(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 113674861 A
(43)申请公布日 2021.11.19

(21)申请号 202110504717.X

(22)申请日 2021.05.10

(30)优先权数据
102020000010861 2020.05.13 IT

(71)申请人 艾力集团有限责任公司-卡皮贾尼
地址 意大利米兰

(72)发明人 A·库奇 C·吉安内利
R·拉扎里尼 C·斯特范林
F·塔西

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

(51)Int.Cl.
G16H 50/30(2018.01)
G16H 10/40(2018.01)
G06F 21/62(2013.01)
G06F 16/27(2019.01)

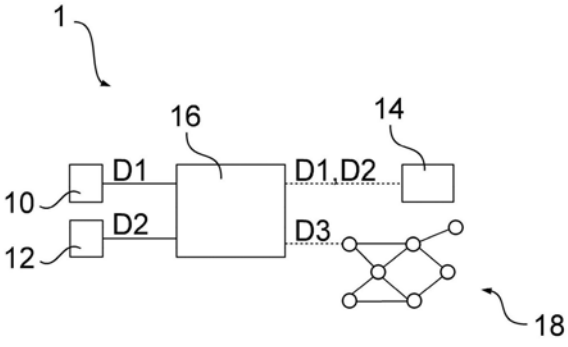
权利要求书3页 说明书6页 附图1页

(54)发明名称

基于区块链的健康监测系统

(57)摘要

描述了一种健康监督系统(1),包括:识别站(10),被配置成获得指示用户身份的至少一个第一数据项(D1),健康站(12),被配置成获得指示所识别的用户的健康状况的至少一个第二数据项(D2),至少一个本地数据存储库(14),以及控制单元(16),被配置成用于:接收至少一个第一数据项(D1)和至少一个第二数据项(D2),使用加密函数作为至少一个第一数据项(D1)和/或至少一个第二数据项(D2)的函数来计算字符串(D3),将至少一个第一数据项(D1)和/或至少一个第二数据项(D2)存储在至少一个本地数据存储库(14)中,以及将字符串(D3)传送给分布式账本类型的分布式架构数据库(18),以将字符串(D3)写入分布式架构数据库(18)。



CN 113674861 A

1.一种健康监督系统(1),包括:

-识别站(10),其被配置为获得指示用户身份的至少一个第一数据项(D1),

-健康站(12),其被配置成获得指示所识别的用户的健康状况的至少一个第二数据项(D2),

-至少一个本地数据存储库(14),以及

-控制单元(16),被配置成用于:

-接收所述至少一个第一数据项(D1)和所述至少一个第二数据项(D2),

-使用加密函数作为所述至少一个第一数据项(D1)和/或所述至少一个第二数据项(D2)的函数来计算字符串(D3),

-将所述至少一个第一数据项(D1)和/或所述至少一个第二数据项(D2)存储在至少一个本地数据存储库(14)中,以及

-将所述字符串(D3)传送给分布式账本类型的分布式架构数据库(18),以将所述字符串(D3)写入所述分布式架构数据库(18)。

2.如权利要求1所述的监督系统(1),其特征在于,所述识别站(12)包括扫描器,优选为照相机或条形码扫描器,其被配置成获得包括识别用户身份的一个或多个元素的所述至少一个第一数据项(D1)。

3.如权利要求1或2所述的监督系统(1),其特征在于,所述健康站(12)包括实验室,其被配置成对来自所述用户的样本执行血清学和/或分子测试,并获得包括所述血清学和/或分子测试的结果的所述至少一个第二数据项(D2)。

4.如权利要求1到3中任一项所述的监督系统(1),其特征在于,所述至少一个本地数据存储库(14)包括集中式数据存储库,所述数据存储库受到保护并且能由所述控制单元(16)在授权之后访问。

5.如前述权利要求中任一项所述的监督系统(1),其特征在于,所述至少一个本地数据存储库(14)至少部分地由多个个人电子设备,优选地为智能手机,来定义,其中所述个人电子设备中的每一者与某个用户相关联,以便:

-所述至少一个第二数据项(D2)仅能被存储在所识别的用户的所述个人电子设备中,和/或

-在来自所述用户和/或来自所述控制单元(16)的请求之后,能访问所述至少一个第二数据项(D2),和/或

-所述至少一个第二数据项(D2)只能在来自所述控制单元(16)的命令之后被删除。

6.如前述权利要求中任一项所述的监督系统(1),其特征在于,包括分布式账本类型的所述分布式架构数据库(18)。

7.如前一权利要求所述的监督系统(1),其特征在于,所述分布式账本类型的分布式架构数据库(18)是区块链类型的,并且包括分组在通过密码算法互连的多个信息块中的信息。

8.如权利要求6或7所述的监督系统(1),其特征在于,所述分布式账本类型的分布式架构数据库(18)在以太坊或以太坊经典或Iota或Eos或NEO或Waves或Qtum或NEM或Multiversum或R3 Corda或R3 Corda企业或Hyperledger或Ripple或Stellar平台上构建。

9.如前述权利要求中任一项所述的监督系统(1),其特征在于,所述分布式账本类型的

分布式架构数据库(18)与用于写入所述数据库(18)的一致协议一起操作,并从以下类型中选择:

-工作证明;

-权益证明;

-Corda共识协议(被配置成就特定"状态对象"达成共识);

-CFT(崩溃容错),优选地用Kafka和/或Zookeeper实现;

-Solo;

-BFT(拜占庭容错);

-PBFT(实际BFT);

-SBFT(简化BFT);

-Raft;

-Sumeragi;

-PoET(消逝时间证明);

-基于许可制投票。

10.如前述权利要求中任一项所述的健康监督系统(1),其特征在于,计算所述字符串(D3)的步骤包括使用加密哈希函数计算所述字符串(D3)。

11.如前述权利要求中任一项所述的健康监督系统(1),其特征在于:

-所述字符串(D3)与从中计算所述字符串(D3)的所述至少一个第一数据项(D1)和/或所述至少一个第二数据项(D2)是一对一匹配的,和/或

-不能从所述字符串(D3)获得所述至少一个第一数据项(D1)和/或所述至少一个第二数据项(D2)。

12.如前述权利要求中任一项所述的健康监督系统(1),其特征在于,所述控制单元(16)被配置成用于:

将时间戳与所述至少一个第一数据项(D1)和/或所述至少一个第二数据项(D2)相关联,以及

如果所述时间戳指示所述数据在某个日期之前被存储,则删除存储在所述至少一个本地数据存储库(14)中的多个第一数据项(D1)和/或第二数据项(D2)之间的数据。

13.如前述权利要求中任一项所述的健康监督系统(1),其特征在于,所述控制单元(16)被配置成用于在所述至少一个第二数据项(D2)指示存在SARS-CoV-2病毒抗原的情况下传送警报信号。

14.一种健康监督方法,包括:

-提供根据前述权利要求中任一项所述的健康监督系统(1),

-通过所述识别站(10)获得指示用户的身份的至少一个第一数据项(D1),

-通过所述健康站(12)获得指示所识别的用户的健康状况的至少一个第二数据项(D2),

-通过所述标识站(10)和所述健康站(12)一起接收所述至少一个第一数据项(D1)和所述至少一个第二数据项(D2),

-使用加密函数作为所述至少一个第一数据项(D1)和/或所述至少一个第二数据项(D2)的函数来计算字符串(D3),

-将所述至少一个第一数据项(D1)和/或所述至少一个第二数据项(D2)存储在至少一个本地数据存储库(14)中,以及

-将所述字符串(D3)传送给分布式账本类型的分布式架构数据库(18),以将所述字符串(D3)写入所述分布式架构数据库(18)。

基于区块链的健康监测系统

[0001] 本发明涉及一种健康监督系统，例如，能够记录多个用户的健康状况的健康监督系统。

[0002] 新冠肺炎(Covid-19)的传播已经导致了限制性措施的采用，这些措施已经导致了贸易的急剧减少，并且在许多情况下已经带来了生产活动的停止。结束这一限制期将必然需要高度的预防措施以防止新的感染群。直到疫苗变得可用之前，不仅是国内聚集的死灰复燃的风险，还有从国外输入感染的风险仍然很高。在这种情况下，工作场所被认为是潜在的生物危害源。

[0003] 因此，在目前的情况下，正在出现的许多新挑战涉及最小化并且监测新的感染或改善在工作的人员的安全。

[0004] 监测用户的健康状况可能与以下一个或多个问题有关：确保数据的不变性，只允许经授权的人(例如卫生和/或司法当局)访问信息，并且保障被监测者的隐私和被遗忘的权利。

[0005] 因此，本发明的目的是通过提供如本公开中所述的健康监督系统来满足上述需要，该系统能够以限制病毒的传播的视角来监测公众的健康状况。

[0006] 本发明的另一目的是允许所记录的数据保持不变，同时保证用户被遗忘的权利。

[0007] 本发明的又一目的是确保所执行试验的可追溯性，如由Emilia Romagna地区委员会通过的日期为2020年4月16日的第350号决议所述。

[0008] 参考上述目的，本公开的技术特征在下面的权利要求中被清楚地描述，并且其优点从下面的详细描述中显而易见，参考附图，其例示了优选的、非限制性的示例实施例，其中：

[0009] -图1示出了代表根据一个或多个实施例的健康监督系统的框图。

[0010] 图1示出了根据一个或多个实施例的健康监督系统1。系统1允许设立公司检查点，其中用户，例如雇员、访客及其家庭成员可以在自愿的基础上接受流行病学检查。例如，以第二数据项D2的形式的测试结果可被记录在本地数据存储库16(例如，公司数据库)中，并且可以通过区块链技术进行认证，如下文更详细描述的。有利地，因此可以周期性地监测一组用户的健康状态，以便为公司提供更好的保护。例如，用户可以周期性地与系统1交互以接受健康检查。例如，每个用户可以以预定的定期间隔(例如，每周或每周两次)与系统1交互。

[0011] 有利的是，将一家公司转变为保健中心以保障雇员及其家庭成员的健康，可以使商店、餐馆和其他贸易企业更容易地重新安全开业，从而能够安全有效地从紧急情况中过渡出来。

[0012] 系统1包括：

[0013] -识别站10，其被配置成获得指示用户的身份的至少一个第一数据项D1，

[0014] -健康站12，其被配置成获得指示所识别的用户的健康状况的至少一个第二数据项D2，

[0015] -至少一个本地数据存储库14，以及

[0016] -控制单元16,被配置成用于:

[0017] -接收至少一个第一数据项D1和至少一个第二数据项D2,

[0018] -使用加密函数作为至少一个第一数据项D1和/或至少一个第二数据项D2的函数来计算字符串D3,其中字符串D3例如指示第一数据项D1和/或第二数据项D2,

[0019] -将至少一个第一数据项D1和/或至少一个第二数据项D2存储在至少一个本地数据存储库14中,以及

[0020] -将字符串D3传送给分布式账本类型的分布式架构数据库18以将字符串D3写入分布式架构数据库,例如,基于区块链的数据库。

[0021] 根据一方面,系统1可以包括分布式账本类型的分布式架构数据库18。例如,数据库18可以由基于区块链技术的对等网络来定义。数据库18可以由形成健康监督网络的一部分的一个或多个公司内和/或本地医疗保健机构(ASL)内的多个节点来定义。

[0022] 根据一方面,控制单元16可以被配置为将字符串D3写入分布式架构数据库18。

[0023] 有利地,该系统允许确保数据的不变性,因为它基于分布式架构数据库18的使用,同时保证用户被遗忘的权利,因为至少一个第一数据项D1和至少一个第二数据项D2不被存储在数据库18中。相反,指示数据项D1和D2的字符串D3被存储在数据库18中。实际上,如果雇员的拭子测试结果被存储在区块链中,则该信息将变得不可更改(防篡改),但将对于形成同一区块链一部分的一个或多个组织可见,这与在敏感或健康数据的情况下其遵守更为严格的个人数据隐私权形成对比。

[0024] 在一个或多个实施例中,识别站10可以包括扫描器,优选为条形码扫描器或照相机,其被配置成获得包括识别用户身份的一个或多个元素的至少一个第一数据项D1。例如,扫描器可被配置成借助诸如举例而言,身份证、驾驶执照和/或社会保险卡之类的身份证件来识别用户。扫描器因此可以捕获至少一个第一数据项D1,其可以包括用户的姓名、姓氏和/或纳税人ID号。识别站10可以直接或间接地连接到控制单元16,并且可以被配置为将至少一个第一数据项D1传送给控制单元16。

[0025] 在一个或多个实施例中,健康站12可包括实验室,其被配置成对从所识别的用户提取(获取)的生物样本执行血清学和/或分子测试,并获得包括血清学和/或分子测试结果的至少一个第二数据项D2。健康站12可以直接或间接地连接到控制单元16,并且可以被配置为将至少一个第二数据项D2传送给控制单元16。

[0026] 根据一方面,健康监督系统1可以包括一个或多个公司的办公室。识别站10可位于一个或多个公司的办公室内,每个公司具有与其相关联的识别站10和健康站12。健康站12(例如,实验室)可以位于一个或多个公司的办公室内,也可以位于远离公司场所的偏远位置。在后一种情况下,在识别之后,可以将从用户提取(获取)的样本传送给健康站12以供处理。

[0027] 根据一方面,实验室包括能够基于工业方法和时间表与公司合作的高素质人员。

[0028] 根据一方面,健康站12可被配置成通过使用免疫层析板以检测IG-G和IG-M抗体来分析血液样本,以执行快速血清学测试。健康站12可包括多个一次性试剂盒,其能够在相对较短的时间内执行血清学测试并提供结果。

[0029] 流行病学筛查过程可能要求每个相关人员接受快速血清学测试(须征得同意)。在阴性结果(IG-M和IG-G阴性)的情况下,可在预定时间间隔内(例如,15-20天)重复测试。如

果快速血清学测试结果呈阳性(IG-M和/或IG-G),则筛查过程可能涉及化学发光分析或ELISA。在化学发光测试或ELISA之后,筛查过程可包括执行分子测试以确认对测试的IG-M阳性和IG-G阳性或阴性的人的诊断。

[0030] 化学发光测试(ELISA)是针对人体抗体的半定量体外试验,为整合病原体的直接搜索提供了有力的证据。所需仪器包括经批准的专用工具以及对执行测试有用的辅助仪器。为了获得ELISA测试的结果,实验室可以包括基本的实验室仪器和耗材(校准移液管、尖端(tip)、计时器、培养箱和恒温槽、冰箱)以及用于读取结果的仪器(分光光度计)。

[0031] 健康站12还可以被配置成基于RT-PCR方法来执行分子测试,以扩增在SARS-CoV-2感染期间表达的病毒基因。在这种情况下,实验室还可以包括诸如离心机、镊子、用于核酸(DNA/RNA)样本质量分析和通过单荧光PCR对来自人体的病原体的基因进行分析的测试器之类的仪器。

[0032] 健康站12可被划分为专用区域:例如,用于取样的第一区域;用于收集样本(在其中样本是在公司场所外加工的情况下)的第二区域;最后,用于分析和最终检查的第三实验室区域。如果健康站12完全是内部的,则第一、第二和第三区域可以都位于公司场所上;替换地,包括实验室的第三区域可以位于公司外部的位置。

[0033] 有利的是,与现有技术相比,创建内部实验室将允许通过结构的集中化减少测试时间,实现高度创新,为整个生产链带来好处。与使用外部实验室相比,在长期来看,并考虑到要进行大量的测试以保持对雇员及其家属的监测,内部实验室在经济和财务方面也将是有利的。

[0034] 根据一方面,系统1可以要求同意处理所收集的数据,即处理和记录至少一个第一数据项D1和至少一个第二数据项D2,无论结果是阳性还是阴性。例如,可以通过使用经认证的数据存储库来进行存储。

[0035] 如上所述,系统1可以被细分为公司网络,以便能够监测多个用户。因此,每个公司可以例如在一个或多个本地数据存储库14中彼此独立地记录第一和第二数据项D1、D2,并且每个公司可以基于相同的区块链来将数据串D3记录在相同的分布式架构数据库18中,以确保所有数据都被正确和不被篡改地记录。

[0036] 有利的是,当相对大量的公司形成同一区块链的一部分时,例如,即使没有地方卫生当局(ASL)或其他公共当局的协作,健康监督系统1也可以变为防篡改或几乎防篡改的。

[0037] 根据一方面,至少一个数据存储库14可以硬连线或无线方式连接到控制单元16,并且可以配置成从其接收至少一个第一和/或第二数据项D1、D2。

[0038] 在一个或多个实施例中,该至少一个本地数据存储库14包括集中式数据存储库,该数据存储库受到保护并且可由控制单元16在授权的情况下访问。

[0039] 例如,第一数据项D1和第二数据项D2可以仅在例如输入密码之后通过控制单元16访问。这样,只有经过授权才能访问敏感数据。

[0040] 例如,第一和第二数据项D1、D2可仅对公共卫生和/或司法组织或公司医生可访问。

[0041] 另外或者可替换地,至少一个本地数据存储库16可以至少部分地由多个个人电子设备、优选个人智能手机来定义。例如,某个电子设备可以与每个用户相关联。这样,某个已识别的用户的至少一个第二数据项D2只能被保存到该用户的个人电子设备。换句话说,个

体用户的第二数据项D2可被保存到不同的个人设备(数据项的副本可以存在于集中的公司数据库中)。

[0042] 另外或者可替换地,在来自用户和/或来自控制单元16的请求之后,可以访问至少一个第二数据项D2。有利的是,用户甚至可以在公司的环境之外访问他们的个人数据,例如,如果他们被要求在其他情况下显示他们对病毒是阴性的,诸如在电影院、餐馆、体育场等。同时,控制单元16可以访问个人电子设备中存在的数据,以便公共卫生和/或司法机构可以在需要时获得每个用户的第一和第二数据项D1、D2。

[0043] 另外或者可替换地,至少一个第二数据项D2只能在来自控制单元16的命令之后被删除。有利地,这样,用户不能删除第二数据项D2。

[0044] 个人电子设备中的第二数据项D2可以由用户通过移动应用程序(以下称为“app”)来访问。

[0045] 对包含测试结果的app的使用可以具有一个或多个优点:例如,用户可以通过该app显示测试结果,以便证明在测试日期没有感染,从而允许公共商业机构在安全的环境中与其客户建立交互。

[0046] 这样,本地数据存储库14的至少一部分可以驻留在个人电子设备中。

[0047] 根据一方面,数据库18可以硬连线或无线方式连接到控制单元16,并且可以被配置为从其接收字符串D3。

[0048] 在一个或多个实施例中,分布式账本类型的分布式架构数据库18是区块链类型的,并且包括分组在通过密码算法互连的多个信息块中的信息。

[0049] 根据一方面,在某一地理区域中创建由不同公司共享的区块链可以具有一个或多个优点:例如,它允许认证由每个个体公司记录的第一和第二数据项D1、D2的不变性。例如,每个公司可以独立于其他公司在本地数据存储库14中记录数据D1、D2,同时可以记录表示同一区块链中的数据D1、D2的字符串D3,以确保所有数据都被正确且不可变地记录。

[0050] 有利的是,当足够多数量的不同公司在区块链上记录其数据时,将更容易保证防篡改系统。

[0051] 根据一方面,分布式账本类型的分布式架构数据库18可以在以太坊或以太坊经典或Iota或Eos或NEO或Waves或Qtum或NEM或Multiversum或R3 Corda或R3 Corda企业或Hyperledger(超级分类帐)或Ripple或Stellar平台上来定义或构建。

[0052] 根据一方面,分布式账本类型的分布式架构数据库18可以与用于写入数据库18的一致协议一起操作,并从以下类型中选择:

[0053] -工作证明;

[0054] -权益证明;

[0055] -Corda共识协议(被配置成就特定“状态对象”达成共识);

[0056] -CFT(崩溃容错),优选地用Kafka和/或Zookeeper实现;

[0057] -Solo;

[0058] -BFT(拜占庭容错);

[0059] -PBFT(实际BFT);

[0060] -SBFT(简化BFT);

[0061] -Raft;

[0062] -Sumeragi;

[0063] -PoET(消逝时间证明);

[0064] -基于许可制投票(Permissioned Voting-based)。

[0065] 如本文前面所述,数据库18可以由多个处理节点来定义。每个公司可与特定节点相关联,该特定节点是要检查并同意将字符串D3添加到分布式账本类型的分布式架构数据库18的第一个节点。

[0066] 根据一方面,处理节点可以包括第一组处理器,其被配置为保持分布式架构数据库18的完整副本,以及第二组处理器,其被配置为保持分布式架构数据库18的部分副本。以此方式,有利地,第二组的处理节点可以比第一组的那些处理节点更简单并且集成减少的容量存储器。

[0067] 优选地,每个字符串D3具有与其相关联的时间戳。优选地,字符串D3可以通过密码算法彼此互连。

[0068] 在一个或多个实施例中,控制单元16因此被配置成在至少一个本地数据存储库14中记录、检索和/或删除第一和第二数据项D1、D2。同时,控制单元16被配置成将指示第一和/或第二数据项D1、D2的字符串D3保存到数据库18。

[0069] 字符串D3可以指示数据项D1、D2,但同时它可以保护用户的隐私,因为数据项D1、D2以未加密的形式不可见。换句话说,字符串D3可以加密地计算。

[0070] 使用加密函数计算字符串的步骤可以包括使用加密哈希函数(例如,使用安全哈希算法SHA-256)计算字符串D3。

[0071] 在一个或多个实施例中:

[0072] -所计算的字符串D3与从中计算字符串D3的至少一个第一数据项D1和/或至少一个第二数据项D2具有一对一匹配,和/或

[0073] -不能从字符串D3获得至少一个第一和/或第二数据项D1、D2。

[0074] 这样,测试结果(即,未加密的第二健康数据项D2)可被保存在本地数据存储库14中,其中数据存储库14的可访问性经受授权。相反,指示至少从中计算它们的第二数据项D2的字符串D3可由能够访问数据库18的任何人自由地访问,以便允许数据被认证。实际上,所提供的数据的真实性通过这些结果的安全哈希已被保存在区块链中的事实来保证。

[0075] 在一个或多个实施例中,控制单元16被配置成用于:

[0076] -将时间戳与至少一个第一数据项D1和/或至少一个第二数据项D2相关联,以及

[0077] -如果时间戳指示数据是在某个日期之前被存储的(例如,如果数据是在六个月前的日期当天或之前存储的),则自动删除例如存储在至少一个本地数据存储库14中的多个第一数据项D1和/或第二数据项D2之间的数据。

[0078] 有利的是,这允许根据意大利和欧洲法规以及数据保护局的建议,保护经受健康监督的用户的隐私和被遗忘的权利。实际上,所记录的数据不以未加密的形式发布在数据库18中,并且可以在预定的时间间隔之后被删除,该预定时间间隔例如是与权威机构协商建立的。在该时间段结束时,系统1自动移除过时的数据。

[0079] 在一个或多个实施例中,如果至少一个第二数据项D2指示存在SARS-CoV-2病毒抗原,也就是说,如果用户可能是严重急性呼吸综合征冠状病毒2的携带者或者可能表现出Covid-19的症状,则控制单元16可被配置为传送警报信号。

[0080] 根据一方面，该警报可被显示在已经对病毒测试为阳性的用户的个人电子设备上；另外或可替换地，可以将警报传送给公司官员，例如医生，以允许开始控制感染传播的程序。

[0081] 一个或多个实施例涉及健康监督方法，包括以下步骤：

[0082] -提供根据一个或多个实施例的健康监督系统1，

[0083] -通过识别站10获得指示用户的身份的至少一个第一数据项D1，

[0084] -通过健康站12获得指示所识别的用户的健康状况的至少一个第二数据项D2，

[0085] -通过标识站10和健康站12一起接收至少一个第一数据项D1和至少一个第二数据项D2，

[0086] -使用加密函数作为至少一个第一数据项D1和/或至少一个第二数据项D2的函数来计算字符串D3，

[0087] -将至少一个第一数据项D1和/或至少一个第二数据项D2存储在至少一个本地数据存储库14中，以及

[0088] -将字符串D3传送给分布式账本类型的分布式架构数据库18，以将字符串D3写入分布式架构数据库18。

[0089] 根据一方面，该监督方法可包括将字符串D3写入数据库18。

[0090] 根据另一方面，该方法可以包括以下步骤：

[0091] -识别用户；

[0092] -读取分布式架构数据库18和本地数据存储库14以检索与该用户相关联的信息；

[0093] -如果分布式架构数据库18与本地数据存储库14的结合的读取结果给出与用户相关联的异常健康状况，则发出警报信号。

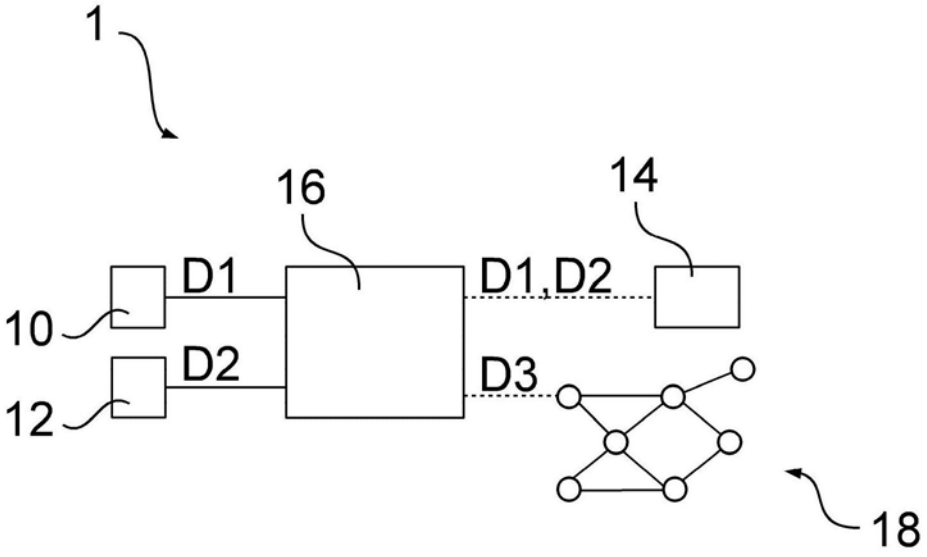


图1