(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 111190974 B
(45)授权公告日 2021.01.26

(21)申请号 202010277163.X
(22)申请日 2020.04.10
(65)同一申请的已公布的文献号
申请公布号 CN 111190974 A
(43)申请公布日 2020.05.22
(73)专利权人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路556号8层B段801-11
(72)发明人 杨仁慧
(74)专利代理机构 北京晋德允升知识产权代理有限公司 11623
代理人 王戈
(51)Int.Cl.
G06F 16/28(2019.01)
G06Q 20/38(2012.01)

(56)对比文件
WO 2019143582 A1,2019.07.25

审查员 赵阳

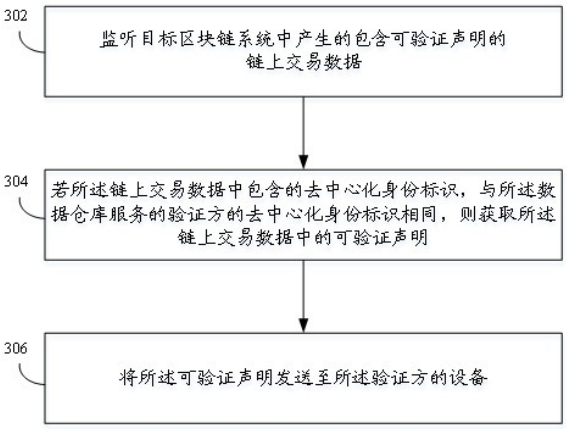
权利要求书4页 说明书12页 附图5页

(54)发明名称

可验证声明的转发、获取方法、装置及设备

(57)摘要

本说明书实施例公开了可验证声明的转发、获取方法、装置及设备。方案包括:验证方对接的数据仓库从区块链系统中的链上交易数据中获取待验证的可验证声明,然后将该可验证声明发送至验证方的设备。



CN 111190974 B

1.一种可验证声明的转发方法,包括:

数据仓库监听目标区块链系统中产生的包含可验证声明的链上交易数据;所述目标区块链系统为与所述数据仓库连接的区块链系统;

若所述链上交易数据中包含的去中心化身份标识,与所述数据仓库服务的验证方的去中心化身份标识相同,则获取所述链上交易数据中的可验证声明;所述链上交易数据的标的物为所述可验证声明;所述链上交易数据的目的地址为所述链上交易数据中包含的去中心化身份标识;

将所述可验证声明发送至所述验证方的设备。

2.根据权利要求1所述的方法,所述获取所述链上交易数据中的可验证声明,具体包括:

从所述链上交易数据中获取加密的可验证声明;

所述将所述可验证声明发送至所述验证方的设备,具体包括:

将所述加密的可验证声明发给所述验证方的设备。

3.根据权利要求1所述的方法,所述获取所述链上交易数据中的可验证声明,具体包括:

从所述链上交易数据中获取加密的可验证声明;

从所述链上交易数据中获取授权密钥;

采用所述验证方的私钥对所述授权密钥进行解密,得到对称密钥;

采用所述对称密钥对所述加密的可验证声明进行解密,得到所述可验证声明。

4.根据权利要求1所述的方法,所述获取所述链上交易数据中的可验证声明,具体包括:

从所述链上交易数据中获取加密的可验证声明;

从所述链上交易数据中获取授权密钥;

向去中心化身份标识服务器发送所述授权密钥;

获取所述去中心化身份标识服务器对所述授权密钥进行解密得到的对称密钥;

采用所述对称密钥对所述加密的可验证声明进行解密,得到所述可验证声明。

5.根据权利要求1至4任一项所述的方法,所述获取所述链上交易数据中的可验证声明之后,还包括:

将所述可验证声明保存在所述数据仓库连接的数据库中;

所述将所述可验证声明发送至所述验证方的设备之前,还包括:

获取所述验证方发送的验证请求;所述验证请求中至少包含所述可验证声明的标识;

所述将所述可验证声明发送至所述验证方的设备,具体包括:

根据所述标识,从所述数据库中查找所述可验证声明;

将查找到的所述可验证声明发送至所述验证方的设备。

6.根据权利要求5所述的方法,所述获取所述验证方发送的验证请求之后,还包括:

获取所述可验证声明的验证方的去中心化身份标识;

根据所述去中心化身份标识,判断所述验证方是否具有所述数据仓库的使用权限;

所述根据所述标识,从所述数据库中查找所述可验证声明,具体包括:

当所述验证方具有所述数据仓库的使用权限,则根据所述标识,从所述数据库中查找

所述可验证声明。

7.一种可验证声明的获取方法,包括

可验证声明的验证方获取所述可验证声明的持有方发送的第一验证请求;所述第一验证请求中至少包含所述可验证声明的标识;

向数据仓库发送获取所述可验证声明的第二验证请求;所述第二验证请求中包含所述标识;

获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明;所述基于所述第二验证请求反馈的所述可验证声明是所述数据仓库根据所述第二验证请求包含的所述标识从与所述数据仓库连接的数据库中查找到的可验证声明;

其中,所述可验证声明是所述数据仓库从目标区块链系统中的链上交易数据中获取的;所述目标区块链系统为与所述数据仓库连接的区块链系统;所述链上交易数据的标的物为所述可验证声明;所述链上交易数据的目的地址为所述验证方的去中心化身份标识。

8.根据权利要求7所述的方法,所述第二验证请求中还包括所述验证方的去中心化身份标识。

9.一种可验证声明的转发装置,所述装置应用于数据仓库,所述装置包括:

监听模块,用于监听目标区块链系统中产生的包含可验证声明的链上交易数据;所述目标区块链系统为与所述数据仓库连接的区块链系统;

可验证声明获取模块,用于若所述链上交易数据中包含的去中心化身份标识,与所述数据仓库服务的验证方的去中心化身份标识相同,则获取所述链上交易数据中的可验证声明;所述链上交易数据的标的物为所述可验证声明;所述链上交易数据的目的地址为所述链上交易数据中包含的去中心化身份标识;

可验证声明发送模块,用于将所述可验证声明发送至所述验证方的设备。

10.根据权利要求9所述的装置,所述可验证声明获取模块,具体包括:

第一可验证声明获取单元,用于从所述链上交易数据中获取加密的可验证声明;

所述可验证声明发送模块,具体包括:

第一可验证声明发送单元,用于将所述加密的可验证声明发给所述验证方的设备。

11.根据权利要求9所述的装置,所述可验证声明获取模块,具体包括:

第二可验证声明获取单元,用于从所述链上交易数据中获取加密的可验证声明;

第一授权密钥获取单元,用于从所述链上交易数据中获取授权密钥;

第一解密单元,用于采用所述验证方的私钥对所述授权密钥进行解密,得到对称密钥;

第二解密单元,用于采用所述对称密钥对所述加密的可验证声明进行解密,得到所述可验证声明。

12.根据权利要求9所述的装置,所述可验证声明获取模块,具体包括:

第三可验证声明获取单元,用于从所述链上交易数据中获取加密的可验证声明;

第二授权密钥获取单元,用于从所述链上交易数据中获取授权密钥;

授权密钥发送单元,用于向去中心化身份标识服务器发送所述授权密钥;

对称密钥获取单元,用于获取所述去中心化身份标识服务器对所述授权密钥进行解密得到的对称密钥;

第三解密单元,用于采用所述对称密钥对所述加密的可验证声明进行解密,得到所述

可验证声明。

13.根据权利要求9至12任一项所述的装置,还包括:

可验证声明保存模块,用于在获取所述链上交易数据中的可验证声明之后,将所述可验证声明保存在所述数据仓库连接的数据库中;

验证请求获取模块,用于在将所述可验证声明发送至所述验证方的设备之前,获取所述验证方发送的验证请求;所述验证请求中至少包含所述可验证声明的标识;

所述可验证声明发送模块,具体包括:

可验证声明查找单元,用于根据所述标识,从所述数据库中查找所述可验证声明;

第二可验证声明发送单元,用于将查找到的所述可验证声明发送至所述验证方的设备。

14.根据权利要求13所述的装置,还包括:

去中心化身份标识获取模块,用于在获取所述验证方发送的验证请求之后,获取所述可验证声明的验证方的去中心化身份标识;

判断模块,用于根据所述去中心化身份标识,判断所述验证方是否具有所述数据仓库的使用权限;

所述可验证声明查找单元,具体包括:

可验证声明查找子单元,用于当所述验证方具有所述数据仓库的使用权限,则根据所述标识,从所述数据库中查找所述可验证声明。

15.一种可验证声明的获取装置,所述装置应用于可验证声明的验证方,所述装置包括:

第一验证请求获取模块,用于获取所述可验证声明的持有方发送的第一验证请求;所述第一验证请求中至少包含所述可验证声明的标识;

第二验证请求发送模块,用于向数据仓库发送获取所述可验证声明的第二验证请求;所述第二验证请求中包含所述标识;

可验证声明获取模块,用于获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明;所述基于所述第二验证请求反馈的所述可验证声明是所述数据仓库根据所述第二验证请求包含的所述标识从与所述数据仓库连接的数据库中查找到的可验证声明;

其中,所述可验证声明是所述数据仓库从目标区块链系统中的链上交易数据中获取的;所述目标区块链系统为与所述数据仓库连接的区块链系统;所述链上交易数据的标的物为所述可验证声明;所述链上交易数据的目的地址为所述验证方的去中心化身份标识。

16.根据权利要求15所述的装置,所述第二验证请求中还包括所述验证方的去中心化身份标识。

17.一种可验证声明的转发设备,包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:

监听目标区块链系统中产生的包含可验证声明的链上交易数据;所述目标区块链系统为与数据仓库连接的区块链系统;

若所述链上交易数据中包含的去中心化身份标识，与数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明；所述链上交易数据的标的物为所述可验证声明；所述链上交易数据的目的地址为所述链上交易数据中包含的去中心化身份标识；

将所述可验证声明发送至所述验证方的设备。

18.一种可验证声明的获取设备，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

获取所述可验证声明的持有方发送的第一验证请求；所述第一验证请求中至少包含所述可验证声明的标识；

向数据仓库发送获取所述可验证声明的第二验证请求；所述第二验证请求中包含所述标识；

获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明；所述基于所述第二验证请求反馈的所述可验证声明是所述数据仓库根据所述第二验证请求包含的所述标识从与所述数据仓库连接的数据库中查找到的可验证声明；

其中，所述可验证声明是所述数据仓库从目标区块链系统中的链上交易数据中获取的；所述目标区块链系统为与所述数据仓库连接的区块链系统；所述链上交易数据的标的物为所述可验证声明；所述链上交易数据的目的地址为验证方的去中心化身份标识。

可验证声明的转发、获取方法、装置及设备

技术领域

[0001] 本申请涉及计算机技术领域，尤其涉及可验证声明的转发、获取方法、装置及设备。

背景技术

[0002] 去中心化身份标识(Decentralized IDentifier,DID)是一种新类型的标识符，具有全局唯一性、高可用性、可解析性和加密可验证性。

[0003] DID技术投入使用后，一个DID可以对应于多个可验证声明(Verifiable Claim，VC)。当VC的数量过多，就产生了对于VC进行存储与管理的需求。于是，VC数据仓库应运而生。该数据仓库可以对于用户的VC进行存储与管理。

[0004] 实际应用中，数据仓库的用户希望对于VC的使用过程进行记录，以便后续对于VC的使用过程进行统计分析。但是，VC数据仓库并不具备这一功能。

[0005] 因此，如何使VC数据仓库中的VC的使用过程可被追溯，成为一个重要的技术问题。

[0006] 发明人经研究发现，可以利用区块链系统对VC进行传输，从而使得VC的使用过程可被追溯。但是，当VC上传到区块链系统后，如何使得VC的验证方获取到区块链系统上的VC，又成为亟待解决的技术问题。

发明内容

[0007] 有鉴于此，本申请实施例提供了可验证声明的转发、获取方法、装置及设备，用于使得VC的验证方获取到区块链系统上的VC。

[0008] 为解决上述技术问题，本说明书实施例是这样实现的：

[0009] 本说明书实施例提供的一种可验证声明的转发方法，包括：

[0010] 数据仓库监听目标区块链系统中产生的包含可验证声明的链上交易数据；

[0011] 若所述链上交易数据中包含的去中心化身份标识，与所述数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明；

[0012] 将所述可验证声明发送至所述验证方的设备。

[0013] 本说明书实施例提供的一种可验证声明的获取方法，包括

[0014] 可验证声明的验证方获取所述可验证声明的持有方发送的第一验证请求；所述第一验证请求中至少包含所述可验证声明的标识；

[0015] 向数据仓库发送获取所述可验证声明的第二验证请求；所述第二验证请求中包含所述标识；

[0016] 获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明；

[0017] 其中，所述可验证声明是所述数据仓库从目标区块链系统中获取的。

[0018] 本说明书实施例提供的一种可验证声明的转发装置，所述装置应用于数据仓库，所述装置包括：

[0019] 监听模块，用于监听目标区块链系统中产生的包含可验证声明的链上交易数据；

[0020] 可验证声明获取模块，用于若所述链上交易数据中包含的去中心化身份标识，与所述数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明；

[0021] 可验证声明发送模块，用于将所述可验证声明发送至所述验证方的设备。

[0022] 本说明书实施例提供的一种可验证声明的获取装置，所述装置应用于可验证声明的验证方，所述装置包括：

[0023] 第一验证请求获取模块，用于获取所述可验证声明的持有方发送的第一验证请求；所述第一验证请求中至少包含所述可验证声明的标识；

[0024] 第二验证请求发送模块，用于向数据仓库发送获取所述可验证声明的第二验证请求；所述第二验证请求中包含所述标识；

[0025] 可验证声明获取模块，用于获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明；

[0026] 其中，所述可验证声明是所述数据仓库从目标区块链系统中获取的。

[0027] 本说明书实施例提供的一种可验证声明的转发设备，包括：

[0028] 至少一个处理器；以及，

[0029] 与所述至少一个处理器通信连接的存储器；其中，

[0030] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

[0031] 监听目标区块链系统中产生的包含可验证声明的链上交易数据；

[0032] 若所述链上交易数据中包含的去中心化身份标识，与所述数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明；

[0033] 将所述可验证声明发送至所述验证方的设备。

[0034] 本说明书实施例提供的一种可验证声明的获取设备，包括：

[0035] 至少一个处理器；以及，

[0036] 与所述至少一个处理器通信连接的存储器；其中，

[0037] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

[0038] 获取所述可验证声明的持有方发送的第一验证请求；所述第一验证请求中至少包含所述可验证声明的标识；

[0039] 向数据仓库发送获取所述可验证声明的第二验证请求；所述第二验证请求中包含所述标识；

[0040] 获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明；

[0041] 其中，所述可验证声明是所述数据仓库从目标区块链系统中获取的。

[0042] 本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果：

[0043] 一方面，数据仓库从区块链上获取待验证的VC，然后发送至验证方，由于通过区块链将可验证声明由持有方设备发送至验证方设备，可以使得可验证声明的传输过程被区块链系统记录，可被追溯。

[0044] 另一方面，上述方案，对于数据仓库如何向验证方传输待验证VC，验证方如何从数据仓库获取待验证VC，均提供了具体实现流程，可以作为标准流程进行参考使用。

附图说明

[0045] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0046] 图1为本说明书实施例中的方法的应用背景的示意图；

[0047] 图2为本说明书实施例提供的一种可验证声明的传输系统的架构示意图；

[0048] 图3为本说明书实施例提供的一种可验证声明的转发方法的流程示意图；

[0049] 图4为本说明书实施例提供的链上交易数据的字段结构示意图；

[0050] 图5为本说明书实施例提供的另一种可验证声明的转发方法的流程示意图；

[0051] 图6为本说明书实施例提供的一种可验证声明的获取方法的流程示意图；

[0052] 图7为本说明书实施例提供的对应于图3的一种可验证声明的转发装置的结构示意图；

[0053] 图8为本说明书实施例提供的对应于图6的一种可验证声明的获取装置的结构示意图；

[0054] 图9为本说明书实施例提供的对应于图3的可验证声明的转发设备以及对应于图6的可验证声明的获取设备的结构示意图。

具体实施方式

[0055] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0056] 以下结合附图，详细说明本申请各实施例提供的技术方案。

[0057] 图1为本说明书实施例中的方法的应用背景的示意图。如图1所示，客户端101可以是手机等移动终端，也可以是台式电脑等设备。客户端上登录有用户的账号，每个账号可以对应的具有一个去中心化身份标识(DID)102。实际应用中：一个DID可以对应于一个个人用户，或者一个设备，或者对应于一个商家，或者对应于一个公司等等。

[0058] 可验证声明(VC)可以理解为对于一个DID所标识的身份是否具有某种资质的声明。具体到数据层面，VC可以是记录这种声明的数据。

[0059] 一个DID可以具有多个可验证声明103。比如：对于用户A使用的一个DID来说，这个DID可以包含用于证明用户A年满18周岁的VC1，用于证明用户A的财产大于100万的VC2，用于证明用户A具有机动车辆驾驶资格的VC3等等。实际应用中，用户A也即一个DID对应的VC可以有很多(n个)。此时，众多的VC需要进行统一存储和管理，因此，可以采用数据仓库104来存储DID对应的可验证声明103。

[0060] 用于存储VC的数据仓库，简称VC Repo。需要说明的是，VC Repo是一个逻辑概念，具体可以是一个应用或一段程序。VC Repo可以部署在各种类型的硬件设备上。VC Repo在对VC进行存储时，可以将VC存储在VC Repo具有使用权限的数据库。

[0061] 图2为本说明书实施例提供的一种可验证声明的传输系统的架构示意图。本说明书实施例提供的可验证声明的发送方法和获取方法，可以基于该系统运行。如图2所示，200为用户终端(也是可验证声明的传输请求的发送设备)，201为第一数据仓库，202为第二数

据仓库，203为第一数据仓库可操作的数据库，204为可验证声明的验证方的服务器。11为第一区块链节点，12为第二区块链节点，13为第三区块链节点，区块链节点11、12和13属于第一区块链系统。21为第四区块链节点，22为第五区块链节点，23为第六区块链节点，区块链节点21、22和23属于第二区块链系统。31为第七区块链节点，32为第八区块链节点，33为第九区块链节点，区块链节点31、32和33属于第三区块链系统。需要说明的是，图2只是示意图，实际应用中，数据仓库可以连接的区块链系统的个数可以更多，一个区块链系统中的节点数目也可以更多。还需要说明的是，在某些情况下，第一数据仓库201与第二数据仓库202在物理空间上，可以位于同一地点，或部署在同一设备。但是从软件功能的角度，还是可以被划分为两个功能模块，一个为第一数据仓库201，另一个为第二数据仓库202，两个数据仓库分别对应VC的持有方和验证方。当有VC需要从第一数据仓库201传输至第二数据仓库202时，VC仍然会被第一数据仓库201通过区块链系统发送至第二数据仓库202。

[0062] 本说明书实施例中，对于可验证声明的传输，作用之一是将可验证声明发送至验证方的服务器204进行验证。最初将可验证声明发送至第一数据仓库的，可以是可验证声明的持有方的设备。所述持有方的设备登录有持有方的账户(可以是DID)。所述持有方需要将VC发送至验证方的设备进行验证。持有方也是第一数据仓库的用户，需要验证的VC，预先可以存储在第一数据仓库。当持有方发起将VC发送至验证方进行验证的请求后，第一数据仓库接收到该请求，可以将对应的VC上传至一个区块链系统，对应的VC存储在该区块链系统的链上交易数据中。上传到区块链系统后，第二数据仓库需要从该区块链系统上获取对应的VC，并将该VC发送至验证方的设备。

[0063] 图3为本说明书实施例提供的一种可验证声明的转发方法的流程示意图。从程序角度而言，流程的执行主体可以为搭载于应用服务器的程序或应用客户端。具体的，可以是图2中的第二数据仓库。如图3所示，该方法可以包括以下步骤：

[0064] 步骤302：监听目标区块链系统中产生的包含可验证声明的链上交易数据；

[0065] 步骤304：若所述链上交易数据中包含的去中心化身份标识，与所述数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明；

[0066] 步骤306：将所述可验证声明发送至所述验证方的设备；

[0067] 其中，所述数据仓库在所述目标区块链系统中可以具有账户。所述数据仓库通过所述账户登录区块链系统后，可以获取区块链系统中的数据。或者，所述数据仓库不具有账户，可以通过具有账户的第三方平台获取区块链系统中的数据。本说明书实施例中对此不作限定。

[0068] 步骤302中，数据仓库可以监听自身连接的所有区块链系统中的部分或全部区块链系统。VC的验证方具有对应的DID。链上交易数据中，可以包含该DID。VC的验证方，可以是该数据仓库的用户。数据仓库需要为该用户提供服务。该数据仓库可以对于属于自身的用户的全部验证方的待验证VC进行监听。该数据仓库也可以不对属于自身的用户的全部验证方的待验证VC进行监听，而是对于目标区块链系统中的所有新生成的链上交易数据全部进行获取，获取到该数据仓库本地后，再分析该新生成的链上交易数据中包含的待验证VC是否是需要发送至该数据仓库所管理的用户的。两种方式相对而言，采用监听的方式，可以减少数据仓库对于不必进行转发处理的链上交易数据的获取，减轻数据仓库的压力，提高数据仓库的效率。所述可验证声明，可以以标的物的形式包含在所述链上交易数据中。所述链

上交易数据中，还可以在授权列表中(可以参照图4中的AuthList)，添加验证方的DID等标识，用于表示该链上交易数据中包含的VC是需要哪个验证方进行验证的。具体在进行监听时，可以主要监听授权列表中的信息，当监听到授权列表中包含该数据仓库自身的用户的DID时，再对完整的链上交易数据进行获取。

[0069] 上述步骤中，由第二数据仓库主动监听区块链系统中的链上交易数据的生成情况。当监听到包含第二数据仓库所负责的验证方的DID的链上交易数据后，第二数据仓库主动获取链上交易数据，从中读取作为标的物的VC，然后将VC发送至验证方的设备，概括的说，相当于一种主动将待验证的VC推送给验证方的设备的方法。采用这种方法，一方面可以简化验证方的设备的操作，验证方的设备只需要与第二数据仓库之间进行交互，就可以获取到待验证的VC，从而对VC进行验证；另一方面，由于是通过区块链将可验证声明由持有方设备发送至验证方设备的，可以使得可验证声明的传输过程被区块链系统记录，可被追溯。

[0070] 实际应用中，步骤302中，对于区块链系统中新产生的链上交易数据的监听方式，具体可以是：数据仓库按照设定时间点，扫描区块链系统中的区块头部数据。该区块头部数据中可以包含新产生的链上交易数据所在的区块高度，以及该链上交易数据的目的地址。其中，当扫描得到的区块高度发生改变，则数据仓库可以确定有新的链上交易数据产生。区块头部数据中的目的地址，可以采用验证方的DID进行表示。数据仓库可以通过判断目的地址中是否包含该数据仓库负责管理的验证方的DID，如果在目的地址中检测到该数据仓库负责管理的验证方的DID，则执行步骤304，从区块链系统中拉取所述链上交易数据上链，获取所述链上交易数据中的可验证声明。

[0071] 实际应用中，由于VC中存储的信息通常是用户的隐私信息，为了提高对于用户的隐私的保护，可以采用以下方式。

[0072] 所述获取所述链上交易数据中的可验证声明，具体可以包括：

[0073] 从所述链上交易数据中获取加密的可验证声明；

[0074] 所述将所述可验证声明发送至所述验证方，具体可以包括：

[0075] 将所述加密的可验证声明发给所述验证方。

[0076] 上述方式中，链上交易数据中的VC是经过加密后的VC，不是VC原文。即使区块链上的数据具有公开透明的特性，第三方获取到链上交易数据后，也无法得到VC原文，可以提高对于用户的隐私的保护程度。

[0077] 实际应用中，为了可以进一步提高对于VC的隐私保护程度，可以先采用对称密钥对可验证声明进行加密，再采用验证方的公钥对该对称密钥进行加密，加密后的对称密钥可以称为授权密钥。将授权密钥添加至链上交易数据中，再将链上交易数据上传至目标区块链系统。

[0078] 相应的，采用上述方式对可验证声明进行加密后，步骤304：获取所述链上交易数据中的可验证声明，具体可以采用以下方式：

[0079] 从所述链上交易数据中获取加密的可验证声明；

[0080] 从所述链上交易数据中获取授权密钥；

[0081] 采用所述验证方的私钥对所述授权密钥进行解密，得到对称密钥；

[0082] 采用所述对称密钥对所述加密的可验证声明进行解密，得到所述可验证声明。

[0083] 图4为本说明书实施例提供的链上交易数据的字段结构示意图。需要说明的是，图

4只是示意图，图4中所示出的字段，可以包含在链上交易数据中，但对于这些字段在链上交易数据中的位置，并不进行限定。如图4所示，第一部分字段内，可以是采用高级加密标准(Advanced Encryption Standard，AES)进行加密的VC原文(VC Content)。可以采用对称密钥对VC原文进行加密。第二部分字段内，可以是采用验证方B的公钥对上述对称密钥进行加密后得到的授权密钥。第三部分字段，可以是授权列表。授权列表中可以包含验证方的DID。授权列表中包含的标识，可以用于表示该链上交易数据中包含的VC需要发送至的目标验证方。

[0084] 验证方这一侧的数据仓库，可以获得验证方的私钥的使用权限。该数据仓库在获取到与图4所示字段结构相同或相似的链上交易数据后，可以先从链上交易数据中获取第二部分字段内的授权密钥，然后采用验证方的私钥对授权密钥进行解密。解密后，可以得到对称密钥，再用对称密钥对加密的VC进行解密，就可以得到VC原文。

[0085] 采用上述方式，对于VC原文的解密过程，全部交由数据仓库执行，无需验证方设备进行解密，可以减轻验证方设备的负担。

[0086] 实际应用中，也可以将验证方的私钥委托给用于提供去中心化身份标识服务(DID Service)的去中心化身份标识服务器使用。此时，验证方一侧的数据仓库，不再具有验证方的私钥的使用权限。该数据仓库可以采用以下方式从链上交易数据中获取VC原文：

[0087] 从所述链上交易数据中获取加密的可验证声明；

[0088] 从所述链上交易数据中获取授权密钥；

[0089] 向去中心化身份标识服务器发送所述授权密钥；

[0090] 获取所述去中心化身份标识服务器对所述授权密钥进行解密得到的对称密钥；

[0091] 采用所述对称密钥对所述加密的可验证声明进行解密，得到所述可验证声明。

[0092] 上述方式中，向去中心化身份标识服务器发送所述授权密钥后，所述去中心化身份标识服务器可以采用验证方的私钥对所述授权密钥进行解密，得到对称密钥，然后将对称密钥发送至验证方的数据仓库。

[0093] 图5为本说明书实施例提供的另一种可验证声明的转发方法的流程示意图。从程序角度而言，流程的执行主体可以为搭载于应用服务器的程序或应用客户端。具体的，可以是图2中的第二数据仓库。如图5所示，该方法可以包括以下步骤：

[0094] 步骤502：监听目标区块链系统中产生的包含可验证声明的链上交易数据；

[0095] 步骤504：若所述链上交易数据中包含的去中心化身份标识，与所述数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明；

[0096] 具体可以采用前述的各种方式，从目标区块链系统中获取所述链上交易数据中的可验证声明。

[0097] 步骤506：将所述可验证声明保存在所述数据仓库连接的数据库中；

[0098] 图5所示的方法中，验证方具有使用权限的数据仓库，在获取到所述可验证声明后，可以不必立即发送至验证方的设备，而可以将所述可验证声明先存储在该数据仓库连接的数据库中。等到该数据仓库获取到验证方的设备向该数据仓库发送的验证请求(该验证请求用于请求获取该可验证声明进行验证)后，再将该可验证声明发送至该验证方的设备。

[0099] 步骤508：获取所述验证方发送的验证请求；所述验证请求中至少包含所述可验证

声明的标识；

[0100] 所述验证方可以通过登录有验证方的账户的设备发送该验证请求。所述验证方在发送该验证请求之前，可以先被所述可验证声明的持有方发送的验证请求触发。即，所述可验证声明的持有方可以通过登录有持有方的账户的设备先向验证方的设备发送第一验证请求。该第一验证请求，可以用于告知验证方设备有待验证的VC，等待验证方进行验证。验证方设备在接收到第一验证请求后，可以向数据仓库发送第二验证请求(即步骤508中的验证请求)。

[0101] 所述可验证声明的标识，可以表示为Vcid，用于表明等待验证的VC。

[0102] 步骤510：根据所述标识，从所述数据库中查找所述可验证声明；

[0103] 步骤512：将查找到的所述可验证声明发送至所述验证方的设备。

[0104] 图5所示的方法，数据仓库不必主动向验证方设备发送该可验证声明，因此，验证方设备相应的可以不必设计用于接收数据仓库发送的可验证声明的接口，可以简化对于验证方设备的改动。另一方面，在某些场景下，持有方设备可能会发送多个等待验证的VC，但是这些待验证的VC的验证顺序是有一定规则的。通常，如果某个VC没有验证通过，就不必验证剩余的VC。例如，某个用户希望访问某个网站。该网站要求访问的用户需要年满25周岁，资产大于30万，未婚。这三个条件可以对应三个VC。访问网站的用户可以一次性将自身的与年龄，资产，婚姻状况相关的三个VC一起上传。但验证方可以按照先年龄，再资产，最后婚姻状况的顺序，对三个VC依次进行验证。这种情况下，采用图5的方法，验证方可以不必一次获取三个VC进行验证，而可以按照顺序，逐一从数据仓库获取待验证的VC。一旦发现某一个VC没有通过验证，就无需获取另外的VC。这可以进一步减轻验证方的负担。

[0105] 实际应用中，为了确保发送验证请求的验证方是该数据仓库的用户，具有该数据仓库的使用权限，步骤508获取所述验证方发送的验证请求之后，还可以包括以下步骤：

[0106] 获取所述可验证声明的验证方的去中心化身份标识；

[0107] 根据所述去中心化身份标识，判断所述验证方是否具有所述数据仓库的使用权限；

[0108] 当所述验证方具有所述数据仓库的使用权限，再执行步骤510根据所述标识，从所述数据库中查找所述可验证声明。

[0109] 图6为本说明书实施例提供的一种可验证声明的获取方法的流程示意图。从程序角度而言，流程的执行主体可以为搭载于应用服务器的程序或应用客户端。具体的，可以为搭载于可验证声明的验证方设备上的程序或应用。如图6所示，该方法可以包括以下步骤：

[0110] 步骤602：可验证声明的验证方获取所述可验证声明的持有方发送的第一验证请求；所述第一验证请求中至少包含所述可验证声明的标识；

[0111] 需要说明的是，本步骤中，从硬件角度而言，可验证声明的验证方可以是指验证方所登录或使用的设备。所述第一验证请求，是用于请求验证方对所述可验证声明进行验证的请求。

[0112] 所述可验证声明的标识，可以表示为Vcid，用于表明等待验证的VC。

[0113] 步骤604：向数据仓库发送获取所述可验证声明的第二验证请求；所述第二验证请求中包含所述标识；

[0114] 步骤606：获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明；

[0115] 数据仓库在接收到所述可验证声明后，可以按照图5中的方法，根据该标识，从数据库中查找所述可验证声明。将查找到的VC反馈至验证方。

[0116] 其中，所述可验证声明是所述数据仓库从目标区块链系统中获取的。

[0117] 图6中的方法是与图5的方法相对应的，可以带来与图5的方法相同的技术效果，在此不再赘述。

[0118] 基于同样的思路，本说明书实施例还提供了上述方法对应的装置。图7为本说明书实施例提供的对应于图3的一种可验证声明的转发装置的结构示意图。该装置可以应用于数据仓库。如图7所示，该装置可以包括：

[0119] 监听模块701，用于监听目标区块链系统中产生的包含可验证声明的链上交易数据；

[0120] 可验证声明获取模块702，用于若所述链上交易数据中包含的去中心化身份标识，与所述数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明；

[0121] 可验证声明发送模块703，用于将所述可验证声明发送至所述验证方的设备。

[0122] 其中，所述数据仓库在所述目标区块链系统中可以具有账户。

[0123] 实际应用中，所述可验证声明获取模块702，具体可以包括：

[0124] 第一可验证声明获取单元，用于从所述链上交易数据中获取加密的可验证声明；

[0125] 所述可验证声明发送模块703，具体可以包括：

[0126] 第一可验证声明发送单元，用于将所述加密的可验证声明发给所述验证方的设备。

[0127] 实际应用中，所述可验证声明获取模块702，具体可以包括：

[0128] 第二可验证声明获取单元，用于从所述链上交易数据中获取加密的可验证声明；

[0129] 第一授权密钥获取单元，用于从所述链上交易数据中获取授权密钥；

[0130] 第一解密单元，用于采用所述验证方的私钥对所述授权密钥进行解密，得到对称密钥；

[0131] 第二解密单元，用于采用所述对称密钥对所述加密的可验证声明进行解密，得到所述可验证声明。

[0132] 实际应用中，所述可验证声明获取模块702，具体可以包括：

[0133] 第三可验证声明获取单元，用于从所述链上交易数据中获取加密的可验证声明；

[0134] 第二授权密钥获取单元，用于从所述链上交易数据中获取授权密钥；

[0135] 授权密钥发送单元，用于向去中心化身份标识服务器发送所述授权密钥；

[0136] 对称密钥获取单元，用于获取所述去中心化身份标识服务器对所述授权密钥进行解密得到的对称密钥；

[0137] 第三解密单元，用于采用所述对称密钥对所述加密的可验证声明进行解密，得到所述可验证声明。

[0138] 实际应用中，上述装置，还可以包括：

[0139] 可验证声明保存模块，用于在获取所述链上交易数据中的可验证声明之后，将所述可验证声明保存在所述数据仓库连接的数据库中；

[0140] 验证请求获取模块，用于在将所述可验证声明发送至所述验证方的设备之前，获

取所述验证方发送的验证请求;所述验证请求中至少包含所述可验证声明的标识;

[0141] 所述可验证声明发送模块703,具体可以包括:

[0142] 可验证声明查找单元,用于根据所述标识,从所述数据库中查找所述可验证声明;

[0143] 第二可验证声明发送单元,用于将查找到的所述可验证声明发送至所述验证方的设备。

[0144] 实际应用中,该装置还可以包括:

[0145] 去中心化身份标识获取模块,用于在获取所述验证方发送的验证请求之后,获取所述可验证声明的验证方的去中心化身份标识;

[0146] 判断模块,用于根据所述去中心化身份标识,判断所述验证方是否具有所述数据仓库的使用权限;

[0147] 所述可验证声明查找单元,具体可以包括:

[0148] 可验证声明查找子单元,用于当所述验证方具有所述数据仓库的使用权限,则根据所述标识,从所述数据库中查找所述可验证声明。

[0149] 图8为本说明书实施例提供的对应于图6的一种可验证声明的获取装置的结构示意图。该装置可以应用于可验证声明的验证方。如图8所示,该装置可以包括:

[0150] 第一验证请求获取模块801,用于获取所述可验证声明的持有方发送的第一验证请求;所述第一验证请求中至少包含所述可验证声明的标识;

[0151] 第二验证请求发送模块802,用于向数据仓库发送获取所述可验证声明的第二验证请求;所述第二验证请求中包含所述标识;

[0152] 可验证声明获取模块803,用于获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明;

[0153] 其中,所述可验证声明是所述数据仓库从目标区块链系统中获取的。

[0154] 实际应用中,所述第二验证请求中还可以包括所述验证方的去中心化身份标识。

[0155] 基于同样的思路,本说明书实施例还提供了上述方法对应的设备。

[0156] 图9为本说明书实施例提供的对应于图3的可验证声明的转发设备以及对应于图6的可验证声明的获取设备的结构示意图。如图9所示,设备900可以包括:

[0157] 至少一个处理器910;以及,

[0158] 与所述至少一个处理器通信连接的存储器930;其中,

[0159] 所述存储器930存储有可被所述至少一个处理器910执行的指令920,所述指令被所述至少一个处理器910执行,以使所述至少一个处理器910能够:

[0160] 监听目标区块链系统中产生的包含可验证声明的链上交易数据;

[0161] 若所述链上交易数据中包含的去中心化身份标识,与所述数据仓库服务的验证方的去中心化身份标识相同,则获取所述链上交易数据中的可验证声明;

[0162] 将所述可验证声明发送至所述验证方的设备。

[0163] 或者,所述指令被所述至少一个处理器910执行,以使所述至少一个处理器910能够:

[0164] 获取所述可验证声明的持有方发送的第一验证请求;所述第一验证请求中至少包含所述可验证声明的标识;

[0165] 向数据仓库发送获取所述可验证声明的第二验证请求;所述第二验证请求中包含

所述标识；

[0166] 获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明；

[0167] 其中，所述可验证声明是所述数据仓库从目标区块链系统中获取的。

[0168] 在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进(例如，对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件(Programmable Logic Device, PLD)(例如现场可编程门阵列(Field Programmable Gate Array，FPGA))就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言(Hardware Description Language，HDL)，而HDL也并非仅有一种，而是有许多种，如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等，目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[0169] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit，ASIC)、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0170] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0171] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本

申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0172] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0173] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0174] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0175] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0176] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0177] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0178] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带式磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0179] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0180] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序

模块。一般地，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、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0181] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0182] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

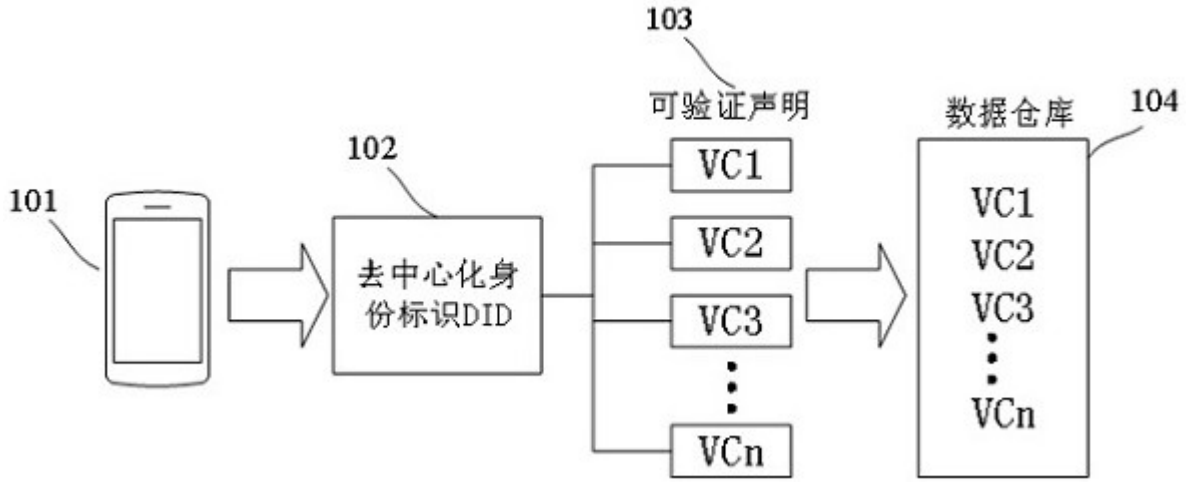

103
可验证声明
数据仓库
104
102
101
去中心化身份标识DID
VC1
VC2
VC3
VCn
VC1
VC2
VC3
VCn

图1

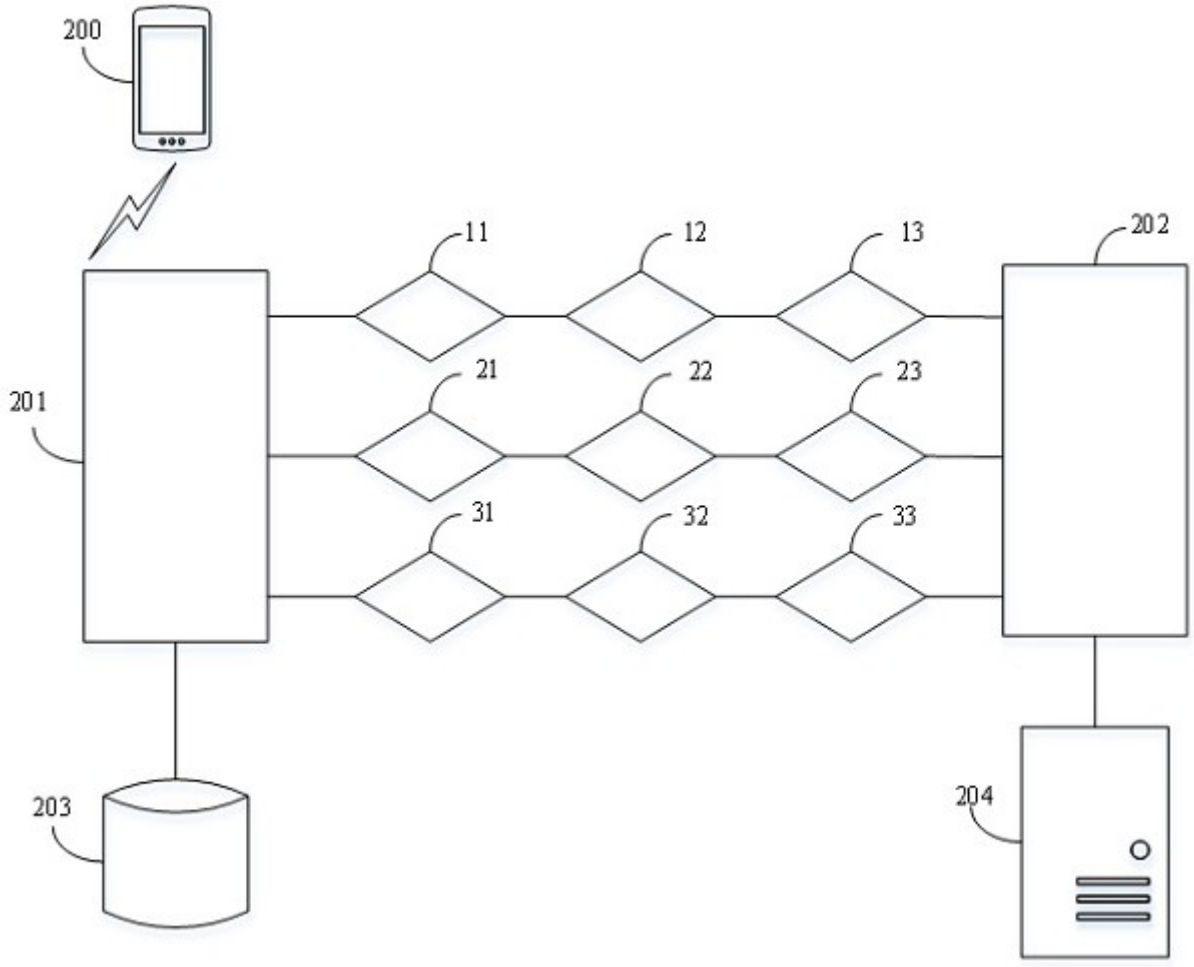

200
11
12
13
202
21
22
23
201
31
32
33
203
204

图2

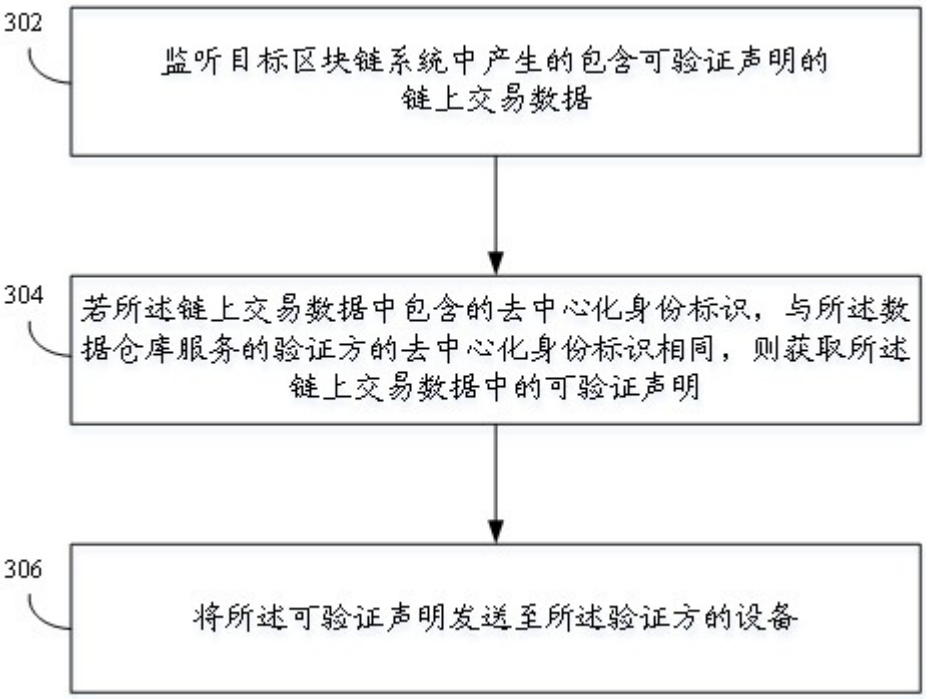

302
监听目标区块链系统中产生的包含可验证声明的链上交易数据
304
若所述链上交易数据中包含的去中心化身份标识，与所述数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明
306
将所述可验证声明发送至所述验证方的设备

图3


AES（VC Content）
B_Public_Key（AES）
AuthList [B]

图4

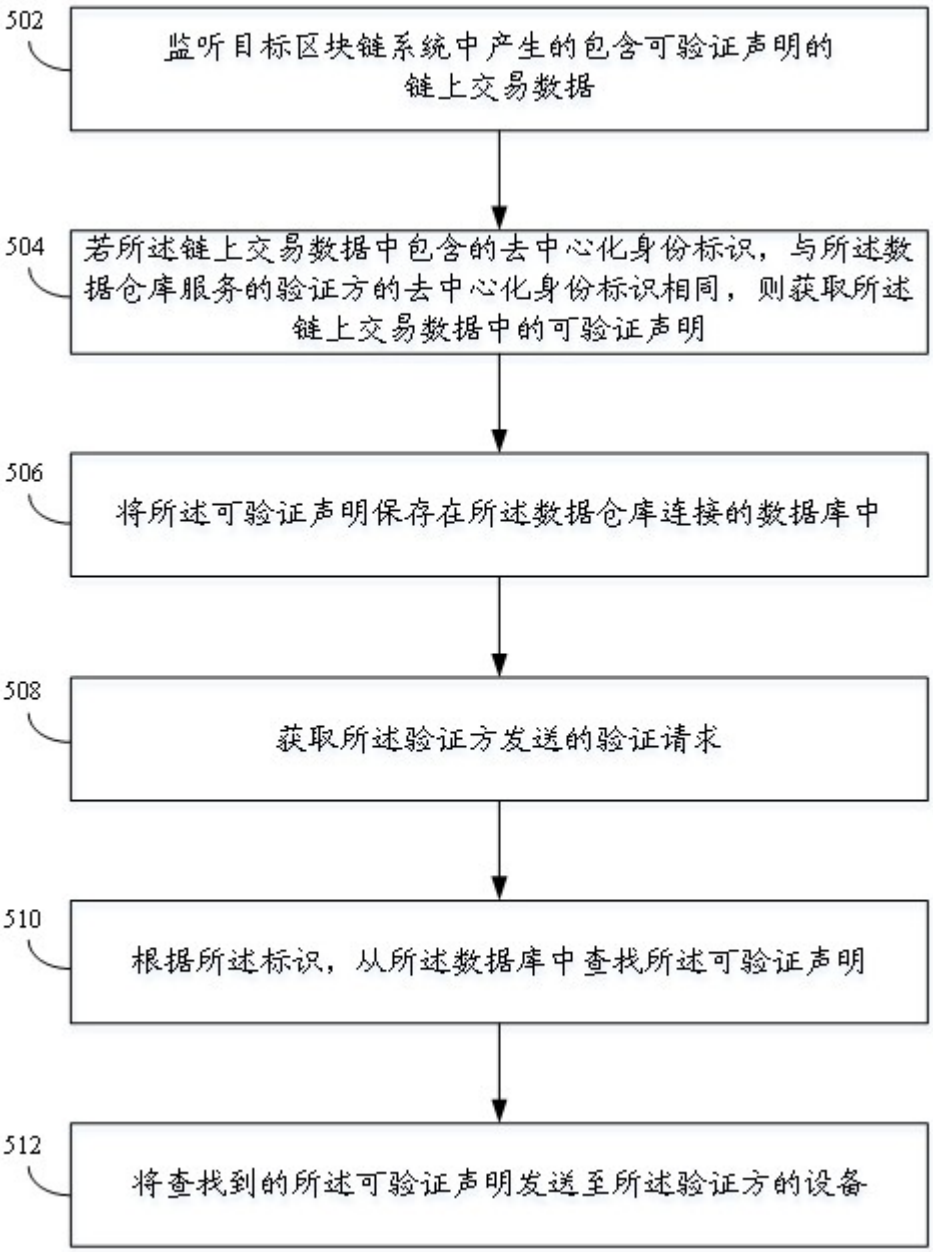

502
监听目标区块链系统中产生的包含可验证声明的链上交易数据
504
若所述链上交易数据中包含的去中心化身份标识，与所述数据仓库服务的验证方的去中心化身份标识相同，则获取所述链上交易数据中的可验证声明
506
将所述可验证声明保存在所述数据仓库连接的数据库中
508
获取所述验证方发送的验证请求
510
根据所述标识，从所述数据库中查找所述可验证声明
512
将查找到的所述可验证声明发送至所述验证方的设备

图5

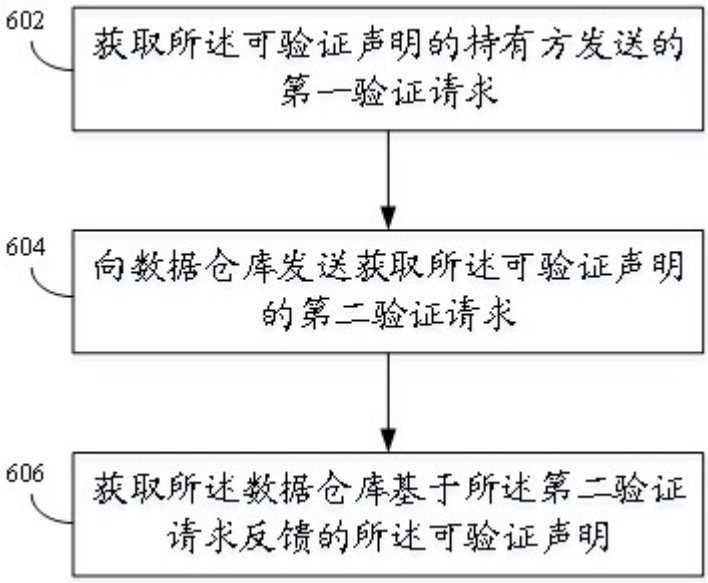

602
获取所述可验证声明的持有方发送的第一验证请求
604
向数据仓库发送获取所述可验证声明的第二验证请求
606
获取所述数据仓库基于所述第二验证请求反馈的所述可验证声明

图6

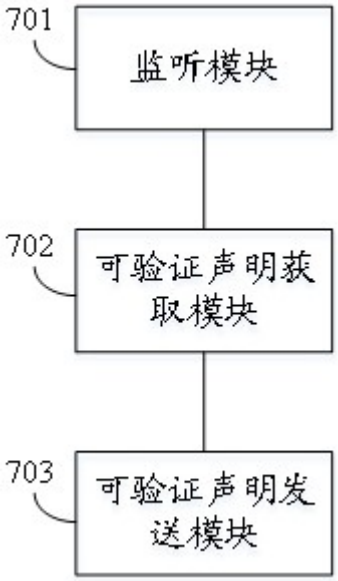

701
监听模块
702
可验证声明获取模块
703
可验证声明发送模块

图7

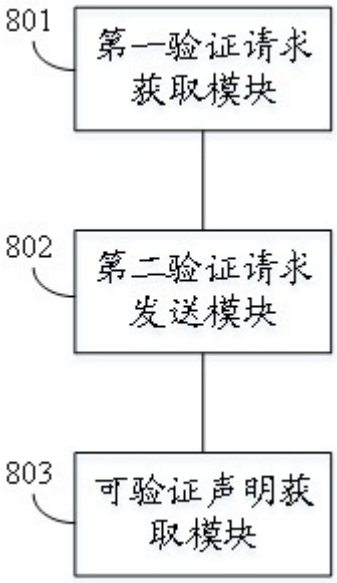

801
第一验证请求获取模块
802
第二验证请求发送模块
803
可验证声明获取模块

图8

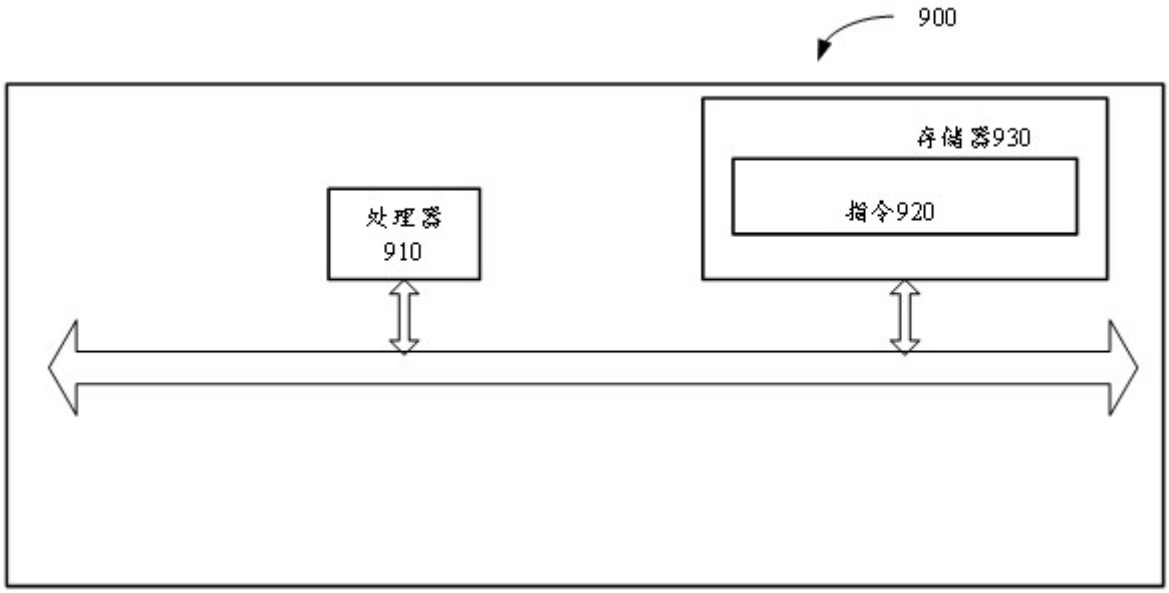

900
存储器930
指令920
处理器910

图9