(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 108140137 A
(43)申请公布日 2018.06.08

(21)申请号 201680046007.4

(22)申请日 2016.06.03

(30)优先权数据
62/230,344 2015.06.04 US
62/231,586 2015.07.10 US
62/285,085 2015.10.19 US
62/285,748 2015.11.09 US
62/342,850 2016.05.27 US

(85)PCT国际申请进入国家阶段日
2018.02.05

(86)PCT国际申请的申请数据
PCT/US2016/035902 2016.06.03

(87)PCT国际申请的公布数据
WO2016/197055 EN 2016.12.08

(71)申请人 编年史公司
地址 美国加利福尼亚州

(72)发明人 S·拉多奇亚 D·阿霍 R·奥尔 M·格雷科

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 郑立柱 彭梦晔

(51)Int.Cl.
G06K 19/07(2006.01)
G06Q 30/06(2006.01)
G06Q 10/08(2006.01)
H04W 12/06(2006.01)

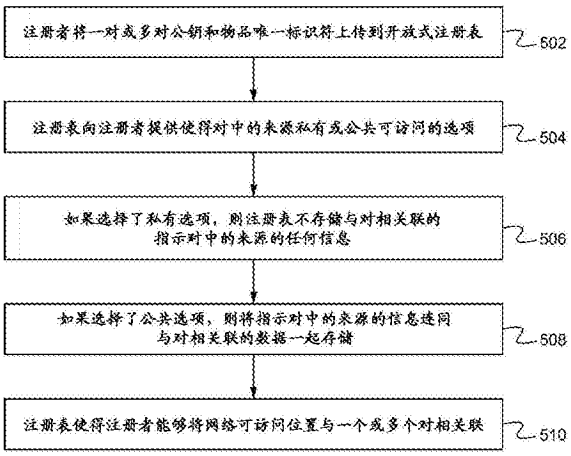
权利要求书5页 说明书12页 附图7页

(54)发明名称

用于事物身份的开放式注册表

(57)摘要

一种用于物联网(IOT)的身份系统,其使得用户和机器能够标识、认证产品和收藏品并且与其交互,而不依赖于第三方控制的认证服务。该系统包括耦合到产品的无线防篡改标签和物品的所有权链能够存储在其中的开放式注册表数据库。开放式注册表使得公众能够访问物品身份和结合有物品注册匿名的数据。



CN 108140137 A

1.一种物品开放式注册和认证系统,包括:

一个或多个物理物品,每个物理物品具有耦合到所述物品的身份标签,所述身份标签每个存储私钥和唯一标识符并且被配置为使得所述唯一标识符能够被无线地读取但是防止所述私钥从所述标签被读取;

移动设备,被配置为当接近所述标签中的一个或多个标签时,从所述身份标签中的一个或多个身份标签无线地读取所述唯一标识符;以及

开放式注册表,存储所述物品中的每个物品的所述唯一标识符、物品信息和公钥,其中所述公钥与存储在耦合到所述物品的所述身份标签上的所述私钥相关联。

2.根据权利要求1所述的系统,其中所述开放式注册表存储物品信息,所述物品信息包括所有权链,所述所有权链定义所述物品的所有者的序列和在所有者对之间授予所述物品的所有权的所述所有者对之间的交易的序列。

3.根据权利要求1所述的系统,其中所述开放式注册表使得多个实体中的每个实体能够向所述注册表上传所述公钥和所述唯一标识符中的一个或多个而不上传标识数据,使得所述开放式注册表不呈现指示所述实体中的哪个实体上传了所述公钥或所述唯一标识符的数据。

4.根据权利要求3所述的系统,其中所述开放式注册表使得所述实体中的每个实体能够上传网络可访问位置,并且将所述网络可访问位置与由所述实体向所述注册表上传的所述公钥和所述唯一标识符中的所述一个或多个中的至少一个相关联。

5.根据权利要求4所述的系统,其中所述移动设备包括身份验证功能,所述身份验证功能在读取所述物品之一的所述身份标签的所述唯一标识符时使得所述移动设备:

生成并且向所述身份标签传输询问消息;

向所述注册表传输所述唯一标识符并且从所述注册表访问与所述唯一标识符相关联的所述公钥;

从所述身份标签接收数字签名;以及

通过使用访问的所述公钥确定所述数字签名是否由存储在所述身份标签中的所述私钥所生成来认证所述物品。

6.根据权利要求5所述的系统,其中如果所述物品被认证,则所述移动设备被配置为自动访问并且在所述移动设备上向用户呈现所述网络可访问位置。

7.根据权利要求6所述的系统,其中所述网络可访问位置是包括关于所述物品的信息的与所述物品相关的网站。

8.根据权利要求5所述的系统,其中在接收到所述询问消息时,所述身份标签被配置为:

对所述询问消息进行数字签名,从而基于存储在所述身份标签中的所述私钥来生成所述数字签名;以及

向所述移动设备传输所述数字签名。

9.根据权利要求8所述的系统,其中在接收到所述唯一标识符时,所述注册表被配置为:

查找存储在所述注册表上的所述公钥中的哪一个公钥与所述唯一标识符相关联;以及

向所述移动设备传输所述公钥中的所述一个公钥。

10.根据权利要求9所述的系统，其中所述开放式注册表是区块链、数据库或智能合约。

11.根据权利要求10所述的系统，其中所述标签由防篡改紧固件组成，所述防篡改紧固件与由单个连续塑料外壳包封的无线信号接收/传输电路物理耦合。

12.根据权利要求10所述的系统，其中所述标签由被缝合在所述物品的标记内的无线信号接收/传输电路组成。

13.根据权利要求10所述的系统，其中所述标签以电路板、微芯片、固件或软件的形式集成在事物身份(IoT)设备中。

14.一种使用物品开放式注册和认证系统进行物品认证的方法，所述方法包括：

利用移动设备无线地发现存储在耦合到物理物品的身份标签上的唯一标识符，其中所述身份标签存储私钥并且被配置为使得所述唯一标识符能够被无线地读取但是防止所述私钥被读取；以及进一步地，其中所述移动设备被配置为当接近所述标签时从所述身份标签自动无线地读取所述唯一标识符；

从所述移动设备向开放式注册表传输所述唯一标识符，所述注册表存储所述物品的所述唯一标识符、物品信息和公钥，其中所述公钥与存储在耦合到所述物品的所述身份标签上的所述私钥相关联；

利用所述移动设备从所述注册表接收与所述唯一标识符相关联的所述公钥，并且从所述身份标签接收数字签名；以及

利用所述移动设备通过使用接收的所述公钥确定所述数字签名是否由存储在所述身份标签中的所述私钥所生成来认证所述物品。

15.根据权利要求14所述的方法，其中所述开放式注册表存储物品信息，所述物品信息包括所有权链，所述所有权链定义所述物品的所有者的序列和在所有者对之间授予所述物品的所有权的所述所有者对之间的交易的序列。

16.根据权利要求14所述的方法，其中所述标签在没有来自所述移动设备的提示的情况下无线地广播所述唯一标识符。

17.根据权利要求14所述的方法，其中所述移动设备从所述标签中取得所述唯一标识符。

18.根据权利要求17所述的方法，还包括在接收到所述询问消息时，所述身份标签：

对所述询问消息进行数字签名，从而基于存储在所述身份标签中的所述私钥来生成所述数字签名；以及

向所述移动设备传输所述数字签名。

19.根据权利要求18所述的方法，还包括在接收到所述唯一标识符时，所述注册表：

查找存储在所述注册表上的所述公钥中的哪一个公钥与所述唯一标识符相关联；以及

向所述移动设备传输所述公钥中的所述一个公钥。

20.根据权利要求19所述的方法，其中所述标签由防篡改紧固件组成，所述防篡改紧固件与由单个连续塑料外壳包封的无线信号接收/传输电路物理耦合。

21.根据权利要求19所述的方法，其中所述标签由被缝合在所述物品的标记内的无线信号接收/传输电路组成。

22.根据权利要求19所述的方法，其中所述标签以电路板、微芯片、固件或软件的形式集成在事物身份(IoT)设备中。

23.一种在物品开放式注册和认证系统的开放式注册表上注册物品的方法，所述物品开放式注册和认证系统包括以防篡改方式耦合到一个或多个物理物品的身份标签，所述身份标签每个存储私钥和唯一标识符并且被配置为使得所述唯一标识符能够被无线地读取但是防止所述私钥从所述标签被读取，所述方法包括：

使用所述开放式注册表将所述物品中的每个物品的所述唯一标识符和公钥存储作为配对，其中所述物品中的每个物品的所述公钥与存储在耦合到所述物品的所述身份标签上的所述私钥相关联；

上传一个或多个网络可访问位置中的每个网络可访问位置并且使用所述注册表将所述一个或多个网络可访问位置中的每个网络可访问位置与所述公钥和所述唯一标识符的所述配对中的至少一个配对相关联；

提供对所述公钥和所述唯一标识符的访问；以及

使用所述注册表提供私有上传选项，所述私有上传选项在被选择时显示所述公钥和所述唯一标识符，而不呈现标识所述唯一标识符和所述公钥中的至少一个的来源的关联数据。

24.根据权利要求23所述的方法，其中所述来源与耦合到存储所述唯一标识符的所述标签的所述物品相关联。

25.根据权利要求24所述的方法，还包括：对于所述网络可访问位置中的每个网络可访问位置，使用所述网络可访问位置向所述网络可访问位置导入与所述位置相关联的所述配对中的所述公钥。

26.根据权利要求25所述的方法，其中所述网络可访问位置是云服务器，所述云服务器能够传递关于所述物品的信息或执行与所述物品相关的程序。

27.根据权利要求26所述的方法，还包括所述注册表维护所述来源的列表并且防止不在所述列表上的来源上传到所述注册表。

28.根据权利要求27所述的方法，其中所述标签由防篡改紧固件组成，所述防篡改紧固件与由单个连续塑料外壳包封的无线信号接收/传输电路物理耦合。

29.根据权利要求27所述的方法，其中所述标签由被缝合在所述物品的标记内的无线信号接收/发射电路组成。

30.根据权利要求27所述的方法，其中所述标签以电路板、微芯片、固件或软件的形式集成在事物身份(IoT)设备中。

31.一种用于在物品开放式注册和认证系统中使用的移动设备，所述移动设备包括：

无线信号收发器，用于在所述移动设备与一个或多个身份标签之间无线地传送数据，所述一个或多个身份标签每个耦合到一个或多个物理物品中的一个物理物品，所述身份标签每个存储私钥和唯一标识符并且被配置为使得所述唯一标识符能够被无线地读取但是防止所述私钥从所述标签被读取；

网络接口，用于与存储所述物品中的每个物品的所述唯一标识符、物品信息和公钥的开放式注册表进行通信，其中所述公钥与存储在耦合到所述物品的所述身份标签上的所述私钥相关联；以及

非暂态计算机可读介质，存储物品代理，所述物品代理控制所述移动设备与所述标签和所述注册表之间的通信，自动无线地搜索所述标签，并且在发现所述标签之一时在所述

移动设备上提示用户。

32.根据权利要求31所述的设备，其中响应于所述物品代理的认证特征对所述物品之一的成功认证，所述物品代理自动地访问并且在所述移动设备的显示器上显示网络可访问位置。

33.根据权利要求32所述的设备，其中所述网络可访问位置是包括关于所述物品的信息的与所述物品相关的网站。

34.根据权利要求33所述的设备，其中所述认证特征包括在读取所述物品之一的所述身份标签的所述唯一标识符时：

向所述身份标签传输询问消息；

向所述注册表传输读取的所述标签的所述唯一标识符；

访问与所述注册表上的所述唯一标识符相关联的所述公钥；

从所述身份标签接收数字签名；以及

通过使用访问的所述公钥确定所述数字签名是否由存储在所述身份标签中的所述私钥所生成来认证所述物品。

35.根据权利要求34所述的设备，其中在接收到所述询问消息时，所述身份标签被配置为：

基于存储在所述身份标签中的所述私钥来生成所述数字签名；以及

向所述移动设备传输所述数字签名。

36.根据权利要求35所述的设备，其中在接收到所述唯一标识符时，所述注册表被配置为：

查找存储在所述注册表上的所述公钥中的哪一个公钥与所述唯一标识符相关联；以及

向所述移动设备传输相关联的所述公钥。

37.一种在物品开放式注册和认证系统上执行接近认证的证明的方法，所述方法包括：

使用移动设备无线地发现身份标签并且读取存储在所述身份标签上的唯一标识符，其中所述身份标签耦合到物理物品，存储私钥并且被配置为使得所述唯一标识符能够被无线地读取但是防止所述私钥从所述标签被读取，并且进一步地，其中所述移动设备被配置为当接近所述标签时从所述身份标签自动无线地读取所述唯一标识符；

从所述移动设备向开放式注册表传输所述唯一标识符，所述注册表存储耦合到所述物品的所述标签的所述唯一标识符、网络可访问位置和公钥，所述唯一标识符、所述网络可访问位置和所述公钥在所述注册表上彼此相关联，其中所述公钥与存储在耦合到所述物品的所述身份标签上的所述私钥相关联；

利用所述移动设备从所述注册表确定并且尝试访问与从所述标签中读取的所述唯一标识符相关联的所述网络可访问位置；

利用所述网络可访问位置处的服务器生成并且向所述移动设备传输接近询问；

从所述移动设备向耦合到所述物理物品的所述身份标签转发所述接近询问；

利用所述身份标签使用所述私钥生成并且向所述移动设备传输所述接近询问的数字签名；

从所述移动设备向所述网络可访问位置转发所述数字签名；

通过使用所述公钥确定所述数字签名是否由存储在所述身份标签中的所述私钥所生

成来验证所述数字签名的有效性;以及

如果所述验证成功,则利用所述服务器向所述移动设备给予和提供对所述网络可访问位置的访问。

38.根据权利要求37所述的方法,还包括所述网络可访问位置基于所述唯一标识符以及存储在所述注册表上的所述公钥和所述唯一标识符的配对,来确定和访问与存储在所述标签上的所述私钥相关联的所述公钥。

39.根据权利要求38所述的方法,其中所述网络可访问位置是云服务器,所述云服务器提供与所述物品相关的云服务,包括关于所述物品的信息或与所述物品相关的程序。

40.根据权利要求39所述的方法,其中所述提供对所述网络可访问位置的访问包括:

自动访问并且在所述移动设备上显示所述网络可访问位置。

41.根据权利要求40所述的方法,其中所述云服务器由向所述开放式注册表上传了所述唯一标识符和所述公钥的实体提供。

42.根据权利要求40所述的方法,其中所述云服务器由向所述开放式注册表上传了所述唯一标识符和所述公钥的实体指定的第三方提供。

43.根据权利要求42所述的方法,其中所述云服务是在区块链数据库上运行的智能合约。

用于事物身份的开放式注册表

[0001] 相关申请

[0002] 本申请根据35U.S.C.§119(e)要求于2015年6月4日提交的题为“SMART APPAREL LABEL CONTAINING A MICROCHIP SO THAT A CONSUMER CAN VERIFY AUTHENTICITY OF AN APPAREL Γ Γ E MFROM A MOBILE DEVICE”的共同未决的美国临时专利申请序列号62/230,344、于2015年7月10日提交的题为“PKI-ENABLED TAG”的共同未决的美国临时专利申请序列号62/231,586、于2015年10月19日提交的题为“TIMELINE FOR CONSUMER/LUXURY PRODUCTS THAT TRACKS OWNERSHIP,PROVENANCE,AND KEY DATA POINTS/EVENTS IN THE LIFE OF THE PRODUCT”的共同未决的美国临时专利申请序列号62/285,085、于2015年11月9日提交的题为“ONE-PIECE EXTERNAL PLASTIC TAG CONTAINING ENCRYPTED MICROCHIP FOR COLLECTIBLE AND LUXURY CONSUMER GOODS AUTHENTICITY VERIFICATION AND CONSUMER-BRAND ENGAGEMENT”的共同未决的美国临时专利申请序列号62/285,748、以及于2016年5月27日提交的题为“USING PROOF OF PROXIMITY TO SERVE-UP PRIVATE DATA ABOUT PHYSICAL OBJECTS IN THE CONSUMER INTERNET WOF THINGS,AND TO SUPPORT AN VARITY PROVABLE LOGISTICS,SOCIAL,COMMERCE,AND SECONDARY”的共同未决的美国临时专利申请序列号62/342,850的优先权,所有这些通过引用合并于此。

技术领域

[0003] 本发明涉及事物的唯一身份领域,包括产品、收藏品和事物身份/物联网设备。更具体地,本发明涉及使用标识标签和开放式注册表的标识、认证和出处跟踪。

背景技术

[0004] 有形资产在互联网、公共数据库或市场上的表示很差。目前的标识方法通常不是机器可读的。另外,现有标签不安全,因为它们能够被容易地伪造和/或重新应用于不同的非真实资产。特别地,有助于防止标签复制的技术是薄弱的,并且依赖于模糊方法(其可能被黑客攻击)或要求使用依赖于信任第三方(例如,控制方)来准确地维护数据库的私有数据库(例如,私有控制的)。这样的方法不会阻止第三方创建复制的标签或数据库记录,也不能在第三方解散或停业的情况下存在。最后,这样的第三方控制的系统缺乏用户将其身份和/或所有权证明无缝地迁移到其他系统的能力。

发明内容

[0005] 身份验证和认证系统使得用户和机器能够分配和认证事物身份而不依赖于第三方控制的身份验证或认证服务。事物是任何物理对象,包括产品、收藏品和事物身份设备。该系统包括耦合到事物的无线防篡改标签和事物的所有权链能够存储在其中的开放式注册表数据库。开放式注册表使得公众能够通过可选的物品注册匿名来访问标识数据。在一些实施例中,开放式注册表是数据库、区块链或智能合约。

[0006] 第一方面涉及一种物品开放式注册和认证系统。该系统包括:一个或多个物理物

品，每个物理物品具有耦合到物品的身份标签，身份标签每个存储私钥和唯一标识符并且被配置为使得唯一标识符能够被无线地读取但是防止私钥从标签被读取；被配置为当接近一个或多个标签时从一个或多个身份标签无线地读取唯一标识符的移动设备；以及存储每个物品的唯一标识符、物品信息和公钥的开放式注册表，其中公钥与存储在耦合到物品的身份标签上的私钥相关联。在一些实施例中，开放式注册表存储物品信息，物品信息包括定义物品的所有者的序列和在所有者对之间授予物品的所有权的所有者对之间的交易的序列的所有权链。在一些实施例中，开放式注册表使得多个实体中的每个能够向注册表上传公钥和唯一标识符中的一个或多个而不上传标识数据，使得开放式注册表不呈现指示哪个实体上传了公钥或唯一标识符的数据。在一些实施例中，开放式注册表使得每个实体能够上传网络可访问位置并且将网络可访问位置与由实体向注册表上传的公钥和唯一标识符中的一个或多个中的至少一个相关联。在一些实施例中，移动设备包括身份验证功能，身份验证功能在读取物品之一的身份标签的唯一标识符时引起移动设备：生成并且向身份标签传输询问消息，向注册表传输唯一标识符并且从注册表访问与唯一标识符相关联的公钥，从身份标签接收数字签名，并且通过使用所访问的公钥确定数字签名是否由存储在身份标签中的私钥生成来认证物品。在一些实施例中，如果物品被认证，则移动设备被配置为自动访问并且在移动设备上向用户呈现网络可访问位置。在一些实施例中，网络可访问位置是包括关于物品的信息的与物品相关的网站。在一些实施例中，在接收到询问消息时，身份标签被配置为对询问消息进行数字签名，从而基于存储在身份标签中的私钥来生成数字签名，并且向移动设备传输数字签名。在一些实施例中，在接收到唯一标识符时，注册表被配置为：查找存储在注册表上的公钥中的哪一个与唯一标识符相关联，并且向移动设备传输该公钥。在一些实施例中，开放式注册表是区块链、数据库或智能合约。在一些实施例中，标签由防篡改紧固件组成，防篡改紧固件与由单个连续塑料外壳包封的无线信号接收/传输电路物理耦合。在一些实施例中，标签由被缝合在物品的标签内的无线信号接收/传输电路组成。在一些实施例中，标签以电路板、微芯片、固件或软件的形式集成在事物身份(IoT)设备中。

[0007] 第二方面涉及一种使用物品开放式注册和认证系统进行物品认证的方法。该方法包括：使用移动设备无线地发现存储在耦合到物理物品的身份标签上的唯一标识符，其中身份标签存储私钥并且被配置为使得唯一标识符能够被无线地读取但是防止私钥被读取，并且进一步地，其中移动设备被配置为当接近标签时从身份标签自动无线地读取唯一标识符；从移动设备向开放式注册表传输唯一标识符，注册表存储物品的唯一标识符、物品信息和公钥，其中公钥与存储在与物品耦合的身份标签上的私钥相关联；使用移动设备从注册表接收与唯一标识符相关联的公钥，并且从身份标签接收数字签名；以及通过使用所接收的公钥确定数字签名是否由存储在身份标签中的私钥生成来使用移动设备认证物品。在一些实施例中，开放式注册表存储物品信息，物品信息包括定义物品的所有者的序列和在所有者对之间授予物品的所有权的所有者对之间的交易的序列的所有权链。在一些实施例中，标签无线地广播唯一标识符而没有来自移动设备的提示。在一些实施例中，移动设备从标签中取得唯一标识符。在一些实施例中，该方法还包括在接收到询问消息时，身份标签对询问消息进行数字签名，从而基于存储在身份标签中的私钥来生成数字签名，并且向移动设备传输数字签名。在一些实施例中，该方法还包括在接收到唯一标识符时，注册表查找存

储在注册表上的公钥中的哪一个与唯一标识符相关联，并且向移动设备传输该公钥。在一些实施例中，标签由防篡改紧固件组成，防篡改紧固件与由单个连续塑料外壳包封的无线信号接收/传输电路物理耦合。在一些实施例中，标签由被缝合在物品的标记内的无线信号接收/传输电路组成。在一些实施例中，标签以电路板、微芯片、固件或软件的形式集成在事物身份(IoT)设备中。

[0008] 第三方面涉及一种在物品开放式注册和认证系统的开放式注册表上注册物品的方法，物品开放式注册和认证系统包括以防篡改方式耦合到一个或多个物理物品的身份标签，身份标签每个存储私钥和唯一标识符并且被配置为使得唯一标识符能够被无线地读取但是防止私钥从标签被读取。该方法包括：使用开放式注册表将每个物品的唯一标识符和公钥成对地存储，其中每个物品的公钥与存储在耦合到物品的身份标签上的私钥相关联；上传一个或多个网络可访问位置中的每个并且使用所述注册表将一个或多个网络可访问位置中的每个与公钥和唯一标识符的对中的至少一个对相关联；提供对公钥和唯一标识符的访问；并且使用注册表提供私有上传选项，私有上传选项在被选择时显示公钥和唯一标识符，而不呈现标识唯一标识符和公钥中的至少一个的来源的关联数据。在一些实施例中，来源与耦合到存储唯一标识符的标签的物品相关联。在一些实施例中，该方法还包括：对于每个网络可访问位置，使用网络可访问位置向网络可访问位置导入与位置相关联的对中的公钥。在一些实施例中，网络可访问位置是能够传递关于物品的信息或执行与物品相关的程序的云服务器。在一些实施例中，该方法还包括注册表维护来源的列表并且防止向注册表上传不在列表上的来源。在一些实施例中，标签由防篡改紧固件组成，该防篡改紧固件与由单个连续塑料外壳包封的无线信号接收/传输电路物理耦合。在一些实施例中，标签由被缝合在物品的标记内的无线信号接收/传输电路组成。在一些实施例中，标签以电路板、微芯片、固件或软件的形式集成在事物身份(IoT)设备中。

[0009] 第四方面涉及一种用于在物品开放式注册和认证系统中使用的移动设备。该移动设备包括用于在移动设备与一个或多个身份标签之间无线地传送数据的无线信号收发器，身份标签每个耦合到一个或多个物理物品之一，身份标签每个存储私钥和唯一标识符并且被配置为使得唯一标识符能够被无线地读取但是防止私钥从标签被读取；用于与存储每个物品的唯一标识符、物品信息和公钥的开放式注册表进行通信的网络接口，其中公钥与存储在耦合到物品的身份标签上的私钥相关联；以及存储物品代理的非暂态计算机可读介质，物品代理控制移动设备与标签和注册表之间的通信，自动无线地搜索标签，并且在发现标签之一时在移动设备上提示用户。在一些实施例中，响应于物品代理的认证特征对物品之一的成功认证，物品代理自动地访问并且在移动设备的显示器上显示网络可访问位置。在一些实施例中，网络可访问位置是包括关于物品的信息的与物品相关的网站。在一些实施例中，认证特征包括在读取物品之一的身份标签的唯一标识符时：向身份标签传输询问消息，向注册表传输读取的标签的唯一标识符，访问与注册表上的唯一标识符相关联的公钥，从身份标签接收数字签名，并且通过使用所访问的公钥确定数字签名是否由存储在身份标签中的私钥生成来认证物品。在一些实施例中，在接收到询问消息时，身份标签被配置为：基于存储在身份标签中的私钥来生成数字签名，并且向移动设备传输数字签名。在一些实施例中，在接收到唯一标识符时，注册表被配置为：查找存储在注册表上的公钥中的哪一个与唯一标识符相关联，并且向移动设备传输相关联的公钥。

[0010] 第五方面涉及一种在物品开放式注册和认证系统上执行接近认证的证明的方法。该方法包括：使用移动设备无线地发现身份标签并且读取存储在身份标签上的唯一标识符，其中身份标签耦合到物理物品，存储私钥并且被配置为使得唯一标识符能够被无线地读取但是防止私钥从标签被读取，并且进一步地，其中移动设备被配置为当接近标签时从身份标签自动无线地读取唯一标识符；从移动设备向开放式注册表传输唯一标识符，注册表存储耦合到物品的标签的唯一标识符、网络可访问位置和公钥，唯一标识符、网络可访问位置和公钥在注册表上彼此相关联，其中公钥与存储在耦合到物品的身份标签上的私钥相关联；使用移动设备从注册表确定并且尝试访问与从标签中读取的唯一标识符相关联的网络可访问位置；使用可访问位置处的服务器生成并且向移动设备传输网络接近询问；从移动设备向耦合到物理物品的身份标签转发接近询问；使用身份标签使用私钥生成并且向移动设备传输接近询问的数字签名；从移动设备向网络可访问位置转发数字签名；通过使用公钥确定数字签名是否由存储在身份标签中的私钥生成来验证数字签名的有效性；以及如果验证成功，则使用服务器向移动设备授予和提供对网络可访问位置的访问。在一些实施例中，该方法还包括网络可访问位置基于唯一标识符以及存储在注册表上的公钥和唯一标识符的对来确定和访问与存储在标签上的私钥相关联的公钥。在一些实施例中，网络可访问位置是提供包括关于物品的信息或与物品相关的程序的与物品相关的云服务器。在一些实施例中，提供对网络可访问位置的访问包括自动访问和在移动设备上显示网络可访问位置。在一些实施例中，云服务器由向开放式注册表上传唯一标识符和公钥的实体提供。在一些实施例中，云服务是在区块链数据库上运行的智能合约。在一些实施例中，云服务器由向开放式注册表上传唯一标识符和公钥的实体指定的第三方提供。在一些实施例中，标签以电路板、微芯片、固件或软件的形式集成在事物身份(IoT)设备中。

附图说明

[0011] 图1示出了根据一些实施例的物品开放式注册认证系统。

[0012] 图2A示出了根据一些实施例的标签。

[0013] 图2B示出了根据一些实施例的标签。

[0014] 图2C示出了根据一些实施例的标签。

[0015] 图3示出了根据一些实施例的使用该系统的物品认证方法。

[0016] 图4示出了根据一些实施例的呈现物品信息的方法。

[0017] 图5示出了根据一些实施例的在开放式数据库上注册物品的方法。

[0018] 图6示出了根据一些实施例的接近证明方法。

[0019] 图7示出了根据一些实施例的被配置为实现该系统的示例性计算设备的框图。

具体实施方式

[0020] 本文中描述的实施例涉及身份验证和认证系统，其使得用户、设备和机器能够验证事物身份并且对其进行认证而不依赖于第三方控制的认证服务。该系统使得用户能够认证有收藏价值的产品。该系统包括耦合到事物的无线防篡改标签和事物的所有权链能够存储在其中的开放式注册表数据库。因此，通过使用具有认证应用的设备容易地扫描标签，用户能够使用该系统立即确定耦合到标签的事物是否真实、以及被提供有所有权的历史和事

物的描述以确保实体有权出售事物。因此，该系统在普通伪造领域提供了事物和购买确定性的优点。此外，开放式注册表使得公众能够访问与技术不可知的并且具有可选择的物品注册匿名的注册协议结合的认证数据，使得用户不必依赖于第三方进行认证，而商家或注册者可以注册他们的产品而不在数据库上向竞争对手公开产品线的推出/发布数量。最后，开放式注册表的注册协议能够使得能够提交物品数据，包括系统可以用来访问云服务的网络可访问位置(链接和/或地址)，云服务可以服务于与事物/产品相关的数字内容或执行与事物/产品相关的程序。

[0021] 图1示出了根据一些实施例的物品开放式注册表认证系统100。如图1所示，系统100包括每个具有标识(和/或认证)标签103的一个或多个物品102、每个具有接收器/传输器105的一个或多个计算设备104、开放式注册表106和一个或多个服务器108，其中服务器108、注册表106和/或设备104经由一个或多个网络110通信地耦合。虽然如图1所示，单个服务器108与两个客户端设备104耦合，但是应当理解，任何数目的服务器108能够与任何数目的设备104耦合。网络110能够是本领域公知的有线或无线网络中的一种或组合。一个或多个服务器108能够将包括图形用户界面的物品认证代理和/或应用107的至少一部分存储在一个或多个服务器108的存储器上。因此，用户能够通过网络110将应用107从服务器108下载到一个或多个设备104上。在被下载到客户端设备104之后，应用107能够创建和使用设备104上的本地存储器内的应用数据库来存储和利用操作所必需的数据。

[0022] 替代地，一些或全部数据可以存储在服务器108上的存储器上的服务器数据库中，使得应用107能够通过网络110连接到服务器108，以便利用服务器数据库上的数据。例如，设备104上的本地执行的应用107能够通过网络110与服务器108远程通信，以执行应用107的任何特征和/或访问服务器数据库上仅使用设备104上的数据不可用的任何数据。在一些实施例中，相同的数据存储在服务器数据库和一个或多个设备104两者上，使得本地或远程数据访问是可能的。在这样的实施例中，服务器108和/或设备104上的数据能够由应用同步。在一些实施例中，服务器数据库和/或应用107跨多个服务器108分布。替代地或另外地，一个或多个服务器108能够存储所有的数据库和/或应用数据。在这样的实施例中，服务器108能够执行同步过程，使得所有数据库和/或其他应用数据被同步。

[0023] 替代地，应用107能够用存储在服务器存储器上并且由服务器108执行的物品代理和/或网站来替换或补充，其中代理和/或网站向应用107的一些或全部功能提供与应用用户界面基本类似的网站用户界面。在这样的实施例中，设备104能够访问代理和/或网站，并且使用通过网络110与服务器108通信的web浏览器来利用代理和/或网站的特征。在一些实施例中，网站的功能能够被限制以支持将应用107下载到一个或多个设备104上。换言之，应用/代理107能够仅在服务器108上操作，仅在设备104上操作，或者在服务器108和设备104的组合上操作。因此，应当注意，尽管本文中根据示例性功能分布进行描述，但是应用/代理107的功能在服务器108(经由代理/网站)与设备104(经由应用)之间的其他分布是可预期的，但是为了简洁起见而没有被包括在内。替代地，设备104能够是诸如无人机或事务身份/物联网(IOT)设备的自主机器。在这样的实施例中，应用107能够已经安装在设备104中或能够作为操作设备104的软件或固件本身的部分。

[0024] 此外，服务器108能够存储描述一个或多个物品102(例如，描述品牌/产品的文本、音频、照片和/或视频)并且与存储在耦合到物品102的标签103上的公钥和/或唯一标识符

相关联的的物品信息。因此，当设备104之一扫描/读取一个或多个物品102上的一个或多个标签103时，设备104上的应用能够将扫描的标签103的公钥和/或唯一标识符传送到一个或多个服务器108，服务器108然后能够向设备104提供与密钥/标识符相关联的物品信息以向用户显示。在一些实施例中，物品信息能够包括到网络可访问位置的一个或多个链接或地址(例如，统一资源标识符)，其中位置包括关于物品的信息。在这样的实施例中，当设备104之一扫描/读取一个或多个物品102上的一个或多个标签103时，设备104上的应用能够将扫描的标签103的公钥和/或唯一标识符传送到一个或多个服务器108，服务器108然后能够提供使得设备上的应用107能够访问设备104上的位置(和操作位置的一个或多个服务器)的链接/地址(例如，经由web浏览器)。在一些实施例中，物品信息和相关联的公钥/唯一标识符在注册过程期间被上传到服务器108。

[0025] 计算设备104能够是具有用于存储应用107的至少一部分的存储器和能够与标签103无线地读取和/或通信的无线标签读取特征105的任何计算设备。在一些实施例中，设备104包括显示器(例如，触摸屏)。能够包括读取特征105和/或存储应用107的合适的计算设备104的示例包括智能珠宝(例如，智能手表)、个人计算机、膝上型计算机、计算机工作站、服务器、大型计算机、手持计算机、个人数字助理、蜂窝/移动电话、IOT设备、智能电器、游戏机、数码相机、数码摄像机、照相电话、智能电话、便携式音乐播放器、平板电脑、移动设备、视频播放器、视频盘写入器/播放器(例如，DVD写入器/播放器、高清晰度盘写入器/播放器、超高清晰度盘写入器/播放器)、电视机、家庭娱乐系统或任何其他合适的计算设备。

[0026] 物品102能够是收藏品、IOT设备、服饰、鞋子、手提包、服装或其他通常伪造或有收藏价值的物品。例如，物品能够是品牌钱包或一双鞋子，其中由于存在大量的假冒品，可能难以证明物品是真正的而用于从当前所有者转移/销售到准买家的目的。在一些实施例中，物品102也能够是汽车、车辆、船只、收藏品等。

[0027] 图2A-C示出了根据一些实施例的标签103。如图2A所示，标签103能够是包括防篡改本体202、防篡改紧固机构204(例如，环)的外部标签，本体202容纳认证电路206。本体202和/或紧固机构204能够由单个连续的塑料片形成，使得电路206完全密封在本体202和/或紧固机构204内。因此，电路206不能被物理地移除或篡改而不破坏本体202和/或紧固机构204。另外，本体202和/或紧固机构204能够与电路206耦合，使得标签103与物品102的去耦合损坏电路206，使得电路206不能读取和/或传输任何存储的数据，或者电路206传输指示发生篡改的警告数据。如图2B所示，标签103也能够是与图2A的外部标签基本类似的内部标签，不同之处在与，替代紧固机构204，内部标签能够被缝合到物品102的标记或其他材料中。具体地，本体202能够被围绕本体202缝合或以其他方式耦合在一起的物品102的两块/层织物或其他材料(例如，像密封袋)完全密封。在一些实施例中，至少一个层能够是物品102的标记，并且包括描述物品102的文字(例如，品牌名称)。在一些实施例中，本体202和内部标签的本体202内的电路206能够是柔性的，使得物品102能够弯曲而不损坏标签103。如图2C所示，标签103能够成为电子设备210，其中电路206被集成到电子设备210的电路中。例如，电子设备210能够是印刷电路板或具有无线通信能力的其他电子设备(例如，IOT设备)。因此，标签103的所有实施例提供确保存储在标签103上的标识和认证数据安全地耦合到适当的物品102以用于认证/标识目的或者篡改标签103和/或物品102很容易确定的益处。

[0028] 电路206能够经由近场通信、蓝牙低功耗、射频识别、蓝牙、WiFi或本领域已知的其

他类型的无线通信来无线地通信。此外，电路206能够是公钥基础设施启用的。具体地，电路206能够存储唯一标识符和私钥，并且与设备104的读取器105无线地通信。私钥是秘密的并且不能从标签103读取或提取(例如，不能被读取器105读取)。相比之下，唯一标识符能够被读取器105读取和/或在被设备104请求时以其他方式从标签103传输到设备104中的一个或多个。私钥是加密密钥，其与对应的公钥相关联。换言之，公钥和私钥是相关的，使得用公钥加密的数据仅能够使用私钥解密，而由私钥生成的数字签名仅能够使用公钥来验证。因此，如下面详细描述的，每个标签103的私钥能够用于认证标签103被耦合到的物品102。具体地，电路206能够使用私钥对从设备104(经由读取器105)接收的询问消息进行数字签名，并且将数字签名传输回设备104用于对物品102进行认证。替代地，电路206能够响应于来自设备104的询问消息使用私钥对询问消息执行其他认证过程。

[0029] 唯一标识符能够是公钥(与存储在标签103上的私钥相关联)、公钥的散列、通用唯一标识符(UUID)或其他唯一标识符。此外，在一些实施例中，电路206能够存储与标签103被附接到的物品102相关的数据(例如，描述物品102和/或注册者的文本、照片、视频和/或音频)。在这样的实施例中，当由读取器105扫描时，电路206能够将物品相关的数据发送到设备104上的应用，其然后自动将数据呈现给设备104的用户。

[0030] 开放式注册表106存储注册表数据，并且能够是其记录对公众开放的数据库、区块链或智能合约(例如，对查看记录的访问不是基于权限的，而是用于更改数据库的所有权/转移协议要求)。例如，注册表106能够是分布式数据库(例如，跨多个计算设备，每个计算设备存储一个或多个链接块中的事务的副本)，其维护数据记录的连续增长的列表(例如，与唯一标识符相关联的物品的描述、与公钥和唯一标识符的对相关联的所有权事务的起源或链)，从而防止篡改和修改。在一些实施例中，注册表106由排他性地保存数据(例如，公钥、所有权数据、物品标识数据)的数据结构块组成，每个数据结构块持有成批的个体事务以及任何区块链可执行文件的结果。替代地，块能够存储数据和程序。区块链中的每个区块包含时间戳和将其链接到前一区块的信息，由此定义链并且维持每个记录/事务的时间顺序。因此，注册表106提供与由第三方控制并且经常需要数据访问权限的私有第三方数据库不同的优点，开放式注册表106的数据(例如，所有权信息链、与和唯一标识符相关联的物品相关的其他信息)能够自我控制(基于数据库固有的事务规则)并且公开地可访问/可查看而不需要任何特许权限。替代地，开放式注册表106能够是非区块链数据库。

[0031] 注册表数据能够包括由注册者或密钥/物品的其他所有者上传的公钥和物品唯一标识符的对。注册者能够是与物品102相关联的制造者、认证者、所有者和/或其他实体。注册数据还能够包括诸如网络可访问位置(例如，网站、云服务器)或到其的链接等物品信息。该物品信息能够与一个或多个对相关联，并且可选地可以被公众访问或不能被公众访问。另外，与其他数据库不同，注册表106能够实现物品标识符和公钥的对的新条目的上传或创建(例如，如由刚刚制造与标识符相关联的物品102的注册者所注册的)，而不将数据与标识对的来源的对相关联。换言之，如果需要，注册表106通过将对的来源从公共视图中屏蔽来防止来自竞争对手的注册者能够访问注册表106，并且基于对的数目来确定新产品/物品推出或释放的数量。在一些实施例中，屏蔽是防止公众访问相关联的来源数据的形式。替代地，屏蔽能够是能够在没有任何来源信息的情况下注册新的对的形式，使得即使所有数据都是可公开访问的，注册表106也不包括要访问的任何来源信息(其与对相关联)。替代地，

注册表106向注册者提供包括来源信息的选项，使得来源信息与新的对公开地相关联。

[0032] 而且，如上所述，由注册者与对一起上传到注册器106上的物品信息数据能够包括到网络可访问位置的一个或多个链接或地址(例如，统一资源标识符)，其中位置(例如，云、网站)包括关于物品的信息。在这样的实施例中，当设备104之一扫描/读取一个或多个物品102上的一个或多个标签103时，设备104上的应用107能够将扫描的标签103的公钥和/或唯一标识符传送到注册表106以便取得相关联的一个或多个网络可访问位置。在一些实施例中，该访问是如下所述的接近证明过程的一部分。因此，注册者能够限制对位置的访问，除非设备104能够证明它接近物品102并且帮助提供上述来源屏蔽。替代地或另外地，在注册过程期间，物品信息和相关联的公钥和/或唯一标识符被上传到服务器108和/或设备104，如下面详细描述的。

[0033] 应用107能够包括认证模块、接近模块和描述模块，其中应用107和模块使用应用数据库来存储、维护和访问应用107的操作所必需的数据。认证模块能够在设备104读取耦合到物品102的标签103之一时自动执行下面描述的认证过程。类似地，描述模块也能够在读取标签103之一时在设备104上提供物品描述。特别地，描述模块能够访问存储在设备104和/或服务器108上的物品信息，如上所述。

[0034] 另外，在一些实施例中，应用能够包括登录和注册模块以及支付模块，其中应用用户界面被配置为使得用户能够利用应用模块。登录和注册模块使得用户能够经由图形用户界面输入用户名和密码信息来创建用户简档/账户，用户名和密码信息因此与账户相关联，使得当登录到应用时该信息能够用来标识用户。替代地，可以省略登录信息，并且用户能够使用应用而不创建用户帐户或登录。在创建用户帐户之后，用户能够通过输入用户名和密码来访问帐户以便向应用标识自己。在一些实施例中，在创建账户期间或随后，附加信息能够被存储并且与账户相关联，诸如但不限于联系人信息(例如，电话号码、电子邮件、地址)、提交的内容(例如，物品图像、说明)、账户特权/订阅信息(例如，解锁的应用特征)、系统上的朋友或其他可信账户以及支付信息。在一些实施例中，附加信息由用户在登录到账户时提交。替代地，基于用户与应用的交互，一些或全部附加信息能够被应用自动应用于账户。

[0035] 图3示出了根据一些实施例的使用系统100的物品认证方法。如图3所示，在步骤302，物品102上的标签103的电路206在空中无线地广播存储在标签103上的唯一标识符。替代地，电路206只能在被读取器(例如，设备104的应用107)询问之后广播。在步骤304，标签103附近的设备104的应用107发现标签103和标签103的唯一标识符。在一些实施例中，应用107在设备104上向用户提供认证模块的认证选项并且自动/连续地监测标签103(和/或相关联的标识符)以发现认证选项何时被选择。替代地，应用107能够自动监测标签103(和/或标识符)并且当发现标签103(和/或标识符)时在设备104上显示认证模块的认证选项。在这样的实施例中，在继续剩下的方法步骤之前，应用107能够等待认证选项的选择。在接收到唯一标识符之后，在步骤306，设备103上的应用107通过网络110将唯一标识符传输到开放式注册表106。在接收到唯一标识符之后，在步骤308，开放式注册表106取得与和接收到的唯一标识符相匹配的唯一标识符配对的存储的公钥标识符并且通过网络110将公钥传送到设备104。另外，在一些实施例中，注册表106能够将与唯一标识符相关联的所有权链或其他物品相关数据(例如，当前所有者)传输到设备104。如果没有对与所接收的唯一标识符相匹配，则认证失败并且注册表106改为向设备104发送失败消息，设备104然后经由应用107向

用户指示设备104上的失败。

[0036] 在步骤306和306之后或同时，在步骤310，设备104上的应用107生成询问消息(例如，从注册表106接收的随机数据集，数据集)并且将其传输到标签103。在接收到询问消息之后，在步骤312，标签103的电路206使用存储在标签103上的私钥对询问消息进行数字签名并且经由读取器105将签名的询问(例如，数字签名和询问消息)传输到设备104。在一些实施例中，数字签名是使用私钥的询问消息的散列。替代地，数字签名能够是使用私钥对消息执行的其他调制和/或操作。

[0037] 在步骤314，应用107确定签名的询问的消息是否与原始询问消息相匹配。如果消息不匹配，则认证失败，并且应用107在设备104上向用户指示失败。在步骤316，如果消息匹配，则应用107使用从注册表106接收的公钥来确定来自标签103的数字签名是否有效。在一些实施例中，确定数字签名是否有效包括使用公钥和询问消息来生成公共签名，并且确定它是否匹配或对应于数字签名。替代地，其他签名验证方法能够基于公钥和询问消息来使用。替代地，开放式注册表106能够执行一些或全部签名验证。具体地，开放式注册表106能够从设备104接收询问消息，并且基于公共签名和询问消息生成公共签名并且将其发送到应用107。在这样的实施例中，应用107仅需要确定公共签名是否匹配或对应于来自标签103的数字签名以便确定数字签名是否有效。替代地，应用107能够进一步将从标签103接收的签名消息(例如，数字签名和询问消息)转发到注册表106，使得所有验证由注册表106执行，注册表106然后向设备104指示认证是否成功。

[0038] 如果数字签名未被使用公钥验证或确认，则认证失败并且应用107在设备104上向用户指示失败。在步骤318，如果数字签名被验证/确认，则认证成功并且应用107在设备上向用户指示成功。因此，该方法提供了使得用户能够认证物品102是真实的和/或物品102的当前所有者的优点。在一些实施例中，在设备104上向用户指示成功包括使用描述模块在设备104上向用户呈现对应于物品102的所有权信息链和/或物品信息(例如，存储在设备104、服务器108或两者上)。在这样的实施例中，物品信息的呈现能够包括到物品信息的网络可访问地址的自动导航(例如，经由应用107或web浏览器)和/或向用户的到网络可访问地址的链接的呈现。在一些实施例中，该方法还包括从用户获取所有权证明数据，并且基于注册表106的记录和/或协议来认证所有权证明数据以认证所有权。在这样的实施例中，应用107能够在设备104上向用户指示所有权的成功认证。在一些实施例中，认证方法由IOT设备和自主机器使用来识别对象并且相应地执行它们的编程行为。在一些实施例中，认证方法由IOT设备和自主机器使用来识别其他IOT设备和机器，并且相应地使它们参与到它们的程序中，包括执行任务和建立连接/通信。

[0039] 图4示出了根据一些实施例的呈现物品信息的方法。如图4所示，在步骤402，物品102上的标签103的电路206在空中无线地广播存储在标签103上的唯一标识符。替代地，电路206仅能够在被读取器(例如，设备104的应用107)询问之后广播。在步骤404，在标签103附近的设备104的应用107发现标签103和标签103的唯一标识符。在一些实施例中，应用107在设备104上向用户提供认证模块的认证选项并且自动/连续地监测标签103(和/或相关联的标识符)以发现认证选项何时被选择。替代地，应用107能够自动监测标签103(和/或标识符)并且当发现标签103(和/或标识符)时在设备104上显示认证模块的认证选项。在这样的实施例中，在继续剩下的方法步骤之前，应用107能够等待认证选项的选择。在接收到唯一

标识符之后，在步骤406，设备103上的应用107访问与所接收的唯一标识符相关联的物品信息(在设备104和/或服务器108上)和/或所有权信息链，并且使用描述模块在设备104上向用户呈现所有权信息链/或物品信息。在一些实施例中，物品信息的呈现能够包括到物品信息的网络可访问地址的自动导航(例如，通过应用107或web浏览器)和/或到网络可访问地址的链接在设备104上向用户的呈现。替代地或另外地，物品信息的呈现能够包括在服务器108上、在设备104上本地和/或通过网络110在开放式注册表106上访问与唯一标识符相关联的物品信息。因此，该方法提供了使得用户能够快速找到关于物品的认证信息和/或将其与关于物品的信息一起转发到位置(例如，网站)的优点。

[0040] 图5示出了根据一些实施例的在注册表106上注册物品102的方法。如图5所示，在步骤502，注册者通过网络110将一对或多对公钥和物品唯一标识符上传到开放式注册表106。公钥对应于存储在标签103中的私钥以及公钥与之配对的物品唯一标识符。在步骤504，注册表106向注册者提供使得对中的来源(例如，注册者或所有者)私有或公共可访问的选项。在步骤506，如果选择了私有选项，则注册表106不存储与对相关联的指示对中的来源的任何信息。在步骤508，如果选择了公共选项，则将指示对中的来源的信息连同与对(例如，可选的所有权数据链、其他物品信息数据)相关联的数据一起存储。

[0041] 在步骤510，注册器106使得注册者能够将网络可访问位置(例如，云服务器、网站)与一个或多个对相关联。在一些实施例中，在启用访问数字内容和/或执行与由网络可访问位置提供的对相关的服务或程序之前，网络可访问位置需要证明接近，如下所述。因此，注册方法提供使得所有者或注册者能够在需要的情况下保持匿名和/或限制对与物品102相关联的网络可访问位置(与上传的对相关联)的访问的优点，除非接近证明或认证过程完成。因此，该方法使得注册者能够保护自己免受竞争性的产品大小释放确定，同时仍然利用开放式注册表106。

[0042] 图6示出了根据一些实施例的接近证明方法。如图6所示，在步骤602，物品102上的标签103的电路206在空中无线地广播存储在标签103上的唯一标识符。替代地，电路206仅能够在被读取器(例如，设备104的应用107)询问之后广播。在步骤604，标签103附近的设备104的应用107发现标签103和标签103的唯一标识符。在一些实施例中，应用107在设备104上向用户提供接近证明模块的接近证明选项并且自动地/连续地监测标签103(和/或相关联的标识符)以发现接近证明选项何时被选择。替代地，应用107能够自动监测标签103(和/或标识符)并且当发现标签103(和/或标识符)时在设备104上显示接近证明模块的接近证明选项。在这样的实施例中，应用107能够在继续剩余的方法步骤之前等待接近证明选项的选择。在一些实施例中，接近证明和认证选项能够由应用107同时和/或并发地呈现，使得用户能够选择他们是否想要对所发现的标签103执行认证方法、接近方法或两者。

[0043] 在接收到唯一标识符之后，在步骤606，应用107访问开放式注册表106并且使用唯一标识符来取得存储在注册表106上的相关联的网络可访问位置。另外，在一些实施例中，应用107能够同时访问与注册表106上的唯一标识符相关联的其他数据(例如，所有权链和/或其他物品信息数据)。如果没有对与接收到的唯一标识符相匹配，则接近证明失败并且设备104经由应用107在设备104上向用户指示失败。替代地，如果网络可访问位置和相关联的唯一标识符存储在服务器108和/或设备104上，则设备104上的应用107能够省略与注册表106的通信，并且代替地本地地或以相同的方式从服务器108获取与唯一标识符相关联的网

络可访问位置。

[0044] 在步骤608，应用107请求访问网络可访问位置和/或在该位置提供的服务。在一些实施例中，服务包括与唯一标识符(和/或耦合到标签103的物品102)相关的数字内容、原始数据、程序的执行或其他服务中的一个或多个。在步骤610，网络可访问位置(例如，云服务器、网站服务器)响应于访问请求来生成并且在设备104上向应用107传输接近询问消息。在一些实施例中，接近询问消息能够类似于上述认证询问消息。例如，接近询问消息能够是随机字符串、唯一标识符或其他数据集。在步骤612，在接收到接近询问消息时，设备104上的应用107将消息转发给标签103的电路206，标签103的电路206使用存储在标签103上的私钥对询问消息进行数字签名。然后，在步骤614，电路206经由读取器105向设备104传输签名的接近询问(例如，数字签名和询问消息)，设备104然后经由网络110将其转发到网络可访问位置。在一些实施例中，数字签名是使用私钥的询问消息的散列。替代地，数字签名能够是使用私钥对消息进行的其他调制或操作。

[0045] 在步骤618，网络可访问位置使用公钥确定签名的接近询问消息是否有效。在一些实施例中，网络可访问位置在本地存储与唯一标识符相配对的公钥的副本。替代地，该位置能够从注册表106、服务器108、设备104或其组合请求/接收公钥。签名的询问的验证能够以与上述物品认证方法中所述的签名的认证消息的验证相同的方式来执行。具体地，如果签名的询问与原始接近询问消息相匹配，并且所提交的签名针对与标签103的私钥相关联的公钥进行验证，则网络可访问位置能够确定有效性。在步骤618，如果验证失败(例如，由于消息不匹配和/或由于签名不正确)，则接近证明失败并且位置向应用107发送在设备104上向用户指示失败的失败消息。在步骤620，如果数字签名被验证/确认，则接近证明成功，使得位置向设备/应用104/107提供对由位置提供的服务的访问。然后，应用107能够向用户提供经由设备104对服务的访问。因此，该方法提供了使得注册者能够在提供从网络可访问位置对物品相关信息和/或特征的访问之前要求接近证明的优点。实际上，这还用于帮助确保注册表106的匿名，因为物品相关信息(其可能指示物品102的来源/注册者)能够与开放式注册表106上的数据分离(使得它从公众被屏蔽)。

[0046] 在一些实施例中，网络可访问位置能够基于与其他协议(例如，开发者令牌、用户认证)结合的接近证明方法来限制访问，使得两者必须被满足才能被授予访问权限。在一些实施例中，网络可访问位置是在区块链数据库(例如，注册表106)上操作的智能合约。在一些实施例中，提供对位置的内容/特征的访问能够包括由设备104(例如，经由应用107或web浏览器)对网络可访问地址的自动导航和/或到网络可访问地址的链接在设备/应用104/107上向用户的呈现。在一些实施例中，设备104和/或服务器108上的应用107能够执行签名的接近询问消息的验证。在这样的实施例中，如果在设备104上执行，则不需要转发签名的消息，而是从注册表106和/或网络可访问位置请求/接收公钥以执行验证。类似地，如果由服务器108(例如，由服务器108上的代理/应用107)执行，则签名的消息被转发到服务器108，服务器108当前从注册表106和/或网络可访问位置存储或请求/接收公钥以执行验证。本文中描述的网络可访问位置能够指代地址本身和/或操作网站和/或在网络可访问位置处提供的其他服务的计算机/服务器。

[0047] 图7示出了根据一些实施例的被配置为实现系统100的示例性计算设备700的框图。除了上述特征之外，计算设备104和/或服务器108能够基本上类似于设备700。通常，适

合于实现计算设备700的硬件结构包括网络接口702、存储器704、处理器706、一个或多个I/O设备708(例如,读取器105)、总线710和存储设备712。替代地,所示部件中的一个或多个能够被去除或替代本领域公知的其他部件。处理器的选择并不重要,只要选择具有足够速度的合适的处理器即可。存储器704能够是本领域已知的任何常规计算机存储器。存储设备712能够包括硬盘驱动器、CDROM、CDRW、DVD、DVDRW、闪存卡或任何其他存储设备。计算设备700能够包括一个或多个网络接口702。网络接口的示例包括连接到以太网或其他类型的LAN的网卡。一个或多个I/O设备708能够包括以下中的一个或多个:键盘、鼠标、监视器、显示器、打印机、调制解调器、触摸屏、按钮接口和其他设备。认证系统应用107或其一个或多个模块可能被存储在存储设备712和存储器704中,并且在应用通常被处理时被处理。图7所示的更多或更少的部件能够被包括在计算设备700中。在一些实施例中,包括认证系统硬件720。尽管图7中的计算设备700包括用于认证系统的应用730和硬件720,但是认证系统能够以硬件、固件、软件或其任何组合在计算设备上实现。

[0048] 已经在包含细节的特定实施例方面描述了本发明,以支持理解本发明的构造和操作的原理。本文中对具体实施例及其细节的这样的引用不意图限制所附权利要求的范围。本领域技术人员将容易明白,在不脱离由权利要求限定的本发明的精神和范围的情况下,可以对为了说明而选择的实施例进行其他各种修改。

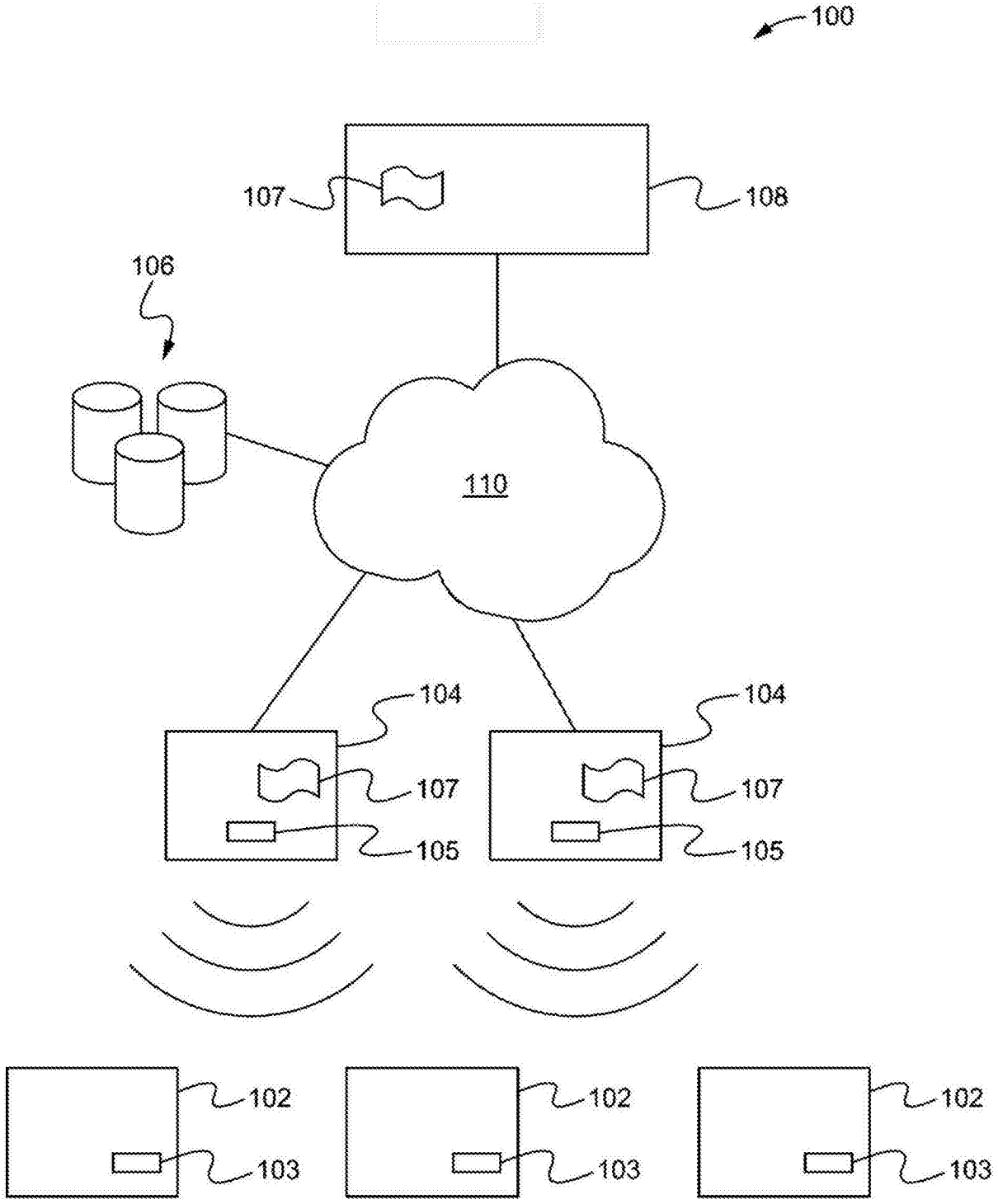

100
107
108
106
110
104
104
107
107
105
105
102
102
102
103
103
103

图1

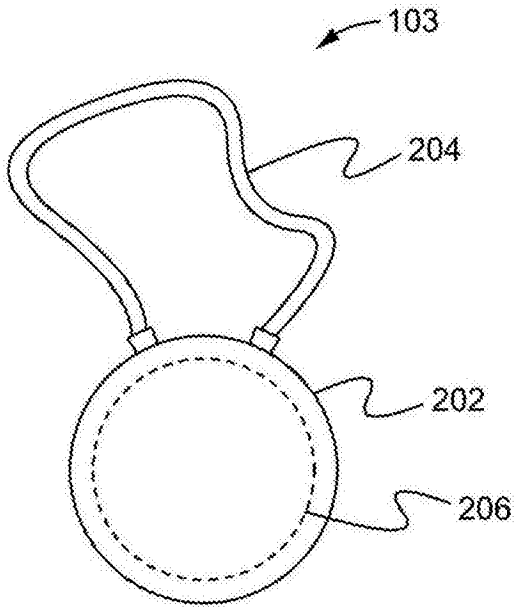


图2A

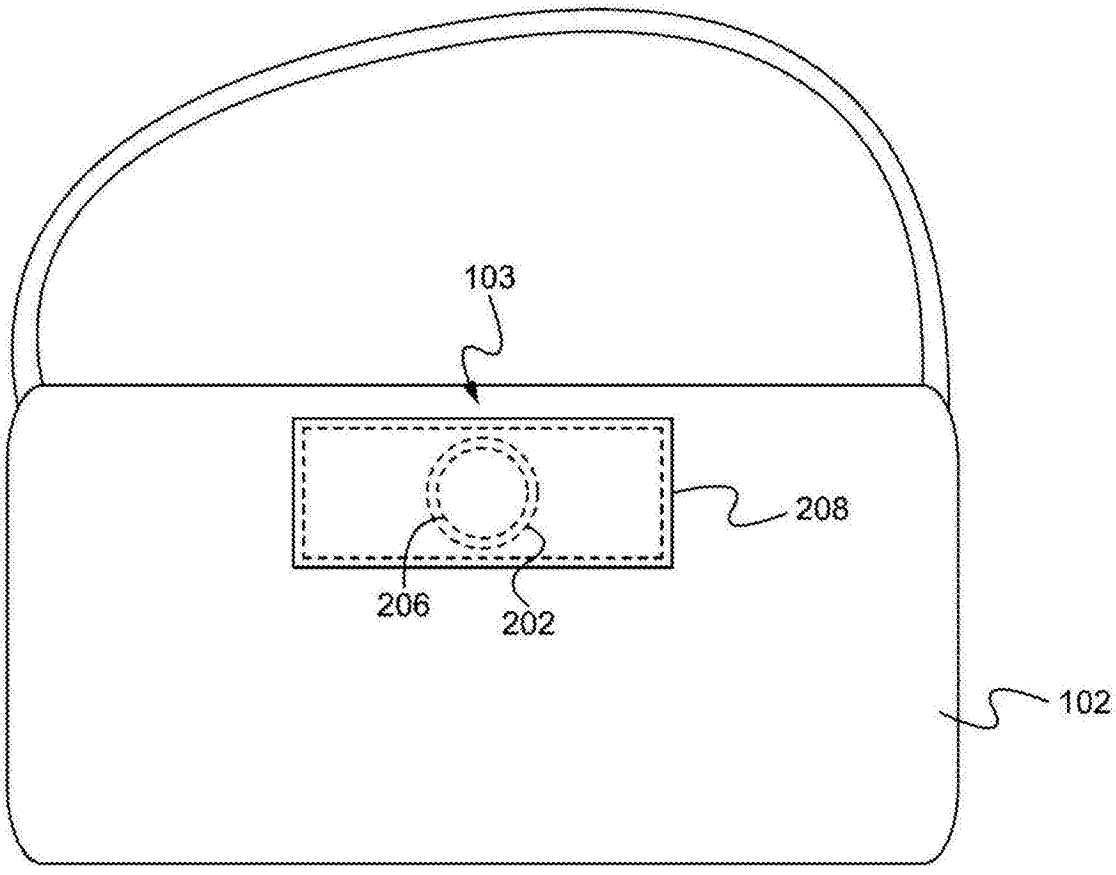


图2B

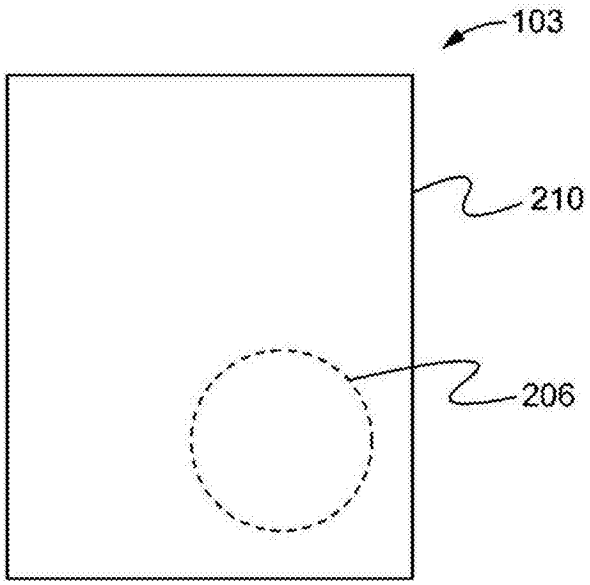


图2C

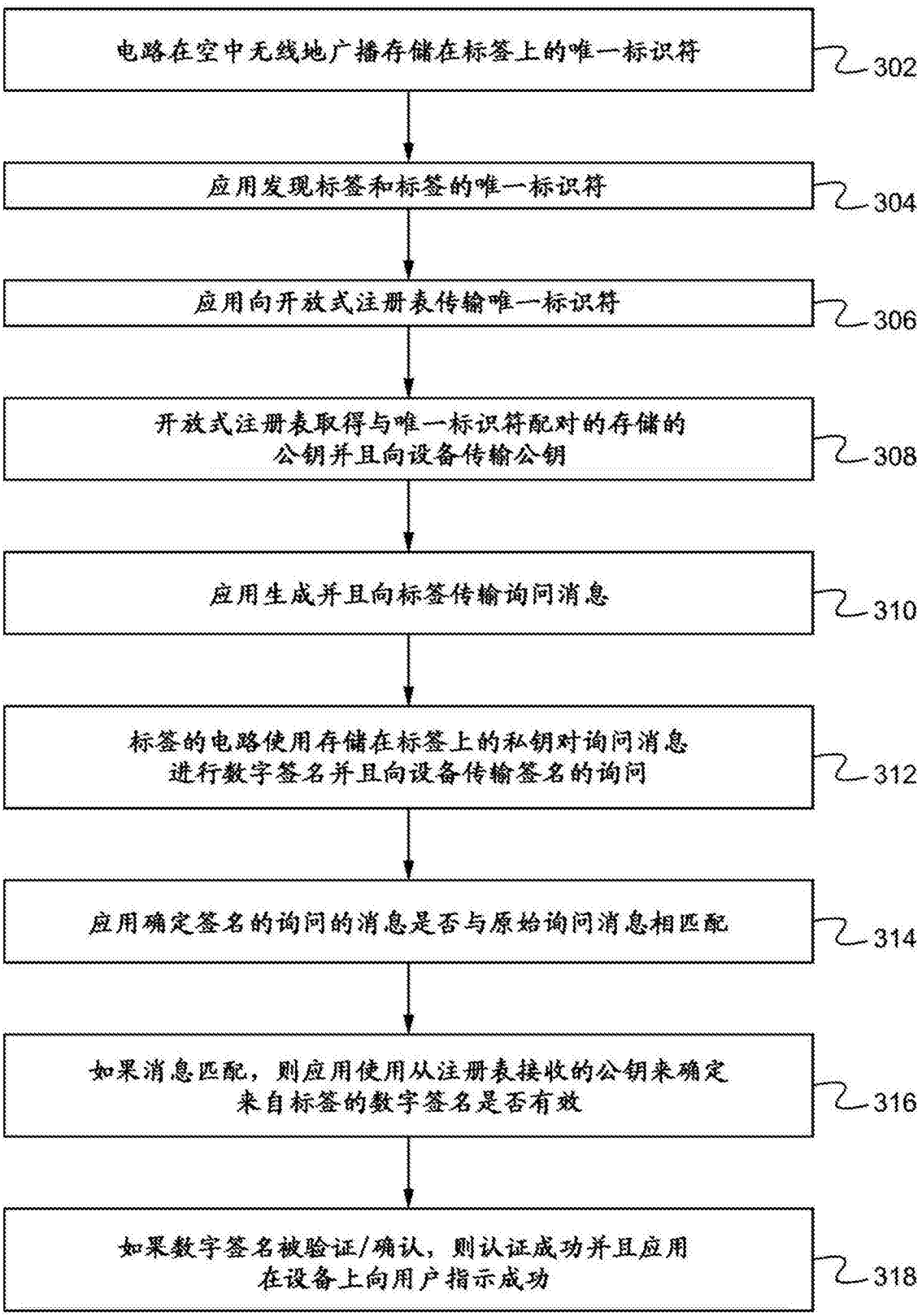

电路在空中无线地广播存储在标签上的唯一标识符
302
应用发现标签和标签的唯一标识符
304
应用向开放式注册表传输唯一标识符
306
开放式注册表取得与唯一标识符配对的存储的公钥并且向设备传输公钥
308
应用生成并且向标签传输询问消息
310
标签的电路使用存储在标签上的私钥对询问消息进行数字签名并且向设备传输签名的询问
312
应用确定签名的询问的消息是否与原始询问消息相匹配
314
如果消息匹配，则应用使用从注册表接收的公钥来确定来自标签的数字签名是否有效
316
如果数字签名被验证/确认，则认证成功并且应用在设备上向用户指示成功
318

图3

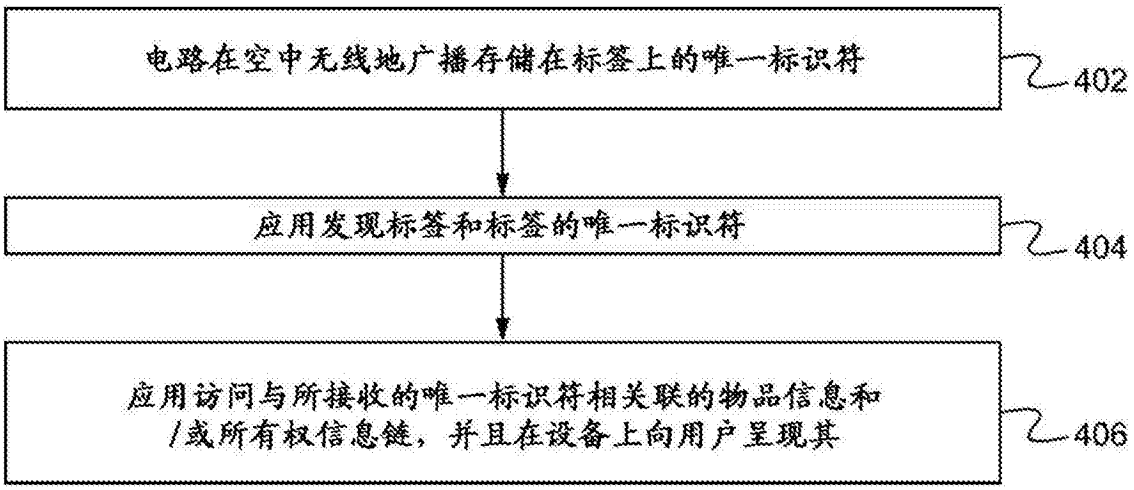

电路在空中无线地广播存储在标签上的唯一标识符
402
应用发现标签和标签的唯一标识符
404
应用访问与所接收的唯一标识符相关联的物品信息和/或所有权信息链，并且在设备上向用户呈现其
406

图4

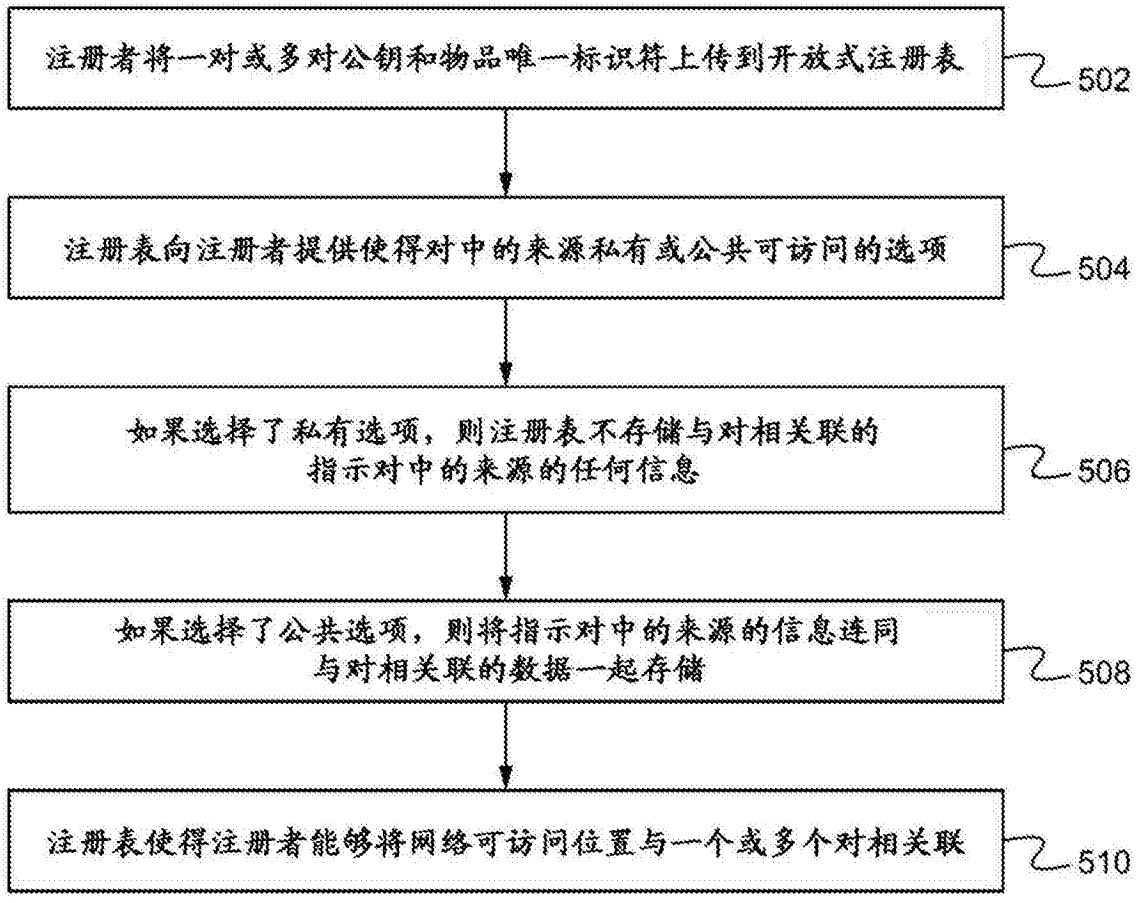

注册者将一对或多对公钥和物品唯一标识符上传到开放式注册表
502
注册表向注册者提供使得对中的来源私有或公共可访问的选项
504
如果选择了私有选项，则注册表不存储与对相关联的指示对中的来源的任何信息
506
如果选择了公共选项，则将指示对中的来源的信息连同与对相关联的数据一起存储
508
注册表使得注册者能够将网络可访问位置与一个或多个对相关联
510

图5

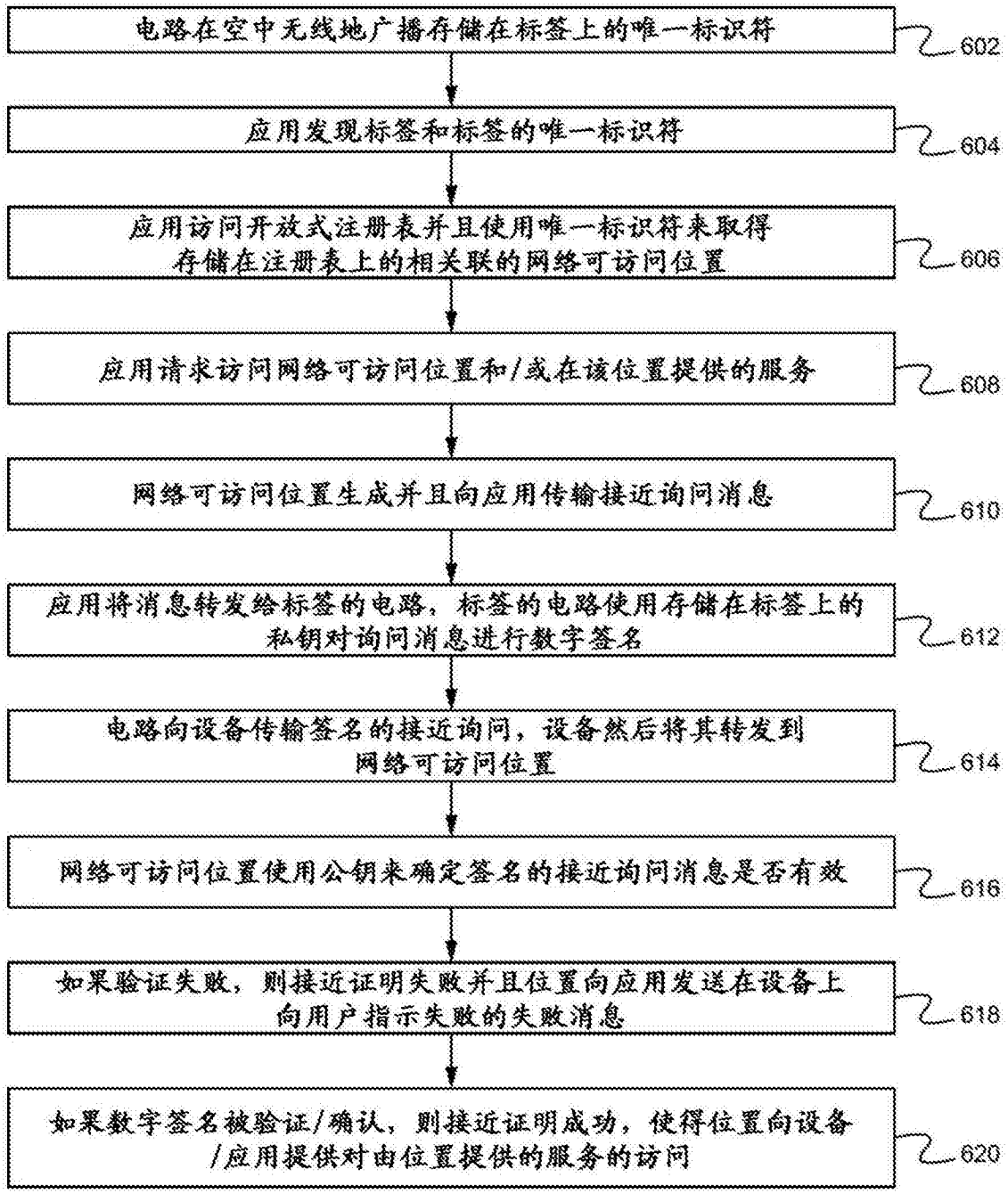

电路在空中无线地广播存储在标签上的唯一标识符
602
应用发现标签和标签的唯一标识符
604
应用访问开放式注册表并且使用唯一标识符来取得
存储在注册表上的相关联的网络可访问位置
606
应用请求访问网络可访问位置和/或在该位置提供的服务
608
网络可访问位置生成并且向应用传输接近询问消息
610
应用将消息转发给标签的电路，标签的电路使用存储在标签上的
私钥对询问消息进行数字签名
612
电路向设备传输签名的接近询问，设备然后将其转发到
网络可访问位置
614
网络可访问位置使用公钥来确定签名的接近询问消息是否有效
616
如果验证失败，则接近证明失败并且位置向应用发送在设备上
向用户指示失败的失败消息
618
如果数字签名被验证/确认，则接近证明成功，使得位置向设备
/应用提供对由位置提供的服务的访问
620

图6

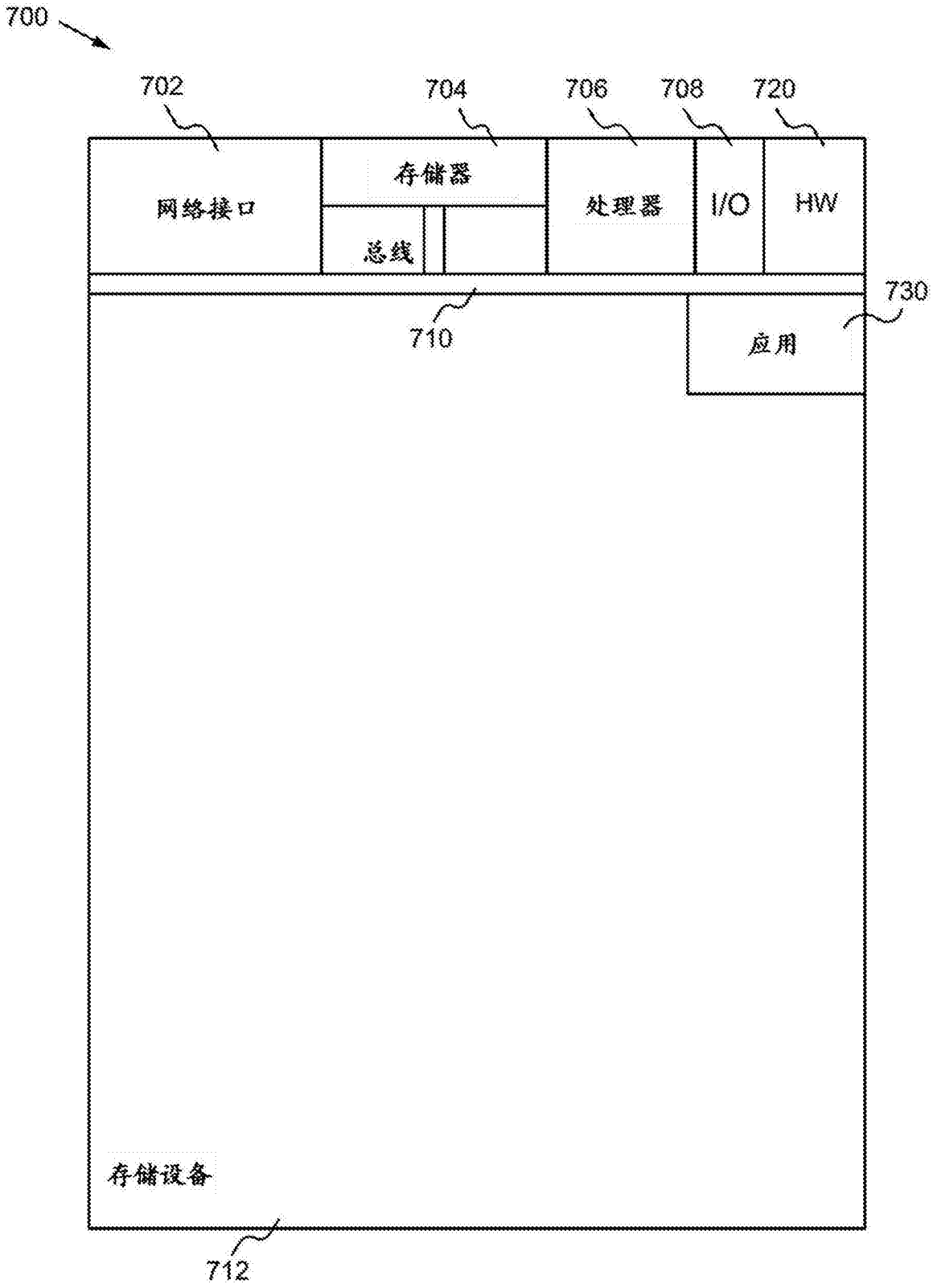


图7