike的签名
Mike的公钥
Mike的私钥
3714
3708
3710
3712
3716
3718

图37

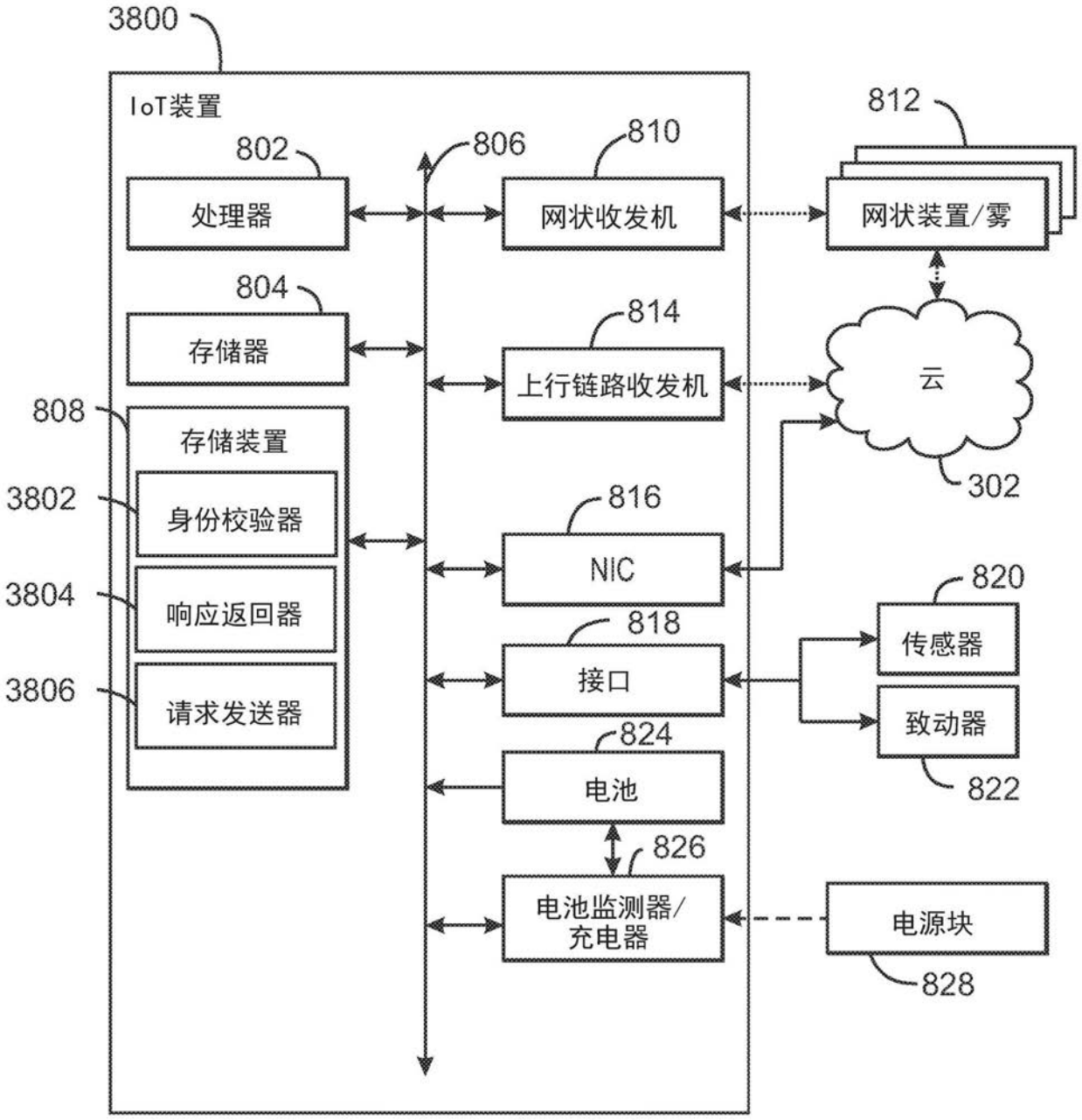

3800
IoT装置
802
处理器
804
存储器
808
存储装置
3802
身份校验器
3804
响应返回器
3806
请求发送器
806
810
网状收发机
814
上行链路收发机
816
NIC
818
接口
824
电池
826
电池监测器/
充电器
812
网状装置/雾
云
302
820
传感器
致动器
822
电源块
828

图38

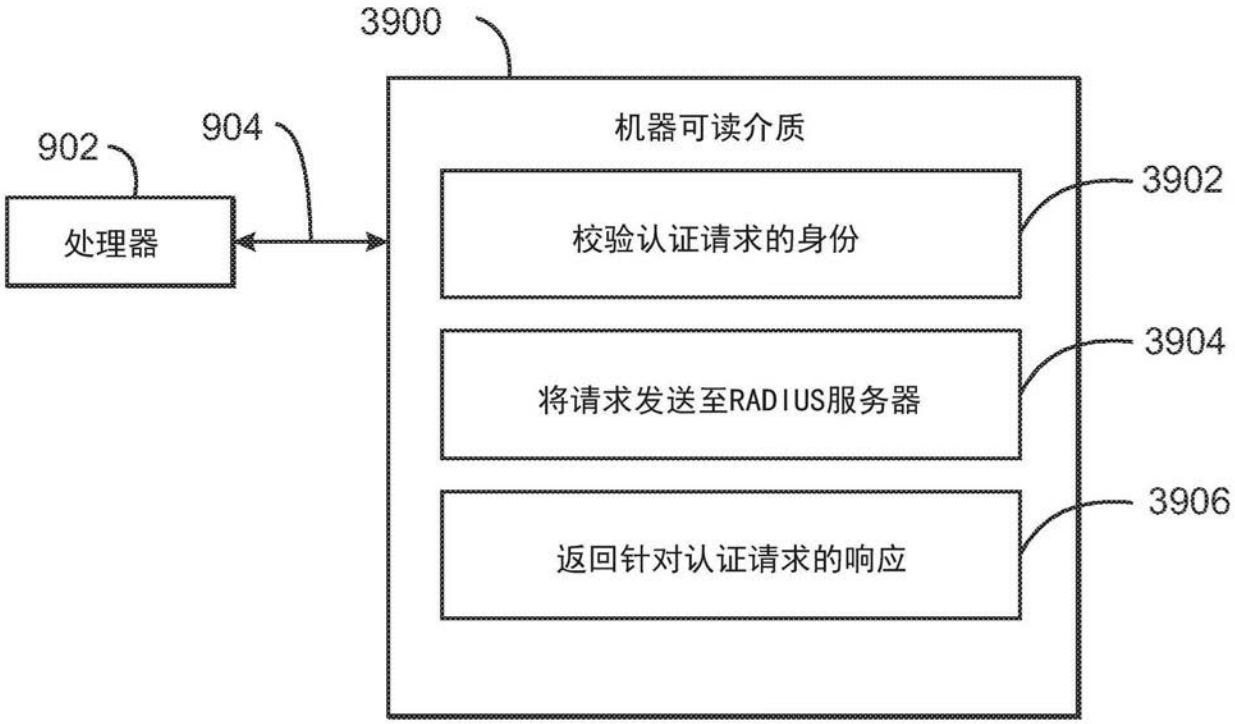
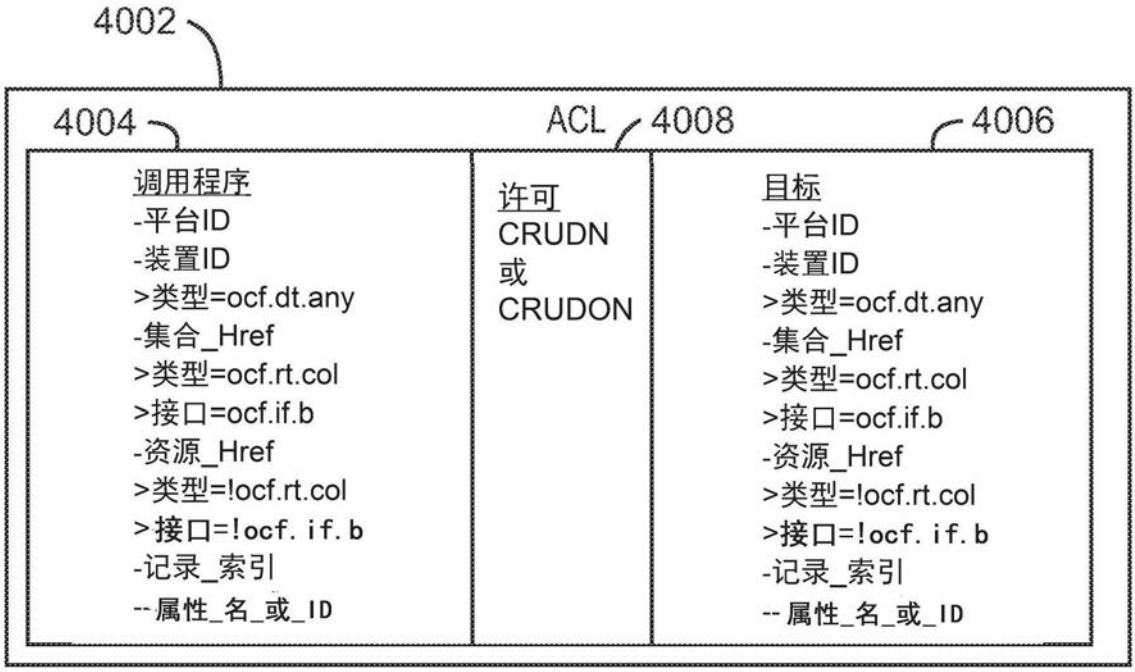

3900
机器可读介质
902
处理器
904
校验认证请求的身份
3902
将请求发送至RADIUS服务器
3904
返回针对认证请求的响应
3906

图39


4002
4004
调用程序
-平台ID
-装置ID
>类型=ocf.dt.any
-集合_Href
>类型=ocf.rt.col
>接口=ocf.if.b
-资源_Href
>类型=!ocf.rt.col
>接口=!ocf.if.b
-记录_索引
--属性_名_或_ID
ACL
4008
许可
CRUDN
或
CRUDON
4006
目标
-平台ID
-装置ID
>类型=ocf.dt.any
-集合_Href
>类型=ocf.rt.col
>接口=ocf.if.b
-资源_Href
>类型=!ocf.rt.col
>接口=!ocf.if.b
-记录_索引
--属性_名_或_ID

4000

图40

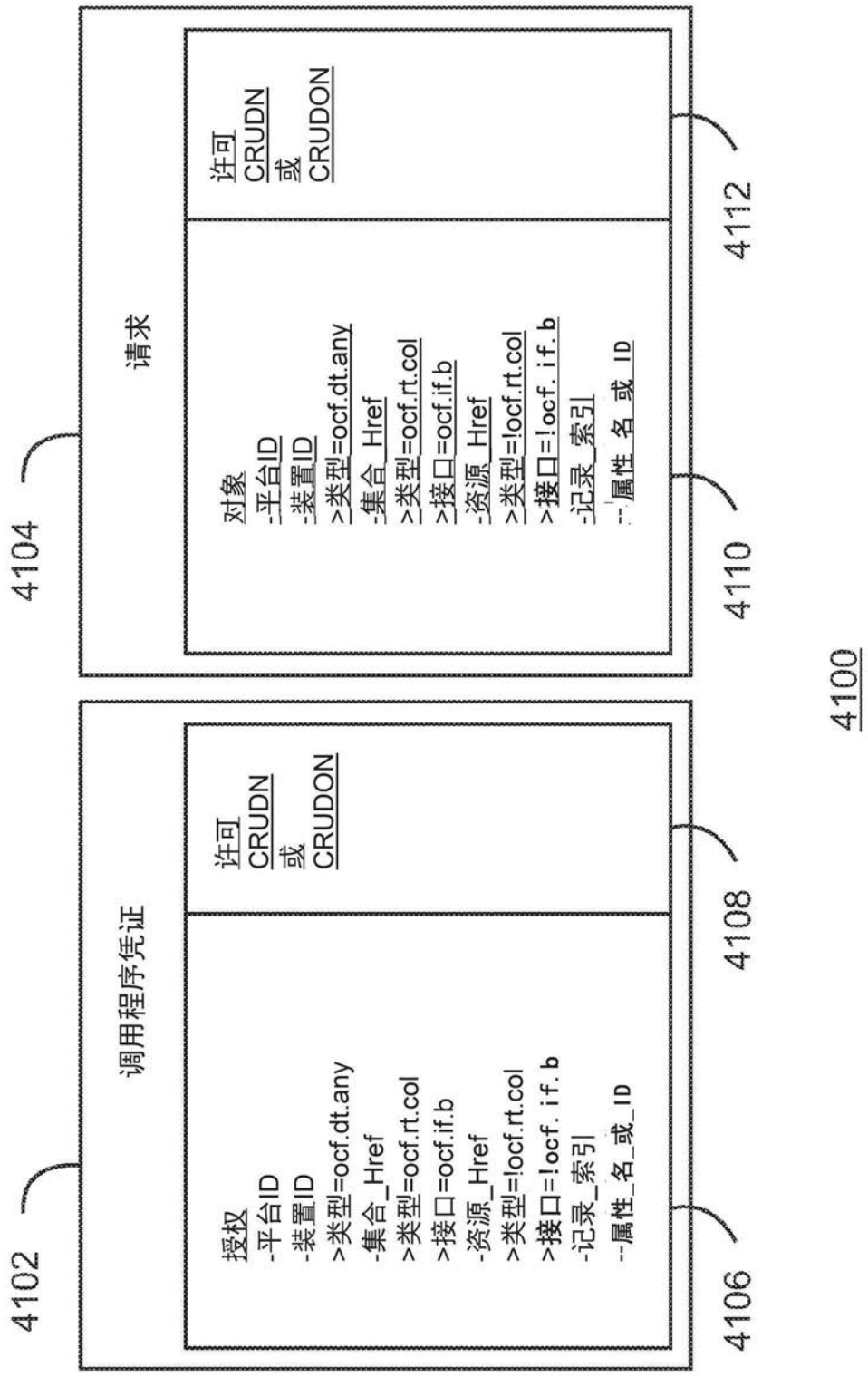

4102
调用程序凭证
授权
-平台ID
-装置ID
>类型=ocf.dt.any
-集合_Href
>类型=ocf.rt.col
>接口=ocf.if.b
-资源_Href
>类型=!ocf.rt.col
>接口=!ocf.if.b
-记录_索引
--属性_名_或_ID
许可
CRUDN
或
CRUDON
4106
4108
4104
请求
对象
-平台ID
-装置ID
>类型=ocf.dt.any
-集合_Href
>类型=ocf.rt.col
>接口=ocf.if.b
-资源_Href
>类型=!ocf.rt.col
>接口=!ocf.if.b
-记录_索引
--属性_名_或_ID
许可
CRUDN
或
CRUDON
4110
4112
4100

图41

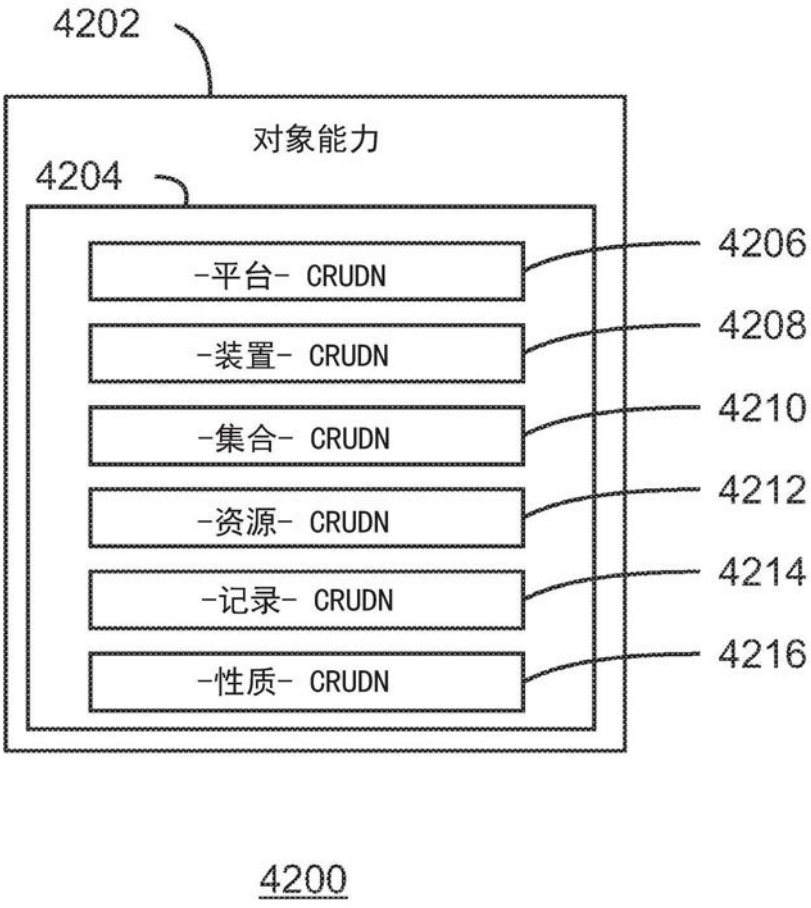

4202
对象能力
4204
-平台- CRUDN
-装置- CRUDN
-集合- CRUDN
-资源- CRUDN
-记录- CRUDN
-性质- CRUDN
4206
4208
4210
4212
4214
4216
4200

图42

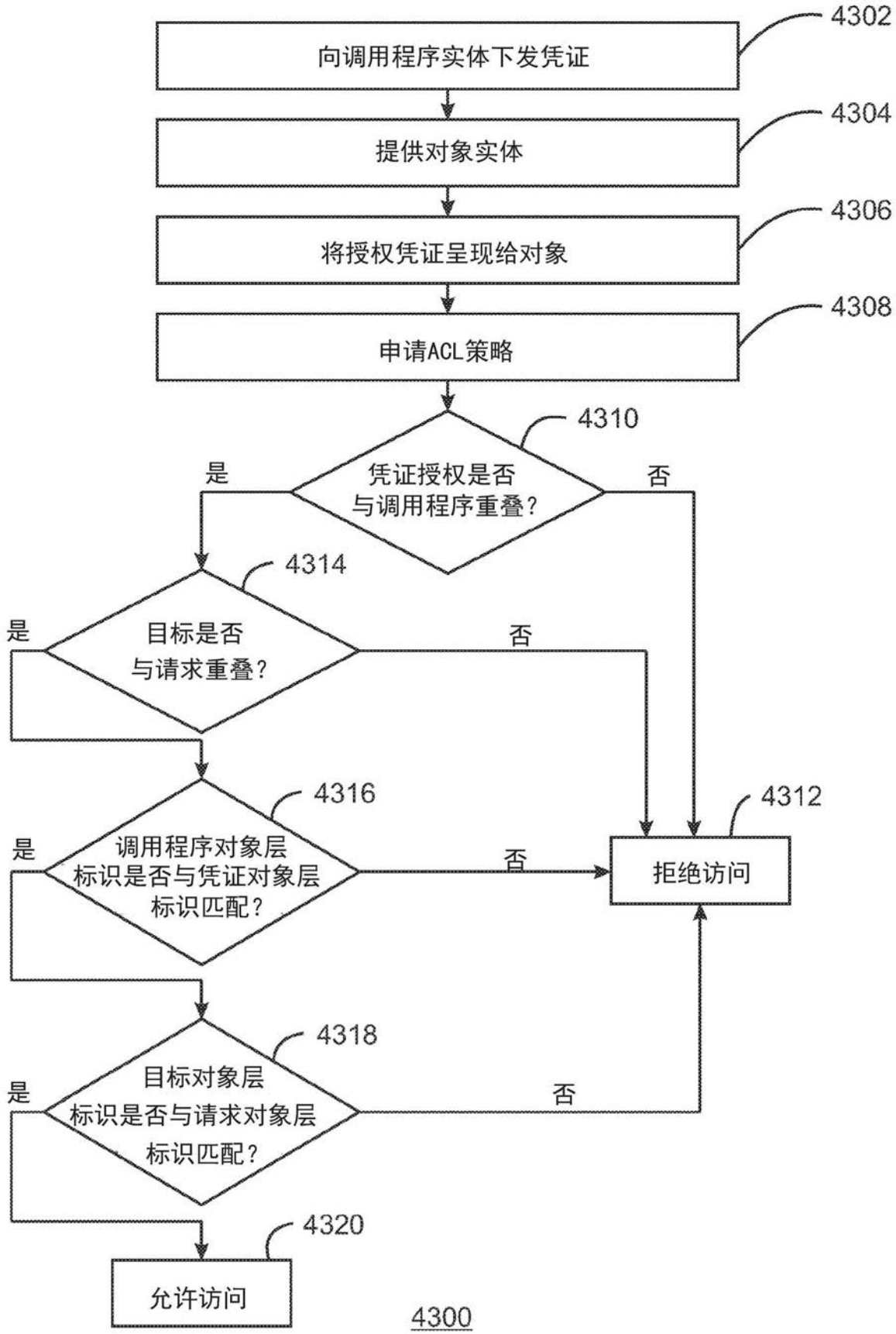

向调用程序实体下发凭证
4302
提供对象实体
4304
将授权凭证呈现给对象
4306
申请ACL策略
4308
凭证授权是否与调用程序重叠？
4310
是
否
目标是否与请求重叠？
4314
是
否
调用程序对象层标识是否与凭证对象层标识匹配？
4316
是
否
拒绝访问
4312
目标对象层标识是否与请求对象层标识匹配？
4318
是
否
允许访问
4320
4300

图43

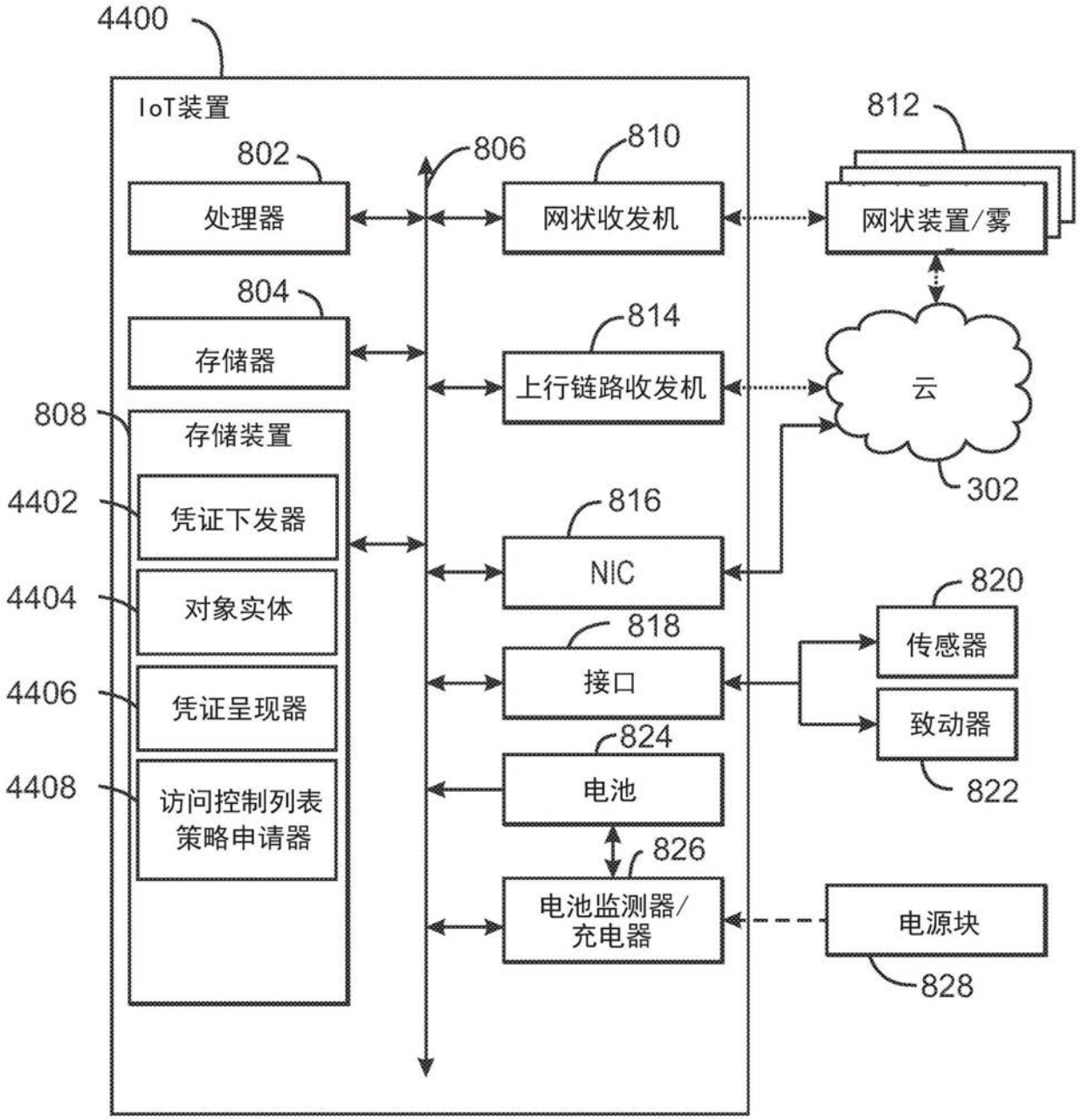

4400
IoT装置
802
处理器
804
存储器
808
存储装置
4402
凭证下发器
4404
对象实体
4406
凭证呈现器
4408
访问控制列表
策略申请器
806
810
网状收发机
814
上行链路收发机
816
NIC
818
接口
824
电池
826
电池监测器/
充电器
812
网状装置/雾
云
302
820
传感器
致动器
822
电源块
828

图44

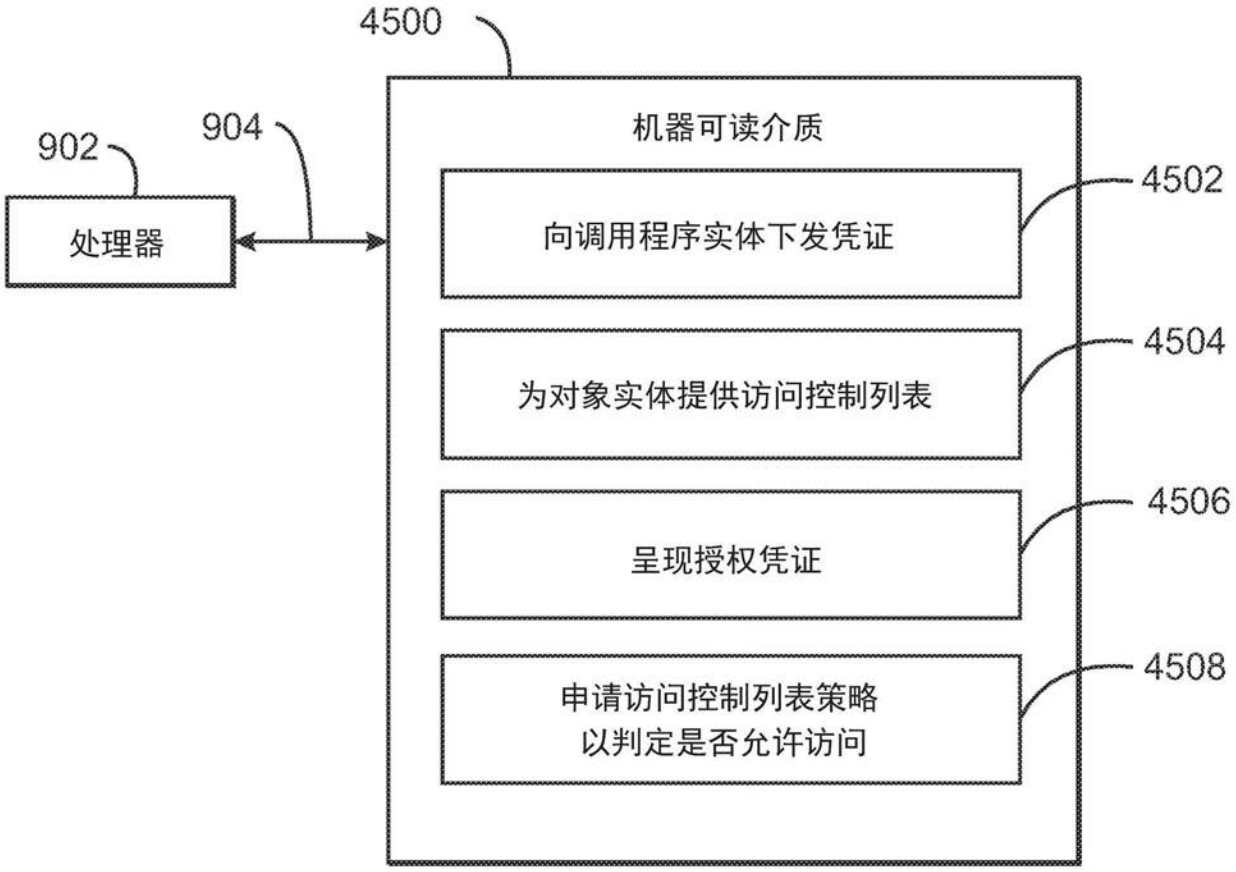

4500
机器可读介质
902
处理器
904
向调用程序实体下发凭证
4502
为对象实体提供访问控制列表
4504
呈现授权凭证
4506
申请访问控制列表策略
以判定是否允许访问
4508

图45