(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108701276 B
(45)授权公告日 2022.04.12

(21)申请号 201680063454.0
(22)申请日 2016.10.14
(65)同一申请的已公布的文献号
申请公布号 CN 108701276 A
(43)申请公布日 2018.10.23
(30)优先权数据
62/241,436 2015.10.14 US
62/264,418 2015.12.08 US
62/325,880 2016.04.21 US
62/380,467 2016.08.28 US
(85)PCT国际申请进入国家阶段日
2018.04.27
(86)PCT国际申请的申请数据
PCT/US2016/057232 2016.10.14
(87)PCT国际申请的公布数据
WO2017/066715 EN 2017.04.20

(73)专利权人 剑桥区块链有限责任公司
地址 美国马萨诸塞州
(72)发明人 亚历克斯·奥伯豪泽尔
马修·康芒斯 阿洛科·巴尔加瓦
(74)专利代理机构 北京睿邦知识产权代理事务所(普通合伙) 11481
代理人 徐丁峰 张玮

(51)Int.Cl.
G06Q 10/06(2006.01)
H04L 9/32(2006.01)
(56)对比文件
CN 103312675 A,2013.09.18
CN 101425903 A,2009.05.06
CN 1308803 A,2001.08.15
CN 101546407 A,2009.09.30
US 2015244690 A1,2015.08.27
审查员 贾越

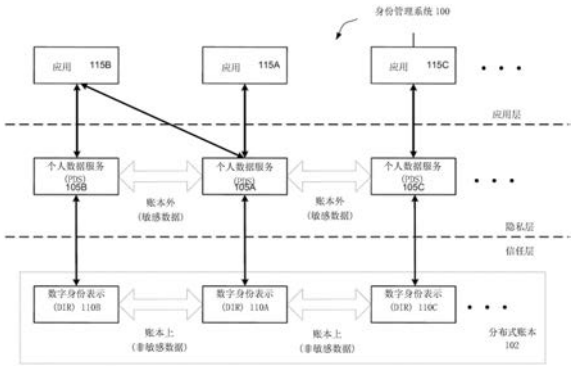
权利要求书4页 说明书28页 附图10页

(54)发明名称

用于管理数字身份的系统和方法

(57)摘要

用于管理数字身份的系统和方法。在一些实施例中,提供了一种方法,所述方法包括以下动作:使用从用户获取的多个测量值来为用户生成标识符,该标识符包括所述多个测量值的加密证据;实例化与该用户的标识符相关联的数字身份表示,该数字身份表示包括实现用于证明的规则的程序代码;在数字身份表示上生成电子签名;以及将数字身份表示和电子签名发布到分布式账本系统。



CN 108701276 B

1.一种计算机实现的方法,包括以下动作:

使用指针从分布式账本系统访问身份所有者的至少一个属性的至少一个证明,其中:

所述至少一个证明可在所述分布式账本系统中的至少两个状态之间移动,所述至少两个状态包括已验证状态,

所述至少一个证明包括加密证据;且

所述至少一个证明从存储在所述分布式账本中的数字身份表示访问;

经由所述分布式账本外部的通道接收对应于所述至少一个属性的值;以及

确定所述至少一个属性的所述至少一个证明是否处于所述已验证状态;

确定是否信任指示为负责验证所述至少一个证明的实体;

确定所述至少一个证明中的所述加密证据是否是所接收的对应于所述至少一个属性的值的有效证据;

确定所述至少一个证明是否由所述指示为负责验证所述至少一个证明的实体电子签名;以及

响应于确定所述至少一个证明处于所述已验证状态,所述指示为负责验证所述至少一个证明的实体是被信任的,所述加密证据是所接收的值的有效证据,并且所述至少一个证明由所述负责验证所述至少一个证明的实体电子签名:

与所述身份所有者进行交易。

2.根据权利要求1所述的计算机实现的方法,其中:

所述分布式账本系统使用至少一个区块链实现。

3.根据权利要求1所述的计算机实现的方法,其中所述至少一个证明存储在与所述身份所有者相关联的徽章中,并且其中所述指针包括对所述徽章的引用。

4.根据权利要求3所述的计算机实现的方法,其中:

所述徽章根据从用于徽章的多个模式中选择的模式生成,所述模式包括多个属性,所述多个属性包括所述至少一个属性。

5.根据权利要求1所述的计算机实现的方法,其中所述至少一个证明的所述至少两个状态包括未决状态,并且其中所述方法进一步包括以下动作:

当所述对应于所述至少一个属性的值已经由所述指示为负责验证所述至少一个证明的实体所验证,使所述至少一个证明从所述未决状态转变为所述已验证状态。

6.根据权利要求1所述的计算机实现的方法,其中所述至少一个证明的所述至少两个状态包括过期状态,并且其中所述方法进一步包括以下动作:

在当上次验证所述对应于所述至少一个属性的值时设置的定时器过期后,使所述至少一个证明从所述已验证状态转变为所述过期状态。

7.根据权利要求1所述的计算机实现的方法,其中:

仅当所述至少一个证明处于所述已验证状态时,允许访问所述至少一个证明中的所述加密证据。

8.根据权利要求1所述的计算机实现的方法,其中所述身份所有者是用户。

9.根据权利要求1所述的计算机实现的方法,其中所述数字身份表示与所述身份所有者相关联并包括实现用于证明的规则的程序代码。

10.一种计算机系统,包括:

至少一个处理器;以及

存储多个指令的至少一个非暂时性计算机可读介质,当所述至少一个处理器执行所述多个指令时,所述多个指令使所述至少一个处理器:

使用指针从分布式账本系统访问身份所有者的至少一个属性的至少一个证明,其中:

所述至少一个证明可在所述分布式账本系统中的至少两个状态之间移动,所述至少两个状态包括已验证状态,

所述至少一个证明包括加密证据;且

所述至少一个证明从存储在所述分布式账本中的数字身份表示访问;

经由所述分布式账本外部的通道接收对应于所述至少一个属性的值;以及

确定所述至少一个属性的所述至少一个证明是否处于所述已验证状态;

确定是否信任指示为负责验证所述至少一个证明的实体;

确定所述至少一个证明中的所述加密证据是否是所接收的对应于所述至少一个属性的值的有效证据;

确定所述至少一个证明是否由所述指示为负责验证所述至少一个证明的实体电子签名;以及

响应于确定所述至少一个证明处于所述已验证状态,信任所述指示为负责验证所述至少一个证明的实体,所述加密证据是所接收的值的有效证据,并且所述至少一个证明由所述负责验证所述至少一个证明的实体电子签名:

与所述身份所有者进行交易。

11.根据权利要求10所述的计算机系统,其中:

所述分布式账本系统使用至少一个区块链实现。

12.根据权利要求10所述的计算机系统,其中所述至少一个证明存储在与所述身份所有者相关联的徽章中,并且其中所述指针包括对所述徽章的引用。

13.根据权利要求12所述的计算机系统,其中:

所述徽章根据从用于徽章的多个模式中选择的模式生成,所述模式包括多个属性,所述多个属性包括所述至少一个属性。

14.根据权利要求10所述的计算机系统,其中所述至少一个证明的所述至少两个状态包括未决状态,并且其中当所述至少一个处理器执行所述多个指令时,所述多个指令进一步使所述至少一个处理器:

当所述对应于所述至少一个属性的值已经由所述指示为负责验证所述至少一个证明的实体所验证,使所述至少一个证明从所述未决状态转变为所述已验证状态。

15.根据权利要求10所述的计算机系统,其中所述至少一个证明的所述至少两个状态包括过期状态,并且其中当所述至少一个处理器执行所述多个指令时,所述多个指令进一步使所述至少一个处理器:

在当上次验证所述对应于所述至少一个属性的值时设置的定时器过期后,使所述至少一个证明从所述已验证状态转变为所述过期状态。

16.根据权利要求10所述的计算机系统,其中:

仅当所述至少一个证明处于所述已验证状态时,允许访问所述至少一个证明中的所述加密证据。

17.根据权利要求10所述的计算机系统，其中所述身份所有者是用户。

18.根据权利要求10所述的计算机系统，其中所述数字身份表示与所述身份所有者相关联并包括实现用于证明的规则的程序代码。

19.一种用多个指令编码的非暂时性计算机可读介质，当至少一个处理器执行所述多个指令时，执行包括以下动作的方法：

使用指针从分布式账本系统访问身份所有者的至少一个属性的至少一个证明，其中：

所述至少一个证明可在所述分布式账本系统中的至少两个状态之间移动，所述至少两个状态包括已验证状态，且

所述至少一个证明包括加密证据；

所述至少一个证明从存储在所述分布式账本中的数字身份表示访问；

经由所述分布式账本外部的通道接收对应于所述至少一个属性的值；以及

确定所述至少一个属性的所述至少一个证明是否处于所述已验证状态；

确定是否信任指示为负责验证所述至少一个证明的实体；

确定所述至少一个证明中的所述加密证据是否是所接收的对应于所述至少一个属性的值的有效证据；

确定所述至少一个证明是否由所述指示为负责验证所述至少一个证明的实体电子签名；以及

响应于确定所述至少一个证明处于所述已验证状态，所述指示为负责验证所述至少一个证明的实体是被信任的，所述加密证据是所接收的值的有效证据，并且所述至少一个证明由所述负责验证所述至少一个证明的实体电子签名：

与所述身份所有者进行交易。

20.根据权利要求19所述的非暂时性计算机可读介质，其中：

所述分布式账本系统使用至少一个区块链实现。

21.根据权利要求19所述的非暂时性计算机可读介质，其中所述至少一个证明存储在与所述身份所有者相关联的徽章中，并且其中所述指针包括对所述徽章的引用。

22.根据权利要求21所述的非暂时性计算机可读介质，其中：

所述徽章根据从用于徽章的多个模式中选择的模式生成，所述模式包括多个属性，所述多个属性包括所述至少一个属性。

23.根据权利要求19所述的非暂时性计算机可读介质，其中所述至少一个证明的所述至少两个状态包括未决状态，并且其中所述方法进一步包括以下动作：

当所述对应于所述至少一个属性的值已经由所述指示为负责验证所述至少一个证明的实体所验证，使所述至少一个证明从所述未决状态转变为所述已验证状态。

24.根据权利要求19所述的非暂时性计算机可读介质，其中所述至少一个证明的所述至少两个状态包括过期状态，并且其中所述方法进一步包括以下动作：

在当上次验证所述对应于所述至少一个属性的值时设置的定时器过期后，使所述至少一个证明从所述已验证状态转变为所述过期状态。

25.根据权利要求19所述的非暂时性计算机可读介质，其中：

仅当所述至少一个证明处于所述已验证状态时，允许访问所述至少一个证明中的所述加密证据。

26.根据权利要求19所述的非暂时性计算机可读介质,其中所述身份所有者是用户。

27.根据权利要求19所述的非暂时性计算机可读介质,其中所述数字身份表示与所述身份所有者相关联并包括实现用于证明的规则的程序代码。

用于管理数字身份的系统和方法

[0001] 相关专利申请

[0002] 本申请依据35 U.S.C.§119(e)要求2016年8月28日提交的名称为“AN APPROACH FOR STRONG DIGITAL IDENTITIES”的美国临时申请序列号62/380,467的优先权，该申请全文引入本文以供参考。本申请依据35 U.S.C.§119(e)要求2016年4月21日提交的名称为“COUNTERPARTY CHECKS IN THE CONTEXT OF A BLOCKCHAIN ECOSYSTEM”的美国临时申请序列号62/325,880的优先权，该申请全文引入本文以供参考。本申请依据35 U.S.C.§119(e)要求2015年12月8日提交的名称为“SELECTIVE INFORMATION SHARING PLATFORM”的美国临时申请序列号62/264,418的优先权，该申请全文引入本文以供参考。本申请依据35 U.S.C.§119(e)要求2015年10月14日提交的名称为“IDENTITY MANAGEMENT WITH A MULTI-BLOCKCHAIN APPROACH”的美国临时申请序列号62/241,436的优先权，该申请全文引入本文以供参考。

背景技术

[0003] 几乎所有组织(例如，政府机构、医疗保健机构、金融机构、零售商、社交网络服务提供商、雇主等)都收集和维护个人数据。在某些受到严格监管的行业(例如银行和保险)中，要求组织建立严格的“了解客户”流程来验证客户身份。这些流程对于防止身份盗窃、金融诈骗、洗钱和恐怖主义融资十分重要。

[0004] 此类个人数据宝库经常因财务、政治或其他原因而被滥用。为了保护公民的隐私，许多国家政府通过了限制组织可以处理个人数据的方式的法规。

发明内容

[0005] 在一些实施例中，提供了一种计算机实现的方法，该方法包括以下动作：使用从用户获取的多个测量值来为用户生成标识符，该标识符包括所述多个测量值的加密证据；实例化与该用户的标识符相关联的数字身份表示，该数字身份表示包括实现用于证明的规则的程序代码；在数字身份表示上生成电子签名；以及将数字身份表示和电子签名发布到分布式账本系统。

[0006] 在一些实施例中，提供了一种计算机实现的方法，该方法包括以下动作：从用于徽章的多个模式中选择模式，该模式包括多个属性；根据所述模式生成用于证明用户身份的徽章，其中生成的动作包括：识别多个值，每个值对应于所述模式中的所述多个属性中的属性；为所述多个值中的每个值生成至少一个加密证据；以及识别用于验证所述多个值的可信实体；以及将徽章发布到分布式账本系统。

[0007] 在一些实施例中，提供了一种计算机实现的方法，该方法包括：经由分布式账本系统接收验证徽章的请求，该徽章包括分别对应于用户的多个属性的多个属性证明，其中对于每个属性，对应的属性证明包括加密证据；经由分布式账本系统外部的通道接收分别对应于所述多个属性的多个值；对于所述多个属性中的至少一个属性：验证与所述至少一个属性相对应的值是否是所述用户的所述至少一个属性的正确值；以及响应于验证对应于所

述至少一个属性的值是所述用户的所述至少一个属性的正确值，经由分布式账本系统使得对应于所述至少一个属性的属性证明处于已验证状态。

[0008] 在一些实施例中，一种计算机实现的方法包括：经由分布式账本系统接收验证第一徽章的请求，第一徽章包括分别对应于用户的多个属性的多个属性证明，其中对于每个属性，对应的属性证明包括加密证据；经由分布式账本系统外部的通道接收分别对应于所述多个属性的多个值；对于所述多个属性中的至少一个属性：从第一徽章识别对应于所述至少一个属性的第一属性证明，第一属性证明包括第一加密证据；从第一属性证明识别指向第二徽章的指针；使用所述指针从分布式账本访问第二徽章；从第二徽章识别负责验证第二徽章的实体以及对应于所述至少一个属性的第二属性证明；确定负责验证第二徽章的实体是否可信；以及响应于确定负责验证第二徽章的实体是可信的，检查：(1)第二属性证明是否处于已验证状态；(2)第二加密证据是否是对应于所述至少一个属性的接收值的有效证据；以及(3)第二属性证明是否由负责验证第二徽章的实体电子签名。

[0009] 根据一些实施例，提供了一种系统，该系统包括至少一个处理器和其上存储有指令的至少一个计算机可读存储介质，所述指令在被执行时对所述至少一个处理器编程以执行上述方法中的任何一种。

[0010] 根据一些实施例，提供了其上存储有指令的至少一个计算机可读存储介质，所述指令在被执行时对至少一个处理器编程以执行上述方法中的任何一种。

附图说明

[0011] 图1示出了根据一些实施例的说明性身份管理系统100。

[0012] 图2示出了根据一些实施例的说明性个人数据服务(PDS)200。

[0013] 图3示出了根据一些实施例的说明性数字身份表示(DIR)300。

[0014] 图4示出了根据一些实施例的管理属性证明的不同状态之间的转变的说明性状态机400。

[0015] 图5示出了根据一些实施例的用于证明的说明性过程500。

[0016] 图6示出了根据一些实施例的说明性信任结构600。

[0017] 图7示出了根据一些实施例的用于交易对手检查的说明性过程700。

[0018] 图8示出了根据一些实施例的用于隐私层组件(例如PDS)中的数据改变和信任层(例如DIR)中的所得状态改变的说明性过程800。

[0019] 图9示出了根据一些实施例的网络900中的说明性分布式账本发现机制。

[0020] 图10示意性地示出了可以在其上实现本公开的任何方面的说明性计算机10000。

具体实施方式

[0021] 本公开的方面涉及用于管理数字身份的系统和方法。

[0022] 为了遵守限制个人数据共享的隐私法规，许多组织实施了自己的数字身份管理系统。发明人已经认识并意识到这种方法可能是低效的。例如，用户可能需要为用户希望创建的每个帐户完成单独的身份验证过程，例如银行帐户、经纪帐户、保险帐户、退休金帐户、医疗保健提供商帐户、公用事业帐户等。同样，用户可能需要完成单独的身份验证过程以获准进入每个受限区域，例如办公楼、校园、休闲娱乐区等。在每个身份验证过程中，用户可能需

要提供相同的个人数据(例如,名字、姓氏、驾驶证号码、出生日期、社会安全号码等)。在一些情况下,繁琐的身份验证过程可能延迟交易,和/或阻止用户完成交易。因此,在一些实施例中,提供了用于简化身份验证过程并由此改善用户体验的技术。

[0023] 发明人已经认识并意识到,从组织的角度来看,也可能存在低效率。例如,客户可能已经在美国的A银行拥有一个帐户,并可能请求在德国的相同的A银行创建一个新帐户。在这种情况下,A银行可能再次执行身份验证,即使客户的身份在创建美国帐户时已经被验证。因此,可能执行冗余的过程,并且可能维护重复的记录,从而浪费时间和资源(例如,处理器周期、存储等)。因此,在一些实施例中,提供了用于减少冗余同时保持适当安全级别的技术。

[0024] I.个人数据服务

[0025] 在一些实施例中,可以提供以所有者为中心的身份管理方法,其允许用户控制与实体(例如,另一用户或组织)共享个人识别信息(PII)和/或其他个人数据的一个或多个项目的方式。例如,个人数据服务(PDS)可以用于存储个人数据,并且可以提供用户接口,用户可以通过该用户接口管理个人数据(例如,通过添加、删除和/或修改一个或多个项目)。附加地或备选地,PDS可以提供一个或多个应用程序编程接口(API),其可以由诸如移动或web应用程序的软件应用程序调用。例如,当用户下载应用程序并试图开立帐户时,该应用程序可以调用PDS的API来启动身份验证过程。该应用程序可以通知PDS哪个实体在请求验证,和/或个人数据的哪些项目将被验证。

[0026] 在一些实施例中,PDS可以被编程以例如通过限制对存储在PDS中的个人数据的访问来保护隐私。例如,可能需要一个或多个凭证来认证试图登录到PDS以查看或修改个人数据的用户。附加地或备选地,PDS可以仅在已认证用户明确指示时与实体共享个人数据的一个或多个项目。

[0027] 在一些实施例中,PDS可以实现为虚拟容器,其不仅包括用户接口、应用程序编程接口、数据管理、信任管理和/或其他功能,而且还包括运行时环境(例如,具有库、配置文件等)。发明人已经认识并意识到,将PDS实现为容器可以有助于部署到不同的计算平台。然而,应当理解,本公开的方面不限于将PDS实现为容器,因为其他实施方式也可能是合适的。

[0028] II.信任结构

[0029] 在一些实施例中,可以提供信任结构以允许证明(例如,身份证明)在多个实体均被信赖,从而减少冗余。例如,如果用户已经完成了第一组织(例如,诸如机动车辆管理局或DMV的政府机构)的身份验证过程,并且正试图在第二组织(例如,公用事业公司)开立帐户,则只要第二组织信任第一组织,就可以大大简化第二组织的身份验证过程。因此,在一些实施例中,提供了用于实现信任结构的技术,该信任结构允许组织简单地检查个人数据项目已经被另一组织验证,而不必再次验证该个人数据项目。

[0030] 在一些实施例中,可以提供信任结构,该信任结构允许用户精确地指定要与哪个实体共享和/或向哪个实体证明哪些个人数据项目。例如,当第一组织(例如,DMV)验证多项个人数据(例如,出生日期、社会安全号码等)时,可以为每个项目提供单独的证据。以这种方式,用户随后可以决定向第二组织(例如,提供酒精饮料的酒吧)提交第一项目的证据(例如,超过21岁),而不提交第二项目的证据(例如,社会安全号码、家庭地址,或者甚至确切的出生日期)。

[0031] III.分布式账本

[0032] 2009年推出的比特币协议使用区块链来提供没有中央结算所的数字货币。区块链在网络中的多个节点之间被共享，并用于以密码安全方式记录和检查交易。例如，虽然新的交易可以被附加到区块链，但是在不破坏加密证据链的情况下，不能改变过去的交易。

[0033] 比特币协议使用区块链的防篡改特性来强化某些规则。例如，一旦第一实体向第二实体发送比特币，交易的记录就通过网络传播，并且除非攻击者控制网络中一半以上的处理能力，否则交易不能被逆转。以这种方式，第三实体可以容易地发现第一实体不再拥有该比特币，使得第一实体不能双倍地花费该比特币。

[0034] 发明人已经认识并意识到，诸如区块链的分布式账本可以用于除数字货币之外的应用中。例如，分布式账本可以用于实现信任结构以允许证明(例如，身份证明)在多个实体均被信赖。在一些实施例中，分布式账本可以用于记录可信实体提供的证明，使得其他实体不需要单独地验证已证明的事实。

[0035] IV.身份管理协议

[0036] 发明人已经认识并意识到数字身份管理中的各种相互矛盾的问题。例如，可能希望限制对用户的个人数据的访问(例如，通过将个人数据存储在由用户控制的虚拟容器中)，从而保护用户的隐私。另一方面，可能希望使用透明机制来记录证明(例如，通过将证明存储在在网络中的多个节点处复制的公共可用数据结构中)，使得攻击者不能容易地伪造证明。因此，在一些实施例中，提供了允许用户控制共享多少个人数据同时保持证明的透明度的方式。以这种方式，可以在不过度共享个人数据的情况下实现信任结构。

[0037] 在一些实施例中，可以提供身份管理协议以允许通过用于记录证明的透明机制来实现隐私保护。例如，可以提供包括信任层、隐私层和应用层这三层的协议栈。信任层可以包括用于存储证明的分布式账本，隐私层可以包括由各个用户控制的虚拟容器，并且应用层可以包括使用身份管理协议来验证身份和/或其他个人数据的一个或多个应用。

[0038] 在一些实施例中，可以在身份管理协议的不同层交换不同类型的数据。例如，敏感数据(例如，PII和/或其他个人数据的项目)可以在隐私层中交换(例如，经由加密通信)，而非敏感数据(例如，PII和/或其他个人数据的项目的加密证据)可以在信任层中交换。以这种方式，可以在信任层中提供高水平的透明度，而不损害隐私。

[0039] 在一些实施例中，可以提供身份管理协议，其中与组织相反，用户控制PII和/或其他个人数据的项目与其他实体共享的方式，而可信实体证明PII和/或其他个人数据的项目的真实性。以这种方式，用户可以精确地决定与另一实体(例如，另一用户)共享哪一项或多项个人数据，并且另一实体可以检查所述一项或多项个人数据是否已经由一个或多个可信实体(例如，一个或多个政府机构和/或雇主)验证，而不必经历繁琐的验证过程(例如，实际地检查诸如护照、社会保障卡、工资单等的文档)。

[0040] 应当理解，可以以多种方式中的任何一种来实现上面介绍的和下面更详细讨论的技术，因为这些技术不限于任何特定的实现方式。本文仅出于说明性目的而提供实施方式细节的示例。此外，本文公开的技术可以单独使用或以任何合适的组合使用，因为本公开的方面不限于使用任何特定技术或技术的组合。

[0041] V.说明性实施例的详细讨论

[0042] 图1示出了根据一些实施例的说明性身份管理系统100。在该示例中，身份管理系

统100包括具有三层的身份管理协议栈。例如，可以存在具有用于存储证明(例如，身份证明)的分布式账本102的信任层。附加地或备选地，可以存在包括多个个人数据服务(PDS)105A、105B、105C、…的隐私层、和/或包括多个应用115A、115B、115C、…的应用层。PDS可以存储经由应用进行交易(例如，开立帐户、进行购买等)的各个用户的个人数据。

[0043] 在一些实施例中，PDS可以包括用于管理PII和/或其他个人数据的软件程序。例如，PDS可以实现为虚拟容器，其将软件程序封装在文件系统中以允许软件程序在任何环境中一致地运行。例如，文件系统可以包括运行时系统、一个或多个系统工具、一个或多个系统库等。然而，应当理解，本公开的方面不限于此。备选地或附加地，PDS可以简单地包括用于管理个人数据的软件程序，而不需要伴随的文件系统。

[0044] 在一些实施例中，PDS可以与分布式账本102中的数字身份表示(DIR)相关联。例如，PDS 105A、105B、105C、…可以分别与DIR 110A、110B、110C、…相关联。在一些实施例中，每个单独的用户可以控制PDS和对应的DIR。PDS可以存储敏感数据(例如，PII和/或其他个人数据的项目)，而对应的DIR可以存储非敏感数据(例如，PII和/或其他个人数据的项目的加密证据)。PDS可以彼此通信并且以安全的方式共享敏感数据，而DIR可以将非敏感数据(例如，PII和/或其他个人数据的项目的加密证据)记录在分布式账本102中。

[0045] 在一些实施例中，加密证据可以以已知方式从个人数据的项目导出，并且可以由验证个人数据项的真实性的可信实体签名。用户与其共享个人数据项目(例如，社会安全号码)的实体可以容易地检查所声称的加密证据是否确实是从该个人数据项目导出的，并且加密证据是否确实是由可信实体(例如，政府机构或雇主)签名的。然而，对于另一实体来说，仅从加密证据重构个人数据项目在计算上可能是不可行的。以这种方式，可以同时实现隐私和透明度的相互矛盾的目标。

[0046] 在一些实施例中，分布式账本102可以包括在对等网络中的多个节点之间复制的数字记录。节点可以执行同步协议，由此可以通过网络传播在节点处对数字记录的本地副本所作的改变，并且其他节点可以相应地更新它们对相同数字记录的相应的副本。

[0047] 在一些实施例中，分布式账本可以使用区块链来实现。区块链可以包括多个块，其中每个块可以包括多个交易。在一些实施例中，多个交易可以例如按时间顺序排序。附加地或备选地，多个块可以被排序，其中每个新添加的块可以链接到最近的先前块。在一些实施例中，这种结构可以是防篡改的，并且因此可以用于确认给定交易是否发生，和/或该交易何时发生。例如，只有在实现区块链的网络中的所有节点(或具有足够计算能力的节点子集)都同意该块时，才可以将块添加到区块链。

[0048] 在一些实施例中，块生成节点(有时称为矿工)可以投入计算能力以生成链接到最近的先前块的新块。能够解出计算密集型数学难题(例如，识别具有一定数量前导零的散列的前像)的最快节点得到内部数字资产(例如，比特币)的奖励。根据在给定时间点网络中有多少计算能力可用，可以使用更复杂或更不复杂的数学难题。以这种方式，可以在选定的时间窗口中生成块，并且可以减少冲突。

[0049] 应当理解，本公开的方面不限于使用诸如上述那样的工作量证明方法。在一些实施例中，可以使用权益证明方法来实现分布式一致性。此外，应当理解，可以使用任何合适的区块链实施方式来提供信任层，包括但不限于Ethereum和Hyperledger Fabric。

[0050] 图2示出了根据一些实施例的说明性PDS 200。例如，PDS 200可以是图1所示的说

明性隐私层中的说明性PDS 105A-C之一。在一些实施例中，个人用户可以使用PDS 200来管理该用户的数字身份。作为一个示例，用户可以是公司的雇员，并且可以使用PDS 200来请求公司签署用户年收入的加密证据。附加地或备选地，公司可以使用类似于PDS 200的PDS来签署加密证据并将签名发布到分布式账本(例如，图1所示的说明性分布式账本102)。

[0051] 作为另一示例，用户可以是汽车经销商的客户，并且可以使用PDS 200来向汽车经销商证明用户的年收入。附加地或备选地，汽车经销商可以使用类似于PDS 200的PDS来从分布式账本(例如，图1所示的说明性分布式账本102)查找由用户提供的年收入数字的所声称的加密证据以及所声称的加密证据的所声称的签名。汽车经销商的PDS可以检查所声称的加密证据是否确实从由用户提供的年收入数字导出，并且加密证据是否确实由用户的雇主签署。

[0052] 在一些实施例中，PDS 200可以包括用户接口202和个人数据管理组件208。用户接口202和个人数据管理组件208可以允许用户存储PII和/或其他个人数据，并且管理(例如，添加、删除、修改、共享等)存储的数据。在一些实施例中，用户接口202可以使用多因素认证机制来限制对存储的数据和PDS 200的各种功能的访问。

[0053] 在一些实施例中，个人数据管理组件208可以维护经由用户接口202执行的一些或所有动作的审计跟踪。这可以允许用户识别任何未经授权的动作(例如，由攻击者使用从用户窃取的凭证)。附加地或备选地，调查者可以使用审计跟踪来确定用户是否涉及任何欺诈行为。

[0054] 在一些实施例中，用户接口202和个人数据管理组件208可以允许用户指定和/或批准与另一实体对一个或多个个人数据项目的共享。附加地或备选地，个人数据管理组件208可以应用一个或多个规则来管理与另一实体对一个或多个个人数据项目的共享。例如，规则可以指定一个或多个条件，并且可以在当前背景中满足所述一个或多个条件时被触发。该规则还可以指定要共享的一个或多个个人数据项目，和/或要与其共享一个或多个个人数据项目的一个或多个实体。在一些实施例中，可以在每次触发规则时通知用户，并且仅在用户同意的情况下执行所提议的个人数据共享。然而，这不是必需的，因为在一些实施例中，用户可以在特定规则下预先批准个人数据的共享。

[0055] 在一些实施例中，规则可以由用户指定，或者随时间(例如，使用一个或多个机器学习算法)从用户的行为和/或观察用户行为的背景中学习。附加地或备选地，可以从负责证明一个或多个个人数据项目的真实性的可信实体检索与所述一个或多个个人数据项目有关的规则。

[0056] 返回图2，在一些实施例中，PDS 200可以包括API 206，PDS 200可以经由API 206与一个或多个应用(例如，图1所示的说明性应用层中的说明性应用115A-C)进行交互。作为一个示例，PDS 200可以与雇主的工资管理应用交互以请求用户的年收入的证明。作为另一示例，PDS 200可以与汽车经销商的贷款处理应用交互以证明用户的年收入。应用的其他示例包括但不限于合同签署、教育状况验证、信用评分验证、数字访问控制、物理访问控制等。

[0057] 在一些实施例中，PDS 200可以包括通信管理组件210，PDS 200可以经由通信管理组件210与一个或多个其他PDS(例如，图1所示的说明性隐私层中的说明性PDS 105A-C)通信。作为一个示例，PDS 200可以与用户的雇主的PDS通信，以请求雇主签署用户年收入的加密证据。作为另一示例，PDS 200可以与汽车经销商的PDS通信以证明用户的年收入，以便用

户可以获得汽车贷款。

[0058] 在一些实施例中,PDS 200可以包括信任管理组件212,PDS 200可以经由信任管理组件212管理分布式账本(例如,图1所示的说明性分布式账本102)中的DIR(例如,图1所示的说明性信任层中的说明性DIR 110A-C之一)。例如,信任管理组件212可以包括用于基于背景信息(例如,哪个应用程序正在调用PDS 200)来管理DIR的程序逻辑。程序逻辑可以例如基于经由用户接口202从用户接收的指令、经由API 206从应用程序的输入、经由通信组件210从另一PDS接收的账本外通信等来引起DIR中的状态改变。

[0059] 在一些实施例中,PDS 200可以是一个或多个分布式账本(例如,图1所示的说明性分布式账本102)中的直接参与者。附加地或备选地,PDS 200可以与代表PDS 200管理一个或多个分布式账本的可信实体交互。在一些实施例中,可以使用一个或多个标准来确定PDS 200是直接参与还是间接参与或者既直接参与又间接参与包括但不限于系统部署和/或应用考虑。

[0060] 尽管在图2中示出并在上文讨论了PDS的实施方式的细节,但是应当理解,本公开的方面不限于使用任何特定组件或组件的组合或者组件的任何特定布置。例如,在一些实施例中,可以基于管理本地存储数据的核心来提供支持动态可扩展功能的PDS。例如,可以使用模块体系结构(例如,微服务体系结构),使得PDS可以容易地适应于满足变化的需求(例如,新的用例和/或过程流)。

[0061] 图3示出了根据一些实施例的说明性DIR 300。例如,DIR 300可以是图1所示的说明性信任层中的说明性DIR 110A-C之一。在一些实施例中,DIR 300可以由PDS(例如,图2所示的说明性PDS 200)控制。

[0062] 在一些实施例中,DIR 300可以在分布式账本(例如,图1所示的说明性分布式账本102)中实现,并且可以使用标识符来引用分布式账本中的DIR300。在图3所示的示例中,使用全局唯一身份标识符(GUII)302来引用DIR300,使得分布式账本中没有两个DIR共享相同的标识符。在一些实施例中,每个DIR可以由PDS控制,并且DIR的GUII可以基于与PDS相关联的用户的一个或多个度量来生成。可以选择度量的组合,使得在给定任何两个用户的情况下,这两个用户的DIR具有相同GUII的可能性极小,由此使得用户能够创建多于一个DIR的可能性极小。度量的示例包括但不限于生物特征(例如指纹扫描、视网膜扫描、声纹等)、行为度量(例如,位置历史、行走模式、睡眠模式等)等。

[0063] 在一些实施例中,可以使用加密单向函数从一个或多个基础度量值生成GUII,使得即使GUII公开可用,该一个或多个值也可以保持私有。基础度量值可以由相应的PDS连同指示用于从基础度量值生成GUII的一个或多个算法的元数据一起安全地存储。可以对基础度量值加以高的安全级别。例如,基础度量值不可以与其他实体共享。

[0064] 在一些实施例中,DIR可以用作非敏感数据的公共数据储存库,并且可以包括管理对这种数据的访问的逻辑。例如,在图3所示的示例中,DIR 300包括组织在一个或多个徽章306中的非敏感数据,以及指定可以经由DIR300执行的动作和/或可以由DIR 300中的改变触发的事件的动作和事件规范304。例如,为了提供透明度,每次在DIR 300中进行改变时,可以通知维护分布式账本的利益相关者。

[0065] 在一些实施例中,DIR 300可以在任何给定时间处于多个可能状态之一。例如,DIR 300中的徽章306可以包括一个或多个属性证明310,并且属性证明可以处于若干状态(例

如,“未决”、“已验证”、“无效”、“过期”等)之一。DIR 300的总体状态可以取决于DIR 300的一些或全部组成属性证明的状态。

[0066] 在一些实施例中,DIR 300从第一状态到第二状态的改变可以经由分布式账本中的交易发生。一旦交易被维护分布式账本的大多数利益相关者确认,DIR 300可以保持在第二状态,直到另一交易被确认。在一些实施例中,DIR 300的所有状态改变可以被记录在分布式账本中,并且可以对所有利益相关者可见,从而产生透明的审计跟踪。

[0067] 在一些实施例中,DIR 300可包括管理如何可以触发状态转变和/或哪些实体可以触发哪些转变的规则。例如,这样的规则可以由DIR 300的动作和事件规范304捕获。一旦经由分布式账本建立并部署了DIR 300,就不再可以改变动作和事件规范304中的程序逻辑,并且分布式账本可以确保DIR300的状态改变符合动作和事件规范304。

[0068] 在一些实施例中,可以仅允许一个或多个授权实体创建交易,从而引起DIR 300的状态改变。每个交易可以由创建交易的实体签名。这样,DIR 300的状态改变可以是可审计的。在一些实施例中,多个实体可以参与引起状态改变。可以要求所有或至少阈值数量的实体在所选时间间隔内签名,或者可以不确认状态改变。

[0069] 在一些实施例中,属性可以包括个人数据项目、个人数据项目的名称和/或相关元数据。例如,直接属性可以包括PII的项目,例如名字、姓氏、出生日期、出生地、护照号码、驾驶证号码、社会安全号码、地址、电话号码、保险识别号码、指纹扫描、视网膜扫描、声纹等。间接属性可以包括其他个人数据,例如拥有的财产(例如,车辆、房地产等)、财产状况等。附加地或备选地,间接属性(例如,至少21岁)可以从直接属性(例如,出生日期)导出。

[0070] 发明人已经认识并意识到,属性值的真实性可以以隐私保护的方式被证明,而无需求助于中央结算所。例如,在一些实施例中,可以在分布式账本中存储属性值的假名而不是属性本身。这样,属性值的假名可以在整个网络中复制,而不暴露属性值本身。

[0071] 在一些实施例中,属性值的假名可以使用加密单向函数来计算。例如,参考图3所示的示例,一个或多个属性可以存储在数据源312中,数据源312可以由控制DIR 300的PDS(例如,由图2所示的说明性个人数据管理组件208)维护。在一些实施例中,可以从数据源312检索属性,并且可以将加密单向函数应用于属性的值以导出属性的证据。可以在属性证明310中包括证据和/或相关元数据(例如,指示何时生成证据的时间戳)而不是值本身。这样,属性证明310可以被发布到分布式账本而不暴露属性的值。

[0072] 发明人已经认识并意识到,希望提供一种用于以颗粒方式管理属性证明的机制。因此,在一些实施例中,属性证明被布置成单独管理的一个或多个徽章(例如,图6所示的说明性徽章306)。

[0073] 在一些实施例中,用户可以指定可信实体负责徽章。对于徽章中的每个属性,可信实体可以验证用户为该属性提供的值的真实性,检查徽章中为该属性提供的证据是否确实是根据用户提供的值计算的,和/或签署该证据。如上所述,证据可以被包括在徽章中并且发布到分布式账本,但是值本身不可以。任何实体都可以充当可信实体,例如政府机构、雇主、金融机构、教育机构等。

[0074] 在一些实施例中,徽章可以是具有多个字段的数据结构。下面提供徽章的非限制性示例。

[0075]

```
{
```

[0076]

```
    label:          "KYC by Trusted Bank"
    trustedParty:   "trusted_party_identifier"
    proofAlgo:      "PBKDF2_SHA256_100000_3"
    salt:           "081627c0583380...83d51cdfdb1c8"
    schemaURI:      "http://schemas.example.org/strictKYCSchema"
    attributes:     [
        {
            label:          "firstname"
            proof:          "db74c940d447e877d...cbc319bcfaeab97a"
            state:          "PENDING"
            confirmedAt:    "1469633204"
            references:     [
                {
                    badgeLabel:     "badgeX"
                    attributeLabel: "firstname"
                    state:          "ACTIVE"
                }
            ]
        }
        {
            label:          "lastname"
            proof:          "55b5c51f867018...187e39a768aa8231ac"
            state:          "PENDING"
            confirmedAt:    "1469633204"
            references:     [
                {
                    badgeLabel:     "badgeX"
                    attributeLabel: "lastname"
                    state:          "ACTIVE"
                }
            ]
        }
        {
            label:          "ssn"
```

[0077]

```
            proof:          "efa5ff7eefcfbe4...e15edbb2095934aa0e0"
            state:          "PENDING"
            expiryPeriod:   "1_YEAR"
            confirmedAt:    "1469633204"
        }
        { /* more attributes */ }
    ]
}
```

[0078] 在上面的示例中，徽章是包括诸如“label”、“trustedParty”、“proofAlgo”、“salt”、“schemaURI”和“attributes”的字段的数据结构。在一些实施例中，“label”字段可以唯一地标识DIR中的徽章。这样的字段可以简化对DIR内的不同徽章的访问。

[0079] 在一些实施例中，“trustedParty”字段可以包括对可信实体的引用。在一些实施例中，被引用的可信实体可以获准对徽章的访问，并且只有被引用的可信实体可以被授权引起徽章中属性证明的状态改变。

[0080] 在一些实施例中，“proofAlg”字段可以识别用于计算存储在徽章中的一个或多个加密证据的算法。该算法可以利用加密单向函数，例如散列函数。作为示例，基于密码的密钥导出函数2(PBKDF2)可以例如与所选伪随机函数(例如SHA256)、伪随机函数的所选迭代次数(例如10,000)和/或所选数量的输出字节(例如32)一起使用。然而，应当理解，本公开的方面不限于使用任何特定算法来计算加密证据。

[0081] 在一些实施例中，“salt”字段可以存储在计算加密证据时用作加密单向函数的输入的随机值。

[0082] 在一些实施例中，“schemaURI”字段可以包括对用于创建徽章的模式的引用。下面提供模式的非限制性示例。

[0083] 在一些实施例中，“attributes”字段可以包括一个或多个属性证明，其中每个属性证明本身可以是具有一个或多个字段的数据结构。例如，属性证明可以包括诸如“label”、“proof”、“state”、“expiryPeriod”、“confirmedAt”和“references”的字段。

[0084] 在一些实施例中，“label”字段可以用于唯一地识别徽章中的属性证明。

[0085] 在一些实施例中，“proof”字段可以存储被证明的属性的值的加密证据。例如，可以使用在“proofAlg”字段中指定的算法计算加密证据，随机值作为附加输入存储在“salt”字段中。

[0086] 在一些实施例中，“state”字段可以存储属性证明的当前状态。例如，在任何给定时间，属性证明可以处于以下状态之一：“未决”、“已验证”、“无效”或“过期”。在图4中示出并在下面描述了控制这些状态之间的转变的说明性状态机。

[0087] 在一些实施例中，“confirmedAt”字段可以指示徽章最后被分布式账本确认的时间。

[0088] 在一些实施例中，“expiryPeriod”字段可以指示属性证明可以保持在已验证状态的时间长度。例如，期满日期可以如下计算：expiryDate＝confirmedAt+expiryPeriod。当达到期满日期时，可以触发内部转变，并且属性证明可以从已验证状态移动到无效状态。

[0089] 在一些实施例中，“references”字段可以包括对另一徽章中的对应属性证明的引用。例如，“references”字段可以包括存储其它徽章的标签的“badgeLabel”字段、存储其它徽章中的引用属性证明的标签的“attributeLabel”字段、以及指示引用属性证明的状态(例如，“有效”、“无效”、“过期”等)的“state”字段。

[0090] 发明人已经认识并意识到，从第一徽章中的属性证明到同一DIR中的第二徽章中的对应属性证明的引用可以允许负责第一徽章的可信实体信赖第二徽章中的对应属性证明。例如，在上述示例中，当用户请求在“trustedParty”字段中识别的可信实体验证标签为“firstname”的属性证明的值(例如，John)时，可信实体可以检查另一徽章中的对应属性证明(例如，标签为“badgeX”的徽章中标签为“firstname”的属性)。如果检查成功，则可信实体可以签署存储在标签为“firstname”的属性证明的“proof”字段中的证据，而不必完成繁琐的验证过程(例如，实际地检查用户护照以确认用户的名字确实是John)。

[0091] 在一些实施例中，为了检查其他徽章中的对应属性证明，可信实体可以使用存储在“badgeLabel”字段中的标签(例如，“badgeX”)来查找其他徽章，并且可以使用存储在“attributeLabel”字段中的标签(例如，“firstname”)来查找其他徽章中的对应属性证明。可信实体可以检查对应属性是否处于“有效”状态，并且可以将在另一徽章的“proofAlgo”字段中指示的算法应用于由用户(例如John)提供的属性值和存储在另一徽章的“salt”字段中的盐(salt)，以检查存储在对应属性证明的“proof”字段中的证据是否确实通过将该算法应用于属性值和该盐而生成。

[0092] 在一些实施例中，仅当可信实体信任在另一徽章的“trustedParty”字段中识别的实体时，可信实体可以信赖另一徽章中的对应属性证明。例如，如果在另一徽章的“trustedParty”字段中识别的实体是政府机构，则可信实体可以决定信赖该证明，但是如果在另一徽章的“trustedParty”字段中识别的实体是可信实体未知的个人或组织，则可信实体可以决定不信赖该证明。

[0093] 虽然发明人已经认识到并意识到将属性证明组织成徽章的各种优点，但是应当理解，本公开的方面不限于这里提供的特定示例，或者根本不限于徽章的使用。在一些实施例中，属性证明可以以不同的方式组织，或者可以单独管理。

[0094] 在一些实施例中，加密单向函数可以与公共盐和/或一种或多种私有盐结合使用。例如，公共盐可以是由徽章中的所有属性证明共享、在徽章创建期间计算并发布到分布式账本的随机值。这种公共盐可以用作徽章的绑定值。

[0095] 相比之下，在一些实施例中，私有盐可以是每当属性的值被验证时为每个属性单独计算并且不发布到分布式账本的随机值。为了允许可信实体验证属性的值，可以将该属性和该特定验证计算的私有盐连同该属性的值一起经由安全账本外通道与可信实体共享。

[0096] 在一些实施例中，属性值的加密证据可以计算如下：

[0097] (1)public_salt＝random(X)，

[0098] 其中输入X的函数random()输出长度X的随机字节序列。

[0099] (2)private_salt＝random(Y)，

[0100] 其中输入Y的函数random()输出长度Y的随机字节序列。

[0101] (3)proof＝HASH(public_salt||private_salt||attribute_value)，

[0102] 其中||是字节序列串联函数。

[0103] 在一些实施例中，函数HASH()可以是比简单加密散列更复杂的单向函数。例如，PBKDF2算法可以与强散列函数(例如SHA256)、足够大的迭代次数(例如10,000)和/或足够大的输出字节数(例如32)结合使用，以减慢潜在攻击者的速度，从而提高对有针对性的暴力破解的抵抗力。然而，应当理解，本公开的方面不限于使用任何特定的证明算法。在一些实施例中，不同的证明算法可以用于不同的徽章，甚至是相同DIR中的那些徽章。

[0104] 在一些实施例中，为了提高安全性，可以选择盐值以具有至少与函数HASH()的输出一样多的比特。这种盐可以在PDS中独立计算。例如，公共盐不可以在徽章之间重复使用，私有盐不可以在属性证明之间重复使用。

[0105] 发明人已经认识并意识到，使用私有盐可以允许现有证明的失效，即使属性值不改变。例如，证明实体(例如，征信所)可以通过使用新的私有盐来用新的证明替换先前的证明，以便为相同属性值生成新的证据。然而，本公开的方面不限于使用私有盐，因为在一些实施例中，不可以使用私有盐，因此所有先前的证明都可以保持有效。另外，本公开的方面不限于使用公共盐。例如，在一些实施例中，可以使用私有盐代替公共盐。

[0106] 在一些实施例中，徽章可以基于徽章模式(其可以在徽章的“schema”字段中被引用)来创建。徽章模式可以描述哪些数据片段可以存储在徽章中、如何可以组织数据片段、数据片段之间的语义关系和/或决定如何可以管理数据片段的规则。在一些实施例中，可以使用诸如W3C Web本体语言(OWL)或资源描述框架模式(RDFS)的语义语言来编写徽章模式。然而，这不是必需的，因为在一些实施例中还可以使用诸如XML的标记语言。下面提供徽章模式的非限制性示例。

[0107]

{

Id: "http://schemas.example.org/strictKYCSchema"

schemaType: "001 - KYC for Individuals"

riskProfile: "Low"

description: "The following schema defines attributes needed for a Know Your Customer (KYC) check of a low risk individual."

attributes: [

{

label: "firstname"

description: "The first name of the person as specified."

required: true

validationCriteria: "Must match the first name on a government issued photo ID. Checked in person or via high quality scan of the photo ID, transmitted via secure digital channel."

enhancedPrivacy: "The label can be protected by substituting the label 'firstname' with a related one-way salted hash."

storageLocation: "PDS"

dataType: "String"

format: "Plaintext or Hashed"

}

{

label: "lastname"

required: true

validationCriteria: "Must match the last name on the government issued photo ID used to check the first name. Checked in person or via high

[0108]

```
                quality scan of the photo ID, transmitted via secure digital channel."
                enhancedPrivacy: "The label can be protected by substituting the label
                'lastname' with a related one-way salted hash."
                storageLocation: "PDS"
                dataType: "String"
                format: "Plaintext or Hashed"
            }
            {
                label: "ssn"
                required: true
                validationCriteria: "Social Security Number must be related to the same
                person shown on the government issued photo ID used to check the first
                name and the last name "
                enhancedPrivacy: "The label can be protected by substituting the label
                'ssn' with a related one-way salted hash."
                dataType: "String"
                storageLocation: "PDS"
                format: "Plaintext or Hashed"
            }
            { /* more attribute specifications */ }
    ]
}
```

[0109] 在上面的示例中，徽章模式定义了可以在徽章中包括其证明的一组属性。每个属性证明可以在创建徽章时填入，或者在以后添加到徽章中。在一些实施例中，徽章模式可以定义决定如何可以管理属性证明的一个或多个规则。例如，规则可以指定属性证明的有效期必须在5年到10年之间。

[0110] 发明人已经认识并意识到，徽章模式可以允许以标准化的方式创建徽章。这可以简化为不同目的创建的徽章之间的映射，这又可以提高相同垂直机构(例如，不同金融机构)内或横跨不同垂直机构(例如，诸如运输安全管理局或TSA的政府机构，其使用银行"了解客户"或KYC模式来验证乘客身份)的不同系统的互操作性。然而，应当理解，本公开的方面不限于使用徽章模式来创建徽章。

[0111] 图4示出了根据一些实施例的管理属性证明的不同状态之间的转变的说明性状态机400。例如，状态机400可以管理图3所示的说明性徽章306中的一个或多个中的属性证明的状态转变。

[0112] 在一些实施例中，当使用属性证明创建徽章时(或者当属性证明被添加到现有徽章时)，属性证明可以被初始化为未决状态。在此状态下，属性证明可能既不是有效的，也不是无效的。

[0113] 在一些实施例中，为其创建徽章的用户可以请求与徽章相关联的可信实体验证属

性的值。如果可信实体验证了属性的值，则可信实体可以使属性证明处于已验证状态。如果可信实体拒绝了属性的值，则可信实体可以使属性证明处于无效状态。

[0114] 在一些实施例中，如果属性证明处于已验证状态、过期状态或无效状态，并且用户使该属性具有不同的值，则属性证明可以返回到未决状态。

[0115] 在一些实施例中，如果属性证明处于已验证状态，并且可信实体撤销先前的验证，则可信实体可以使属性证明处于无效状态。

[0116] 在一些实施例中，如果属性证明处于已验证状态，并且有效期结束，则属性证明可以移动到过期状态，其中属性证明可以保持直到可信实体重新验证属性的值。

[0117] 应当理解，仅出于说明的目的而在图4中示出并在上文中描述了状态机400，因为本公开的方面不限于状态和/或状态转变的任何特定组合。

[0118] 在一些实施例中，引用属性证明的状态可以与被引用属性证明的状态同步。然而，这不是必需的，因为在一些实施例中，引用属性证明的状态改变可以独立于被引用属性证明的状态改变。

[0119] 如上所述，DIR可以包括管理如何可以触发状态转变和/或哪些实体可以触发哪些转变的规则。例如，这样的规则可以由动作和事件规范(例如，图3所示的说明性动作和事件规范304)捕获。下表列出了可以经由DIR执行的动作(例如，状态改变和/或证据更新)的非限制性示例。

[0120]

动作	输入/输出	属性状态	附带结果
createBadge	输入 (1) 徽章标签 (2) 可信实体 输出：无	无	触发“创建徽章事件”
setAttribute	(1) 徽章标签 (2) 属性标签 (3) 属性证据	未决	触发“设置属性事件”

[0121]

submitVerificationRequest	输入 (1) 徽章标签 输出：无	无	触发“验证请求事件”
changeAttributeState	输入 (1) 徽章标签 (2) 属性标签 (3) 属性状态 输出：无	“未决” 到 “已验证” 或“无效”	触发“属性状态改变事件”

[0122] 在一些实施例中，“createBadge”动作可以将徽章标签和可信实体的标识符作为输入。作为执行“createBadge”动作的用户的DIR的结果，徽章可以用“label”字段中的输入

徽章标签和“trustedParty”字段中的输入可信实体标识符来创建。附加地或备选地，可以触发“创建徽章”事件，该事件可以将新创建的徽章发布到分布式账本。

[0123] 在一些实施例中，“setAttribute”动作可以将徽章标签、属性标签和属性证据作为输入。作为执行“setAttribute”动作的用户的DIR的结果，可以更新由输入徽章标签标识的徽章的“attributes”字段。例如，由输入属性标签标识的属性证明可以添加有“proof”字段中的输入属性证据和/或用“proof”字段中的输入属性证据修改。附加地或备选地，属性证明的状态可以被设置为未决，和/或可以触发“设置属性”事件，其可以将属性证明的这些改变发布到分布式账本。

[0124] 在一些实施例中，“submitVerificationRequest”动作可以将徽章标签作为输入。作为执行“setAttribute”动作的用户的DIR的结果，可以触发“验证请求”事件，该事件可以使得验证请求被发送到负责由输入徽章标签标识的徽章的可信实体的DIR。

[0125] 在一些实施例中，“changeAttributeState”动作可以将徽章标签、属性标签和属性状态(例如，已验证或无效)作为输入。作为执行“changeAttributeState”动作的可信实体的DIR的结果，可以更新由输入徽章标签标识的徽章的“attributes”字段。例如，可以用“state”字段中的输入属性状态(例如，已验证或无效)修改由输入属性标签标识的属性证明。附加地或备选地，可以触发“属性状态改变”事件，该事件可以将属性证明的这种改变发布到分布式账本。

[0126] 下表列出了“创建徽章”、“设置属性”、“验证请求”和“属性状态改变”事件的非限制性示例。

[0127]

创建徽章事件		
字段	**Caller**	触发该事件的实体的 GUII
	Badge	创建的徽章的标签
	Trusted Party	负责验证属性值和证明其真实性的可信实体的 GUII
验证请求事件示例		
字段	**Caller**	创建该事件的实体的 GUII
	Badge	待验证的徽章的标签
设置属性事件示例		
字段	**Caller**	创建该事件的实体的 GUII
	Badge	其中的属性值被设置的徽章的标签
	Attribute Key	设置其值的属性的标签
	Attribute Value	属性值的一个或多个加密证据
属性状态改变事件示例		
字段	**Caller**	创建该事件的实体的 GUII
	Badge	属性证明正在改变状态的徽章的标签
	Attribute Key	正在改变状态的属性证明的标签
	旧状态	状态转变之前的属性证明的状态
	新状态	状态转变之后的属性证明的状态

[0128] 在一些实施例中，属性值可以由诸如政府机构(例如护照管理机构)、雇主、金融机构等的可信实体验证。可信实体可以例如通过检查物理文档(例如出生证明、驾驶证、社会保障卡、工资单等)和/或亲自询问用户来验证属性的值。在成功验证之后，可信实体可以使对应的属性证明处于已验证状态。如果存在任何问题，则可信实体可以使对应的属性证明处于无效状态。

[0129] 图5示出了根据一些实施例的用于由可信实体证明的说明性过程500。例如，过程

500可以在了解客户(KYC)检查期间在用户和金融机构之间执行。

[0130] 在一些实施例中,在发起过程500之前,用户可以经由应用层(例如,图1所示的说明性应用层)中的一个或多个账本外接口与可信实体通信。例如,用户可以访问可信实体的网站,和/或下载并启动可信实体的应用程序。应用层中的这种通信可以导致用户的PDS或可信实体的PDS在动作505中发起隐私层(例如,图1所示的说明性隐私层)中的握手。通过这种握手,可信实体的PDS可以确认可信实体将负责验证一个或多个属性值。附加地或备选地,可信实体的PDS可以向用户的PDS发送可信实体的GUII和/或用于创建具有一个或多个属性证明(例如,与KYC过程相关的那些)的徽章的模式。

[0131] 在动作510中,用户的PDS可以创建徽章(例如,使用可信实体的GUII,和/或根据由可信实体的PDS提供的模式),并且可以将徽章发布到信任层(例如,图1所示的说明性信任层)中的分布式账本。然后,在动作515中,用户的PDS可以经由账本外通信向可信实体的PDS发送对用户的DIR的引用以及要验证的一个或多个属性值。在一些实施例中,用户的DIR可以触发账本上的事件(例如,“验证请求”事件)以通知可信实体的DIR。

[0132] 在动作520中,可信实体的DIR可以使用在动作515中接收的引用来从分布式账本查找徽章。对于徽章中的每个属性证明,可信实体的DIR可以使用徽章中指定的算法检查徽章中的加密证据是否是从接收到的属性值生成的。然后,可信实体的DIR可以继续验证所接收的属性值(例如,经由被引用的徽章间接地,或者由可信实体本身直接地)。

[0133] 例如,对于给定的属性证明,可信实体的DIR可以检查是否存在对另一徽章的引用。如果存在,则可信实体的DIR可以从分布式账本中查找其他徽章,并且可以执行一个或多个检查。例如,可信实体可以检查验证另一徽章的实体是否可信、另一徽章中的加密证据是否是使用在另一徽章中指定的算法从接收到的属性值生成的和/或另一徽章是否被验证实体签名。可以使用任何合适的电子签名方案,因为本公开的方面不限于此。

[0134] 附加地或备选地,可信实体可以例如通过检查物理文档和/或亲自询问用户直接验证接收到的属性值。

[0135] 如果没有问题,则可信实体的DIR可以对徽章进行签名,并使徽章中的每个属性证明处于已验证状态。如果存在一个或多个有问题的属性证明,则可信实体的DIR可以使这样的属性证明处于无效状态。

[0136] 在一些实施例中,实体可以形成信任结构,其中实体可以信任一个或多个其他实体并且可以信赖由所述一个或多个可信实体中的任何一个签署的属性证明(例如,如上面结合图5所讨论的)。这样,实体可能能够验证属性证明而不必执行物理验证。

[0137] 信任结构可以包括在实体之间具有任何合适的信任关系的任何适当数量的实体。此外,随着现有成员离开、新成员加入和/或信任关系改变,信任结构中的成员资格可以随时间演变。

[0138] 图6示出了根据一些实施例的说明性信任结构600。在此示例中,DIR中有四个徽章605A-D。徽章605A-D可以分别对应于可信实体A-D。徽章605A可以包括以下属性证明:“名字”、“姓氏”、“社会安全号码”和“家庭地址”,所有这些都可能已经由实体A(例如银行)直接验证。

[0139] 在一些实施例中,徽章605C可以包括以下属性证明:“家庭地址”、“名字”、“姓氏”和“电子邮件地址”。除了属性证明“家庭地址”包含对徽章605A的引用之外,这些属性证明

中的每一个都可能已经由实体C(例如,在线商家)直接验证,这表明实体C在“家庭地址”属性证明方面信任实体A。这可以允许实体C查看徽章605A中的“家庭地址”属性证明的状态。

[0140] 在一些实施例中,徽章605D可以包括以下属性证明:“家庭地址”、“全名”、“社会安全号码”和“婚姻状况”。除了属性证明“家庭地址”包含对徽章605A的引用之外,这些属性证明中的每一个都可能已经由实体D(例如,社交网络提供商)直接验证,这表明实体D在“家庭地址”属性证明方面信任实体A。这可以允许实体D查看徽章605A中的“家庭地址”属性证明的状态。

[0141] 在一些实施例中,徽章605B可以包括以下属性证明:“姓氏”、“名字”、“护照号码”和“电话号码”。除了属性证明“姓氏”包含对徽章605A的引用和对徽章605C的引用之外,这些属性证明中的每一个都可能已经由实体B(例如旅行社)直接验证,这表明只有当实体A和实体C两者都直接且独立地验证了“姓氏”的属性值时,实体B才可以签署属性证明“姓氏”。这可以允许实体B查看徽章605A中的“姓氏”属性证明的状态和徽章605C中的“姓氏”属性证明的状态。

[0142] 因此,在图6所示的示例中,属性证明“家庭地址”可以具有包括三个实体A、C和D的信任圈,其中实体A已经尽力直接验证“姓氏”的属性值,并且实体C和D信赖实体A关于“家庭地址”的证明。另一方面,属性证明“姓氏”可以具有包括A、B和C三个实体的信任圈,其中实体A和C已经独立地尽力直接验证“姓氏”的属性值,并且实体B信赖实体A关于“家庭地址”的证明。

[0143] 图7示出了根据一些实施例的用于交易对手检查的说明性过程700。在该示例中,用户A可以与用户B进行交互。例如,用户A可以是房地产交易中的买方,而用户B可以是卖方。过程700可以由用户A或用户B发起。

[0144] 在一些实施例中,在过程700之前,用户A和B可以经由一个或多个账本外通道进行通信。例如,用户A和B可以间接(例如,经由一个或多个代理)或直接(例如,经由电子邮件)通信。作为这种通信的结果,在动作705中,用户A可以指示用户A的PDS发起与用户B的PDS在隐私层(例如,图1所示的说明性隐私层)中的握手,反之亦然。

[0145] 附加地或备选地,用户A和B可以经由应用层(例如,图1所示的说明性应用层)中的一个或多个账本外接口进行通信。应用层中的这种通信可导致用户A的PDS或用户B的PDS在动作705中发起在隐私层(例如,图1所示的说明性隐私层)中的握手。

[0146] 在动作710中,用户A的PDS和用户B的PDS可以交换个人数据(例如,全名、家庭地址、电子邮件地址、电话号码等)和/或对相应DIR的引用。如果使用徽章来组织属性证明,则还可以交换相应的徽章的标签。在一些实施例中,可以从任一侧提供同一组个人数据。然而,这不是必需的,因为用户A可以向用户B请求用户B没有向用户A请求的信息,反之亦然。

[0147] 在一些实施例中,用户A的DIR可以使用从用户B接收的信息来查找来自分布式账本的属性证明并执行一个或多个检查。例如,用户A的DIR可以检查验证属性证明的实体是否是可信的,属性证明是否处于已验证状态,是否使用包含属性证明的徽章中指定的算法从接收自用户B的对应属性值生成属性证明中的加密证据,和/或属性证明是否由验证实体签名。用户B的DIR可以执行类似的检查。

[0148] 发明人已经认识并意识到,可能希望增强托管隐私层组件(例如,PDS)的环境的安全性。附加地或备选地,可能希望改进对隐私层和/或信任层的访问控制。

[0149] 在一些实施例中，可以通过加密由隐私层组件(例如，PDS)处理的数据来提高托管环境中的安全性，使得托管实体(例如，公共云提供商)可能不能访问写入物理或虚拟盘的数据。除了在虚拟化环境(例如，每个虚拟机一个PDS，但是每个物理机多个PDS)或专用环境(例如，每个物理机一个PDS)中实现隐私层组件之外，还可以进行这种加密。然而，应当理解，本公开的方面不限于这种数据加密。

[0150] 在一些实施例中，一个或多个加密密钥可以被存储在隐私层组件(例如，PDS)之外，使得托管实体不可以访问该一个或多个加密密钥。可以使用任何合适的密钥管理方案。例如，密钥可以由隐私层组件的用户保持。

[0151] 在一些实施例中，可以对隐私层中的数据改变和/或信任层中的状态改变施加访问控制。图8示出了根据一些实施例的用于隐私层组件(例如PDS)中的数据改变和信任层组件(例如DIR)中的所得状态改变的说明性过程800。

[0152] 在图8所示的示例中，过程800由试图改变存储在隐私层组件中的个人数据项目的用户发起，这可以触发隐私层处的访问控制检查。在一些实施例中，隐私层访问控制机制可以包括认证和/或授权过程，其可以根据用户请求的动作的类型而更严格或较不严格。例如，改变关键数据(例如，护照号码)的尝试可以触发比改变非关键数据(例如，电子邮件地址)的尝试更严格的认证过程(例如，多因素认证)。因此，根据所请求的数据改变的敏感性，可以以颗粒方式提供更强的安全性。

[0153] 在一些实施例中，在隐私层处的成功认证和/或授权可以允许用户在隐私层组件处完成所尝试的数据改变。附加地或备选地，隐私层组件可以响应于成功的认证和/或授权而检索一个或多个信任层密钥以用于访问信任层。例如，信任层密钥可以是要被呈现以证明使信任层组件执行一个或多个动作的权限的加密密钥。

[0154] 在一些实施例中，可以呈现不同的信任层密钥以证明执行不同类型的动作的权限。例如，与改变非关键数据(例如，电子邮件地址)的尝试相比，可以呈现与更高级别的权限相关联的密钥以证明改变关键数据(例如，护照号码)的权限。在一些实施例中，仅当已经获得适当授权(例如，通过呈现一个或多个合适的密钥)时，才可以指示信任层组件执行一个或多个动作(例如，状态改变)。

[0155] 附加地或备选地，可以提供允许基于背景的动态访问控制的一个或多个访问规则。这样，访问不仅可以取决于所请求的动作的性质，还可以取决于一个或多个外部条件，从而提高安全性。例如，如果存在正在进行的攻击，则可以实施更严格的访问规则。

[0156] 在一些实施例中，实体(例如，用户或组织)可以与多个加密密钥相关联。发明人已经认识并意识到，在安全性和可用性之间可能存在折衷。因此，在一些实施例中，可以提供允许实体选择适当数量的密钥以实现安全性和可用性之间的所需平衡的系统。参考图3所示的示例，在一些实施例中，可以提供密钥管理组件308以跟踪与控制DIR的实体相关的多个加密公钥。这样的组件可以提供来自底层公钥基础设施(PKI)的抽象。这样，应用层中的用户和/或应用可以仅经由相应的PDS与DIR交互，而不直接与底层加密密钥交互。

[0157] 在一些实施例中，密钥管理组件308可以执行基于角色的访问控制。例如，至少可以有两个角色：证明者和身份所有者。密钥管理组件308可以仅允许分配给给定徽章的可信实体修改该徽章中的属性证明的状态。

[0158] 如上所述，发明人已经认识并意识到，可能希望对诸如护照信息的某些属性施加

更高程度的安全性。在一些实施例中，这可以经由认证和/或授权的一个或多个度量来实现。例如，可以使用一个或多个生物识别标记来增加认证过程中的置信水平。附加地或备选地，可以使用一个或多个生物识别标记来生成GUII，这可以防止用户创建多个DIR。在一些实施例中，这种生物识别标记可以被视为高度敏感的信息，并且不可以与另一实体共享。

[0159] 附加地或备选地，一个或多个行为度量(例如，位置历史、行走模式、睡眠模式、旅行模式等)可以用于增加认证过程中的置信水平。

[0160] 在一些实施例中，可以使用多密钥授权来保护敏感属性值(例如，护照号码)。例如，用户可以通过在认证时呈现多个密钥来寻求改变这种属性值的授权。在一些实施例中，每个密钥可以与不同的设备相关联。例如，用户可以具有用于膝上型计算机的第一密钥、用于智能电话的第二密钥、用于智能手表的第三密钥等。用于改变属性值的说明性过程可以包括以下步骤：

[0161] 1)用户可以访问PDS的接口(例如，web接口)并触发改变动作。

[0162] 2)改变动作可以被记录为未决动作，并且指示可能需要来自用户的进一步确认。

[0163] 3)用户可以经由至少一个附加的个人设备确认改变动作。例如，可以通过注册智能手机的指纹认证和注册生物识别签名来确认改变动作。

[0164] 在一些实施例中，用户可以具有M个密钥，并且可以使用至少N个密钥(其中N≤M)来执行某个动作(例如，修改属性值)。这样，可以提高安全级别，使得可能更加难以冒充用户。在一些实施例中，M可以等于注册到用户的设备的总数。

[0165] 附加地或备选地，仅当诸如智能手表、智能电话、膝上型计算机等的两个或更多个个人设备彼此在某个指定距离(例如，10米)内时，才可以同意授权。附加地或备选地，仅当个人设备位于指定位置(例如，基于GPS数据确定的位置)时，才可以同意授权。

[0166] 在一些实施例中，如果密钥被泄露(例如，如果设备被盗)，则被泄露的密钥可被撤销并且可用新密钥替换。例如，这可以通过增加请求动作的实体实际上是对应于PDS和DIR的用户的概率来提高安全性。

[0167] 发明人已经认识并意识到，当使用多个密钥时，可以撤销和替换被泄露的认证密钥，同时保留用户在此期间访问PDS和DIR的能力。在一些实施例中，一个或多个密钥以及一个或多个访问权限可以通过分布式账本传播，使得所述一个或多个密钥和一个或多个访问权限可以变得防篡改并且能够由任何实体验证。如上所述，在一些实施例中，可以通过使用加密单向函数导出敏感数据的证据来实现隐私保护。从证据中导出原始敏感数据可能在计算上具有挑战性。通过在共享的分布式账本中仅包括非敏感证据，可以实现高度隐私性。实体之间的安全账本外通信信道可用于共享原始敏感信息。附加地或备选地，模式可以用于提供属性的粒结构，这可以进一步提高隐私性。例如，代替共享不必要的信息(例如，家庭地址或实际出生日期)，可以仅与另一实体共享与特定背景相关的信息(例如，为了购买酒精饮料而共享超过21岁的信息)。为了进一步提高隐私性，在一些实施例中，可以使用不同徽章中的不同标识符来标识实体。这样，攻击者可能更难从交互跟踪回实体。

[0168] 发明人已经认识并意识到，可能希望提供一种机制，以允许用户找到管理特定分布式账本的节点。在某些情况下，可以经由定制发现机制、一个或多个HTTP请求和/或DNS解析过程来发现管理分布式账本的节点。在一些实施例中，可以提供URI方案，该URI方案包括为了允许在因特网规模网络中发现分布式账本而要满足的一组特性。在某些情况下，节点

可以加入和/或离开分布式账本。因此,可能希望返回到请求实体的节点列表是最新的。

[0169] 在一些实施例中,可以使用多于一个分布式账本(例如,多于一个区块链)。在这样的体系结构中,可以提供发现机制来发现遍及多个分布式账本的节点。与单个分布式账本体系结构相比,多个分布式账本体系结构中的通信开销可以很小,并且可以仅包括指定分布式账本标识符的一个请求。响应可以包括当前管理所请求的分布式账本的节点列表。在一些实施例中,底层数据结构可以是分布式散列表(DHT)。每当节点开始管理分布式账本时,它可以向网络通知其动作。节点还可以在停止管理分布式账本时通知。

[0170] 图9示出了根据一些实施例的网络900中的分布式账本发现机制的示例。在动作1中,节点2可以向节点1请求访问区块链X。作为响应,节点1可以在动作2中向节点2授予许可。在动作3中,节点2可以向区块链X通知它现在管理区块链X。在动作3中,节点3还可以向节点1请求对区块链X的访问。作为响应,节点1可以在动作4中向节点3授予许可。在动作5中,节点3可以向区块链X通知它现在管理区块链X。在动作6中,节点2可以决定离开区块链X,并且可以通知区块链X它的离开。在动作7中,节点4可以查找哪些节点正在管理区块链X。在动作8中,区块链可以返回管理节点的更新列表。

[0171] 本文所述的任何一种或多种技术可以在各种环境中使用以简化个人数据的验证。例如,在一些实施例中,可以为每个用例提供包括与该用例相关的所有属性的定制的徽章模式。这样,基于模式生成的徽章可以包括所有相关数据,并且管理徽章的PDS可以保持数据为最新。

[0172] 下面描述用例的非限制性示例。

[0173] I.了解客户(KYC)

[0174] 此类应用中的一种是“了解客户”(KYC)检查,该检查可以由诸如银行的金融机构执行。用户(例如银行的客户)的身份可以通过可信实体(例如,银行)验证用户提交的一个或多个属性值的过程来证实。该过程可以使用本文所述的一种或多种技术来执行。一旦验证了所述一个或多个属性值,则可信实体可以签署一个或多个对应的属性证明,并且只要前一可信实体和后一可信实体是信任结构的一部分,另一可信实体随后就可以信赖这种证明。

[0175] 金融机构可能必须遵守严格的规章制度,以验证客户的身份。一方面,金融机构可能需要维护其客户的记录。另一方面,金融机构可能需要保证此类数据的隐私性和安全性。通过允许用户(例如,银行客户)控制他们自己的数据,并且通过向用户提供管理和共享他们的数据的平台,所得到的KYC检查可以显著地更有效并且可以限制数据重复。从用户的角度来看,数据可以在创建PDS时输入,并且随后仅在属性改变时输入。这样,可以消除多次输入相同信息的负担。从金融机构的角度来看,数据的准确性可以显著提高,因为例如更新可以自动传播到所有相关的可信实体。

[0176] II.雇员证明

[0177] 与KYC检查相比,对雇员的证明监管较少。然而,雇主可以使用本文所述的任何一种或多种技术来证明其雇员的身份和/或其他信息。这种证明可以在内部用于认证和/或授权目的,和/或在外部用于与合作伙伴和/或其他利益相关者安全地共享信息。这样,可以保证对声称的身份的担保。在一些实施例中,可以显著简化授权雇员代表雇主执行某些任务的过程。因为属性可以传播到所有可信的利益相关者,所以期望的授权级别在任何时候都

是最新的。

[0178] III.安全检查

[0179] 本文所述的任何一种或多种技术都可以用于允许加速安全检查(例如,在机场执行的安全检查、用于准许进入受限区域或建筑物的安全检查等)。例如,代替必须手动检查身份文档(ID)或其他识别信息,安全检查可以是自动的。

[0180] 在一些实施例中,自动安全检查可包括实时检索可能已由合适的可信实体证明的最新犯罪记录(例如,在过去六个月内更新的)。

[0181] IV.运输安全管理局(TSA)

[0182] 在一个示例中,旅客可以具有PDS和包括一组属性证明的相关DIR。DIR可以包括适合于TSA检查的模式。这样,机场安全检查可以由TSA代理通过执行交易对手检查来执行。一个这样的交易对手检查的示例可以包括以下步骤:

[0183] 1)旅客可以到达机场的TSA安检口;

[0184] 2)旅客的移动设备可以与TSA系统共享属性值;

[0185] 3)TSA系统可以确认共享属性值的接收;

[0186] 4)TSA代理打开共享属性值并将该值与旅客进行直观比较。附加地或备选地,旅客可以扫描指纹和/或其他生物识别特征。这样的特征可以与包括在共享属性值中的对应特征进行比较。

[0187] 5)TSA系统可以:在确保签名可信实体被TSA信任的同时,通过对照分布式账本检查所接收的属性值,来检查所接收的属性值是否合法;对照外部列表(例如,禁止飞行或恐怖监视列表)交叉检查一个或多个属性值;和/或针对实时视频流执行面部识别或交叉检查所接收的带照片的身份证明。

[0188] 如果上述所有检查都通过,则旅客可以被标记为可信的。因此,TSA可能不再需要维护大型数据库。此外,这种方法可以将实际护照检查和所有背景检查结合在一个简单的步骤中。这样,可以在每次遇到时容易地执行背景检查。

[0189] V.办理登记手续

[0190] 办理登记手续通常需要客户排队等候。通过使用本文所述的一种或多种技术可以显著缩短这种等候。例如,客户可能具有PDS和相关的DIR,并且通过检查属性的引用可以由证明组织(例如,酒店、汽车租赁行等)来证明身份和/或其他相关数据。在预订阶段,客户可以使用PDS与组织共享相关信息。组织的系统可以通知客户需要什么属性值,而不是手动填写个人信息。在办理登记手续阶段,客户可以直接获得酒店房间、车辆等的支配权,而不必见代理或提供个人信息。在一些实施例中,客户可以通过证明他/她有权访问预订阶段使用的数字身份表示来解锁酒店房间或车辆。例如,客户可以使用能够控制PDS的移动设备。

[0191] VI.限制年龄的场所

[0192] 诸如酒吧的某些场所可能要求顾客提供他们年龄超过某个年龄的证据。为了提供年龄证明,客户可以创建徽章以与场所共享相关信息。徽章可以使用特定模式形成,该模式可以仅包括客户的年龄或客户的年龄和姓名。可以使用移动设备来执行信息共享。如果年龄已经由另一可信方证明,则场所可以断定由客户提供的年龄信息实际上是真实的。

[0193] 在一些实施例中,通过分散和保护性存储位置提供有利的技术效果,由此可以通过应用加密单向函数以受保护的方式存储敏感和(非常)易受攻击的用户信息。此外,通过

在相互信任的独立实体之间共享相应的请求的状态信息(例如,属性值是否被验证),可以容易地降低用于确定(用户)信息的真实性的验证过程的冗余性。因此,例如,通过避免不必要的工作流(并因此减少网络流量)、个人数据集的复制(和因此计算机存储)以及为了提供集中式存储和管理系统以在所有可想到的情况下始终使可比较的数据库保持可用的昂贵基础设施(例如中央结算所),不仅可以节省时间,还可以节省其他资源。因此,数据管理效率的提高还可导致例如基础设施和必要计算能力的减少和/或响应时间的减少。

[0194] 在一些实施例中,通过以受保护的方式共享(用户)信息,例如通过使用有利的散列算法,甚至敏感的(用户)信息可以被保持在可访问的位置,而不会在可以相互信任的多个不同实体的网络环境中遭受外部不可信实体的窃取、未经许可或欺诈性的修改等。

[0195] 下面描述本公开的一些说明性方面。由此,多个实体中的至少一个的个人身份表示可以被认为是数字身份表示(DIR),并且多个实体中的至少一个的用户数据结构可以被认为是个人数据服务(PDS)。

[0196] 1.一种计算机实现的方法,包括以下动作:

[0197] 使用从用户获得的多个测量值来生成该用户的标识符,该标识符包括所述多个测量值的加密证据;

[0198] 实例化与用户的标识符相关联的数字身份表示,该数字身份表示包括实现用于证明的规则的程序代码;

[0199] 在数字身份表示上生成电子签名;和

[0200] 将数字身份表示和电子签名发布到分布式账本系统。

[0201] 2.根据方面1所述的计算机实现的方法,其中,所述多个测量值包括至少一个生物识别测量值和至少一个行为测量值。

[0202] 3.根据权利要求1所述的计算机实现的方法,还包括以下动作:

[0203] 从所述分布式账本系统接收已创建所述数字身份表示的记录的确认。

[0204] 4.根据方面3所述的计算机实现的方法,其中,分布式账本系统使用至少一个区块链来实现。

[0205] 5.根据方面1所述的计算机实现的方法,还包括以下动作:

[0206] 经由分布式账本系统向可信实体发送验证徽章的请求,该徽章包括分别对应于多个属性的多个加密证据,其中每个加密证据是基于对应于所述加密证据的属性的值生成的;和

[0207] 经由分布式账本系统外部的通道向可信实体发送所述多个属性的所述多个值。

[0208] 6.根据方面1所述的计算机实现的方法,还包括以下动作:

[0209] 接收指向徽章的指针;

[0210] 使用该指针从分布式账本系统访问徽章,该徽章包括分别对应于所述多个属性的多个属性证明,其中,对于每个属性,对应的属性证明包括加密证据;

[0211] 经由分布式账本系统外部的通道接收分别对应于所述多个属性的多个值;

[0212] 从徽章识别负责验证该徽章的实体;

[0213] 确定是否信任负责验证徽章的实体;和

[0214] 响应于确定负责验证徽章的实体是可信的,针对所述多个属性证明中的每个属性证明,检查是否:

[0215] 属性证明处于已验证状态；

[0216] 属性证明中的加密证据是对应于所述属性的接收到的值的有效证据；和

[0217] 属性证明由负责验证徽章的实体电子签名。

[0218] 7.一种计算机实现的方法，包括以下动作：

[0219] 从用于徽章的多个模式中选择模式，所述模式包括多个属性；

[0220] 根据所述模式生成用于证明用户身份的徽章，其中所述生成动作包括：

[0221] 识别多个值，每个值对应于所述模式中的所述多个属性中的属性；

[0222] 为所述多个值中的每个值生成至少一个加密证据；和

[0223] 识别用于验证所述多个值的可信实体；和

[0224] 将徽章发布到分布式账本系统。

[0225] 8.根据方面7所述的计算机实现的方法，其中，分布式账本系统包括与用户的标识符相关联的数字身份表示，该数字身份表示包括实现用于证明的规则的程序代码。

[0226] 9.根据方面8所述的计算机实现的方法，其中：

[0227] 对于所述多个属性中的每个属性，徽章包括用于该属性的属性证明，其中属性证明包括用于对应属性值的至少一个加密证据；和

[0228] 当由至少一个处理器执行时，程序代码保持用于所述多个属性中的每个属性的属性证明的状态信息。

[0229] 10.根据方面9所述的计算机实现的方法，其中，至少一个属性证明处于选自由下列组成的组的状态：未决、已验证、过期和无效。

[0230] 11.根据方面10所述的计算机实现的方法，其中，当由所述至少一个处理器执行时，程序代码仅响应于来自可信实体的关于对应属性值已经由所述可信实体验证的通知而使所述至少一个属性证明从未决状态转变到已验证状态。

[0231] 12.根据方面10所述的计算机实现的方法，其中，当由所述至少一个处理器执行时，程序代码使所述至少一个属性证明在上次验证对应属性值时设置的定时器过期时从已验证状态转变到过期状态。

[0232] 13.根据方面10所述的计算机实现的方法，其中，当由所述至少一个处理器执行时，程序代码仅当所述至少一个属性证明处于已验证状态时才允许访问对应属性值的加密证据。

[0233] 14.一种计算机实现的方法，包括：

[0234] 经由分布式账本系统接收验证徽章的请求，该徽章包括分别对应于用户的多个属性的多个属性证明，其中对于每个属性，对应的属性证明包括加密证据；

[0235] 经由分布式账本系统外部的通道接收分别对应于所述多个属性的多个值；

[0236] 对于所述多个属性中的至少一个属性：

[0237] 验证对应于所述至少一个属性的值对于用户是否是所述至少一个属性的正确值；

[0238] 响应于验证对应于所述至少一个属性的值对于用户是所述至少一个属性的正确值，经由分布式账本系统使对应于所述至少一个属性的属性证明处于已验证状态。

[0239] 15.一种计算机实现的方法，包括：

[0240] 经由分布式账本系统接收验证第一徽章的请求，该第一徽章包括分别对应于用户的多个属性的多个属性证明，其中对于每个属性，对应的属性证明包括加密证据；

[0241] 经由分布式账本系统外部的通道接收分别对应于所述多个属性的多个值；

[0242] 对于所述多个属性中的至少一个属性：

[0243] 从第一徽章识别对应于所述至少一个属性的第一属性证明，第一属性证明包括第一加密证据；

[0244] 从第一属性证明识别指向第二徽章的指针；

[0245] 使用所述指针从分布式账本访问第二徽章；

[0246] 从第二徽章识别负责验证第二徽章的实体以及对应于所述至少一个属性的第二属性证明；

[0247] 确定是否信任负责验证第二徽章的实体；和

[0248] 响应于确定负责验证第二徽章的实体是可信的，检查是否：

[0249] (1)第二属性证明处于已验证状态；

[0250] (2)第二加密证据是对应于所述至少一个属性的接收值的有效证据；和

[0251] (3)第二属性证明由负责验证第二徽章的实体电子签名。

[0252] 16.根据方面15所述的方法，还包括检查是否：

[0253] (4)第一加密证据是对应于所述至少一个属性的接收值的有效证据；

[0254] 17.根据方面16所述的方法，还包括响应于经检查(1)-(4)被满足而进行的以下动作：

[0255] 电子签署第一属性证明；和

[0256] 使第一属性证明转变到已验证状态。

[0257] 图10示意性地示出了可以在其上实现本公开的任何方面的说明性计算机10000。在图10所示的实施例中，计算机10000包括具有一个或多个处理器的处理单元10001和可以包括例如易失性和/或非易失性存储器的非暂时性计算机可读存储介质10002。存储器10002可以存储一个或多个指令，用于对处理单元10001编程以执行本文所述的任何功能。除了系统存储器10002之外，计算机10000还可以包括其他类型的非暂时性计算机可读介质，例如存储10005(例如，一个或多个磁盘驱动器)。存储10005还可以存储可以加载到存储器10002中的一个或多个应用程序和/或由应用程序(例如，软件库)使用的外部组件。

[0258] 计算机10000可以具有一个或多个输入设备和/或输出设备，例如图10所示的设备10006和10007。这些设备主要可用来呈现用户界面。可用来提供用户界面的输出设备的示例包括用于可视地呈现输出的打印机或显示屏和用于可听地呈现输出的扬声器或其他声音生成设备。可用于用户界面的输入设备的示例包括键盘和诸如鼠标、触摸板和数字化输入板的定点设备。作为另一示例，输入设备10007可以包括用于捕获音频信号的麦克风，并且输出设备10006可以包括用于可视地呈现所识别的文本的显示屏和/或用于可听地呈现所识别的文本的扬声器。

[0259] 如图10所示，计算机10000还可以包括一个或多个网络接口(例如，网络接口10010)，以实现经由各种网络(例如，网络10020)的通信。网络的示例包括局域网或广域网，例如企业网络或因特网。这些网络可基于任何合适的技术并可根据任何合适的协议来操作，并且可包括无线网络、有线网络或光纤网络。

[0260] 至此描述了至少一个实施例的若干方面，应当理解，本领域的技术人员可容易地想到各种更改、修改和改进。这些更改、修改和改进旨在落入本公开的精神和范围内。因此，

以上描述和附图仅仅作为示例。

[0261] 可以用多种方式中的任一种来实现本公开的上述实施例。例如，可使用硬件、软件或它们的组合来实现各实施例。当在软件中实现时，软件代码可在无论设置在单个计算机中或分布在多个计算机之间的任何合适的处理器或处理器的集合上执行。

[0262] 另外，本文略述的各种方法或过程可被编码为可在采用各种操作系统或平台中任何一种的一个或多个处理器上执行的软件。另外，这样的软件可使用多种合适的程序设计语言和/或程序设计或脚本工具中的任一种来编写，并且还可编译为可执行机器语言代码或在框架或虚拟机上执行的中间代码。

[0263] 在这方面，本文所公开的概念可以具体化为用一个或多个程序编码的非暂时性计算机可读介质(或多个计算机可读介质)(例如，计算机存储器、一个或多个软盘、紧致盘、光盘、磁带、闪速存储器、现场可编程门阵列或其它半导体设备中的电路配置、或其它非暂时性有形计算机存储介质)，当在一个或多个计算机或其它处理器上执行时，所述一个或多个程序执行实现上文所论述的本公开的各种实施例的方法。一个或多个计算机可读介质可以是便携的，使得其上存储的一个或多个程序可被加载到一个或多个不同的计算机或其它处理器上以便实现如上所述的本公开的各个方面。

[0264] 本文所用术语“程序”或“软件”来指可用于对计算机或其它处理器编程以实现如上所述的本公开的各个方面的任何类型的计算机代码或计算机可执行指令集。

[0265] 另外，应当理解，根据本实施例的一个方面，当被执行时实现本公开的方法的一个或多个计算机程序不必驻留在单个计算机或处理器上，而是可以按模块化的方式分布在多个不同的计算机或处理器之间以实现本公开的各个方面。

[0266] 计算机可执行指令可具有由一个或多个计算机或其他设备执行的许多形式，例如程序模块。通常，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。通常，程序模块的功能可根据需要在各个实施例中进行组合或分布。

[0267] 另外，数据结构可以任何合适的形式存储在计算机可读介质中。为简化说明，数据结构可被示为具有通过在该数据结构中的位置而相关的字段。这些关系同样可通过为具有传达各字段之间的关系的、计算机可读介质中的位置的各字段分配存储来实现。然而，可以使用任何合适的机制来在数据结构的各字段中的信息之间建立关系，包括通过使用指针、标签或在数据元素之间建立关系的其他机制。

[0268] 本公开的各个特征和方面可以单独地、以两个或更多个的任意组合或以未在上文所述实施例中特别讨论的各种安排来使用，从而并不将其应用限于前述描述中阐述或附图中示出的组件的细节和安排。例如，可以任何方式将一个实施例中描述的方面与其他实施例中描述的各方面组合。

[0269] 另外，本文所公开的概念可以具体化为已经提供了示例的方法。作为该方法的一部分所执行的动作可用任何合适的方式来排序。因此，可以构建各个实施例，其中各动作以与所示次序不同的次序执行，该次序可包括同时执行某些动作，即时这些动作在示例性实施例中被示为顺序的动作。

[0270] 在权利要求书中使用诸如“第一”、“第二”、“第三”等序数词来修饰权利要求元素本身并不意味着一个权利要求元素较之另一个权利要求元素的优先级、先后次序或顺序、或者方法的各动作执行的时间顺序，而仅用作将具有某一名字的一个权利要求元素与(若

不是使用序数词则)具有同一名字的另一元素区分开的标签以区分各权利要求元素。

[0271] 另外,本文所用短语和术语是用于说明的目的,而不应看作是进行限制。本文对“包括”、“包含”、“具有”、“含有”、“涉及”及其变型的使用旨在涵盖其后所列的项目及其等同物,以及附加的项目。

[0272] 权利要求书:

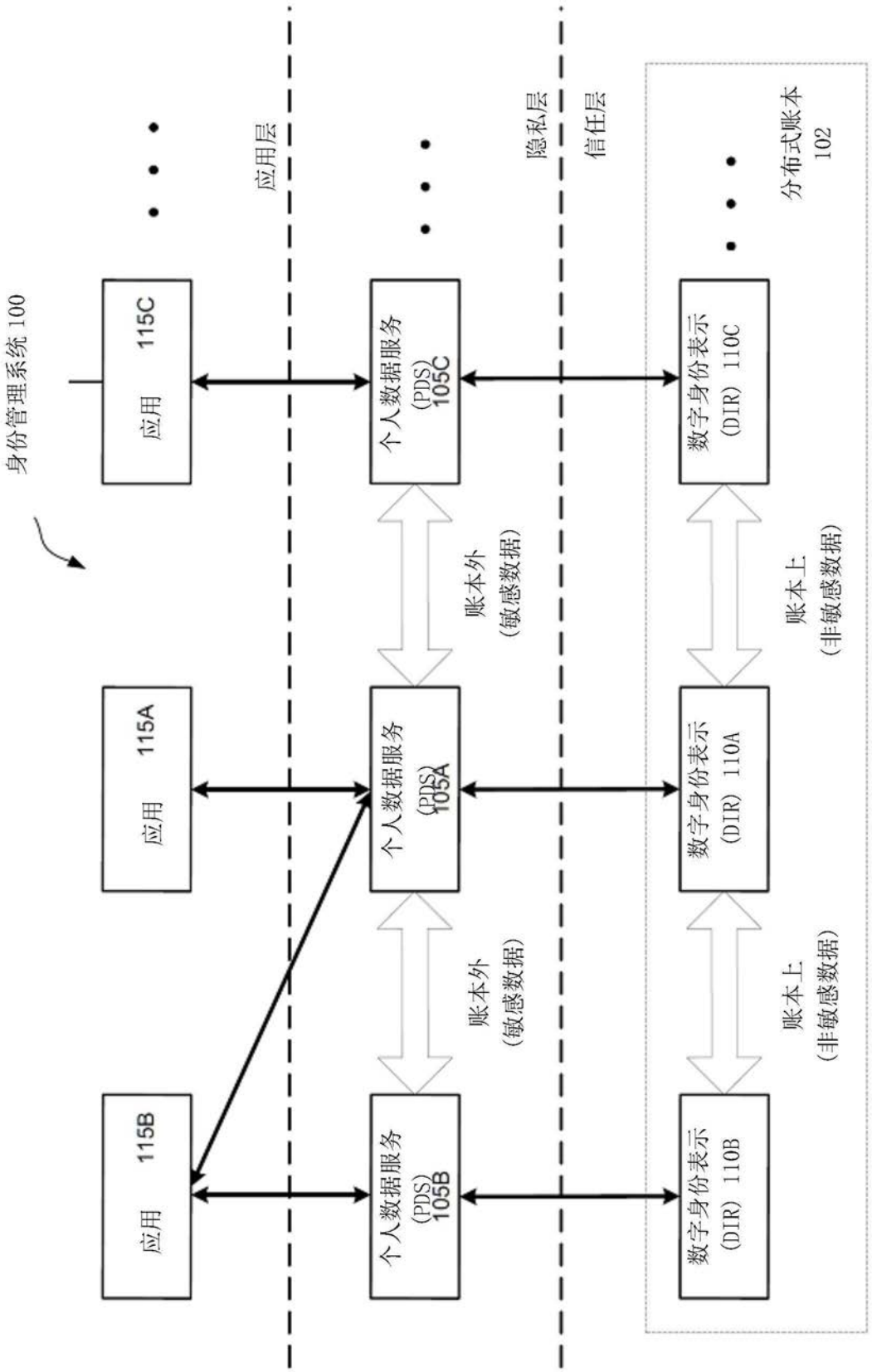

身份管理系统 100
应用层
隐私层
信任层
分布式账本
102
应用 115C
应用 115A
应用 115B
个人数据服务 (PDS) 105C
个人数据服务 (PDS) 105A
个人数据服务 (PDS) 105B
数字身份表示 (DIR) 110C
数字身份表示 (DIR) 110A
数字身份表示 (DIR) 110B
账本外 (敏感数据)
账本外 (敏感数据)
账本上 (非敏感数据)
账本上 (非敏感数据)

图1

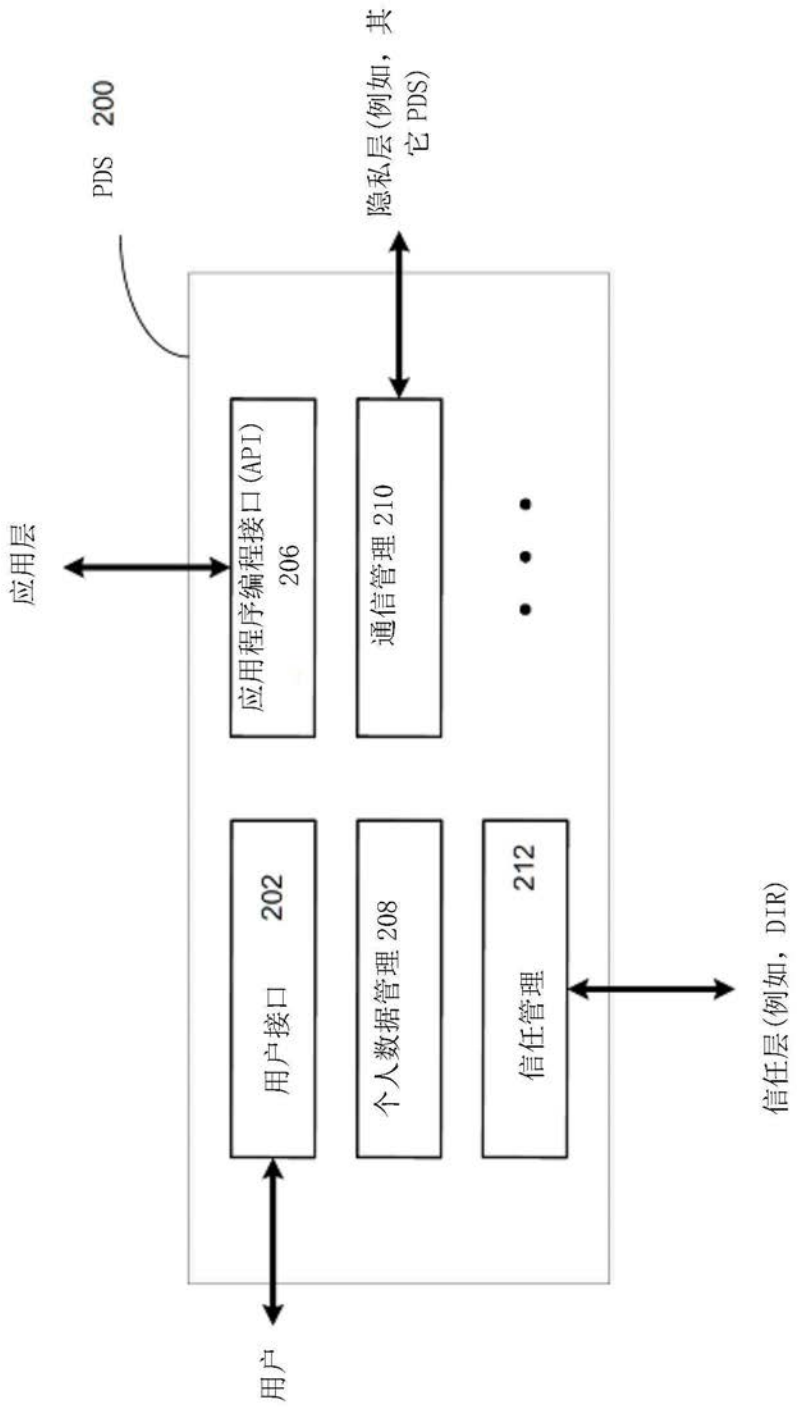

PDS 200
隐私层(例如，其它 PDS)
应用层
应用程序编程接口(API) 206
通信管理 210
用户接口 202
个人数据管理 208
信任管理 212
信任层(例如，DIR)
用户

图2

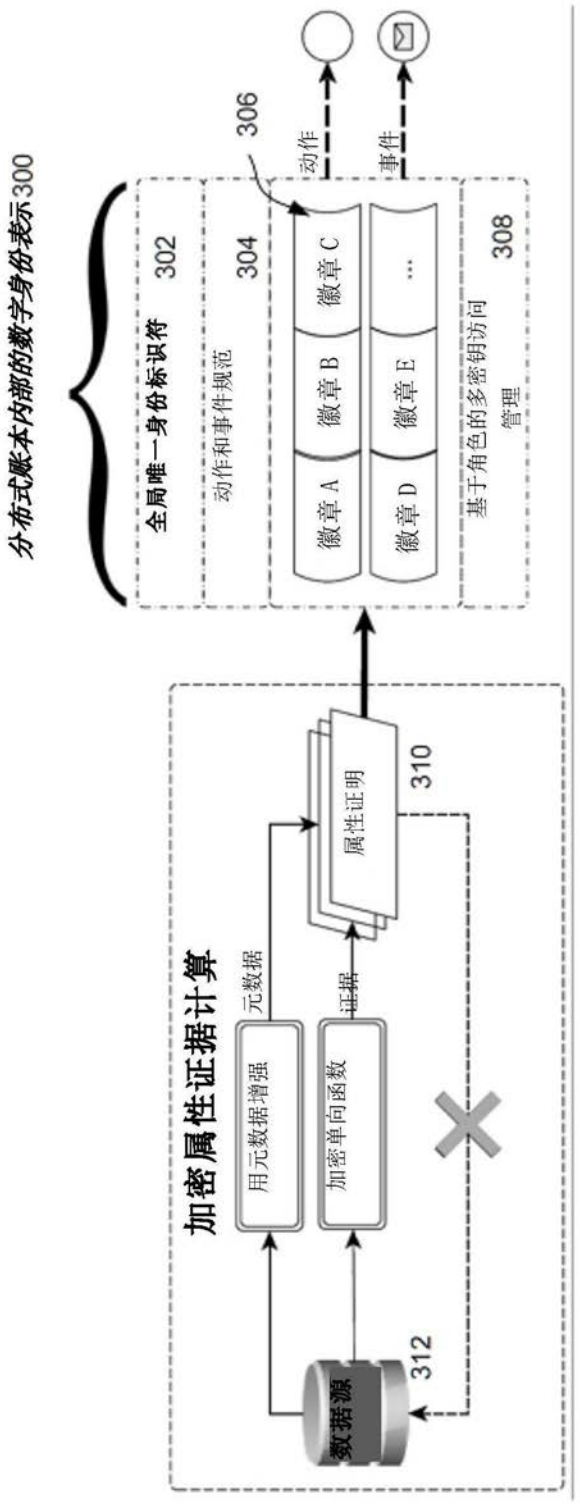

分布式账本内部的数字身份表示300
全局唯一身份标识符
302
动作和事件规范
304
306
动作
事件
徽章 A
徽章 B
徽章 C
徽章 D
徽章 E
...
基于角色的多密钥访问管理
308
加密属性证据计算
用元数据增强
元数据
加密单向函数
证据
属性证明
310
数据源
312

图3

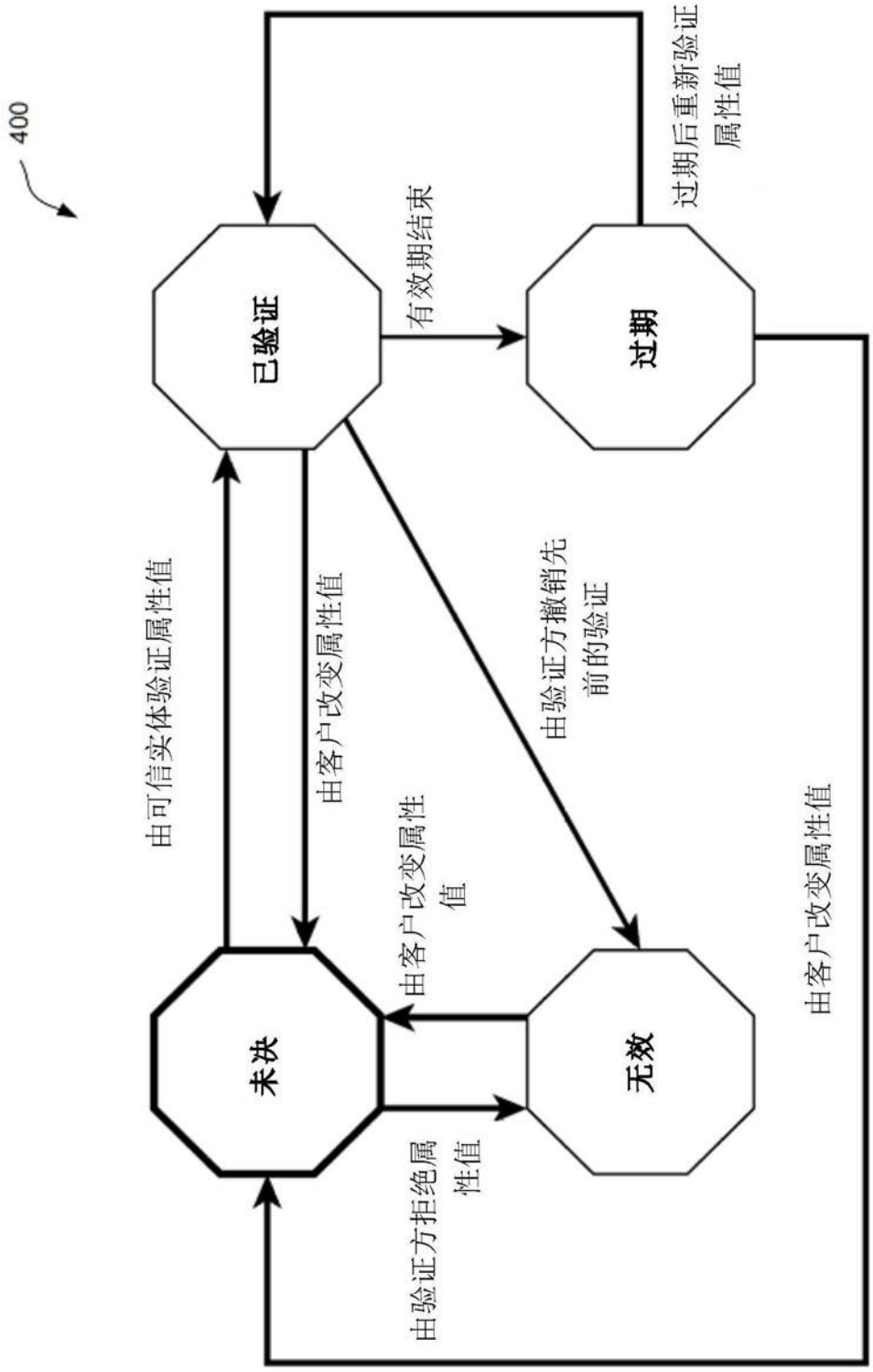

400
已验证
过期
未决
无效
有效期结束
过期后重新验证属性值
由可信实体验证属性值
由客户改变属性值
由验证方撤销先前的验证
由客户改变属性值
由客户改变属性值
由验证方拒绝属性值

图4

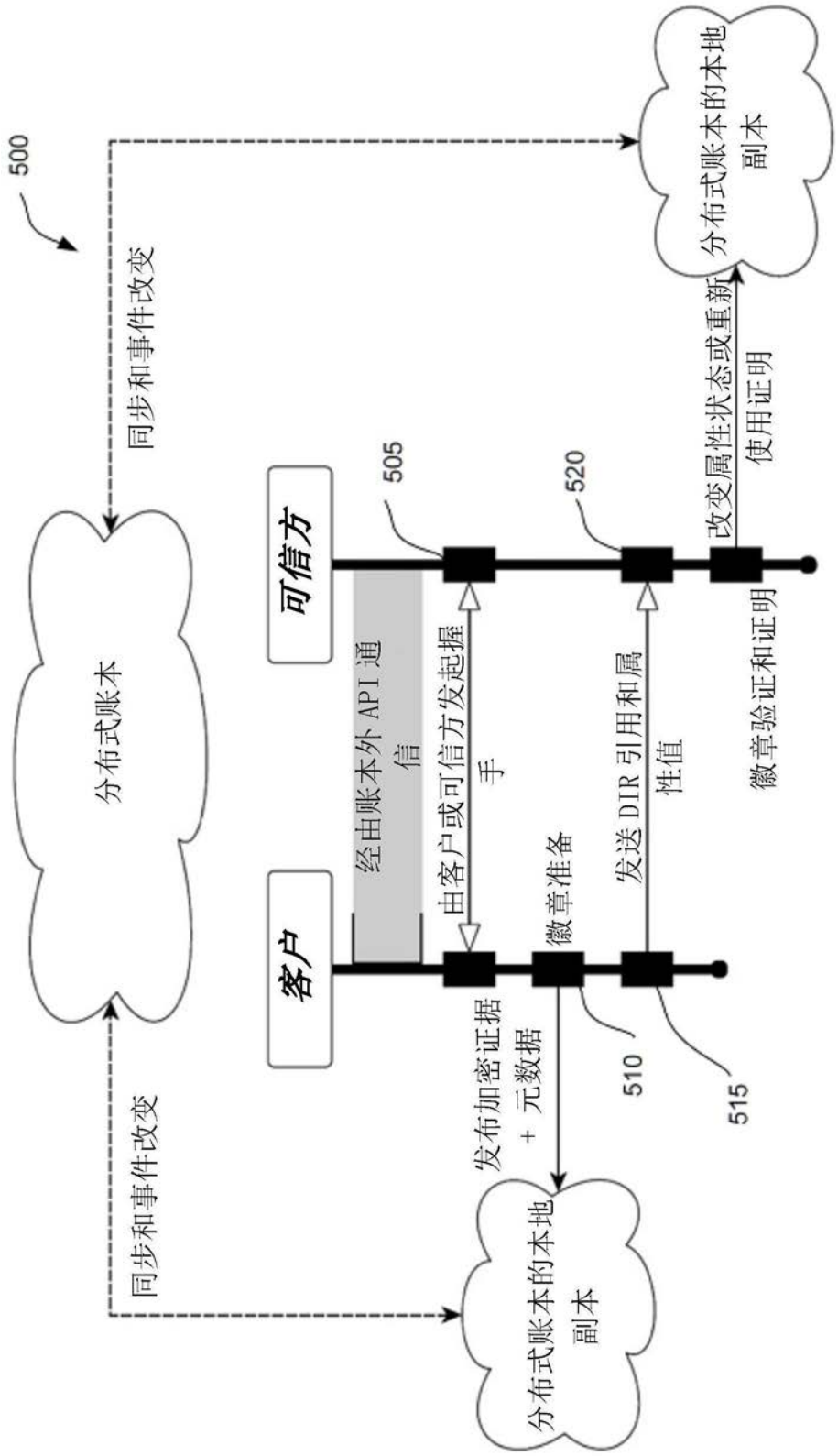

500
同步和事件改变
分布式账本的本地副本
分布式账本
可信方
505
520
改变属性状态或重新使用证明
经由账本外 API 通信
由客户或可信方发起握手
徽章验证和证明
客户
徽章准备
发送 DIR 引用和属性值
发布加密证据 + 元数据
510
515
同步和事件改变
分布式账本的本地副本

图5

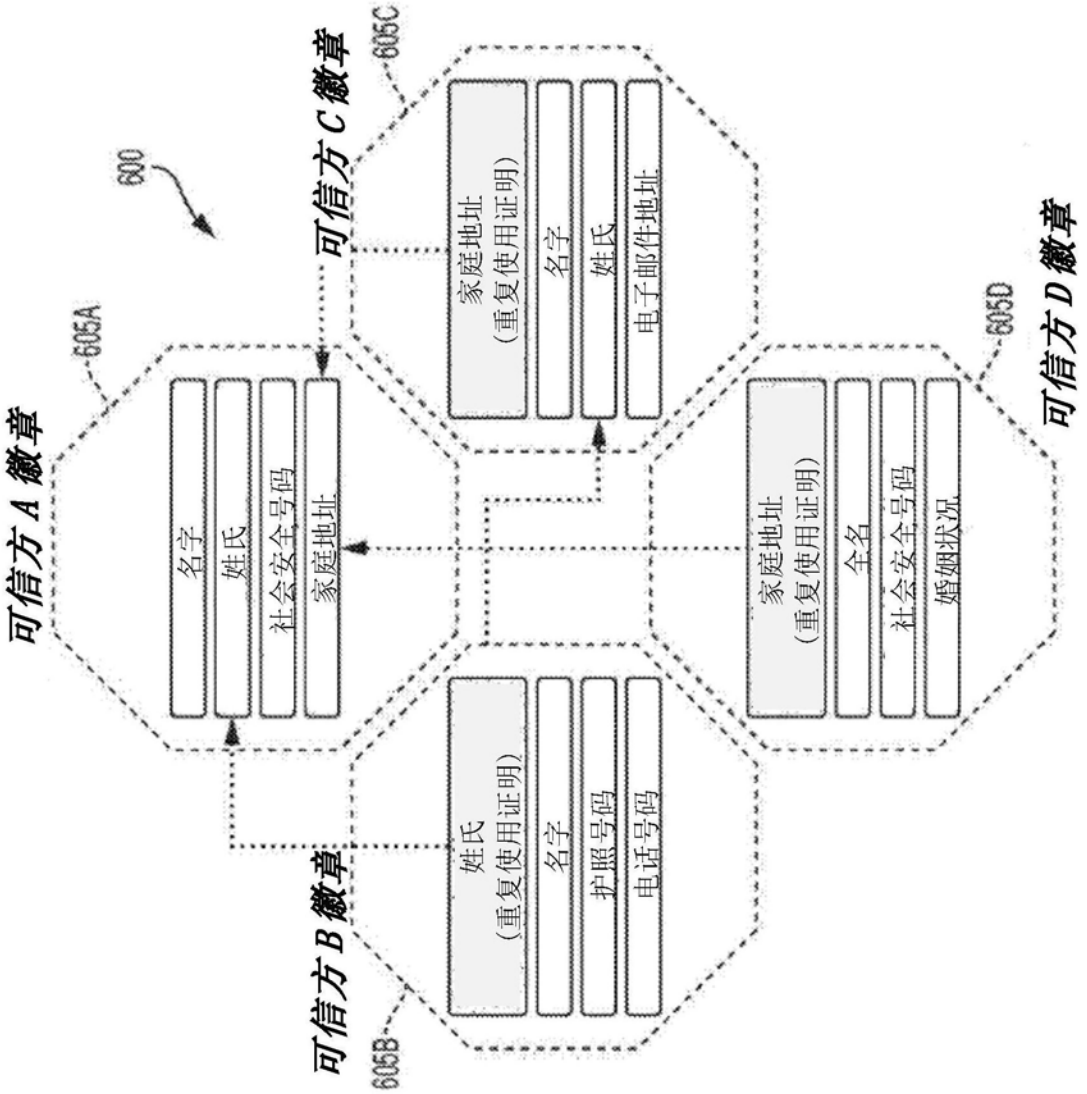

600
可信方 A 徽章
605A
名字
姓氏
社会安全号码
家庭地址
可信方 C 徽章
605C
家庭地址
(重复使用证明)
名字
姓氏
电子邮件地址
可信方 B 徽章
605B
姓氏
(重复使用证明)
名字
护照号码
电话号码
可信方 D 徽章
605D
家庭地址
(重复使用证明)
全名
社会安全号码
婚姻状况

图6

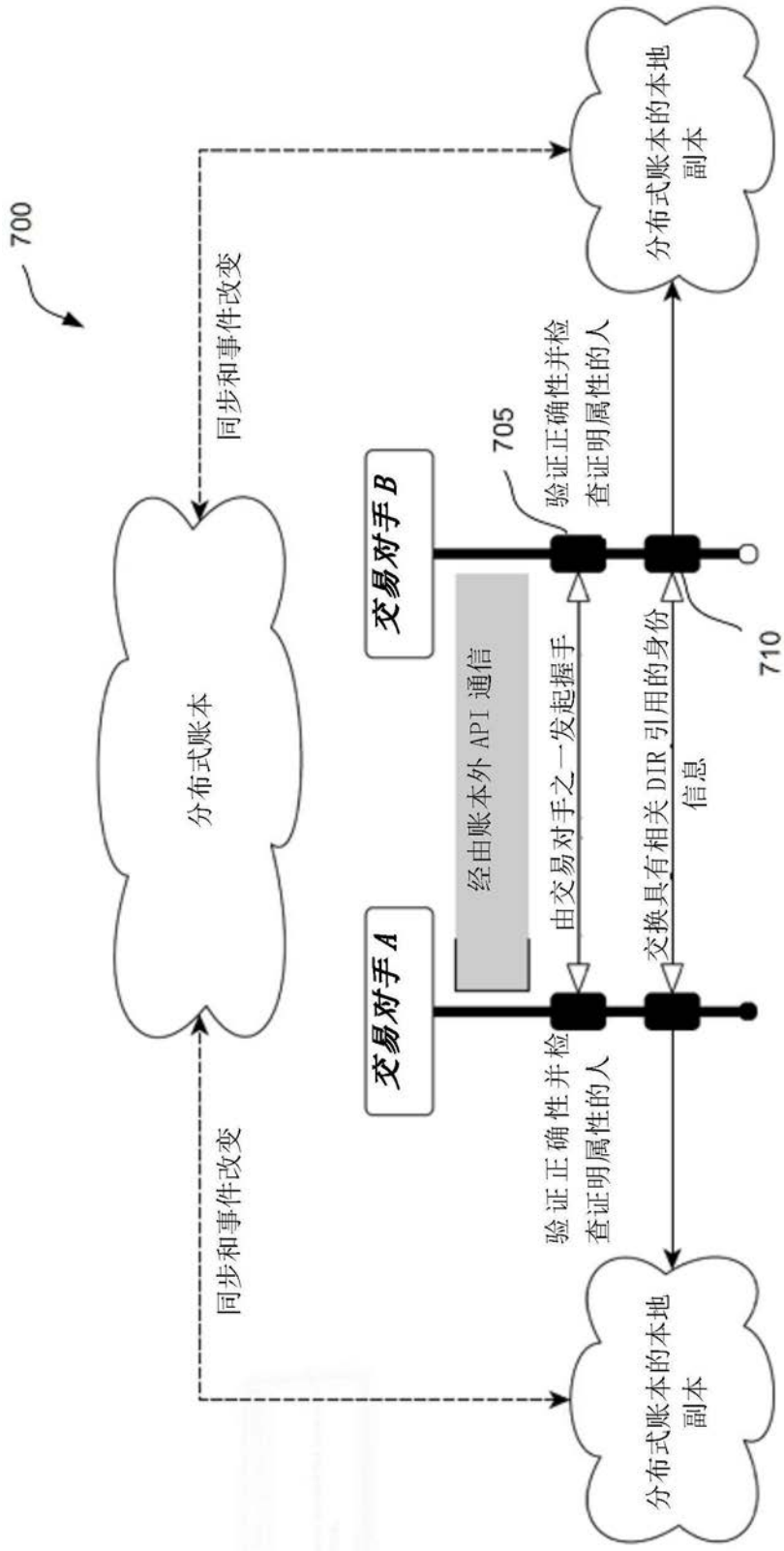

700
同步和事件改变
分布式账本的本地副本
分布式账本
交易对手 B
705
验证正确性并检查证明属性的人
经由账本外 API 通信
由交易对手之一发起握手
交换具有相关 DIR 引用的身份信息
710
交易对手 A
验证正确性并检查证明属性的人
同步和事件改变
分布式账本的本地副本

图7

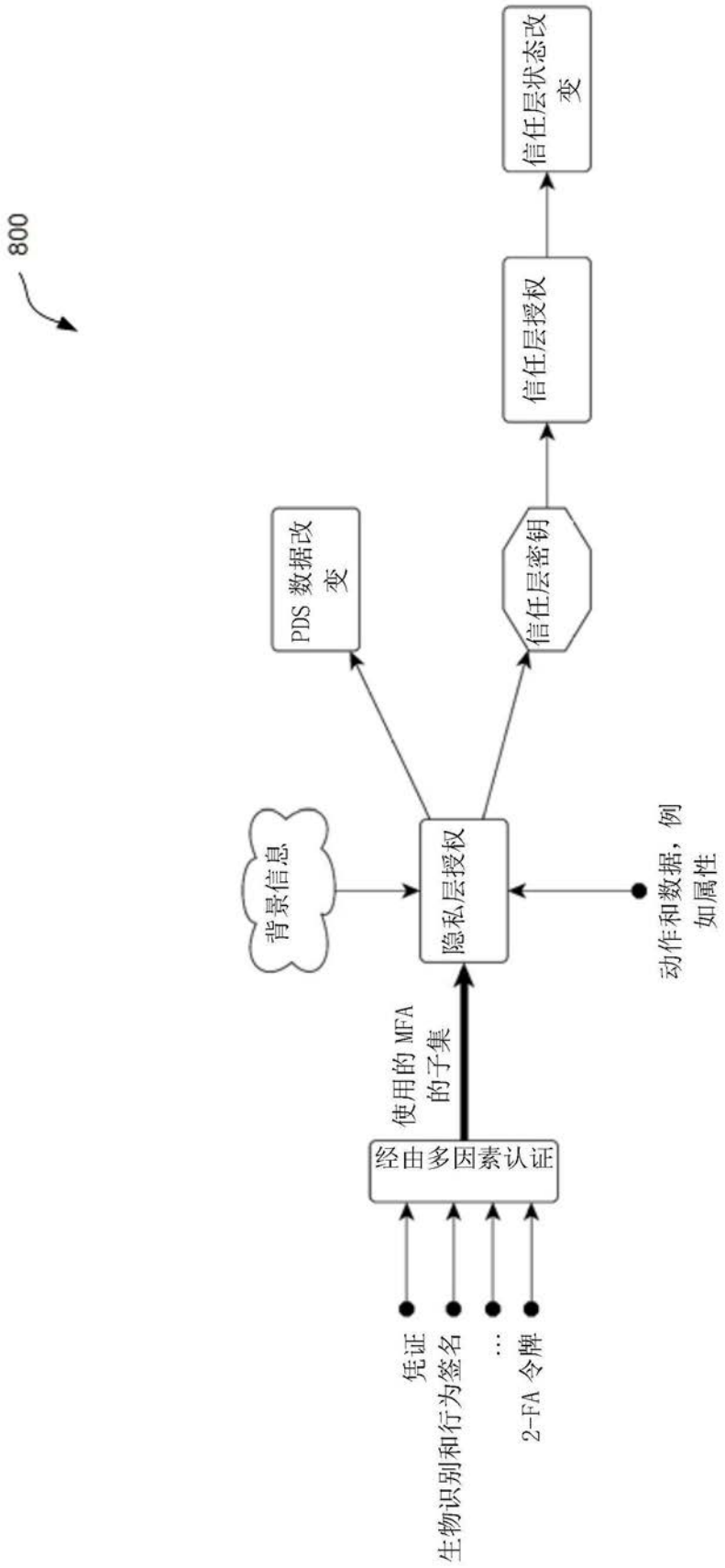

800
信任层状态改变
信任层授权
信任层密钥
PDS 数据改变
背景信息
隐私层授权
动作和数据，例如属性
使用的 MFA 的子集
经由多因素认证
凭证
生物识别和行为签名
…
2-FA 令牌

图8

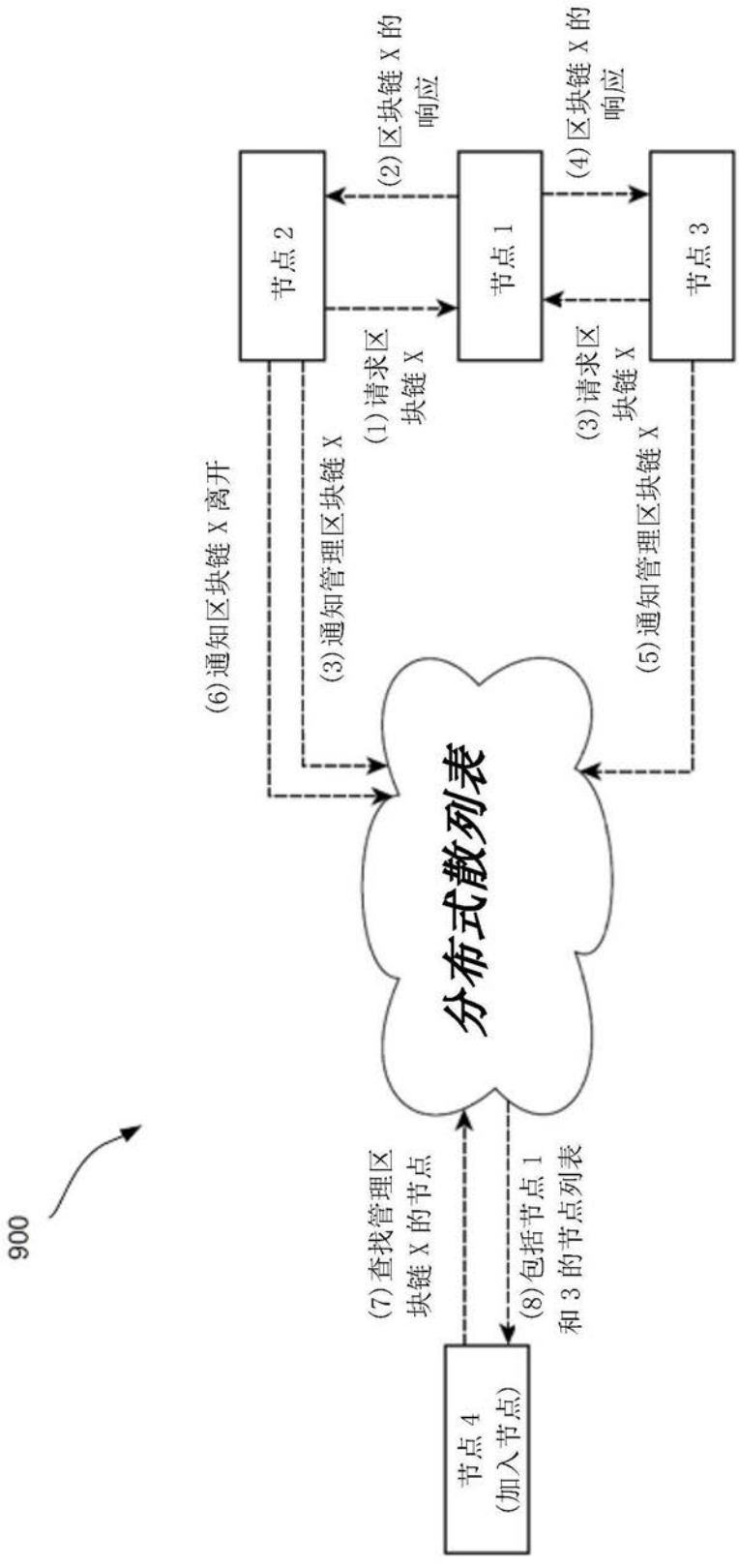

900
节点 2
节点 1
节点 3
节点 4
(加入节点)
分布式散列表
(1) 请求区块链 X
(2) 区块链 X 的响应
(3) 请求区块链 X
(4) 区块链 X 的响应
(3) 通知管理区块链 X
(5) 通知管理区块链 X
(6) 通知区块链 X 离开
(7) 查找管理区块链 X 的节点
(8) 包括节点 1 和 3 的节点列表

图9

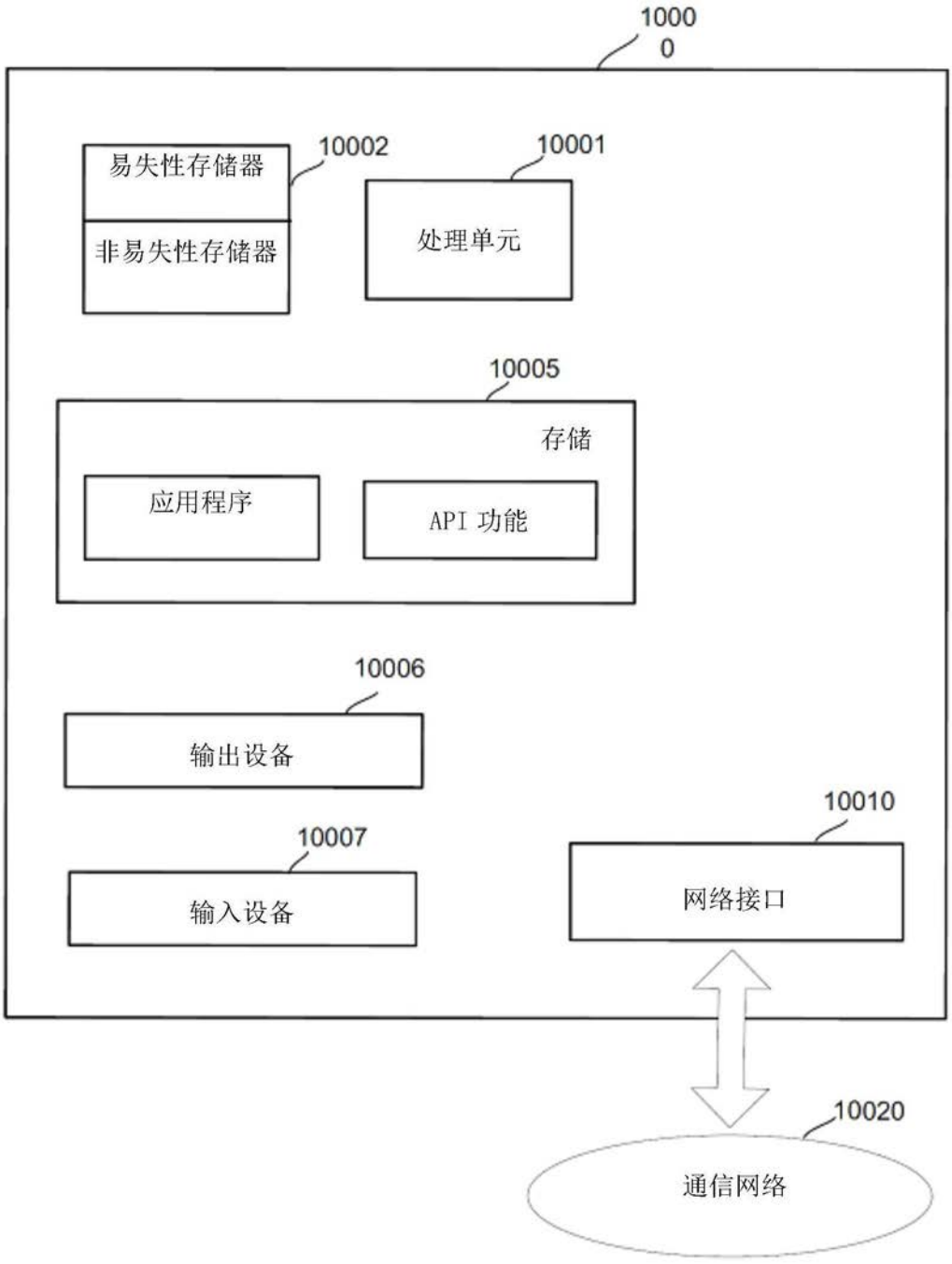

10000
易失性存储器
10002
非易失性存储器
10001
处理单元
10005
存储
应用程序
API 功能
10006
输出设备
10007
输入设备
10010
网络接口
10020
通信网络

图10