(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111316303 B
(45)授权公告日 2023.11.10

(21)申请号 201980004847.8

(22)申请日 2019.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 111316303 A

(43)申请公布日 2020.06.19

(66)本国优先权数据
PCT/CN2019/094396 2019.07.02 CN
PCT/CN2019/095303 2019.07.09 CN
PCT/CN2019/095299 2019.07.09 CN

(85)PCT国际申请进入国家阶段日
2020.04.02

(86)PCT国际申请的申请数据
PCT/CN2019/103758 2019.08.30

(87)PCT国际申请的公布数据
WO2021/000419 EN 2021.01.07

(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心

(72)发明人 李书博 刘佳伟 杨仁慧

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 艾佳

(51)Int.Cl.
*G06Q 20/38*(2012.01)
*G06Q 40/04*(2012.01)

(56)对比文件
US 2018115426 A1,2018.04.26
US 2018343120 A1,2018.11.29
US 2019058595 A1,2019.02.21
WO 2017104899 A1,2017.06.22
WO 2019101227 A2,2019.05.31
US 2019147431 A1,2019.05.16
US 2016275461 A1,2016.09.22
WO 2018167252 A1,2018.09.20
WO 2019104323 A1,2019.05.31
张路.区块链技术应用对产业链协同创新的作用机理.学习与实践.2019,(第04期),17-24.
Asem Othman et al..“The Horcrux Protocol: A Method for Decentralized Biometric-basedSelf-sovereign Identity”.《2018 International Joint Conference on Neural Networks (IJCNN)》.2018,第1-7页.

审查员 崔倩倩

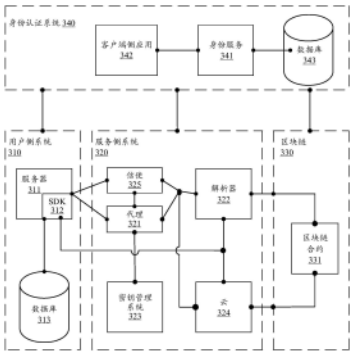
权利要求书2页 说明书42页 附图20页

(54)发明名称

用于基于区块链的交叉实体认证的系统和方法

(57)摘要

本文提供了用于基于区块链的交叉实体认证的方法、系统和装置,包括编码在计算机存储介质上的计算机程序。所述方法之一包括:从区块链获得包括第一实体用于认证用户的认证请求的区块链交易,其中,所述认证请求包括所述用户的去中心化标识(DID);响应于确定所述第一实体被允许访问由第二实体背书的所述用户的认证信息,响应于所述获得的区块链交易获得所述第二实体对所述用户的认证结果,其中,所述认证结果与所述去中心化标识相关联;生成包括所述认证结果的不同的区块链交易;以及将所述不同的区块链交易发送至区块链节点以添加至所述区块链。



CN 111316303 B

1.一种计算机实现的用于基于区块链的交叉实体认证的方法,包括:

获得第一实体用于认证用户的认证请求;其中,所述用户在第二实体注册,以及所述用户未在所述第一实体注册;

生成用于获得所述第二实体对所述用户的认证结果的区块链交易;以及

将所述区块链交易发送至区块链节点以添加至所述区块链;

从区块链获得包括第一实体用于认证用户的认证请求的区块链交易,其中,所述认证请求包括所述用户的去中心化标识DID;

响应于确定所述第一实体被允许访问由第二实体背书的所述用户的认证信息,响应于所述获得的区块链交易获得所述第二实体对所述用户的认证结果,其中,所述认证结果与所述去中心化标识相关联;所述由所述第二实体背书的所述用户的所述认证信息包括与表明所述用户是所述第二实体的注册用户的可验证声明VC相关联的信息,以及所述可验证声明与所述去中心化标识相关联;所述可验证声明的哈希值被存储在所述区块链中;所述可验证声明被存储在数据存储中;以及所述数据存储包括以下中的一个或多个:由所述第二实体维护的本地数据存储、所述第二实体能够访问的公共数据存储以及由平台维护的用于所述第二实体的数据存储;

生成包括所述认证结果的不同的区块链交易;以及

将所述不同的区块链交易发送至区块链节点以添加至所述区块链。

2.如权利要求1所述的方法,还包括:

从所述区块链获得所述不同的区块链交易,所述不同的区块链交易包括所述第二实体对所述用户的所述认证结果,其中,所述认证结果表明所述认证失败;以及

将所述认证结果发送给所述第一实体,以拒绝所述用户访问所述第一实体。

3.如权利要求1所述的方法,其中:

所述获得的区块链交易包括利用所述用户的私钥加密的授权以允许所述第一实体访问由所述第二实体背书的所述用户的所述认证信息;

所述加密的授权包括所述用户的所述去中心化标识;

所述加密的授权包括基于所述第一实体的私钥对所述认证请求的数字签名;以及

在获得所述区块链交易之后并且在获得所述认证结果之前,所述方法还包括:

获得所述用户的公钥;

利用所述用户的所述公钥对所述加密的授权进行解密,以验证所述授权是所述用户签名的并获得所述数字签名;

从所述区块链获得所述第一实体的公钥;

利用所述获得的所述第一实体的公钥对所述数字签名进行解密;以及

将所述解密的数字签名与所述认证请求的哈希值进行比较,以验证所述认证请求是所述第一实体签名的。

4.如权利要求1所述的方法,其中:

所述可验证声明包括由所述第二实体或所述用户配置的用于允许所述第一实体访问所述可验证声明的权限;以及

在获得所述区块链交易之后并且在获得所述认证结果之前,所述方法还包括:基于所述权限验证所述第一实体被允许访问所述可验证声明。

5.如权利要求4所述的方法,其中:

所述可验证声明的哈希值被存储在所述区块链中;

所述可验证声明被存储在数据存储中;以及

所述数据存储包括以下中的一个或多个:由所述第二实体维护的本地数据存储、所述第二实体能够访问的公共数据存储以及由平台维护的用于所述第二实体的数据存储。

6.如权利要求1所述的方法,其中,响应于所述获得的区块链交易获得所述认证结果包括:

查询所述数据存储以获得与所述去中心化标识相关联的所述可验证声明;

基于所述获得的可验证声明验证所述用户是所述第二实体的注册用户,以生成未加密的认证结果;以及

利用所述第二实体的私钥对所述未加密的认证结果进行加密,以生成所述认证结果。

7.如权利要求5所述的方法,在获得所述区块链交易之前,还包括:

从与所述第二实体相关联的计算设备获得用于创建表明所述用户是所述第二实体的注册用户的所述可验证声明的可验证声明创建请求;

获得与所述第二实体相关联的数字签名;以及

基于所述获得的可验证声明创建请求和所述获得的数字签名创建所述可验证声明。

8.如权利要求7所述的方法,在获得所述可验证声明创建请求之前,还包括:

从所述第二实体获得用于创建与所述用户的账户标识相关联的去中心化标识的去中心化标识创建请求;

获得加密密钥对中的公钥;

基于所述公钥获得所述去中心化标识;以及

存储所述账户标识与所述获得的去中心化标识之间的映射关系。

9.如权利要求1所述的方法,其中:

所述去中心化标识是与所述用户的主要去中心化标识相关联的次要去中心化标识;

所述主要去中心化标识与所述用户的隐私信息相关联;以及

基于所述次要去中心化标识不能追踪所述隐私信息。

10.如权利要求9所述的方法,其中:

所述次要去中心化标识是用于所述用户访问所述第一实体的临时去中心化标识。

11.一种用于基于区块链的交叉实体认证的系统,包括:

一个或多个处理器;以及

耦接到所述一个或多个处理器并且其上存储有指令的一个或多个计算机可读存储器,所述指令能够由所述一个或多个处理器执行以执行权利要求1至10中任一项所述的方法。

12.一种用于基于区块链的交叉实体认证的装置,包括用于执行权利要求1至10中任一项所述的方法的多个模块。

13.一种非暂时性计算机可读存储介质,配置有能够由一个或多个处理器执行的指令,以促使所述一个或多个处理器执行权利要求1至9中任一项所述的方法。

# 用于基于区块链的交叉实体认证的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求享有2019年7月9日递交到中国国家知识产权局(SIPO)的国际申请No.PCT/CN2019/095299和国际申请No.PCT/CN2019/095303的优先权和权益。上述两个申请都要求享有2019年7月2日递交到中国国家知识产权局(SIPO)的国际申请No.PCT/CN2019/094396的优先权和权益。这里通过引用的方式结合上述申请的全部内容。

## 技术领域

[0003] 本申请一般涉及用于基于区块链的交叉实体认证的方法和设备。

## 背景技术

[0004] 传统的身份管理系统基于中心化机构,例如公司目录服务、认证机构或域名注册机构。每个中心化机构都可作为信任的根源,为其背书的身份提供可信度。对于这样的系统,与身份相关联的数据通常存储在中心化的数据库中,如果不是存储在传统的信息存储介质中。每个人或实体的身份维护都在中心化机构的控制下。鉴于其性质,传统的身份管理系统会承担每个中心化机构遭受的安全风险,并且提供低效的机制来收集由不同中心化机构提供的身份或凭证。在这样的系统中,个人实体或身份所有者通常既不能自由选择信任的根源,也不能控制他们自己的身份或凭证。对他们身份的认证和验证通常证明是低效的。

[0005] 交叉实体认证提出了其他挑战。交叉实体认证需要不同的机构共享用户身份信息。例如,为了允许第一机构基于用户在第二机构的注册来认证用户,第二机构可能需要与第一机构共享用户的身份和认证信息。传统的交叉认证系统经常面临诸如安全漏洞、隐私泄漏、用户不友好、通知和授权复杂、工作流程效率低下等问题。在大多数情况下,不同的机构通常会发现缺乏用于彼此交互以交叉认证用户的通用协议。例如,用户认证信息可能散布在安全环境之外,从而使用户冒着身份被盗用的风险。对于另一个示例,非必要的用户信息可能与必要的信息一起被提供给其他机构,以用于交叉实体认证,从而泄露用户隐私。对于另一示例,机构和用户必须经过许多层的授权和安全检查,这使系统不便利且不可扩展。

[0006] 区块链技术提供了建立值得信任的去中心化系统的机会,该系统不需要信任系统的每个成员。区块链通过将数据保存在相互之间具有优先关系的一系列数据区块中,以去中心化方式提供数据存储。区块的链由区块链节点的网络维护和更新,区块链节点也负责基于共识方案验证数据。存储的数据可以包括许多数据类型,例如各方之间的金融交易、历史访问信息等。

[0007] 许多区块链(例如,以太坊区块链)已经能够实现通过区块链交易执行的区块链合约(也称为智能合约)。区块链交易为签名的消息,其由外部拥有的账户(例如区块链账户)发起,由区块链网络传送并记录在区块链中。可以编写区块链合约以实现各种功能,例如将数据添加到区块链账户、更改区块链中的数据等。因此,可以通过执行各种区块链交易来维护和更新区块链。

[0008] 区块链技术提供了无需中心化机构即可管理信任的根源的方法。然而,基于区块

链构建的身份管理系统通常通过要求区块链账本的存储、创建和执行区块链交易和合约的能力或区块链共识方案中的参与，而给一般用户带来实质性技术障碍。这样的身份管理系统还可能需要频繁访问区块链网络和与区块链网络交互，这可能是昂贵的并且消耗资源。对于需要管理大量用户身份的商业实体，这种身份管理系统被证明通常是低效且用户不友好的。由这样的身份管理系统管理的身份与由商业实体保存的账户或服务ID之间的映射通常很难维护。最后，身份管理系统通常可允许匿名和任意创建去中心化身份，并且几乎没有提供任何方法来认证去中心化身份背后的个人的真实身份。

## 发明内容

[0009] 本文的各种实施例包括但不限于用于基于区块链的交叉实体认证的系统、方法和非暂时性计算机可读介质。

[0010] 根据一些实施例，一种计算机实现的用于基于区块链的交叉实体认证的方法包括：从区块链获得包括第一实体用于认证用户的认证请求的区块链交易，其中，所述认证请求包括所述用户的去中心化标识(DID)；响应于确定所述第一实体被允许访问由第二实体背书的所述用户的认证信息，并且响应于所获得的区块链交易，获得所述第二实体对所述用户的认证结果，其中，所述认证结果与所述去中心化标识相关联；生成包括所述认证结果的不同的区块链交易；以及将所述不同的区块链交易发送至区块链节点以添加至所述区块链。

[0011] 在一些实施例中，在获得所述区块链交易之前，所述方法还包括：获得所述第一实体用于认证用户的所述认证请求；生成用于获得所述第二实体对所述用户的认证结果的区块链交易；以及将所述区块链交易发送至区块链节点以添加至所述区块链。

[0012] 在一些实施例中，所述方法还包括：从所述区块链获得所述不同的区块链交易，所述不同的区块链交易包括所述第二实体对所述用户的所述认证结果，其中，所述认证结果表明所述认证成功；以及将所述认证结果发送给所述第一实体，以准予所述用户访问所述第一实体。

[0013] 在一些实施例中，所述方法还包括：从所述区块链获得所述不同的区块链交易，所述不同的区块链交易包括所述第二实体对所述用户的所述认证结果，其中，所述认证结果表明所述认证失败；以及将所述认证结果发送给所述第一实体，以拒绝所述用户访问所述第一实体。

[0014] 在一些实施例中，所述用户在所述第二实体注册；并且所述用户未在所述第一实体注册。

[0015] 在一些实施例中，所述获得的区块链交易包括利用所述用户的私钥加密的授权以允许所述第一实体访问由所述第二实体背书的所述用户的所述认证信息；所述加密的授权包括所述用户的所述去中心化标识；所述加密的授权包括基于所述第一实体的私钥对所述认证请求的数字签名。在获得所述区块链交易之后并且在获得所述认证结果之前，所述方法还包括：获得所述用户的公钥；利用所述用户的所述公钥对所述加密的授权进行解密，以验证所述授权是所述用户签名的并获得所述数字签名；从所述区块链获得所述第一实体的公钥；利用所获得的所述第一实体的公钥对所述数字签名进行解密；以及将所解密的数字签名与所述认证请求的哈希值进行比较，以验证所述认证请求是所述第一实体签名的。

[0016] 在一些实施例中，由所述第二实体背书的所述用户的所述认证信息包括与表明所述用户是所述第二实体的注册用户的可验证声明(VC)相关联的信息；所述可验证声明与所述去中心化标识相关联。

[0017] 在一些实施例中，所述可验证声明包括由所述第二实体或所述用户配置的用于允许所述第一实体访问所述可验证声明的权限；以及在获得所述区块链交易之后并且在获得所述认证结果之前，所述方法还包括：基于所述权限验证所述第一实体被允许访问所述可验证声明。

[0018] 在一些实施例中，所述可验证声明的哈希值被存储在所述区块链中；所述可验证声明被存储在数据存储中；所述数据存储包括以下中的一个或多个：由所述第二实体维护的本地数据存储、所述第二实体可访问的公共数据存储以及由平台维护的用于所述第二实体的数据存储。

[0019] 在一些实施例中，响应于所获得的区块链交易获得所述认证结果包括：查询所述数据存储以获得与所述去中心化标识相关联的可验证声明；基于所获得的可验证声明验证所述用户是所述第二实体的注册用户，以生成未加密的认证结果；以及利用所述第二实体的私钥对所述未加密的认证结果进行加密，以生成所述认证结果。

[0020] 在一些实施例中，在获得所述区块链交易之前，所述方法还包括：从与所述第二实体相关联的计算设备获得用于创建表明所述用户是所述第二实体的注册用户的所述可验证声明的可验证声明创建请求；获得与所述第二实体相关联的数字签名；以及基于所获得的可验证声明创建请求和所获得的数字签名创建所述可验证声明。

[0021] 在一些实施例中，在获得所述可验证声明创建请求之前，所述方法还包括：从所述第二实体获得用于创建与所述用户的账户标识相关联的去中心化标识的去中心化标识创建请求；获得加密密钥对中的公钥；基于所述公钥获得所述去中心化标识；以及存储所述账户标识与所获得的去中心化标识之间的映射关系。

[0022] 在一些实施例中，所述去中心化标识是与所述用户的主要去中心化标识相关联的次要去中心化标识；所述主要去中心化标识与所述用户的隐私信息相关联；基于所述次要去中心化标识不能追踪所述隐私信息。

[0023] 在一些实施例中，所述次要去中心化标识是用于所述用户访问所述第一实体的临时去中心化标识。

[0024] 根据其他实施例，一种用于基于区块链的交叉实体认证的系统包括：一个或多个处理器；以及耦接到所述一个或多个处理器并且其上存储有指令的一个或多个计算机可读存储器，所述指令可由所述一个或多个处理器执行以执行前述实施例中任一个的方法。

[0025] 根据又一其他实施例，一种非暂时性计算机可读存储介质配置有可由一个或多个处理器执行的指令，以促使一个或多个处理器执行前述实施例中任一个的方法。

[0026] 根据其他实施例，一种用于基于区块链的交叉实体认证的装置包括用于执行前述实施例中任一个的方法的多个模块。

[0027] 根据一些实施例，一种用于基于区块链的交叉实体认证的系统包括：一个或多个处理器；以及耦接到所述一个或多个处理器并且其上存储有指令的一个或多个计算机可读存储器，所述指令可由所述一个或多个处理器执行以执行包括以下的操作：从区块链获得包括由第一实体用于认证用户的认证请求的区块链交易，其中，所述认证请求包括所述用

户的去中心化标识(DID);响应于确定所述第一实体被允许访问由第二实体背书的所述用户的认证信息,并且响应于所获得的区块链交易,获得所述第二实体对所述用户的认证结果,其中,所述认证结果与所述去中心化标识相关联;生成包括所述认证结果的不同的区块链交易;以及将所述不同的区块链交易发送至区块链节点以添加至所述区块链。

[0028] 根据其他实施例,一种非暂时性计算机可读存储介质配置有可由一个或多个处理器执行的指令,以促使所述一个或多个处理器执行包括以下的操作:从区块链获得包括第一实体用于认证用户的认证请求的区块链交易,其中,所述认证请求包括所述用户的去中心化标识(DID);响应于确定所述第一实体被允许访问由第二实体背书的所述用户的认证信息,并且响应于所获得的区块链交易,获得所述第二实体对所述用户的认证结果,其中,所述认证结果与所述去中心化标识相关联;生成包括所述认证结果的不同的区块链交易;以及将所述不同的区块链交易发送至区块链节点以添加至所述区块链。

[0029] 根据其他实施例,一种用于基于区块链的交叉实体认证的装置包括:第一获得模块,用于从区块链获得包括第一实体用于认证用户的认证请求的区块链交易,其中,所述认证请求包括所述用户的去中心化标识(DID);第二获得模块,用于响应于确定所述第一实体被允许访问由第二实体背书的所述用户的认证信息,并且响应于所获得的区块链交易,获得所述第二实体对所述用户的认证结果,其中,所述认证结果与所述去中心化标识相关联;生成模块,用于生成包括所述认证结果的不同的区块链交易;以及发送模块,用于将所述不同的区块链交易发送至区块链节点以添加至所述区块链。

[0030] 本文公开的实施例具有一个或多个技术效果。在一些实施例中,在线平台为基于区块链的交叉实体认证提供在线服务。交叉实体通信、授权和通知的复杂性显著降低。在一个实施例中,这允许使用除区块链所要求的编程语言或协议之外的编程语言或协议来控制与去中心化身份(DID)管理有关的操作。在一个实施例中,这降低了关于用户独立创建和存储重要身份凭证的安全风险。在一个实施例中,这有助于针对单个个人或实体使用简化的控制动作以及有效的不同身份交叉引用来创建大量去中心化标识或可验证声明。在一些实施例中,在线平台可以被表现为集成服务,并且使得用户可以经由API接口访问这样的在线服务。这允许用户方便地访问在线服务,并根据他们先前在另一实体注册的认证信息来请求对一个实体的访问。在一些实施例中,在线平台可以表现为分布式和去中心化服务。这允许大型实体例如通过成为区块链的区块链节点而方便地加入服务。通过用户授权,大型实体可以针对注册用户请求的对其他实体的访问相应地认证注册用户。在一些实施例中,基于用户访问实体的请求,基于用户的去中心化标识和用户对实体访问用户在不同实体注册的认证信息的授权来发起交叉实体认证以认证该用户。这允许通过区块链进行快速、针对性和安全的查询,以从不同实体获得用户的认证,从而最小化用户的认证信息的安全风险。在一些实施例中,用户可基于在不同实体注册的用户的认证信息仅出于访问实体的目的而使用临时去中心化标识。这可以保护隐私并增强安全性,因为临时去中心化标识可以被除去非必要的用户信息和/或限制其有效性。在一些实施例中,实体可以通过与区块链的交互来方便地管理其用户和去中心化标识。在一些实施例中,由于用户在一个实体处的注册可以被其他实体交叉使用,因此减少了实体之间重复的认证信息。因此,减少了功耗和存储消耗。

[0031] 参考附图考虑以下描述和所附权利要求,本文公开的系统、方法和非暂时性计算

机可读介质的这些和其他特征，以及操作方法和相关结构元件的功能以及部件的组合和制造经济性将变得更加明显，上述都形成本说明书的一部分，其中在各个附图中相同的附图标记表示对应的部分。然而，应该清楚地理解，附图仅用于说明和描述的目的，而不是限制性的。

## 附图说明

[0032] 图1示出了根据一些实施例的与区块链相关联的网络环境。

[0033] 图2示出了根据一些实施例的用于实现区块链交易的框架。

[0034] 图3示出了根据一些实施例的与用于基于区块链的交叉实体认证的系统相关联的网络环境。

[0035] 图4示出了根据一些实施例的与用于基于区块链的交叉实体认证的系统相关联的架构。

[0036] 图5示出了根据一些实施例的与用于实现与去中心化标识和可验证声明相关联的各种功能示例的系统相关联的网络环境。

[0037] 图6A和图6B示出了根据一些实施例的用于创建去中心化标识的方法。

[0038] 图7示出了根据一些实施例的用于使用去中心化标识认证服务来认证去中心化标识的方法。

[0039] 图8示出了根据一些实施例的使用身份管理应用来认证去中心化标识的方法。

[0040] 图9示出了根据一些实施例的用于发布可验证声明的方法。

[0041] 图10示出了根据一些实施例的用于验证可验证声明的方法。

[0042] 图11示出了根据一些实施例的用于使用代理服务创建去中心化标识的方法。

[0043] 图12示出了根据一些实施例的用于使用代理服务认证去中心化标识的方法。

[0044] 图13示出了根据一些实施例的用于代表验证者或所有者认证去中心化标识的方法。

[0045] 图14示出了根据一些实施例的用于使用代理服务发布可验证声明的方法。

[0046] 图15示出了根据一些实施例的用于使用代理服务验证可验证声明的方法。

[0047] 图16示出了根据一些实施例的用于基于区块链的交叉实体认证的方法。

[0048] 图17A示出了根据一些实施例的用于基于区块链的交叉实体认证的方法的流程图。

[0049] 图17B示出了根据一些实施例的用于基于区块链的交叉实体认证的方法的流程图。

[0050] 图18A示出了根据一些实施例的用于基于区块链的交叉实体认证的计算机系统的框图。

[0051] 图18B示出了根据一些实施例的用于基于区块链的交叉实体认证的计算机系统的框图。

[0052] 图19示出了可以实现本文描述的实施例中任一个的计算机系统的框图。

## 具体实施方式

[0053] 本文描述的实施例提供了与用于可以为实体提供唯一且可验证的身份的去中心

化身份管理的生态系统相关联的方法、系统和装置。实体的去中心化标识(DID)可允许该实体获得对其身份以及与身份相关联的信息的完全控制。例如,实体可以是具有许多用户的商业实体,也可以是用户之一。可验证声明(VC)可允许不同实体之间进行授权、背书和确认。在商业环境中,服务或产品提供商可以使用其客户的去中心化标识和可验证声明来识别并认证客户,并相应地提供服务或产品。

[0054] 在一些实施例中,去中心化标识可以是表明真实实体和在线实体之间的映射关系的唯一标识。去中心化标识可以包括URL方案标识、用于去中心化标识方法的标识以及去中心化标识方法专用标识。每个去中心化标识可以指向对应的去中心化标识文档。去中心化标识文档可以包括关于去中心化标识和去中心化标识的所有者的预设格式(例如,JSON-LD)的描述性文本。去中心化标识可以用作用于定位去中心化标识文档的统一资源标识(URI)。去中心化标识文档可以包括各种属性,例如上下文、去中心化标识主题、公钥、认证、授权和委托、服务端点、创建、控制、更新、证明、可扩展性、其他合适的属性或其任意组合。这些属性可以表现为与所有者的去中心化标识相关联的去中心化标识文档的参数。例如,对于控制者参数,第一去中心化标识的去中心化标识文档可以记录用于控制第一去中心化标识的第二去中心化标识(例如,第二去中心化标识的所有者是被信任以作为控制者来管理第一去中心化标识的实体)。对于另一个示例,对于创建者参数,第一去中心化标识的去中心化标识文档可以记录创建第一去中心化标识的第二去中心化标识(例如,第二去中心化标识的所有者是代表第一去中心化标识的所有者创建第一去中心化标识的实体)。去中心化标识文档可以定义或指向定义多个操作的资源,所述操作可以相对于去中心化标识执行。

[0055] 在一些实施例中,可验证声明可以提供关于实体的质量、特征、关系和其他相关信息的可验证在线信息。可验证声明可以包含预设格式(例如JSON-LD)的描述性文本,该文本描述有关去中心化标识的一个或多个声明(例如,去中心化标识所有者的年龄、去中心化标识所有者的教育背景)以及实体对声明的背书。可验证声明可以包括各种属性,例如上下文、标识、类型、凭证主题、发布者、发布日期、证明、到期日、状态、表示、其他合适的属性或其任意组合。可验证声明可以指定其声明的类型,该类型可以表明该声明的结构。这可以促使可验证声明发布者和可验证声明验证者自动进行处理。

[0056] 去中心化标识的所有者可以以不同的角色参与身份管理系统。例如,个人可能期望使用由商业实体提供的服务,该服务需要证明该个人已超过18岁。该个人可以是去中心化标识的所有者,并且可以请求由提供公民年龄验证的政府机构发布的可验证声明。商业实体可以验证可验证声明,以确保该个人符合年龄要求。在这种情况下,个人可以是去中心化标识所有者和可验证声明持有者;政府机构可以是可验证声明发布者,而商业实体可以是可验证声明验证者。作为另一示例,用户可以向第一企业发布可验证声明,以允许第一企业使用由第二企业存储的用户数据。在这种情况下,用户可以充当可验证声明发布者;第一企业可以充当去中心化标识所有者和可验证声明持有者;第二企业可以充当可验证声明验证者。

[0057] 一些实施例集成了各种组件,例如区块链网络、云应用、代理服务、解析器服务、用户应用、应用编程接口(API)服务、密钥管理系统(KMS)、身份认证系统和其他合适的组件,以实现诸如创建和认证去中心化标识以及发布和验证可验证声明的功能。在一些实施例

中,集成这些组件中的一个或多个的在线平台可以促进商业实体顺利地为其用户创建去中心化标识和发布可验证声明。商业实体可以通过一个或多个API接口与在线平台进行交互,并将多个加密密钥信托给在线平台。在线平台可以提供代表商业实体和/或其用户来执行与去中心化标识和可验证声明有关的各种操作的代理服务。可选地,在线平台可以提供可以集成到商业实体的应用中以直接执行与去中心化标识和可验证声明有关的操作的软件开发套件(SDK)。在线平台还可以促进商业实体对去中心化标识、商业实体所维护的账户以及与去中心化标识和账户相对应的真实个人的身份之间的关系的管理。

[0058] 图1示出了根据一些实施例的与区块链相关联的网络环境。如图所示,在环境100中,客户端侧计算设备111可以耦接到服务器端118,并且服务器端118和节点B可以通过各种通信网络耦接到区块链系统112。类似地,服务器端118可以可选地耦接到更多类似于区块链系统112的区块链系统,例如区块链系统113、区块链系统114等。每个区块链系统可以维护一个或多个区块链。

[0059] 在一些实施例中,客户端侧计算设备111可以包括一个或多个服务器(例如,节点C)以及一个或多个其他计算设备(例如,节点A1、节点A2、节点A3)。节点A1、节点A2和节点A3可以耦接到节点C。在一些实施例中,节点C可以由具有各种本地账户(从节点A1、节点A2、节点A3评估的本地账户)的实体(例如,网站、移动电话应用、组织、公司、企业)来实现。例如,移动电话应用可具有数百万个从相应的用户账户访问应用的服务器的端用户(end-user)。应用的服务器可以相应地存储数百万个用户账户。客户端侧计算设备111的组件及其布置可以具有许多其他配置。

[0060] 在一些实施例中,区块链系统112可包括维护一个或多个区块链(例如,公有区块链、私有区块链、联盟区块链)的多个区块链节点(例如,区块链节点1、区块链节点2、区块链节点3、区块链节点4、区块链节点i等)。其他区块链系统(例如,区块链系统113等)可以包括维护其他区块链的区块链节点的类似布置。每个区块链节点都可以在一个或多个区块链系统中找到。区块链节点可以包括全节点。全节点可以下载每个区块和区块链交易,并对照区块链的共识规则对他们进行检查。区块链节点可以形成网络,在所述网络中一个区块链节点与另一个区块链节点通信。所示的区块链节点的次序和数量仅仅是为了说明的示例。区块链节点可以在服务器、计算机等中实现。例如,每个区块链节点可以在服务器或服务器集群中实现。服务器集群可以采用负载平衡。每个区块链节点可以对应于经由诸如TCP/IP的各种类型的通信方法耦接在一起的一个或多个物理硬件设备或者虚拟设备。根据分类,区块链节点还可以被称为全节点、Geth节点、共识节点等。

[0061] 在一些实施例中,节点B可以包括轻节点。轻节点可能无法下载完整的区块链,而只下载区块头以验证区块链交易的真实性。轻节点可以由全节点(例如,区块链系统112中的区块链节点)服务并且有效地依赖于全节点来访问区块链的更多功能。通过安装适当的软件,可以在诸如膝上型电脑、移动电话等的电子设备中实现轻节点。在一个实施例中,节点B可将区块链交易发送至区块链系统112以添加至区块链。

[0062] 在一些实施例中,可以有更多类似于客户端侧计算设备111的客户端侧计算设备耦接到服务器端118。服务器端118可以提供区块链即服务(BaaS),并且被称为BaaS云。在一个实施例中,BaaS是一种云服务模型,其中客户端或开发人员将Web或移动应用的幕后方面外包。BaaS可以为区块链上发生的活动提供预先编写的软件,例如用户认证、数据库管理和

远程更新。BaaS云可以在服务器、服务器集群或其他设备中实现。在一个实施例中，BaaS云提供基于区块链技术的企业级平台服务。这项服务可以帮助客户端构建安全且稳定的区块链环境，并轻松管理区块链的部署、操作、维护和开发。该服务具有高安全性、高稳定性、易用性以及开放性和共享性的特征。基于云的丰富的安全策略和多租户隔离，BaaS云可以使用芯片加密技术来提供高级的安全保护。基于高度可靠的数据存储，这项服务提供了可以快速扩展而不会中断的端到端并具有高可用性的服务。BaaS云可以提供增强的管理功能，以帮助客户构建企业级区块链网络环境。BaaS云可以为标准区块链应用和数据提供本地支持，支持例如Hyperledger Fabric和Enterprise Ethereum-Quorum的主流开源区块链技术，以构建开放且包容的技术生态系统。

[0063] 在环境100中，系统、节点和设备中的每一个可以安装有适当的软件(例如，应用编程接口)和/或硬件(例如，有线、无线连接)以访问环境100的其他设备。通常，系统、节点和设备可以能够通过一个或多个有线或无线网络(例如，互联网)彼此通信，通过所述网络可以通信数据。系统、节点和设备中的每一个可以包括一个或多个处理器以及耦接到一个或多个处理器的一个或多个存储器。存储器可以是非暂时性的且计算机可读的，并且配置有可一个或多个处理器执行以促进所述一个或多个处理器执行本文描述的操作的指令。所述指令可以存储在存储器中或通过通信网络下载而不必存储在存储器中。尽管在此附图中系统、节点和设备被示为单独的组件，但是应当理解，这些系统、节点和设备可以实现为单个设备或耦接在一起的多个设备。例如，节点B可以可选地集成到区块链节点2中。

[0064] 诸如节点A1、节点A2、节点A3、节点B和节点C之类的设备可以安装有适当的区块链软件以发起、转发或访问区块链交易。术语“区块链交易”可以指在验证后在区块链系统中执行并记录在区块链中的任务单元。在一些实施例中，服务器端118可以基于从节点A1、A2或A3获得的信息来构建区块链合约。服务器端118可以将区块链合约添加至区块链交易中。在服务器端118将区块链交易提交给区块链系统之后，区块链节点可以验证区块链交易以添加到区块链。如果将区块链交易添加到区块链，则区块链合约被部署在区块链上并在特定状态下被发起。通过一个或多个附加区块链交易，可以调用所部署的区块链合约以更新特定状态。

[0065] 可以根据共识规则来验证区块链交易。例如，下面提供了工作量证明(POW)共识处理。尽管如此，诸如POS(权益证明)、DPOS(委托权益证明)和PBFT(实用拜占庭容错)的其他类型的共识处理可以类似地应用于所公开的系统和方法。

[0066] 在关于区块链交易验证的一些实施例中，在接收到未确认的区块链交易的区块链交易请求后，接收方区块链节点可以对区块链交易执行一些初步验证。例如，区块链节点1可以在从节点C接收到区块链交易之后执行初步验证。一旦被验证，区块链交易可以被存储在接收方区块链节点(例如，区块链节点1)的数据库中，该节点也可以将该区块链交易转发到一个或多个其他区块链节点(例如，区块链节点3、区块链节点4)。类似地，每个区块链节点可以包括或耦接到存储数据库的存储器。该数据库可以存储多个未确认的区块链交易。在接收到区块链交易之后，一个或多个其他区块链节点可以重复由接收方区块链节点完成的初步验证和广播处理。

[0067] 对于验证，每个区块链节点可以根据其偏好从数据库中选择一些区块链交易，并将其形成为向区块链提出的新区块。区块链节点可以通过投入计算能力来解决复杂的数学

问题，从而对提出的新区块进行“挖矿”。如果区块链交易涉及区块链合约，则区块链节点可以在对应的虚拟机(VM)中本地执行区块链合约。为了处理区块链合约，区块链网络的每个区块链节点都运行对应的虚拟机，并在区块链合约中执行相同的指令。虚拟机是基于计算机架构的计算机系统的软件仿真并提供物理计算机的功能。区块链环境中的虚拟机可以被理解为被设计用作区块链合约的运行环境的系统。

[0068] 根据共识规则成功挖出所提出的区块链交易的新区块的特定区块链节点可以将新区块打包至其区块链的本地副本中，并将结果多播到其他区块链节点。特定区块链节点可以是首先成功完成验证、已获得验证特权、已经基于另一共识规则被选择等的区块链节点。然后，其他区块链节点可以遵循与特定区块链节点执行的执行顺序相同的执行顺序在本地执行新区块中的区块链交易，彼此验证执行结果(例如，通过执行哈希计算)，并将它们的区块链的副本与特定区块链节点的副本同步。通过更新区块链的本地副本，其他区块链节点可以类似地将区块链交易中这样的信息写入对应的本地存储器。因此，区块链合约可以部署在区块链上。如果在某一时刻验证失败，则拒绝区块链交易。

[0069] 部署的区块链合约可以具有地址，根据该地址可以访问部署的合约。区块链节点可以通过向区块链合约输入特定参数来调用已部署的区块链合约。在一个实施例中，可以调用部署的区块链合约以添加或更新区块链合约中的特定信息，从而更新区块链合约中的一个或多个状态。在一个实施例中，可以通过查询添加到区块链的相应区块链交易来从区块链中检索区块链合约的一个或多个状态。最新更新的状态可以反映在最近的相关区块链交易中。虽然如上所述，但是其他类型的区块链系统和相关联的共识规则可应用于所公开的设备和方法。

[0070] 图2示出了根据一些实施例的用于实现区块链交易的框架。在一些实施例中，客户端侧计算设备111可以向服务器端118发送信息。该信息可以用于创建区块链账户、基于区块链合约执行动作等。区块链可以由区块链系统112维护。服务器端118可以基于从客户端侧计算设备111获得的信息来构建区块链合约。服务器端118可以将区块链合约添加至区块链交易A。服务器端118可以代表与客户端侧计算设备111相关联的用户对区块链交易进行签名。例如，区块链交易A可以包括例如随机数(例如，交易序列号)、从(例如，用户的区块链地址)、至(例如，如果部署区块链合约则为空)、交易费、签名(例如，服务器端118的签名、服务器端118管理的用户的签名)、值(例如，交易金额)、数据(例如，区块链合约)等的信息。然后，服务器端118可以将区块链交易A提交到区块链系统112的一个或多个区块链节点以添加到区块链。

[0071] 在将区块链交易添加到区块链之后，区块链合约被部署在区块链上并在特定状态下被发起。通过一个或多个附加区块链交易，可以调用所部署的区块链合约以更新特定状态。在一些实施例中，节点B可以构建签名的区块链交易B并将其发送到区块链系统112以供执行。在一个实施例中，可以执行区块链交易B来调用所部署的区块链合约以更新状态。在一些实施例中，可以在用户端应用221处用源代码对区块链交易B进行编程。例如，用户或机器可以对区块链交易B进行编程。节点B可以使用相应的编译器来编译源代码，该编译器将源代码转换为字节码。区块链交易B可以包括诸如随机数、从、至、交易费、值、签名、数据等的信息。节点B可以通过远程过程调用(RPC)接口223将区块链交易B发送到区块链系统112的一个或多个区块链节点以供执行。RPC是第一程序(例如，用户端应用)可以用来从位于网

络上的另一计算机(例如,区块链节点)中的第二程序请求服务而不必理解网络细节的协议。当第一程序促使进程在不同地址空间中执行时,其如同正常(本地)进程调用,而无需程序员明确地编码远程交互的细节。

[0072] 在一些实施例中,在接收到区块链交易(例如,区块链交易A或B)时,接收方区块链节点可以验证区块链交易是否有效。例如,可以验证签名和其他格式。如果验证成功,接收方区块链节点就可将接收到的区块链交易广播到区块链网络,该区块链网络包括各种其他区块链节点。一些区块链节点可以参与区块链交易的挖矿过程。区块链交易可以由特定节点选择以进行共识验证从而打包到新区块中。如果区块链交易涉及部署区块链合约,特定节点可以创建与合约账户地址相关联的区块链合约的合约账户。如果区块链交易涉及调用部署的区块链合约,则特定节点可以触发其本地虚拟机以执行接收到的区块链交易,因此从其区块链的本地副本调用部署的区块链合约并更新所部署的区块链合约中的状态。如果特定节点成功挖出新区块,则特定节点可以将新区块广播到其他区块链节点。

[0073] 在接收到新区块时,其他区块链节点可以执行验证。如果对新区块有效达成了共识,则将新区块分别打包到由区块链节点维护的区块链的本地副本中。区块链节点可以类似地触发它们的本地虚拟机(例如,本地虚拟机1、本地虚拟机i、本地虚拟机2)以执行新区块中的区块链交易,从而调用区块链的本地副本(例如,本地区块链副本1、本地区块链副本i、本地区块链副本2)并进行相应的更新。每个区块链节点的硬件机器可以访问一个或多个虚拟机,所述虚拟机可以是相应的区块链节点的一部分或耦接到相应的区块链节点。每次都可以触发相应的本地虚拟机来执行区块链交易。同样,将执行新区块中的所有其他区块链交易。轻节点也可以与更新的区块链同步。

[0074] 图3示出了根据一些实施例的与用于基于区块链的交叉实体认证的系统相关联的网络环境。在一些实施例中,用户侧系统310可以对应于实体。该实体可以是向多个用户提供一个或多个产品或服务的商业实体。该实体还可以是单个用户、用户组、组织、其他合适的实体或其任意组合。用户侧系统310可以包括多个计算机系统、数据存储库、云服务、移动应用、其他合适的组件或其任意组合。用户侧系统310可以包括服务器311和数据库313。数据库313可以存储与实体的用户的多个用户账户相关联的数据。与用户侧系统310对应的实体可能期望为其自身以及其用户创建和管理去中心化标识和可验证声明。它可以包括用于管理去中心化标识的创建和认证或者可验证声明的发布和验证的一个或多个软件开发工具包(SDK)312。

[0075] 在一些实施例中,为了实现与去中心化标识和可验证声明相关联的功能,用户端系统310可以与服务侧系统320对接。在一些实施例中,如图3所示的服务侧系统320可以等同于如图1和图2所示的服务器端118的一个或多个组件、成为其一部分、或将其包括在内。服务侧系统320可以包括一个或多个信使325、一个或多个代理321、一个或多个解析器322、一个或多个密钥管理系统323、一个或多个云324、其他合适的组件或其任意组合。代理321可以提供与去中心化标识或可验证声明有关的各种服务或应用,并维护数据库,该数据库将来自用户端系统310的账户信息或其他商业数据映射到存储在一个或多个区块链上的去中心化标识、可验证声明或者其他信息或数据。代理321可以提供一个或多个应用编程接口(API),用户端系统310可以使用该API来直接提交与去中心化标识或可验证声明有关的请求。代理321可以管理用户端系统310与解析器322和云324之间的通信。信使325可以为用户

侧系统310提供与存储在一个或多个区块链上的去中心化标识、可验证声明或其他信息或数据有关的通知。

[0076] 在一些实施例中，代理321可以耦接到密钥管理系统(KMS)323。KMS 323可以生成、分发和管理用于设备和应用的加密密钥。它们可能涵盖从密钥的安全生成到密钥的安全交换，再到安全的密钥处理和存储的安全性方面。KMS 323的功能可以包括密钥生成、分发和替换以及密钥投入、存储和管理。KMS 323可以包括或耦接到可信执行环境(TEE)。TEE可以是设备的主处理器上与主操作系统分离的隔离区域。TEE可以提供隔离执行环境，该隔离执行环境提供例如隔离执行、使用TEE执行的应用的完整性以及其资产的机密性的安全性特征。它可以保证内部加载的代码和数据在机密性和完整性方面得到保护。在一些实施例中，KMS 323可以在TEE中生成一个或多个加密密钥对。在输出加密密钥对之前，TEE可以对私钥进行加密。私钥的加密可以基于例如数据加密标准(DES)、TripleDES、RSA、高级加密标准(AES)、Twofish等的各种方法或标准。KMS 323可以存储与公钥相关联的加密私钥。为了使用私钥，KMS 323可以将加密私钥馈送到TEE以进行解密和处理。

[0077] 在一些实施例中，代理321可以耦接到解析器322，解析器322可以包括软件应用以管理与去中心化标识或可验证声明有关的交易中代理与区块链330之间的交互(例如，去中心化标识与去中心化标识文档之间的对应关系)。在本文中，根据上下文，区块链330可以指包括去中心化节点网络的区块链系统，所述节点存储记录的账本并参与到共识过程中以将数据添加到记录的账本或由去中心化节点网络存储、维护或更新的记录的账本。在参考区块链系统时，区块链330可以包括图1和图2所示的区块链系统112、113和114中的一个或多个、作为其一部分或体现在其中。解析器322可以是一个或多个基于云的服务的一部分，或者与一个或多个基于云的服务耦接。一个或多个基于云的服务可以与区块链即服务(BaaS)云324或其他合适的云服务相关联。BaaS云324可以构建为一个或多个区块链330提供各种接口的平台。它可以接收来自外部应用的输入并基于输入促进操作的创建和执行，例如区块链交易部署、区块链合约创建和执行、区块链账户创建。BaaS云324还可以从一个或多个区块链330获得信息和数据，并使用BaaS云324将信息和数据馈送到一个或多个其他系统。在一些实施例中，代理321可以直接耦接到云324以使用其服务。在一些实施例中，代理321、解析器322和KMS 323中的一个或多个可以集成为BaaS云324的一部分或另一合适的在线平台的一部分。

[0078] 在一些实施例中，解析器322和云324可以耦接到区块链330。区块链330可以包括一个或多个区块链合约331。一个或多个区块链合约331可以被配置为由与区块链300相关联的虚拟机执行，以执行与去中心化标识和可验证声明相关联的一个或多个操作。所述操作可以包括创建新的去中心化标识、存储去中心化标识文档、更新去中心化标识文档、基于去中心化标识识别去中心化标识文档、存储与可验证声明相关联的信息、检索与可验证声明相关联的信息、其他合适的操作或其任意组合。解析器322和云324可以被配置为在区块链330上部署调用一个或多个区块链合约331的一个或多个交易。所述交易可以触发与去中心化标识和可验证声明有关的一个或多个操作。

[0079] 在一些实施例中，信使325可以耦接到代理321、解析器322和用户侧系统310。信使325可以从解析器322获得通知，并将通知提供给用户侧系统310。

[0080] 在一些实施例中，网络环境可以包括身份认证系统340。身份认证系统340可以用

于建立去中心化标识和真实身份之间的映射关系。身份认证系统340可以与为个人或实体执行身份认证的实体相关联。可以基于个人或实体提供的文档、照片或其他合适的材料来执行身份认证。身份认证还可以基于诸如照片、指纹、密码输入、其他合适的数据或其任意组合等直接收集的数据来执行。身份认证系统340可以耦接到用户侧系统310和/或服务侧系统320。身份认证系统340可以从用户侧系统310或服务侧系统320接收针对身份认证证明的一个或多个请求。作为响应，身份认证系统340可以执行任何必要的身份认证，并将身份认证证明发送回请求者。身份认证证明可以包括例如确认消息、安全密钥、唯一标识码、其他合适的证明或其任意组合。在一些实施例中，身份认证系统340可以耦接到区块链系统。由身份认证系统340连接的区块链系统可以是耦接至服务侧系统320的区块链系统330。可选地，尽管图3示出了将被耦接到区块链系统330的身份认证系统340，但是本公开考虑到身份认证系统340被耦接到不同的区块链系统的场景。身份认证系统340可以直接或经由中间系统(例如，BaaS云324)访问区块链330或另一个适当的区块链。

[0081] 身份认证系统340可以包括身份服务341，身份服务341可以在一个或多个服务器或云平台上实现。在一些实施例中，身份服务341可以被实现为服务侧系统320(例如，云324)的一部分。在其他实施例中，身份服务341可以在与服务侧系统320分离的系统上实现。身份服务341可以被配置为处理对身份认证的请求，以控制客户端侧应用342来收集身份数据，生成身份认证证明，在数据库343中存储或访问身份信息，执行区块链330上的一个或多个操作(例如，获得身份信息、存储身份认证证明)。在一些实施例中，身份认证系统340可以包括经由网络连接到身份服务341的客户端侧应用342。客户端侧应用342可以专用于身份认证，或者可以将身份认证作为其功能之一与一个或多个其他功能合并。客户端侧应用342可以被配置为收集与用户相关联的数据。客户端侧应用342可以进一步被配置为将收集到的数据与对应于用户声称的身份的预存储数据进行比较以认证用户的身份。在一些实施例中，身份认证系统340可以包括连接到身份服务341的数据库343。数据库343可以存储与多个个人或实体相关联的身份信息。身份信息可以包括例如身份认证证明、人的视觉特征、人的语音特征、人的指纹、人的签名、与身份相关联的密码、其他合适的身份信息或其任意组合。

[0082] 图4示出了根据一些实施例的与用于基于区块链的交叉实体认证的系统相关联的架构。在一些实施例中，该系统可以包括三种主要组件：一个或多个代理服务321、一个或多个解析器服务322、一个或多个信使服务325以及一个或多个区块链合约331。一个或多个代理服务321可以被配置为处理从用户接收的与去中心化标识和可验证声明有关的请求。一个或多个代理服务321可以管理用户端系统310上的账户信息与账户所有者的去中心化标识之间的映射关系。代理服务321可以包括用于从用户端系统310接收与去中心化标识相关的请求的去中心化标识代理服务API 410。取决于请求的性质，可以将其馈送到用于执行诸如创建和认证去中心化标识的操作的用户代理411，或者用于执行诸如发布可验证声明的操作的发布代理412。来自期望验证可验证声明的一方的请求可以被馈送到验证者代理413。一个或多个代理服务321还可提供用于存储一个或多个可验证声明的可验证声明存储库414。代理服务321也可以使用一个或多个存储器415以及一个或多个数据库416。代理服务321可耦接到KMS 323和BaaS云324。代理服务321可耦接到解析器服务322。

[0083] 在一些实施例中，代理服务321的一个或多个代理可以向与解析器服务322相关联

的去中心化标识解析器API 420发送一个或多个请求。解析器服务322可以被配置为处理代理服务321与区块链330之间的交互。解析器服务322可以执行诸如从区块链330获得数据、向区块链330添加数据、创建区块链合约331、将交易部署至区块链330以调用区块链合约331、其他合适的操作或其任意组合的操作。解析器服务322可以包括去中心化标识解析器421和可验证声明解析器422，所述去中心化标识解析器421被配置为管理存储在区块链330上的去中心化标识和去中心化标识文档，所述可验证声明解析器422被配置为管理基于区块链330创建的去中心化标识的可验证声明。解析器服务322还可包括用于从区块链331获得数据的监听器424。监听器424可以将获得的数据存储到数据库423。该数据可以由去中心化标识解析器421和可验证声明解析器422使用。去中心化标识解析器421、可验证声明解析器422和监听器424可以耦接到BaaS云324，用于与区块链330交互。

[0084] 在一些实施例中，信使服务325可以包括用于从用户侧系统310接收查询并向用户侧系统310提供通知的信使服务API 430。信使服务API430可以获得由去中心化标识解析器API 420放置在消息队列中的通知。消息队列可以被存储在数据库452中。信使服务API 430可以对所获得的通知进行过滤和分类，并将其存储在存储器451中。

[0085] 在一些实施例中，区块链330可包括用于管理去中心化标识和去中心化标识文档的一个或多个区块链合约(331a、331b、331c)，并且包括用于管理可验证声明的一个或多个合约(331d、331e、331f)。合约可由与区块链330相关联的一个或多个虚拟机执行，以执行诸如创建去中心化标识、存储去中心化标识文档、更新去中心化标识文档、存储与可验证声明相关联的信息、其他合适的操作或其任意组合的操作。

[0086] 图5示出了根据一些实施例的与用于实现与去中心化标识和可验证声明相关联的各种功能的示例的系统相关联的网络环境。网络环境的组件可以分类为三层510、520和530。在一些实施例中，底层或核心层510可以包括一个或多个区块链330，区块链330可以包括可以被执行以进行与去中心化标识和可验证声明有关的操作的一个或多个区块链合约(331g、331h、331i)。区块链330可以存储多个去中心化标识和与所述多个去中心化标识相对应的多个去中心化标识文档。区块链合约(331g、331h、331i)可以被配置为管理去中心化标识和去中心化标识文档之间的映射关系以及去中心化标识文档的创建和更改。区块链330可以对于一个或多个解析器(322a、322b)为可访问的，以进行与去中心化标识和可验证声明有关的操作。解析器(322a、322b)可被配置为基于输入的去中心化标识向外部系统提供例如搜索去中心化标识文档或去中心化标识文档中包含的数据的服务。一个或多个方法库511也可以对于外部系统为可采用的，以与区块链330交互。

[0087] 在一些实施例中，中间层或增强层520可以包括一个或多个用户代理411、一个或多个发布者代理412或一个或多个验证者代理413。中间层或增强层520可以还包括耦接至存储器451和数据库452的信使325。在一些实施例中，区块链330可以包括联盟区块链，该联盟区块链对于不是联盟区块链的共识节点的用户可以直接访问或不可以直接访问。用户代理411可以为普通用户提供与区块链进行交互的接口。在一些实施例中，用户代理411可以被配置为创建一个或多个去中心化标识、认证一个或多个去中心化标识、与一个或多个可验证数据注册表521或者一个或多个去中心化标识中心(DID hub)522交互、向去中心化标识的所有者发送通知、执行其他合适的功能或其任意组合。这里，去中心化标识中心522可以包括去中心化标识所有者在其中存储去中心化标识所有者的敏感数据的系统。所有者可

以准许某些其他实体(例如,发布可验证声明的机构)访问存储在去中心化标识中心522中的数据。可验证数据注册表521可以包括用于存储和管理发布给去中心化标识所有者的可验证声明的可验证声明存储库。发布者代理412可以包括一个或多个API(例如,REST API)或SDK。发布者代理412可以被配置为发布一个或多个可验证声明、撤回一个或多个可验证声明、检查和检验现有的可验证声明、发布可验证声明的模板、维护可验证声明的模板、执行其他合适的操作或它们的任意组合。验证者代理413可以包括一个或多个API(例如,REST API)或SDK,并且被配置为验证可验证声明或执行一个或多个其他合适的操作。在一些实施例中,层520还可包括一个或多个代码库(例如,去中心化标识解析库523、去中心化标识认证库524),所述代码库可被采用并可被用于与去中心化标识解析器322交互或直接与区块链330交互。代码库可被打包到一个或多个SDK中并可被用于执行例如去中心化标识认证、与区块链300的交互或与区块链合约331的对接的功能。发布者代理412和验证者代理413可以由网络环境中与去中心化标识和可验证声明相关联的关键参与者(例如,能够执行了解您的客户(KYC)认证或为用户背书的实体、或者发布或验证可验证声明的实体(例如,政府机构、银行、金融服务提供商))使用。关键参与者可以提供第三方服务,该第三方服务可以通过与发布者代理412、可验证代理413或网络环境的其他合适组件的连接来集成。

[0088] 在一些实施例中,上层或扩展层530可以包括与去中心化标识和可验证声明有关的一个或多个外部服务或应用。服务或应用可以包括一个或多个发布者应用531、一个或多个验证者应用532、身份管理应用533、服务应用534、一个或多个其他合适的服务或应用或者其任意组合。发布者应用531可以与为用户发布由实体签名或背书的可验证声明的实体(例如,政府机构、银行、信贷机构)相对应。发布者应用531可以在用户端系统310上操作。发布者应用531可以包括发布者可验证声明管理器服务,该服务可以允许发布者管理发布的可验证声明、维护其状态(例如,有效性)或执行其他合适的操作。发布者应用531可以通过与发布者代理412或者一个或多个代码库523和524连接或对接来与层510和520交互。验证者应用532可以与需要验证可验证声明以确定用户的信息(例如,身份、年龄、信用评分)的实体(例如,服务提供商、信用发布者)相对应。验证者应用532可以在用户端系统310上操作。验证者应用532可以通过与验证者代理413或者一个或多个代码库523和524连接或对接来与层510和520交互。身份管理应用533可以安装在与用户相关联的客户端设备或终端上。用户可以是去中心化标识所有者,去中心化标识所有者可以是个人、企业、组织、应用或任何其他合适的实体。身份管理应用533可以允许用户管理与去中心化标识、原始数据或可验证声明相关联的加密密钥对,以从用户代理411接收通知、认证去中心化标识、准予对数据的访问权、使用可验证声明、执行其他合适的操作或其任意组合。身份管理应用533可以通过与用户代理411连接或对接来与层510和520交互。服务应用534也可以耦接到用户代理411,并且被配置为管理与一个或多个用户或账户的去中心化标识或可验证声明有关的功能。服务应用534也可以耦接到信使325,并且被配置为发送对一个或多个去中心化标识的查询并获得相应的通知。

[0089] 图6至图10示出了由一个或多个用户侧系统310、一个或多个服务侧系统320、一个或多个解析器322、一个或多个云324、一个或多个信使或者一个或多个区块链系统330执行的与去中心化标识或可验证声明相关联的示例性操作。在一些实施例中,用户侧系统310可以通过与服务侧系统320(例如,包括例如去中心化标识解析器322)以及存储去中心化标识

和去中心化标识文档的区块链330对接来管理一个或多个去中心化标识或者一个或多个可验证声明。用户侧系统310可以使用一个或多个SDK 312来管理与和去中心化标识相关联的方法可兼容的去中心化标识。SDK 312可以与用户侧系统310使用的一个或多个应用集成。用户侧系统310还可以与用于存储可验证声明的一个或多个服务端点、用于存储可验证声明的状态信息的一个或多个服务端点、用于认证去中心化标识的一个或多个服务端点、其他合适的系统或其任意组合进行对接。

[0090] 图6A和图6B示出了根据一些实施例的用于创建去中心化标识的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式，所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。此外，可以将在方法6A或6B中执行的一个或多个步骤替代为在另一方法中执行的一个或多个合适的步骤。执行如图6A和图6B所示的某些步骤的设备或系统也可以由其他合适的设备或系统替代以执行相同的步骤。合适的设备或系统可以包括具有相似功能的子系统、父系统或对应系统。作为示例，由图6A中的用户侧系统310执行的一个或多个步骤可以由图6B中的身份管理应用533执行，反之亦然。作为另一示例，服务侧系统320执行的一个或多个步骤可以由解析器322执行，解析器322可以是服务侧系统320的子系统。尽管本文描述了执行特定步骤的特定设备或系统，但是本文考虑到执行用于创建去中心化标识的任何适当步骤的任何适当设备或系统。

[0091] 在一些实施例中，如图6A所示，用户侧系统310可以为其一个或多个用户中的每个用户创建去中心化标识。用户侧系统310可以控制与去中心化标识相关联的加密密钥对，并使用该加密密钥对执行与去中心化标识有关的各种操作，包括例如对区块链交易进行签名、对可验证声明进行签名或对去中心化标识进行认证。用户侧系统310可以包括用于执行各种操作的SDK312。SDK 312还可以管理用户侧系统310和服务侧系统320提供的各种接口之间的各种交互。所述接口可以包括用于分配去中心化标识的接口、用于创建去中心化标识文档的接口、用于将去中心化标识文档添加到区块链330的接口、用于搜索去中心化标识文档的接口、其他合适的接口或其任意组合。可以通过例如软件程序和网络端口来提供接口。响应于在接口处接收到的请求，服务侧系统320可以执行相应的操作，并且经由接口将结果返回到适当的外部系统。图6A中示出的方法可以从步骤602开始，其中，用户侧系统310的服务器311可以获得对将为其获得去中心化标识的用户的身份认证。身份认证可以已经由身份认证系统340或另一合适的系统执行。在其他实施例中，用户侧系统310可能已经从身份认证系统340获得了用户的身份认证证明。用户的身份认证证明可以包括实名认证的证明(例如，基于政府颁发的身份文件)、真人认证的证明(例如，基于用户基于身份证系统340的指令而拍摄的照片)、其他身份认证的证明或其任意组合。用户侧系统310还可以生成或检索包括公钥和私钥的加密密钥对以用于创建去中心化标识。

[0092] 在步骤604，服务器311可以调用SDK 312的功能以创建新的去中心化标识。服务器311可以向SDK 312提供各种信息以调用功能。该信息可以包括与要创建的去中心化标识相对应的用户的账户标识、针对该去中心化标识生成的加密密钥对的公钥或私钥、与要创建去中心化标识相关联的一个或多个服务的规范、与用于返回确认或其他通信的服务器311相关联的回调网络地址、其他合适的信息或其任意组合。账户标识可以对应于具有与用户侧系统310相关联的实体的用户的企业或服务账户。在步骤606，用户侧系统310可以使用SDK 312向服务侧系统322发送用于创建新的去中心化标识的请求。服务侧系统320由此可

以获得用于创建去中心化标识的请求。该请求可以包括加密密钥对的公钥，其可以已经由用户侧系统310生成。图6A示出了从与第一实体(例如，用户侧系统310)相关联的计算设备接收用于创建去中心化标识的请求以代表第二实体(例如，用户)创建去中心化标识的方案。除了公钥之外，该请求还可以包括与第二实体(例如，用户)相关联的账户标识、与第二实体(例如，用户)相关联的简档信息、关于与去中心化标识相关联的一个或多个服务的信息、与第一实体(例如，用户侧系统310)或第二实体(例如，用户)相关联的回调地址、其他合适的信息或其任意组合。在图6B中示出了替代方案，其中用于创建去中心化标识的请求是直接从与拥有该去中心化标识的实体相关联的计算设备接收的。在一些实施例中，该请求可以是送至服务侧系统所提供的一个或多个接口的应用编程接口(API)消息的形式。

[0093] 响应于从用户侧系统310获得的请求，服务侧系统320可以基于请求中的公钥来创建与区块链330相关联的区块链账户。在步骤608，服务侧系统320可以向区块链系统330发送用于创建新区块链账户的请求。在此，该请求可以以一个或多个区块链交易的形式被直接发送到区块链330的一个或多个区块链节点或经由BaaS云324或与区块链330相关联的其他合适的接口系统被发送。在发送请求之后，在步骤610，服务侧系统320可以从区块链330获得关于已经创建了新区块链账户的表明。区块链账户可以与区块链330上的地址相关联。服务侧系统320可以获得与新创建的区块链地址相关联的信息。

[0094] 然后，服务侧系统320可以基于与区块链账户相关联的信息来创建去中心化标识。在步骤612，服务侧系统320可以基于区块链账户为用户分配去中心化标识。服务侧系统320可以通过确定去中心化标识和与区块链330相关联的任何现有去中心化标识不重复来确保所分配的去中心化标识是唯一的。根据这一实施例，在构建或上传与去中心化标识相对应的去中心化标识文档之前，可以分配该去中心化标识并确定该去中心化标识是唯一的。这可以有效地防止由于去中心化标识的重复而导致的上传去中心化标识文档的潜在失败尝试，从而节省了创建和上传去中心化标识文档的处理和计算工作量。服务侧系统320可以通过存储账户标识和所创建的去中心化标识之间的映射关系，来将去中心化标识与用户账户和用户侧系统310相关联。服务侧系统320可以进一步存储去中心化标识的状态。作为示例并且不作为限制，去中心化标识的状态可以表明去中心化标识是否已经被注册到区块链330，或者对应的去中心化标识文档是否已经被存储在区块链330中。在步骤614，服务侧系统320可以将消息发送回与用户侧系统310相关联的SDK 312。该消息可以包括与新创建的去中心化标识相关联的信息。

[0095] 在步骤616，用户侧系统310可以使用SDK 312来创建与去中心化标识相关联的去中心化标识文档。该去中心化标识文档可以包括与去中心化标识相关联的信息，诸如与去中心化标识相关联的公钥、与去中心化标识相关联的认证信息(例如，一个或多个认证方法)、与去中心化标识相关联的授权信息(例如，与控制者相关联的去中心化标识)、与去中心化标识相关联的委托信息(例如，一个或多个委托方法)、与去中心化标识相关联的一个或多个服务(例如，一个或多个类型的服务，例如凭证存储库服务和代理服务)、与去中心化标识相关联的一个或多个服务端点(例如，一个或多个服务端点中的每一个的URI)、其他合适的信息或其任意组合。当服务器311在步骤604调用SDK 312时，SDK312可以基于从服务器311接收的信息来创建去中心化标识文档。用户侧系统310可以进一步使用SDK 312来创建用于将去中心化标识文档添加到区块链330的区块链交易。在此阶段创建的区块链交易可

能是或不是完整且有效的。在一些实施例中，由用户侧系统310创建的区块链交易可能缺少与区块链330相关联的信息、与区块链330相关联的一个或多个区块链合约、数字签名、其他合适的信息或其任意组合。

[0096] 在步骤618，SDK 312可以将去中心化标识文档发送到服务侧系统320。如果SDK 312已经创建了区块链交易，则其可以将区块链交易发送到可以包括去中心化标识文档的服务侧系统320。在该步骤，SDK 312可以请求服务侧系统320提供与完成但未签名的区块链交易相关联的哈希值，以将去中心化标识文档添加到区块链330。在从用户侧系统310获得与去中心化标识相对应的去中心化标识文档之后，服务侧系统320可以生成或完成用于将去中心化标识文档添加到区块链330的区块链交易。区块链交易可以调用先前部署在区块链330上的用于管理去中心化标识和对应的去中心化标识文档之间的关系的区块链合约331。调用的区块链合约331可以包括一个或多个接口，例如用于将一个或多个去中心化标识文档添加到区块链330的接口。区块链合约331的一个或多个接口可以包括与区块链合约331的一个或多个可执行功能相对应的可执行代码。为了生成区块链交易，服务侧系统320可以在区块链交易中包括一个或多个信息项。一个或多个信息项可以包括与区块链330相关联的地址、与区块链交易相关联的区块链合约331的标识、与区块链交易相关联的区块链合约331的版本信息、与区块链交易相关联的区块链合约331的一个或多个接口的信息、其他合适的信息或其任意组合。由服务侧系统320添加到区块链交易的信息可以包括与区块链系统330相关联的公共或其他合适的信息、区块链330上的区块链合约、或用于创建有效的区块链交易所需的其他信息。服务侧系统320可以自动增添这样的信息，并且减轻用户侧系统310保持跟踪这样的信息的负担。这可以降低用户侧系统310向区块链330添加去中心化标识文档所需的技术能力。

[0097] 由服务侧系统320基于从用户侧系统310接收的去中心化标识文档生成的区块链交易在此阶段可以是未签名的。服务侧系统320可以根据区块链系统330可接受的哈希函数来确定未签名的区块链交易的哈希值。在步骤620，服务侧系统320可以将未签名的区块链交易的哈希值发送到用户侧系统310。然后，在步骤622，与用户侧系统310相关联的SDK312可以在哈希值上创建数字签名。作为示例，可以通过使用与从服务器311接收的与去中心化标识的所有者相关联的加密密钥对的私钥对哈希值进行加密来创建数字签名。在步骤624，SDK 312可以将数字签名返回给服务侧系统320，从而授权区块链交易。在步骤624从用户侧系统310接收到数字签名之后，服务侧系统320可以将数字签名添加到未签名的区块链交易，以生成或完成用于将去中心化标识文档添加到区块链的区块链交易。然后，在步骤626，服务侧系统320可以将区块链交易发送到与区块链330相关联的一个或多个区块链节点以添加到区块链。在步骤628，服务侧系统320可以从区块链330获得确认去中心化标识文档在区块链330中的成功存储的信息。在步骤630，服务侧系统320可以将确认消息返回给SDK312。确认消息可以包括已经创建的去中心化标识和去中心化标识文档。在步骤632，SDK 312可以将去中心化标识和去中心化标识文档提供给服务器311。在此，SDK 312可以基于与从服务器311接收的回调地址相关联的信息来发送与去中心化标识和去中心化标识文档相关联的信息。在步骤634，服务器311可以向用户发送确认去中心化标识和对应的去中心化标识文档成功创建的通知。

[0098] 在一些实施例中，如图6B所示，用户可以使用服务侧系统320提供的一个或多个接

口为其自身创建去中心化标识，而无需使用用户侧系统310提供的服务。用户可以包括个人、企业、组织、其他合适的实体或其任意组合。作为示例，用户可以使用身份管理应用533或另一合适的软件或硬件系统来与服务侧系统320交互。身份管理应用533可以由与服务侧系统320相关联的实体开发，并被提供用于安装在与用户相关联的客户端设备上。身份管理应用533可以被配置为管理与服务侧系统320提供的各种接口的交互。图6B所示的方法可以从步骤642开始，用户可以向身份管理应用533提供一个或多个输入，以便请求为用户创建去中心化标识。身份管理应用533可以请求来自用户的输入，以验证用户的真实身份。可选地，身份管理应用533可以先前已经获得与用户相关联的身份认证信息，并且可以被配置为例如在用户登录身份管理应用533时检索这样的信息。

[0099] 在步骤644，身份管理应用533可以为用户生成加密密钥对。加密密钥对可以包括用于创建与用户相关联的去中心化标识的公钥和私钥。在步骤646，身份管理应用533向服务侧系统320发送用于创建新的去中心化标识的请求。在步骤648，服务侧系统320可以向区块链系统330发送用于创建新区块链账户的请求。在此，该请求可以以一个或多个区块链交易的形式被直接发送到区块链330的一个或多个区块链节点，或者经由BaaS云324或与区块链330相关联的其他合适的接口系统被发送。然后，在步骤650，服务侧系统320可以从区块链330获取表明已经创建了新区块链账户的信息。区块链账户可以与区块链330上的地址相关联。服务侧系统320获得的信息可以包括与新创建的区块链地址相关联的信息。它可以包括足以创建去中心化标识的信息。在步骤652，服务侧系统320可以根据与区块链账户相关联的信息向用户分配唯一的去中心化标识。在步骤654，服务侧系统320可以将消息发送回身份管理应用533。该消息可以包括与新创建的去中心化标识相关联的信息。

[0100] 在一些实施例中，可以创建去中心化标识文档并将其存储在区块链330上。在步骤656，身份管理应用533可以生成去中心化标识文档，并将与新创建的去中心化标识相关联的公钥以及其他合适的信息(例如，认证信息)添加到去中心化标识文档。身份管理应用533可以将与一个或多个服务端点相关联的信息(例如，与认证服务端点相关联的信息、与可验证声明存储库相关联的信息)添加到去中心化标识文档。认证服务端点和可验证声明存储库可以作为服务侧系统320的一部分来提供，或者可以由第三方系统来提供。然后，在步骤658，身份管理应用533可以生成用于将去中心化标识文档添加到区块链330的一个或多个区块链交易。在步骤660，身份管理应用533可以生成区块链交易的哈希值，并使用与去中心化标识相关联的私钥生成交易的数字签名。可选地，身份管理应用533可以以类似于图6A的步骤618、620和622所示的用户侧系统310和服务侧系统320之间交互的方式与服务侧系统320交互，以生成区块链交易并对区块链交易签名。在步骤662，身份管理应用533可以将去中心化标识文档以及区块链交易发送到服务侧系统320，以发送到区块链系统330。在步骤664，服务侧系统320可以将一个或多个交易发送到区块链系统330。一个或多个交易可以调用用于管理区块链330上的去中心化标识和去中心化标识文档的区块链合约331。在步骤666，服务侧系统320可以从区块链330获得表明去中心化标识文档已经被成功存储的信息。在步骤668，服务侧系统320可以将确认转发至身份管理应用533。在步骤670，身份管理应用533可以提供包括与所创建的去中心化标识和去中心化标识文档相关联的信息的通知，以显示给用户。

[0101] 图7示出了根据一些实施例的用于使用去中心化标识认证服务来认证去中心化标

识的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式，所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。在一些实施例中，拥有去中心化标识的用户可以使用由商业实体提供的去中心化标识认证服务来实现对其去中心化标识所有权的认证。所有者可以将与去中心化标识对应的公钥-私钥对信托给商业实体以进行存储。所有者可以提供去中心化标识认证服务的网络位置(例如，由URL标识)作为去中心化标识认证的服务端点。去中心化标识认证服务的位置标识可以被包括在与去中心化标识相关联的去中心化标识文档的“服务”文件中。

[0102] 在一些实施例中，验证者532(例如，需要验证客户信息的服务提供商)可以使用SDK 312来发起去中心化标识认证处理。在步骤702，验证者532可以获得由声明的所有者提供的去中心化标识。在步骤704，验证者532可以调用SDK 312以创建去中心化标识认证质询。验证者532可以将待认证的去中心化标识和要向其发送对质询的响应的网络地址(例如，URL)输入到SDK 312。在步骤706，SDK 312可以将对与待认证的去中心化标识相关联的去中心化标识文档的查询发送到解析器322。在步骤708，解析器322可以制定调用用于管理去中心化标识的区块链合约331的区块链交易，并将该区块链交易发送到与区块链330相关联的一个或多个区块链节点以供执行。结果，解析器322可在步骤710获得与去中心化标识相对应的去中心化标识文档，并在步骤712将其转发至SDK 312。在步骤714，验证者532可以使用SDK 312基于获得的去中心化标识文档来创建去中心化标识认证质询。在一些实施例中，去中心化标识认证质询可以包括通过使用与记录在去中心化标识文档中的与去中心化标识相关联的公钥对原始文本进行加密而创建的密文。质询还可以包括要向其发送响应的网络地址。在步骤716，验证者532可以从去中心化标识文档获得与去中心化标识的认证服务端点相关联的信息。在步骤718，验证者532可以使用SDK 312将质询发送到与去中心化标识相关联的去中心化标识认证服务。

[0103] 在一些实施例中，在从验证者532获得去中心化标识认证质询之后，在步骤720，去中心化标识认证服务可以从所有者获得对于这种认证请求的同意。如果所有者提供了对于身份认证的同意或许可，则在步骤722，去中心化标识认证服务可以调用它的SDK 312版本以创建对去中心化标识认证质询的响应。在一些实施例中，对去中心化标识认证质询的响应可以包括明文，该明文是使用与去中心化标识相关联的私钥对质询中的密文进行解密的结果。在步骤724，SDK 312可以将响应返回至去中心化标识认证服务，然后在步骤726，去中心化标识认证服务可以将响应发送到由验证者432提供的网络地址。在接收到对去中心化标识认证质询的响应之后，在步骤728，验证者532可以调用它的SDK 312以检查响应。在步骤730，SDK 312可以确定响应是否证明提供去中心化标识的用户是该去中心化标识的所有者。在一些实施例中，SDK 312可以通过将响应中的解密文本与用于创建去中心化标识认证质询的原始文本进行比较来检查响应。如果确定响应正确，则在步骤732，SDK 312可以向验证者532返回表明去中心化标识是用户身份的有效证明的消息。在步骤734，验证者532可以将去中心化标识的有效性通知给用户。

[0104] 图8示出了根据一些实施例的使用身份管理应用来认证去中心化标识的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式，所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。在一些实施例中，用户可以使用终端来管理去中心化标识，该终端可以包括身份管理应用或另一合适的应用。该应用可以包括SDK 312的版

本。在此示例中，用户可能需要来自服务提供商(即验证者)的服务，该服务提供商需要验证用户拥有特定的去中心化标识以便提供其服务。用户可以向验证者发送服务请求。服务请求可以是HTTP请求的形式。

[0105] 在步骤802，用户可以调用身份管理应用533以提供用于服务请求的认证信息。用户可以将原始服务请求作为输入提供给包括在身份管理应用533中的SDK 312。在步骤804，SDK 312可以使用与去中心化标识相关联的加密密钥对中的私钥对原始服务请求的内容进行签名。SDK312可用于将原始服务请求的去中心化标识和数字签名添加到原始服务请求，以创建签名的服务请求。在原始服务请求是HTTP请求的情况下，SDK 312可以将去中心化标识和数字签名添加到HTTP请求的报头。在步骤806，SDK 312可以将签名的服务请求发送到验证者532。

[0106] 在一些实施例中，在步骤808，验证者532可以调用其SDK 312版本以认证包括在签名的服务请求中的去中心化标识。在步骤810，SDK312可以获得包括在签名的服务请求中的去中心化标识和数字签名。在签名的服务请求是HTTP请求的情况下，可以从HTTP请求的报头获得去中心化标识和数字签名。在步骤812，SDK 312可以将对与待认证的去中心化标识相关联的去中心化标识文档的查询发送到解析器322。在步骤814，解析器322可以制定调用用于管理去中心化标识的区块链合约331的交易，并将该交易发送到与区块链330相关联的一个或多个区块链节点以供执行。结果，解析器322可在步骤816获得与去中心化标识相对应的去中心化标识文档，并在步骤818将其转发至SDK 312。在步骤820，与验证者532相关联的SDK 312可以基于获得的去中心化标识文档检查签名的服务请求，以确定它是否来自去中心化标识的所有者。在一些实施例中，SDK 312可以使用从去中心化标识文档获得的公钥对数字签名进行解密，并对照初始服务请求的哈希值来检查解密结果，以确定公钥是否与用于创建签名的服务请求中的数字签名的密钥相关联。如果是，则SDK 312可以确定来自用户的服务请求是有效的。然后，在步骤822，SDK 312可以将服务请求发送到验证者532以供处理。在步骤824，验证者532可以处理服务请求并向用户提供适当的服务。然后，在步骤826，验证者532可以向用户发送响应以确认所请求的服务的完成。

[0107] 图9示出了根据一些实施例的用于发布可验证声明的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式，所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。在一些实施例中，发布者531可以向用户发布可验证声明。可验证声明可以用作对发布者531背书的用户的某些事实或特征的证明。

[0108] 在步骤902，发布者531可以获得与用户相关联的去中心化标识以及要包括在可验证声明中的事实的证明。这里，要包括在可验证声明中的事实的证明可以基于用户向发布者531提交的材料、发布者531从第三方系统获得的信息或数据、事实的本人验证、其他合适的证明来源或其任意组合。在获得去中心化标识和证明之后，在步骤904，发布者531可以调用与可验证声明的创建相关联的SDK 312以发起用于创建可验证声明的处理。来自发布者531的消息可以包括关于用户的被证明的事实的陈述或声明。在步骤906，SDK 312可以使用与发布者531相关联的加密密钥对来创建包括声明的可验证声明文档。在一些实施例中，可验证声明可以包括基于与发布者531相关联的私钥创建的数字签名。在步骤908，SDK 312可以更新可验证声明的本地存储状态。

[0109] 在步骤910，SDK 312可以将对与被发布了可验证声明的去中心化标识相关联的去

中心化标识文档的查询发送到解析器322。在步骤912,解析器322可以制定调用用于管理去中心化标识的区块链合约331的交易,并将该交易发送到与区块链330相关联的一个或多个区块链节点以供执行。结果,解析器322可在步骤914获得与去中心化标识相对应的去中心化标识文档,并在步骤916将其转发至SDK 312。在步骤918,SDK 312可以识别与用户的去中心化标识相关联的用于存储可验证声明的可验证声明服务端点。可验证声明服务端点可以与去中心化标识的用户或所有者使用的可验证声明存储库414相对应。然后,在步骤920,发布者可以使用SDK 312将可验证声明发送到可验证声明存储库414以进行存储。可验证声明还可以包括与可验证声明状态服务端点相关联的信息,该可验证声明状态服务端点可以存储并提供可验证声明的状态信息。在一些实施例中,该信息可以包括由发布者531用来保存可验证声明的状态的发布代理服务的网络地址(例如,URL)。可验证声明状态服务端点可以或可以不与可验证声明存储库414相关联。SDK 312可以将新生成的可验证声明的当前状态提供给可验证声明状态服务端点以进行存储。可验证声明的状态可以存储在区块链上。

[0110] 图10示出了根据一些实施例的用于验证可验证声明的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式,所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。在一些实施例中,用户可以向另一方(例如,验证者532)提供可验证声明以证明可验证声明中陈述的事实。可以在验证者532已经验证用户是与可验证声明相关联的去中心化标识的所有者之后提供可验证声明。

[0111] 在步骤1002,验证者532可以调用包括与可验证声明验证相关联的代码库的SDK 312以验证可验证声明。SDK 312可以从可验证声明(例如,在“凭证状态”字段中)识别与用于可验证声明的可验证声明状态服务端点相关联的信息。可验证声明状态服务端点可以与发布者531相关联。在步骤1004,SDK 312可以向发布者531发送对可验证声明的状态的查询。作为响应,在步骤1006,发布者531可以调用SDK 312以获得可验证声明的状态。SDK 531可以获得可验证声明的状态。作为示例,在步骤1008,SDK 312可以确定可验证声明具有有效状态并且可以将信息返回给发布者531。然后,在步骤1010,发布者可以将有效状态信息返回给与验证者532相关联的SDK 312。

[0112] 验证者532可以获得与可验证声明的发布者531相关联的标识。例如,标识可以是发布者531的去中心化标识。在步骤1012,SDK 312可以将对与可验证声明的发布者531的去中心化标识相关联的公钥的查询发送到解析器322。在步骤1014,解析器322可以制定调用用于管理去中心化标识的区块链合约331的交易,并将该交易发送到与区块链330相关联的一个或多个区块链节点以供执行。结果,解析器322可以在步骤1016获得与去中心化标识相对应的公钥,并且在步骤1018将其转发到与验证者532相关联的SDK 312。在步骤1020,与验证者532相关联的SDK 312可以基于其中包括的数字签名以及与可验证声明的发布者531相关联的公钥来验证可验证声明。在步骤1022,如果可验证声明被验证,SDK 312可以将确认发送至验证者532。

[0113] 图11至图15示出了与由一个或多个用户侧系统310、一个或多个服务侧系统320、一个或多个代理321、一个或多个解析器322、一个或多个云324、一个或多个区块链系统330、一个或多个KMS或其他合适的系统、应用、服务执行的与去中心化标识或可验证声明相关联的示例性操作。在一些实施例中,用户侧系统310可以通过经由一个或多个API接口(例如,REST API)与集成了一个或多个上述组件的在线平台进行交互来管理一个或多个去中

心化标识或可验证声明。用户侧系统310可以将诸如加密密钥对的机密信息信托给在线平台以进行安全保存。

[0114] 图11示出了根据一些实施例的用于使用代理服务创建去中心化标识的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式，所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。在一些实施例中，与实体相关联的用户端系统310可以使用一个或多个代理服务321来为该实体的一个或多个用户创建一个或多个去中心化标识，并将该去中心化标识与由实体维护的内部账户或标识(例如，服务ID)相关联。为了为其用户创建去中心化标识，该实体可能已被在线平台认证为可信实体，并且可能已承诺提供真实信息。在一些实施例中，该实体可能已经由引导程序(bootstrap)发布者去中心化标识发布了可验证声明，以证明该实体已由权威实体认证。实体可能需要认证其用户的身份。用户端系统310可以使用一个或多个KMS 323和它们提供的安全环境(例如，TEE)来管理与所创建的去中心化标识相关联的加密密钥并将加密密钥映射到实体所维护的内部账户或标识。借助于代理服务321，用户端系统310可以使用与去中心化标识相关联的服务，而无需保留去中心化标识的记录。替代地，它可以简单地经由与代理服务321相关联的一个或多个接口来提供其用于识别去中心化标识的内部账户信息或标识信息。

[0115] 在一些实施例中，用于管理去中心化标识的在线平台可以接收用于创建去中心化标识的请求。该请求可以来自代表第二实体的第一实体，用于为第二实体创建去中心化标识。在图11所示的示例中，实体(例如，第一实体)可以为用户(例如，第二实体)创建去中心化标识，该用户可以具有商业实体的账户。在一些实施例中，实体可以在为用户创建去中心化标识之前认证用户的身份。例如，在图11的步骤1102，与实体相关联的用户端系统310的服务器311可以执行身份认证或以其他方式获得用户的身份认证信息。该实体可能先前验证了用户的身份，并且可以在数据库中维护这样的信息。在步骤1104，服务器311可以检索这样的信息。然后，服务器311可以将用于创建去中心化标识的请求发送到与用户代理411相关联的代理服务API 410，用户代理411与在线平台相关联。该请求可以包括与用户相对应的账户标识。该请求可以采取API消息的形式。在步骤1106，代理服务API 410可以将请求发送到用户代理411以创建去中心化标识。

[0116] 在步骤1108，用户代理411可以检查对于所需信息的请求。在一些实施例中，为了创建用户的去中心化标识，可以要求实体具有其自身的现有去中心化标识。用户代理411可以检查该请求以确定该请求的发送者具有现有去中心化标识并且确定与该发送者相关联的去中心化标识。在一些实施例中，可能需要实体为用户提供身份认证证明。身份认证证明可以包括真人认证的证明、实名认证的证明、其他合适的认证证明或其任意组合。例如，实名认证的证明可以基于用户的官方标识(例如，政府颁发的ID)。示例性证明可以例如是通过将哈希函数(例如SHA-256)应用于ID类型、ID号和用户编号的组合而创建的数字。这样的证明可以在维护用户保密的敏感信息的同时确保与特定用户的唯一对应。

[0117] 在一些实施例中，用户代理411可以确定用于创建去中心化标识的请求是否包括身份认证证明。身份认证证明可以包括实名认证的证明、真人认证的证明、其他合适的身份认证方法的证明或其任意组合。如果用户代理411确定该请求确实包括身份认证证明，则用户代理411可以基于该确定来接受该请求。如果用户代理411确定用于创建去中心化标识的请求不包括身份认证证明，则用户代理411可以拒绝该请求。可选地，用户代理411可以向服

务器311发送对身份认证证明的请求。用户代理411然后可以从服务器311接收所需的身份认证证明。用户代理411也可以使用其他方法来获得用户的身份认证。

[0118] 在步骤1109，用户代理411可以获得与要创建的去中心化标识相对应的用户的身份认证证明。在一些实施例中，用户代理411可以基于接收到的请求或从服务器311接收到的其他信息而直接获得身份认证证明。用户侧系统310可能已经通过执行身份认证或通过使用身份服务341获得了证明。用户侧系统310可以在用于创建去中心化标识的请求中包括身份认证证明，或者包括用于获得证明的方式(例如，链接)。在一些实施例中，用户侧系统310可以将发送用于创建去中心化标识的请求的功能委托给身份服务341。服务器311可以向身份服务341发送与打算为其创建去中心化标识的一个或多个用户相关联的信息。身份服务341可以对用户执行身份认证，或者确认已经成功完成了对用户的身份认证。身份服务341可以基于从服务器311接收的信息来创建用于创建去中心化标识的一个或多个请求，该请求包括用户的身份认证证明。在一些实施例中，响应于来自身份服务341的请求而创建的去中心化标识文档可以包括表明该去中心化标识是由身份服务341基于身份认证创建的字段(例如，“创建者”字段)。在一些实施例中，在由身份服务341基于身份认证创建去中心化标识之后，身份服务341可以向去中心化标识发布可验证声明，以证明去中心化标识的所有者的真实身份。在一些实施例中，在另一发布者向去中心化标识的所有者发布可验证声明之前，该另一发布者可以要求身份服务341发布的可验证声明作为去中心化标识所有者的身份认证证明。

[0119] 在一些实施例中，用户代理411可以通过使用身份服务341独立地获得身份认证证明。在一些实施例中，身份服务341可以与被服务侧系统320信任的实体相对应。实体可以对用户执行身份认证(例如，实名认证、真人认证)。身份认证可以包括：收集与对应于一个身份的个人相关联的各种身份信息(例如，姓名、出生日期、地址、外貌特征、指纹)，并将收集到的信息与权威机构源(例如，政府机构)维护的信息进行比较。在成功认证了个人的身份之后，身份服务341可以将成功认证的记录(例如，身份认证证明)和与该个人相关联的身份信息与该个人的标识(例如账户或服务ID)相关联地存储。身份服务341可以将身份信息和身份认证证明存储在数据库343中。可选地，身份服务341可以将身份信息和身份认证证明存储在区块链330中。在一些实施例中，身份服务341可以创建用于将身份信息存储在区块链330中的一个或多个区块链交易，并将该一个或多个区块链交易发送至与区块链330相关联的一个或多个区块链节点。可选地，身份服务341可以经由例如BaaS云324与区块链330交互。身份服务341可以向BaaS云324发送将身份信息和身份认证证明存储在区块链330上的请求。用户代理411可以向身份服务341发送针对用户的身份认证证明的请求。用户可以对应于用于创建去中心化标识的请求。身份服务341可发送回所请求的身份认证证明。

[0120] 在一些实施例中，用户代理411可以响应于请求而获得去中心化标识，而无需获得身份认证证明。可以将以这种方式创建的去中心化标识分配为“认证中”的状态。其可以被映射到虚拟账户标识。该状态可以在与去中心化标识对应的去中心化标识文档中表示，可以保存在存储去中心化标识的状态信息的系统中，或者可以由用户代理411保存。可以限制关于具有这种状态的去中心化标识可以执行的操作。例如，可以禁止去中心化标识的所有者发布可验证声明或被发布可验证声明。在向用户代理411提供身份认证证明之后，可以去除“认证中”的状态。身份服务341可以主动地或在用户侧系统310或用户代理411的请求下

向用户代理411发送身份认证证明。在接收到证明之后，用户代理411可以更新与去中心化标识相关联地存储的状态信息。此外，用户代理411可以存储去中心化标识和与已经认证其身份的用户相关联的账户标识之间的映射关系。参照图15至图18描述关于身份认证的进一步细节。

[0121] 在获得身份认证证明之后，在步骤1110，用户代理411可创建与用户的身份认证证明相对应的密钥别名。在一些实施例中，用户代理411可响应于接收到请求而获得加密密钥对的公钥。公钥以后可以用作创建去中心化标识的基础。在一些实施例中，用户代理411可以从KMS 323获得公钥。在步骤1112，用户代理411可以向KMS 323发送用于生成和存储加密密钥对的请求。KMS 323可以生成加密密钥对。在一些实施例中，KMS 323可促使在与KMS 323相关联的TEE中生成加密密钥对。在密钥对生成之后，KMS 323可以从TEE获得公钥和加密的私钥。在步骤1114，KMS 323可以向用户代理411发送公钥。

[0122] 在一些实施例中，在线平台可以基于公钥获得去中心化标识。在步骤1116，用户代理411可以将用于创建新的去中心化标识的请求发送至解析器322。该请求可以包括公钥。作为响应，解析器322可以基于公钥生成用于创建去中心化标识并将与该去中心化标识相关联的去中心化标识文档添加到区块链的一个或多个区块链交易。可选地，去中心化标识解析器可以将请求发送到BaaS云324以生成这种交易。例如，在步骤1118，解析器322可以向区块链系统330发送创建新的区块链账户的请求。在此，该请求可以以一个或多个区块链交易的形式被直接发送到区块链330的一个或多个区块链节点，或者被发送到BaaS云324或与区块链330相关联的其他合适的接口系统。区块链交易可以调用被配置用于管理去中心化标识的一个或多个区块链合约。响应于来自解析器322的请求，在步骤1120，去中心化标识解析器可以从区块链330或云324获得成功创建新的区块链账户的表明。区块链账户可以与区块链330上的地址相关联。由解析器322获得的信息可以包括与新创建的区块链地址相关联的信息。它可以直接包括新创建的去中心化标识或至少足以构成去中心化标识的信息。在步骤1122，解析器322可以将消息发送回用户代理411。该消息可以包括与新创建的去中心化标识相关联的信息。

[0123] 在一些实施例中，可以创建去中心化标识文档并将其存储在区块链330中。在步骤1124，用户代理411可以生成去中心化标识文档，并将与新创建的去中心化标识相关联的公钥以及认证信息添加到去中心化标识文档。在步骤1126，用户代理411可以将与一个或多个服务端点相关联的信息(例如，与认证服务端点相关联的信息、与可验证声明存储库相关联的信息)添加到去中心化标识文档。认证服务端点和可验证声明存储库414可以被提供为在线平台的一部分。去中心化标识文档可以包括：与所获得的去中心化标识相关联的一个或多个公钥、与所获得的去中心化标识相关联的认证信息、与所获得的去中心化标识相关联的授权信息、与所获得的去中心化标识相关联的委托信息、与所获得的去中心化标识相关联的一个或多个服务、与所获得的去中心化标识相关联的一个或多个服务端点、所获得的去中心化标识的创建者的去中心化标识、其他合适的信息或其任意组合。在一些实施例中，去中心化标识文档可以包括“创建者”字段，该“创建者”字段包含代表用户发送了用于创建去中心化标识的请求的实体的标识信息(例如，去中心化标识)。“创建者”字段可以用作对去中心化标识的所有者的身份进行认证或对去中心化标识的所有者背书的实体的记录。然后，在步骤1128，用户代理411可以生成用于将去中心化标识文档存储到区块链330的一个

或多个区块链交易。用户代理411还可以生成区块链交易的一个或多个哈希值。

[0124] 在一些实施例中，对于将要由区块链330的一个或多个节点执行的一个或多个区块链交易，需要使用与去中心化标识相关联的私钥对它们进行签名。用户代理411可以从KMS 323获得这样的数字签名。在步骤1130，用户代理411可以向KMS 323发送请求，以使用与去中心化标识相关联的加密密钥对中的私钥对区块链交易进行签名。该请求可以包括交易的哈希值和与去中心化标识相关联的公钥。KMS 323可以创建交易的数字签名。在一些实施例中，可以在与KMS 323关联的TEE中生成数字签名。KMS 323可以识别与公钥相关联的加密的私钥，并将该加密的私钥馈送到TEE。加密的私钥可以在TEE中被解密，并用于生成交易的数字签名。然后可以将数字签名馈送回KMS 323。在步骤1132，用户代理411可以从KMS接收签名版本的区块链交易。

[0125] 在步骤1134，用户代理411可以将去中心化标识文档以及签名的区块链交易发送到解析器322，用于发送到区块链系统。在步骤1136，解析器322可以将一个或多个交易发送到区块链系统(例如，一个或多个区块链节点、BaaS云324)。交易可以调用用于管理区块链330上的去中心化标识和去中心化标识文档的区块链合约331。在步骤1138，解析器322可以从区块链330获得表明去中心化标识文档已经被成功存储的信息。在步骤1140，解析器322可以将确认转发至用户代理411。

[0126] 在步骤1142，在已经创建了去中心化标识及其对应的去中心化标识文档之后，用户代理411可以更新数据库416以存储以下之间的映射关系：去中心化标识、用户的账户标识、用户的身份认证的证明、用户的服务ID、与去中心化标识相关联的公钥、与用户或身份认证的证明相关联的密钥别名、其他合适的信息或其任意组合。在一些实施例中，映射关系可以以加密形式存储。为了存储映射关系，用户代理411可以为去中心化标识和其他标识信息中的一项或多项的组合计算哈希值。在一些实施例中，这样的哈希值可以被存储为去中心化标识文档的一部分。所存储的映射关系可以允许用户代理441基于从用户端系统310接收到的信息来识别去中心化标识。在一些实施例中，用户代理411可以接收与所获得的去中心化标识相关联的请求，其中该请求包括账户标识，然后基于账户标识与所获得的去中心化标识之间的映射关系来识别所获得的去中心化标识。在其他实施例中，用户代理441可以接收对身份认证的证明的请求，其中该请求包括去中心化标识，然后基于身份认证的证明和去中心化标识之间的映射关系来定位身份认证的证明。在一些实施例中，用户代理411可以存储用于恢复与和用户的标识信息相关联的去中心化标识对应的私钥的恢复密钥。以这种方式，用户代理411可以允许用户使用恢复密钥来控制去中心化标识。然后，在步骤1144，用户代理411可以将与去中心化标识相关联的信息发送到服务器311，在步骤1146，服务器311可以向用户发送通知，以通知用户去中心化标识的成功创建。

[0127] 图12示出了根据一些实施例的用于使用代理服务认证去中心化标识的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式，所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。在一些实施例中，一方(例如，验证者)可能期望认证另一方(例如，声称的去中心化标识的所有者)是去中心化标识的真实所有者。认证处理可通过双方都可用的代理服务321来促进。

[0128] 在一些实施例中，在步骤1202，验证者532可以获得由声称的所有者提供的去中心化标识。在步骤1204，验证者532可以将请求发送到代理服务API 410以创建去中心化标识

认证质询。该请求可以包括待认证的去中心化标识和对质询的响应要被发送到的网络地址(例如,URL)。该网络地址可以为验证者532可访问的。在步骤1206,可以将请求从代理服务API 410转发到被配置为执行与去中心化标识的认证有关的操作的验证者代理413。在步骤1208,验证者代理413可以将对与待认证的去中心化标识相关联的去中心化标识文档的查询发送到解析器322。在步骤1210,解析器322可以制定调用用于管理去中心化标识的区块链合约331的交易,并将该交易发送到与区块链330相关联的一个或多个区块链节点以供执行。结果,在步骤1212,解析器322可获得与去中心化标识相对应的去中心化标识文档,并在步骤1214将其转发至验证者代理413。在步骤1216,验证者代理413可以基于获得的去中心化标识文档来创建去中心化标识认证质询。在一些实施例中,去中心化标识认证质询可以包括通过使用与记录在去中心化标识文档中的与去中心化标识相关联的公钥对原始文本进行加密而创建的密文。质询还可以包括与验证者关联的网络地址,响应将被发送到该网络地址。在步骤1218,验证者代理413可以从去中心化标识文档获得与去中心化标识的认证服务端点相关联的信息。在步骤1220,验证者代理413可以使用键值结构(key-value structure)将质询的标识存储在存储器中,该质询的标识与和质询相关联的信息相关。例如,验证者代理413可以存储与和待认证的去中心化标识相关联的质询关联的质询ID、用于创建密文的明文以及用于发送对质询的响应的网络地址。在步骤1222,验证者代理413可以基于来自去中心化标识文档的信息将质询发送至与去中心化标识相关联的去中心化标识认证服务。

[0129] 在一些实施例中,在从验证者代理413获得去中心化标识认证质询之后,在步骤1224,去中心化标识认证服务可以从去中心化标识的所有者获得对于这种质询的响应的同意。在步骤1226,如果所有者提供对于身份认证的同意或许可,则去中心化标识认证服务可以向与用户代理411相关联的代理服务API 410发送对去中心化标识认证质询的响应的请求。在步骤1228,代理服务API 410可以调用用户代理411的相应功能以创建对质询的响应。对质询的响应可能要求使用与待认证的去中心化标识相关联的私钥恢复用于创建质询中包含的密文的明文。在步骤1230,用户代理411可以将来自质询的密文和由KMS 323识别的与ID相关联的标识信息一起发送到KMS 323以用于解密。KMS 323可以存储多个公钥-私钥对,所述多个公钥-私钥对与账户的标识信息或与该密钥对对应的去中心化标识相关联。基于从用户代理411接收到的标识信息,KMS 323可以识别与去中心化标识相关联的公钥-私钥对。在一些实施例中,KMS 323可以存储公钥和加密版本的私钥。它可以将加密的私钥发送到与KMS 323关联的TEE以进行解密。然后,可以使用私钥对TEE中的密文进行解密。在步骤1232,用户代理411可以从KMS 323获得解密出的明文。

[0130] 在步骤1234,用户代理411可以使用明文生成对质询的响应,并将该响应发送回去中心化标识认证服务。该响应可以包括原始质询中包含的质询标识。在步骤1236,去中心化标识认证服务可以将响应发送到验证者532提供的网络地址。然后,在步骤1238,验证者532可以将响应转发至验证者代理413以进行检查。在步骤1240,验证者代理413可首先将响应中的质询标识与存储在存储器415中的一个或多个质询标识进行比较,以识别与对应于响应的质询关联的信息。然后在步骤1242,验证者代理413可以确定去中心化标识的声称所有者是否是实际所有者。在一些实施例中,验证者代理可以确定响应中包含的明文是否与用于创建质询中的密文的明文相同。如果是,则验证者代理413可以确定认证成功。在步骤

1244,验证者代理413可以将确认消息发送给验证者,在步骤1246,验证者可以将确认消息转发给去中心化标识的所有者。

[0131] 图13示出了根据一些实施例的用于代表验证者或所有者认证去中心化标识的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式,所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。此外,在图13中所示的任何方法中执行的一个或多个步骤可以被替代为在另一方法中执行的一个或多个合适的步骤。执行如图13中所示的特定步骤的设备或系统也可以由其他合适的设备或系统替代以执行相同的步骤。合适的设备或系统可以包括具有相似功能的子系统、父系统或对应系统。作为示例,用户侧系统310执行的一个或多个步骤可以由身份管理应用533执行,反之亦然。作为另一示例,服务侧系统320执行的一个或多个步骤可以由解析器322或代理321执行,解析器322或代理321可以是服务侧系统320的子系统。尽管本文描述了执行特定步骤的特定设备或系统,但是本文考虑了执行用于认证去中心化标识的任何适当步骤的任何适当的设备或系统。

[0132] 在一些实施例中,一方(例如,验证者532)可能期望认证另一方(例如,声称的去中心化标识的所有者)是去中心化标识的真实所有者。服务侧系统320可以向各方中的任一方或双方提供一个或多个服务和接口,以促进各方完成认证处理的一个或多个步骤。图13中所示的方法可以包括一个或多个步骤,所述一个或多个步骤可以被图12中所示的方法的一个或多个步骤替代或可以用来替代图12中所示的方法的一个或多个步骤。

[0133] 在一些实施例中,如图13所示,声称的去中心化标识所有者可以通过与第一实体相关联的用户侧系统310a与服务侧系统320交互。去中心化标识的验证者532可以通过与第二实体相关联的用户侧系统310b与服务侧系统320交互。第一实体和第二实体可以是或可以不是同一实体。作为示例而非限制,声称的去中心化标识所有者可以对应于单个用户,验证者532可以与在向用户提供服务之前需要认证用户的身份的服务提供商相对应。可能存在声称的去中心化标识所有者或验证者532都不具有直接管理去中心化标识相关操作的技术能力或需求的情况。他们可以依靠用户侧系统310a和310b来与服务侧系统320对接,以便执行去中心化标识相关操作。例如,可以授权用户侧系统310a代表去中心化标识的所有者控制与去中心化标识相关联的一个或多个操作。

[0134] 图13中所示的方法可以从步骤1311开始,其中,声称的去中心化标识所有者可以将去中心化标识提供给验证者532。响应于获得去中心化标识,验证者532可以开始针对该去中心化标识的认证处理。在步骤1312,验证者532可以向声称的去中心化标识所有者提供去中心化标识认证质询。在一些实施例中,去中心化标识认证质询可以包括明文(例如,由去中心化标识验证者选择的一段文本)。为了证明其对去中心化标识的所有权,声称的去中心化标识所有者可能需要使用与去中心化标识相关联的加密密钥对的私钥在明文上提供数字签名。在步骤1313,声称的去中心化标识所有者可以将去中心化标识认证质询转发到用户侧系统310a。在这种情况下,声称的去中心化标识所有者和用户侧系统310a可能已经将与去中心化标识相关联的加密密钥对的管理信托给了服务侧系统320。在步骤1314,用户侧系统310a可向服务侧系统320(例如,向服务侧系统320中的用户代理411)发送对包括在去中心化标识认证质询中的明文上的数字签名的请求。该请求可包括待认证的去中心化标识和明文。

[0135] 服务侧系统320可以从用户侧系统310a获得用于创建数字签名的请求。根据该请

求，服务侧系统320可以获得与去中心化标识相关联的明文和信息。在步骤1315，服务侧系统320可以获得与用于创建数字签名的请求的发送者相关联的一个或多个权限，并且可以基于所获得的一个或多个权限以及与去中心化标识相关联的信息来确定用于创建数字签名的请求的发送者是否被授权来控制与去中心化标识相关的一个或多个操作。服务侧系统320可以基于与发送方的加密或其他安全通信来确定请求的发送方的身份。例如，服务侧系统320可以检查并确定请求的发送者是否为去中心化标识的所有者、去中心化标识的控制者或创建者、或者被授权管理与去中心化标识相关联的一个或多个操作的用户侧系统310。如果确定用于创建数字签名的请求的发送者被授权来控制与去中心化标识相关联的一个或多个操作，则服务侧系统320可以根据该请求来创建数字签名。否则，服务侧系统320可以拒绝该请求。在一些实施例中，服务侧系统320可以附加检查可验证声明的状态。例如，服务侧系统320可以确定去中心化标识是否已经在区块链330上注册或者与去中心化标识相关联的去中心化标识文档是否已经被存储在区块链330上。在一些实施例中，如果去中心化标识已经在区块链330上注册并且处于完全功能状态，则服务侧系统320可以仅继续提供数字签名。

[0136] 如果服务侧系统320接受用于创建数字签名的请求，则其可以进行到步骤1316。在步骤1316，服务侧系统320可以识别与去中心化标识相关联的区块链账户。在步骤1317，服务侧系统320可以向区块链330查询这样的区块链账户信息并且获得这样的信息。服务侧系统320可以使用与去中心化标识相对应的区块链账户的标识来识别与去中心化标识相关联的加密密钥对。例如，服务侧系统320可以基于区块链账户的标识来获得密钥标识，并且基于该密钥标识来访问加密密钥对。然后，在步骤1318，服务侧系统320可以基于用于创建数字签名的请求在明文上创建数字签名。可以通过使用与去中心化标识相关联的私钥对明文的哈希值进行加密来创建数字签名。在一些实施例中，服务侧系统320可以使用KMS 323来生成数字签名。服务侧系统320可以向KMS 323发送用于使用与去中心化标识相关联的私钥对明文进行签名的指令。然后，服务侧系统320可以从KMS 323获得数字签名。例如，服务侧系统320可以识别与去中心化标识相关联的区块链账户，基于所识别的与去中心化标识相关联的区块链账户，确定与去中心化标识相关联的私钥的标识，并且将与去中心化标识相关联的私钥的标识包括在指令中。在一些实施例中，从KMS 323获得的数字签名可能已经在TEE中生成。

[0137] 在步骤1319，服务侧系统320可以将明文上的数字签名返回给用户侧系统310a。在步骤1320，用户侧系统310a可以基于数字签名来生成对去中心化标识认证质询的响应，并将该响应发送给声称的去中心化标识所有者。该响应可以包括与去中心化标识相关联的信息(例如，去中心化标识)，与去中心化标识认证质询相关联的信息(例如，去中心化标识认证质询的标识)、去中心化标识认证质询中包括的明文、数字签名、其他合适的信息或其任意组合。然后，在步骤1321，声称的去中心化标识所有者可以将该响应提供给验证者532。

[0138] 在从声称的去中心化标识所有者接收到对去中心化标识认证质询的响应之后，验证者532可以基于该响应来发起用于认证去中心化标识的所有权的处理。在步骤1322，验证者532可以将该响应发送给用户侧系统310b。在步骤1323，用户侧系统310b可以将该响应作为用于认证去中心化标识的请求的一部分转发到服务侧系统320(例如，转发到服务侧系统320中的验证者代理413)。该请求可以包括去中心化标识、与去中心化标识认证质询相关联

的明文、明文上的数字签名、其他合适的信息或其任意组合。在一些实施例中，该请求可以包括对去中心化标识认证质询的响应，该响应可以包括该请求中包括的信息的部分或全部。服务侧系统320可以响应于获得用于认证去中心化标识的请求来发起用于认证去中心化标识的处理。在一些实施例中，服务侧系统320可以在发起处理之前检查对一个或多个标准的满足。例如，服务侧系统320可以检查去中心化标识认证质询的创建者(例如，验证者532)是否拥有由服务侧系统320管理的去中心化标识、要认证的去中心化标识是否具有有效状态(例如，去中心化标识是否已在区块链330上注册)、是否满足其他合适的标准或其任意组合。如果满足所有要求的标准(如果有的话)，则服务侧系统320可发起用于认证去中心化标识的处理。

[0139] 在一些实施例中，服务侧系统320可以获得与去中心化标识相关联的公钥。在一些实施例中，服务侧系统320可以识别与去中心化标识相关联的区块链330，并从所识别的区块链中获得公钥。在步骤1324，服务侧系统320可以向区块链330查询与去中心化标识相关联的公钥。然后，在步骤1325，认证系统320可以从区块链获得该公钥。例如，服务侧系统320可以向区块链330的一个或多个区块链节点发送区块链交易以检索与去中心化标识相对应的去中心化标识文档。该区块链交易可以包括与去中心化标识相关联的信息，并且可以调用区块链合约来管理去中心化标识和对应的去中心化标识文档之间的关系。例如，区块链交易可以调用区块链合约的接口，该区块链合约是可执行的，以检索与对应于一个或多个去中心化标识的一个或多个去中心化标识文档相关联的信息。服务侧系统320可以从区块链330获得去中心化标识文档，并从去中心化标识文档中检索公钥。

[0140] 在步骤1326，服务侧系统320可以基于明文和公钥来验证数字签名。在一个实施例中，服务侧系统320可以基于所获得的公钥和明文来确定明文上的数字签名是否是基于与去中心化标识相对应的私钥来创建的。例如，服务侧系统320可以计算明文的哈希值，并使用公钥对数字签名进行解密以获得解密出的值。服务侧系统320可以将计算出的哈希值和解密出的值进行比较以确定它们是否相同。如果相同，则服务侧系统320可以确定数字签名是基于与公钥相对应的私钥创建的。在步骤1327，服务侧系统320可以将认证结果返回给用户侧系统310b(用于认证去中心化标识的请求的发送者)。如果服务侧系统320确定明文上的数字签名是基于与去中心化标识相对应的私钥创建的，则服务侧系统320可以生成并发送确认去中心化标识的认证的消息。这确认了声称的去中心化标识所有者是去中心化标识的实际所有者。否则，服务侧系统320可以生成并发送表明去中心化标识的认证失败的消息。在步骤1328，用户侧系统310b可以将结果转发给验证者532，即去中心化标识认证质询的创建者。可选地，服务侧系统320可以将结果直接返回给验证者532，即去中心化标识认证质询的验证者532。

[0141] 图14示出了根据一些实施例的用于使用代理服务发布可验证声明的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式，所述方法可以包括以各种次序或并行执行的附加的、更少的或可选的步骤。在一些实施例中，第一实体(例如，发布者)可能期望为第二实体(例如，用户)发布可验证声明以证明与第二实体有关的事实。第一实体可以被称为可验证声明的发布者，第二实体可以被称为可验证声明的主题。通过实体可用的代理服务321可以促进发布可验证声明的处理。

[0142] 在一些实施例中，在步骤1402，代理服务API 410可以从发布者531接收用于为与

用户相关联的去中心化标识创建未签名的可验证声明的请求。在步骤1404,代理服务API 410可以调用发布者代理412以执行生成新的可验证声明的操作。在步骤1406,发布者代理412可以基于从发布者531接收到的请求来创建可验证声明。可验证声明可以包括请求中包含的消息。在一些实施例中,出于机密性原因,可验证声明可以包括加密版本的消息。该消息可以包括关于用户的声明或陈述,或者可被传输至具有对可验证声明的访问权的一方的其他合适的信息或数据。在一些实施例中,可验证声明可以包括与用户的身份认证(例如,实名认证、真人认证)相对应的声明。该请求可以包括用户的去中心化标识。发布者代理412可以基于去中心化标识直接创建可验证声明。可选地,该请求可以包括与用户(例如,具有发布可验证声明的实体的用户账户)相关联的账户标识。在这种情况下,发布者代理412可以从请求中获得与用户相关联的账户标识,并且基于账户标识和去中心化标识之间的预存储的映射关系来识别去中心化标识。发布者代理412然后可以基于识别的去中心化标识创建未签名的可验证声明。发布者代理412还可以计算未签名的可验证声明的内容的哈希值。

[0143] 在一些实施例中,发布者代理412可以响应于接收到请求而获得与发布者相关联的数字签名。在一些实施例中,可以从KMS 323获得数字签名。在步骤1408,发布者代理412可以确定与发布者531相关联的密钥别名。在步骤1410,发布者代理412可以将针对与发布者531相关联的对可验证声明的数字签名的请求发送到KMS 323。该请求可以包括密钥别名,该密钥别名可以用于识别与发布者531相关联的加密密钥。该请求还可以包括由发布者代理412创建的未签名的可验证声明的哈希值。KMS 323可以存储与实体或用户的密钥别名相关联的多个公钥-私钥对。基于从发布者代理412接收到的密钥别名,KMS 323可以识别与发布者531相关联的公钥-私钥对。在一些实施例中,KMS 323可以存储公钥和加密版本的私钥。它可以将加密的私钥发送到与KMS 323关联的TEE以进行解密。然后可以使用私钥创建发布者对可验证声明的数字签名。可以通过使用私钥对未签名的可验证声明的哈希值进行加密来创建数字签名。在步骤1412,可以将数字签名发送回发布者代理412。然后,在步骤1414,发布者代理412可以将未签名的可验证声明与数字签名结合以组成签名的可验证声明。以这种方式,基于从发布者531接收到的请求和数字签名来生成签名的可验证声明。

[0144] 在一些实施例中,发布者代理412可以将可验证声明上传到与用户或可验证声明的持有者的去中心化标识相关联的服务端点。发布者代理412可以基于与去中心化标识相关联的去中心化标识文档来识别服务端点。在步骤1416,发布者代理412可以向解析器322发送对与被发布了可验证声明的去中心化标识相关联的去中心化标识文档的查询。在步骤1418,解析器322可以制定调用用于管理去中心化标识的区块链合约331的交易,并将该交易发送到与区块链330相关联的一个或多个区块链节点以供执行。该交易可以包括与去中心化标识相关联的信息,并且可以用于检索与该去中心化标识相对应的去中心化标识文档。结果,在步骤1420,解析器322可获得与去中心化标识相对应的去中心化标识文档,并在步骤1422将其转发至SDK 312。基于去中心化标识文档,发布者代理412可以从去中心化标识文档获得与去中心化标识的服务端点(例如,可验证声明存储库414)相关联的信息(例如,网络地址)。在步骤1424,发布者代理412可以将可验证声明上传到服务端点。

[0145] 在一些实施例中,发布者代理412可以存储可验证声明的状态。可验证声明的状态可以被存储在区块链330中。在一些实施例中,与可验证声明的发布者531相关联的服务端点可以使用区块链330。在步骤1426,发布者代理412可以将可验证声明的状态(例如,有效、

无效)和可验证声明的哈希值发送到解析器322以存储在区块链330中。在步骤1428,解析器322可以生成用于将与可验证声明相关联的信息添加至区块链的区块链交易并将其发送至与服务端点相关联的区块链330的区块链节点。该信息可以包括可验证声明的状态和哈希值。在一些实施例中,区块链交易可以调用用于管理可验证声明的区块链合约331。在将交易发送到区块链节点之后,解析器322可以在步骤1430确定已经成功存储了可验证声明的哈希值和状态,并且在步骤1432可以将确认发送至发布者代理412。在一些实施例中,可验证声明的状态也可以被本地存储。在步骤1434,发布者代理412可以将可验证声明及其状态存储在数据库416中。发布者代理412可以在步骤1436接收成功存储的确认,在步骤1438将确认发送至代理服务API 410,然后在步骤1440,代理服务API 410可以向发布者531发送表明可验证声明已经成功创建的确认。发送至发布者的确认可以包括已经创建的可验证声明。

[0146] 在一些实施例中,可将可验证声明提供给用户或可验证声明的持有者。在步骤1442,发布者代理412可以将可验证声明和/或可验证声明的状态发送至与可验证声明的持有者的用户代理411相关联的代理服务API 410。在步骤1444,代理服务API 410可以调用用户代理411以上传可验证声明。这里,用户代理411可用作可验证声明持有者的去中心化标识的服务端点。用户代理411可在与发布者代理412相同的物理系统上实现。在步骤1446,用户代理411可将可验证声明保存到数据库416。在成功保存可验证声明之后,在步骤1448,数据库416可将成功确认返回给用户代理411。在步骤1450,用户代理411可将确认发送至代理服务API 410,在步骤1452,代理服务API 410可将确认转发给发布者代理412。

[0147] 图15示出了根据一些实施例的用于使用代理服务验证可验证声明的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式,所述方法可包括以各种次序或并行执行的附加的、更少的或可选的步骤。在一些实施例中,可验证声明的持有者(或可验证声明的主题)可向第一实体(例如,验证者)展示由第二实体(例如,可验证声明的发布者)发布的可验证声明。验证者可借助于代理服务321来验证可验证声明。

[0148] 在一些实施例中,在步骤1502,代理服务API 410可从验证者532接收验证可验证声明的请求。可验证声明可包括与可验证声明的发布者相关联的数字签名。在步骤1504,代理服务API 410可调用验证者代理413的函数以验证可验证声明。在一些实施例中,验证者532可已经从可验证声明的持有者直接获得了可验证声明。可选地,验证者532可能仅接收到与可验证声明的主题相关联的账户标识。验证者532可通过以下获得可验证声明:基于账户标识和去中心化标识之间的预存储的映射关系来获得与可验证声明的主题相关联的去中心化标识、获得与去中心化标识相关联的去中心化标识文档、从去中心化标识文档获得与用于管理可验证声明的服务端点相关联的信息以及从服务端点获得可验证声明。

[0149] 在一些实施例中,验证者代理413可验证可验证声明的状态。验证者代理413可使用步骤1506a、1508a、1510a和1512a或者步骤1506b、1508b、1510b和1512b获得并验证状态。在一些实施例中,验证者代理413可从存储与多个可验证声明相关联的信息的区块链获得可验证声明的状态。在步骤1506a,验证者代理413可向解析器322发送对可验证声明的状态的查询。该查询可包括可验证声明的标识。在步骤1508a,解析器322可创建用于检索哈希值和可验证声明的状态的区块链交易,并将其发送到与区块链300相关联的一个或多个区块链节点。区块链交易可包括可验证声明的主题的去中心化标识,并且可调用用于管理可验

证声明的区块链合约331。在步骤1510a，解析器322可从区块链330获得可验证声明的状态以及与可验证声明相关联的哈希值。然后，在步骤1512a，解析器322可将哈希值和状态发送给验证者代理413以进行验证。验证者代理413可通过对由持有者提供的可验证声明应用哈希函数来计算哈希值。验证者代理413可通过将从区块链330接收的哈希值与计算出的哈希值进行比较来认证接收到的可验证声明的状态。如果它们相同，则验证者代理413可确定接收到的状态确实对应于可验证声明。如果状态表明可验证声明有效，则验证者代理413可完成该验证步骤。

[0150] 在一些实施例中，验证者代理413可从与可验证声明相关联的服务端点获得可验证声明的状态。在一些实施例中，服务端点可对应于与发布者相关联的发布者代理412。在步骤1506b，验证者代理413可向发布者代理412发送对可验证声明的状态的查询。发布者代理412可在步骤1508b向数据库416查询可验证声明的状态，并且在步骤1510b获得可验证声明的状态和对应的哈希值。在步骤1512b，发布者代理412可将哈希值和状态发送给验证者代理413。验证者代理413可以以上述方式认证该状态并验证可验证声明有效。

[0151] 在一些实施例中，验证者代理413可以确定可验证声明是由对可验证声明标识的发布者发布的。验证者代理413可以基于可验证声明获得与发布者相关联的公钥。验证者代理413可以基于可验证声明中的标识来识别发布者。在一些实施例中，标识可以包括发布者的去中心化标识。可以基于发布者的去中心化标识从区块链330获得公钥。在步骤1514，验证者代理413可以向解析器322发送对与发布者相关联的公钥的请求。该请求可以包括发布者的去中心化标识。在步骤1516，解析器322可以创建用于调用区块链合约331以基于去中心化标识检索公钥或去中心化标识文档的区块链交易，并将区块链交易发送到区块链330的区块链节点。解析器322可以在步骤1518获得公钥(例如，通过从去中心化标识文档中检索)，并且在步骤1520将公钥转发给验证者代理413。然后，在步骤1522，验证者代理413可以通过确定数字签名是基于与公钥相关联的私钥创建的来使用公钥验证可验证声明。在一些实施例中，验证者代理413可以验证关于可验证声明的一个或多个其他事实。例如，验证者代理413可以从可验证声明获得可验证声明的发布日期，并且基于所获得的发布日期和当前日期之间的比较来验证所获得的发布日期。作为另一示例，验证者代理413可以从可验证声明获得可验证声明的到期日期，并且基于到期日期和当前日期来验证可验证声明尚未到期。如果可验证声明的验证成功，则在步骤1524验证者代理可以将确认发送到代理服务API 410。在步骤1526，代理服务API 410可以向验证者532发送确认验证了可验证声明的消息。

[0152] 图16示出了根据一些实施例的用于基于区块链的交叉实体认证的方法。以下呈现的方法的操作旨在是说明性的。取决于实施方式，所述方法可包括以各种次序或并行执行的附加的、更少的或可选的步骤。

[0153] 在一些实施例中，简单概述来看，参考图16描述的步骤可以基于在第二实体1602注册的用户认证信息允许具有计算设备1607(例如，计算机、移动电话、平板电脑、可穿戴计算设备等)的用户访问第一实体1601。可以参考计算设备1607、第一实体1601、第二实体1602、第一数据存储1611、第二数据存储1612、DIS(去中心化身份服务)1603a、DIS 1603b、区块链330或其等价体来执行以下各个步骤。在一些实施例中，第一实体1601、第二实体1602及其用户可以分别与去中心化标识相关联。第一实体1601和第二实体1602可以各自基于用户的认证向用户提供访问。例如，第一实体1601和第二实体1602可以承载网站、提供移

动电话应用、维护组织(例如,公司、工会等)等。当在下面提到时,第一实体1601和第二实体1602可以表示相关联的计算系统或设备(例如,提供在线服务的服务器或计算机集群)或所提供的服务(例如,网站、应用)。第一实体1601和第二实体1602可以分别对应于用户侧系统310,第一数据存储1611和第二数据存储1612可以分别对应于数据库313。第一实体1601和第二实体1602可以收集用户认证。例如,作为雇主公司,实体可以为其雇员收集用户认证。用户可以基于在母公司注册的用户认证信息,请求访问子公司的平台。第一实体1601和第二实体1602可以要求用户认证以准予访问一个或多个账户或功能,例如数据库访问、建筑物访问、工资单搜索、票务订购、消息传递、在线银行业务等。例如,用户可以基于在银行的软件应用或用户的雇主中注册的用户认证来请求访问订餐网站。

[0154] 在一些实施例中,第一实体1601可以与第一数据存储1611相关联,并且第二实体1602可以与第二数据存储1612相关联,以存储信息。第一数据存储1611和第二数据存储1612可以各自包括由相应实体维护的本地数据存储(例如,用于相应实体使用的本地数据存储)、可由相应实体访问的公共数据存储(例如,各个实体共享的公共数据存储,用于存储分别由各实体加密的信息)、由平台维护的针对相应实体的数据存储(例如,DIS 1603a或1603b维护的持久性存储)等。每个数据存储可以提供安全存储和安全性特征以保护隐私。

[0155] 在一些实施例中,DIS 1603a和DIS 1603b可以对应于服务侧系统320。DIS 1603a和DIS 1603b可以共同地或单独地包括各种结构、组件和功能,并执行本文关于服务侧系统320所述的相应方法。DIS 1603a和DIS 1603b可以实现为集成式服务或分布式去中心化服务。尽管在图16中以分开的框示出了DIS 1603a和DIS 1603b,但是它们可以在单个物理系统中或在分开的多个物理系统中实现。第一实体1601和第二实体1602可以包括用于经由API接口提供用户可访问的这种在线服务的一个或多个SDK。例如,作为集成式服务,DIS 1603a和DIS 1603b可以对应于向各种用户提供服务的在线平台。对于另一示例,作为分布式去中心化服务,DIS 1603a和DIS 1603b可以分别对应于区块链330的区块链节点,并且可以分别与第一实体1601和第二实体1602相关联。作为与区块链节点相关联的部分或组件,DIS可以有助于共识验证,执行与区块链数据相关的存储或执行与区块链330相关的其他动作。在一个实施例中,第一实体1601、DIS 1603a和/或第一数据存储1611可以集成在一起;第二实体1602、DIS 1603b和/或第二数据存储1612可以集成在一起。在一个实施例中,DIS 1603a可以管理用于第一实体1601和/或其注册用户的凭证信息(例如,私钥、去中心化标识、可验证声明),并且DIS 1603b可以管理用于第二实体1602和/或其注册用户的凭证信息(例如,私钥、去中心化标识、可验证声明)。

[0156] 在一些实施例中,在步骤1621,用户可以例如通过计算设备1607向第二实体1602发送去中心化标识创建请求。第二实体1602可以将请求转发到DIS 1603b。DIS 1603b可以从第二实体1602获得用于创建与用户的账户标识相关联的去中心化标识的去中心化标识创建请求。DIS1603b可以例如根据参考图6A、图6B或图11所描述的方法为用户执行去中心化标识创建。例如,DIS 1603b可以获得加密密钥对中的公钥,基于该公钥获得去中心化标识,以及存储账户标识与所获得的去中心化标识之间的映射关系。针对去中心化标识创建的进一步细节可以参考上面的描述。所创建的去中心化标识可以被存储在区块链330中。

[0157] 在一些实施例中,用户的去中心化标识可以被设计为主要去中心化标识。DIS 1603b可以为用户创建一个或多个与主要去中心化标识相关联的次要去中心化标识。与主

要去中心化标识相比，次要去中心化标识在关联的用户信息及其功能方面可能受到更多限制。次要去中心化标识可以用于访问第一实体1601(例如，用于一次性访问、用于限时访问、用于对特定实体的访问)，而主要去中心化标识可以用于用户的长期标识。为此，次要去中心化标识可以与限制次要去中心化标识的有效性的相应状态(例如，有效时间、有效使用次数)相关联，并且该状态可以被存储在与次要去中心化标识相关联的去中心化标识文档中。在一个实施例中，次要去中心化标识是用于用户访问第一实体1601的临时去中心化标识。因此，使用次要去中心化标识可以最小化身份被盗用的风险，因为即使次要去中心化标识被暴露在区块链中或以其他方式使第三方可用，次要去中心化标识也无法用于其有限有效性之外的目的。此外，主要去中心化标识可以与用户的隐私信息相关联，该用户的隐私信息不与次要去中心化标识相关联，并且不可以基于次要去中心化标识来追踪隐私信息。因此，由于在交叉实体认证处理中没有使用也没有暴露非必要的隐私信息，因此用户隐私得到保护。

[0158] 在一些实施例中，在步骤1622，DIS 1603b可以将创建的去中心化标识的结果返回给第二实体1602，第二实体1602随后可以相应地通知计算设备1607。通过创建去中心化标识，用户可以将去中心化标识用作认证信息以访问第二实体1602提供的服务。可替代地，可对用户请求并执行在第二实体1602的其他类型的注册，以获得针对用户的认证信息。

[0159] 在一些实施例中，在步骤1623，用户或第二实体1602可以请求创建可验证声明以证明该用户是第二实体1602的注册用户。例如，DIS1603b可以从与第二实体1602相关联的计算设备获得可验证声明创建请求，以创建表明该用户是第二实体1602的注册用户的可验证声明。因此，由第二实体背书的用户的认证信息可以包括与表明该用户是第二实体的注册用户的可验证声明相关联的信息。在步骤1624，DIS 1603b可以获得与第二实体1602相关联的数字签名，并且基于所获得的可验证声明创建请求和所获得的数字签名来创建可验证声明。DIS 1603b可以例如根据参考图9或图14所描述的方法来执行可验证声明创建。细节可以参考相应的描述。在步骤1625，DIS 1603b可以将创建的可验证声明存储在第二数据存储1612中。

[0160] 在一些实施例中，在步骤1626，用户可以例如通过尝试经由计算设备1607登录到第一实体1601来向第一实体1601发送访问请求。在一些实施例中，用户在第二实体1602注册，而不在第一实体1601注册。在步骤1627，响应于访问请求，第一实体1601可以将认证请求转发到DIS1603a，以请求第二实体1602为第一实体1601认证用户，从而实现交叉实体认证。DIS 1603a可以获得第一实体1601的用于认证用户的认证请求，并且该认证请求可以包括用户的去中心化标识(例如，主要去中心化标识、次要去中心化标识)。

[0161] 在一些实施例中，在步骤1628，DIS 1603a可以基于去中心化标识从区块链303获得用户的公钥，并且至少基于所获得的用户的公钥来验证用户拥有去中心化标识。DIS 1603a可以例如根据参考图7、图8、图12或图13描述的方法来执行去中心化标识认证。细节可以参考相应的描述。

[0162] 在一些实施例中，在步骤1628，DIS 1603a可以确定第一实体1601是否被授权访问在第二实体1602存储的认证信息(例如，可验证声明)以认证用户或通过第二实体1602以其他方式认证用户。例如，用户可以将授权包括在访问请求1626中以在发送访问请求1626之前给予授权，或者在发送访问请求1626之后并且在步骤1628之前给予授权。通过该授权，可

以允许第一实体1601访问由第二实体背书的用户的认证信息(例如,可验证声明),并且该用户在第二实体1602注册而不在第一实体1601注册。在一个实施例中,授权可以与用户的数字签名相关联,或者可以由用户的私钥加密以证明用户的背书。

[0163] 在一些实施例中,在步骤1629,DIS 1603a可以使用第一实体1601的私钥在获得的认证请求上生成数字签名,并且获得使用用户的私钥加密的授权以允许第一实体1601访问第二实体1602背书的用户的认证信息。例如,DIS 1803a可以获得使用第一实体1601的私钥对认证请求进行签名的数字签名,然后用户可以通过计算设备1607使用用户的私钥对明文形式的认证请求以及数字签名进行加密。认证请求可以包括用户的去中心化标识,并且请求第二实体1602为第一实体1601认证用户。因此,加密的授权包括用户的去中心化标识和认证请求。此外,加密的授权体现了两层背书:第一实体1601的数字签名,该数字签名表示认证请求是用于准予访问第一实体1601,并且认证结果应发送给第一实体1601;以及用户私钥的加密,该加密表示认证请求被用户确认并且第一实体1601没有篡改认证请求。

[0164] 在一些实施例中,在步骤1629,DIS 1603a可以响应于确定第一实体1601被允许访问由第二实体1602背书的用户的认证信息,由第二实体1602生成用于获得用户的认证结果的区块链交易。生成的区块链交易包括加密的授权。认证结果与去中心化标识相关联。此外,DIS 1603a可以将区块链交易发送到区块链节点以添加到区块链330。

[0165] 在一些实施例中,在步骤1630,DIS 1603b可以从区块链330获得包括第一实体1601的认证请求的区块链交易,以认证用户。该认证请求包括用户的去中心化标识。例如,DIS 1603b可以针对各种去中心化标识的事件监视区块链330,所述去中心化标识例如为第二实体的去中心化标识、第二实体的用户的去中心化标识等。由于添加到区块链330的区块链交易包括用户的去中心化标识,所以DIS 1603b可以接收通知(例如,通过消息队列),从而获得区块链交易。

[0166] 在一些实施例中,获得的区块链交易包括利用用户的私钥加密的授权,以允许第二实体1602与第一实体1601共享用户的认证信息(例如,允许第一实体1601访问可验证声明,该可验证声明表示用户在第二实体1602注册,从而通过在实体之间共享用户认证来准予用户访问第一实体1601)。加密的授权包括用户的去中心化标识。加密的授权包括基于第一实体1601的私钥在认证请求上的数字签名。

[0167] 在一些实施例中,在步骤1631,DIS 1603b可以获得用户的公钥(例如,从区块链330),并使用用户的公钥对加密的授权进行解密,以验证该授权是否得到用户的背书,并获得数字签名。DIS 1603b可以进一步从区块链获得第一实体1601的公钥,使用获得的第一实体1601的公钥对数字签名进行解密,以及将解密的数字签名与认证请求的哈希值进行比较(以明文形式),以验证认证请求是否是由第一实体1601签名的。如果所有验证都成功,则表明用户授权第二实体1602与第一实体1601共享用户的认证信息。

[0168] 在一些实施例中,在步骤1632,DIS 1603b可响应于确定第一实体1601被允许访问由第二实体1602背书的用户的认证信息,响应于所获得的区块链交易,获得第二实体1602对用户的认证结果。为此,DIS1603b可以针对证明用户(由去中心化标识表示)是第二实体的注册用户的任何可验证声明搜索第二数据存储1612,或以其他方式获得相应的搜索结果。如果搜索返回肯定结果,则获得与去中心化标识相关联的认证结果。认证结果包括与可验证声明相关联的信息,该信息表明该用户是第二实体1602的注册用户,并且该可验证声

明与去中心化标识相关联。

[0169] 在一些实施例中,可验证声明的哈希值被存储在区块链中,并且可验证声明被存储在数据存储(例如,第二数据存储1612)中。如前所述,数据存储可包括以下中的一个或多个:由第二实体维护的本地数据存储、第二实体可访问的公共数据存储以及由平台维护的用于第二实体的数据存储。可验证声明包括由第二实体1602或用户配置的用于允许第一实体1601访问可验证声明的权限。例如,如上所述,在步骤1631的成功验证可以表明用户授权第二实体1602与第一实体1601共享用户的认证信息,从而允许第一实体1601访问可验证声明。可选地,第二实体1602可以给予这种权限并且与第一实体1601共享可验证声明。因此,步骤1631可以包括基于权限来验证第一实体被允许访问可验证声明。

[0170] 在一些实施例中,在步骤1632,为了响应于所获得的区块链交易而获得认证结果,DIS 1603b可以查询数据存储以获得与去中心化标识相关联的可验证声明,基于所获得的可验证声明来验证该用户是否为第二实体1602的注册用户,以生成未加密的认证结果(例如,用户在第二实体1602注册或未注册),并使用第二实体1602的私钥对未加密的认证结果进行加密,以生成认证结果。

[0171] 在一些实施例中,在步骤1633,DIS 1603b可以生成包括认证结果的不同的区块链交易。在一些实施例中,在步骤1634,DIS 1603b可以将不同的区块链交易发送到区块链节点以添加到区块链330。

[0172] 在一些实施例中,在步骤1634,DIS 1603a可以从区块链330获得不同的区块链交易。区块链交易获得过程可以类似于步骤1630。不同的区块链交易包括第二实体对用户的认证结果。在一个实施例中,认证结果表明认证成功(例如,第二实体1602已经发布了证明用户在第二实体1602注册的可验证声明),并且在步骤1635,DIS 1603a可以将认证结果发送到第一实体1601,以准予用户访问第一实体1601。因此,对于已经在第二实体1602注册的用户,他们无需在第一实体1601注册,并且可以基于他们在第二实体1602注册的认证信息(例如,去中心化标识)来访问第一实体1601。在一个实施例中,认证结果表明认证失败(例如,第二实体1602尚未发布证明用户在第二实体1602注册的可验证声明),并且在步骤1635,DIS 1603a可将认证结果发送至第一实体1601,以拒绝用户访问第一实体1601。因此,对于从未在第二实体1602注册过或未以产生可验证声明以进行交叉认证的方式注册的用户,他们仍会被拒绝访问第一实体1601。

[0173] 在一些实施例中,在步骤1636,第一实体1601可以基于认证结果执行进一步的动作。第一实体1601可以缓存认证结果以促进用户在将来的有限时间段内访问(如果使用了临时去中心化标识),或者存储认证结果以用于将来的长期访问(如果使用了主要去中心化标识)。

[0174] 图17A示出了根据一些实施例的用于基于区块链的交叉实体认证的方法1700的流程图。方法1700可以由用于基于区块链的交叉实体认证的设备、装置或系统执行。方法1700可以由图1至图5所示的环境或系统的一个或多个组件,例如服务侧系统320的一个或多个组件(例如,DIS 1603a、DIS 1603a和1603b)执行。取决于实施方式,方法1700可以包括以各种顺序或并行执行的附加的、更少的或替代的步骤。

[0175] 框1710包括获得第一实体的用于认证用户的认证请求,其中,认证请求包括用户的去中心化标识(DID)。在一些实施例中,去中心化标识是与用户的主要去中心化标识相关

联的次要去中心化标识;主要去中心化标识与用户的隐私信息相关联;并且基于次要去中心化标识不能追踪隐私信息。在一些实施例中,次要去中心化标识是用于用户访问第一实体的临时去中心化标识。

[0176] 在一些实施例中,在框1720处生成用于获得第二实体对用户的认证结果的区块链交易之前,该方法还包括:基于去中心化标识从区块链获得用户的公钥;以及至少基于所获得的用户的公钥,验证用户是否拥有去中心化标识。

[0177] 在一些实施例中,在生成用于获得第二实体对用户的认证结果的区块链交易之前,该方法还包括:利用第一实体的私钥在获得的认证请求上生成数字签名;以及获得利用用户的私钥加密的授权以允许第一实体访问由第二实体背书的用户的认证信息。加密的授权包括数字签名;加密的授权包括用户的去中心化标识;生成的区块链交易包括加密的授权。

[0178] 框1720包括:响应于确定第一实体被允许访问由第二实体背书的用户的认证信息,生成用于获得第二实体对用户的认证结果的区块链交易,其中,认证结果与去中心化标识相关联。在一些实施例中,用户在第二实体注册;并且用户未在第一实体注册。

[0179] 框1730包括将区块链交易发送到区块链节点以添加到区块链。在一些实施例中,由第二实体背书的用户的认证信息包括与表明该用户是第二实体的注册用户的可验证声明(VC)相关联的信息;并且可验证声明与去中心化标识相关联。在一些实施例中,可验证声明的哈希值被存储在区块链中;可验证声明被存储在数据存储中;数据存储包括以下中的一个或多个:由第二实体维护的本地数据存储、第二实体可访问的公共数据存储以及由平台维护的用于第二实体的数据存储。在一些实施例中,可验证声明包括由第二实体或用户配置的用于允许第一实体访问可验证声明的权限。

[0180] 在一些实施例中,该方法还包括:从区块链获得用于获得用户的认证结果的区块链交易;响应于所获得的区块链交易,获得与去中心化标识相关联的认证结果;生成包括认证结果的不同的区块链交易;以及将不同的区块链交易发送至区块链节点以添加至区块链。

[0181] 在一些实施例中,该方法还包括:从区块链获得不同的区块链交易,该不同的区块链交易包括第二实体对用户的认证结果,其中,认证结果表明认证成功;以及将认证结果发送给第一实体,以准予用户访问第一实体。

[0182] 在一些实施例中,该方法还包括:从区块链获得不同的区块链交易,该不同的区块链交易包括第二实体对用户的认证结果,其中,认证结果表明认证失败;以及将认证结果发送给第一实体,以拒绝用户访问第一实体。

[0183] 图17B示出了根据一些实施例的用于基于区块链的交叉实体认证的方法1701的流程图。方法1701可以由用于基于区块链的交叉实体认证的设备、装置或系统执行。方法1701可以由图1至图5所示的环境或系统的一个或多个组件,例如服务侧系统320的一个或多个组件(例如,DIS 1603b、DIS 1603a和1603b)执行。取决于实施方式,方法1701可以包括以各种顺序或并行执行的附加的、更少的或替代的步骤。

[0184] 框1711包括从区块链获得区块链交易,该区块链交易包括第一实体的用于认证用户的认证请求,其中,认证请求包括用户的去中心化标识(DID)。在一些实施例中,用户在第二实体注册;并且该用户未在第一实体注册。在一些实施例中,去中心化标识是与用户的主

要去中心化标识相关联的次要去中心化标识;主要去中心化标识与用户的隐私信息相关联基于次要去中心化标识不能追踪隐私信息。在一些实施例中,次要去中心化标识是用于用户访问第一实体的临时去中心化标识。

[0185] 在一些实施例中,在框1711处获得区块链交易之前,该方法还包括:从与第二实体相关联的计算设备获得可验证声明创建请求,该可验证声明创建请求用于创建表明该用户是第二实体的注册用户的可验证声明;获得与第二实体相关的数字签名;基于所获得的可验证声明创建请求和获得的数字签名创建可验证声明。在一些实施例中,在获得可验证声明创建请求之前,该方法还包括:从第二实体获得用于创建与用户的账户标识相关联的去中心化标识的去中心化标识创建请求;获得加密密钥对中的公钥;基于公钥获得去中心化标识;以及存储账户标识和所获得的去中心化标识之间的映射关系。

[0186] 在一些实施例中,所获得的区块链交易包括利用用户的私钥加密的授权,以允许第一实体访问第二实体背书的用户的认证信息;加密的授权包括用户的去中心化标识;加密的授权包括基于第一实体的私钥在认证请求上的数字签名。在框1711处获得区块链交易之后并且在框1721处获得认证结果之前,该方法还包括:获得用户的公钥;利用用户的公钥对加密的授权进行解密,以验证授权已由用户签名并获得数字签名;从区块链获得第一实体的公钥;利用所获得的第一实体的公钥对数字签名进行解密;以及将解密的数字签名与认证请求的哈希值进行比较,以验证认证请求是由第一实体签名的。

[0187] 在一些实施例中,由第二实体背书的用户的认证信息包括与表明该用户是第二实体的注册用户的可验证声明(VC)相关联的信息;可验证声明与去中心化标识相关联。在一些实施例中,可验证声明包括由第二实体或用户配置的用于允许第一实体访问可验证声明的权限;在框1711处获得区块链交易之后并且在框1721处获得认证结果之前,该方法还包括:基于所述权限来验证第一实体被允许访问可验证声明。

[0188] 框1721包括:响应于确定第一实体被允许访问由第二实体背书的用户的认证信息,响应于所获得的区块链交易获得第二实体对用户的认证结果,其中,认证结果与去中心化标识相关联。

[0189] 在一些实施例中,可验证声明的哈希值被存储在区块链中;可验证声明被存储在数据存储中;数据存储包括以下中的一个或多个:由第二实体维护的本地数据存储,第二实体可访问的公共数据存储以及由平台维护的用于第二实体的数据存储。在一些实施例中,响应于所获得的区块链交易获得认证结果包括:查询数据存储以获得与去中心化标识相关联的可验证声明;基于获得的可验证声明,验证用户是否为第二实体的注册用户,以生成未加密的认证结果;以及利用第二实体的私钥对未加密的认证结果进行加密,以生成认证结果。

[0190] 框1731包括生成包括认证结果的不同的区块链交易。

[0191] 框1741包括将不同的区块链交易发送到区块链节点以添加到区块链。

[0192] 在一些实施例中,在获得区块链交易之前,该方法还包括:获得第一实体的用于认证用户的认证请求;生成用于获取第二实体对用户的认证结果的区块链交易;以及将区块链交易传送到区块链节点以添加到区块链。

[0193] 在一些实施例中,该方法还包括:从区块链获得不同的区块链交易,该不同的区块链交易包括第二实体对用户的认证结果,其中,认证结果表明认证成功;以及将认证结果发

送给第一实体,以准予用户访问第一实体。

[0194] 在一些实施例中,该方法还包括:从区块链获得不同的区块链交易,该不同的区块链交易包括第二实体对用户的认证结果,其中,认证结果表明认证失败;以及将认证结果发送给第一实体,以拒绝用户访问第一实体。

[0195] 图18A示出了根据一些实施例的用于基于区块链的交叉实体认证的计算机系统1800的框图。系统1800可以是图3的服务侧系统320的一个或多个组件或图1至图5和图16中示出的一个或多个其他组件(例如,DIS 1603a)的实施方式的示例。方法1900可以由计算机系统1800实现。计算机系统1800可以包括一个或多个处理器以及耦接到所述一个或多个处理器并配置有指令的一个或多个非暂时性计算机可读存储介质(例如,一个或多个存储器),所述指令可由一个或多个处理器执行以促使所述系统或设备(例如,处理器)执行上述方法,例如方法1900。计算机系统1800可以包括与指令(例如,软件指令)相对应的各种单元/模块。在一些实施例中,计算机系统1800可以被称为用于基于区块链的交叉实体认证的装置。该装置可以包括:获得模块1810,用于获得第一实体的用于认证用户的认证请求,其中,认证请求包括用户的去中心化标识(DID);生成模块1820,用于响应于确定第一实体被允许访问由第二实体背书的用户的认证信息,生成区块链交易,以获得第二实体对用户的认证结果,其中,认证结果与去中心化标识相关联;以及发送模块1830,用于将区块链交易发送至区块链节点以添加至区块链。

[0196] 图18B示出了根据一些实施例的用于基于区块链的交叉实体认证的计算机系统的1801的框图。系统1801可以是图3的服务侧系统320的一个或多个组件或图1至图5和图16中示出的一个或多个其他组件(例如,DIS 1603b)的实施方式的示例。方法1901可以由计算机系统1801实现。计算机系统1801可以包括一个或多个处理器以及耦接到所述一个或多个处理器并配置有指令的一个或多个非暂时性计算机可读存储介质(例如,一个或多个存储器),所述指令可由一个或多个处理器执行以促使所述系统或设备(例如,处理器)执行上述方法,例如方法1901。计算机系统1801可以包括与指令(例如,软件指令)相对应的各种单元/模块。在一些实施例中,计算机系统1801可以被称为用于基于区块链的交叉实体认证的装置。该装置可以包括:第一获得模块1811,用于从区块链获得包括第一实体的用于认证用户的认证请求的区块链交易,其中,认证请求包括用户的去中心化标识(DID);第二获得模块1821,用于响应于确定第一实体被允许访问由第二实体背书的用户的认证信息,响应于所获得的区块链交易获得第二实体对用户的认证结果,其中认证结果与去中心化标识相关联;生成模块1831,用于生成包括认证结果的不同的区块链交易;发送模块1841,用于将不同的区块链交易发送至区块链节点,以添加至所述区块链。

[0197] 这里描述的技术可以由一个或多个专用计算设备实现。专用计算设备可以是台式计算机系统、服务器计算机系统、便携式计算机系统、手持设备、网络设备或包含硬连线和/或程序逻辑以实现这些技术的任何其他设备或设备的组合。专用计算设备可以被实现为个人计算机、膝上型计算机、蜂窝电话、照相电话、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、平板电脑、可穿戴设备或其组合。计算设备可以通常由操作系统软件控制和协调。传统的操作系统控制和调度用于执行的计算机进程,执行存储器管理,提供文件系统、网络、I/O服务,以及提供用户接口功能,例如图形用户接口(“GUI”)等。这里描述的各种系统、装置、存储介质、模块和单元可以在专用计算设备或一个或多个

专用计算设备的一个或多个计算芯片中实现。在一些实施例中，这里描述的指令可以在专用计算设备上的虚拟机中实现。当被执行时，指令可以促使专用计算设备执行本文描述的各种方法。虚拟机可以包括软件、硬件或其组合。

[0198] 图19示出了可以实现本文描述的任何实施例的计算机系统的框图。系统1900可以在图1至图5所示的环境或系统的任何组件中实现。图1至图5所示的软件应用或服务可以在系统1900上被实现或操作。图6至图16所示的一个或多个示例方法可以由计算机系统1900的一种或多种实施方式执行。

[0199] 计算机系统1900可以包括用于通信信息的总线1902或其他通信机制、与总线1902耦接以处理信息的一个或多个硬件处理器1904。硬件处理器1904可以是例如一个或多个通用微处理器。

[0200] 计算机系统1900还可以包括耦合到总线1902、用于存储可由处理器1904执行的信息和指令的主存储器1906，例如随机存取存储器(RAM)、高速缓存和/或其他动态存储设备。主存储器1906还可以用于在执行可由处理器1904执行的指令期间存储临时变量或其他中间信息。当这些指令存储在处理器1904可访问的存储介质中时，这些指令将计算机系统1900呈现为被定制以执行指令中指定的操作的专用机器。计算机系统1900还可以包括耦合到总线1902、用于存储处理器1904的静态信息和指令的只读存储器(ROM)1908或其他静态存储设备。诸如磁盘、光盘或USB拇指驱动器(闪存驱动器)等的存储设备1910可以被提供并被耦合到总线1902以存储信息和指令。

[0201] 计算机系统1900可以使用与计算机系统相结合使得计算机系统1900成为专用机器或将计算机系统1900编程为专用机器的定制硬连线逻辑、一个或多个ASIC或FPGA、固件和/或程序逻辑实现本文所述的技术。根据一个实施例，这里描述的操作、方法和处理由计算机系统1900响应于处理器1904执行主存储器1906中包含的一个或多个指令的一个或多个序列而执行。这些指令可以从例如存储设备1910的另一存储介质读入主存储器1906。主存储器1906中包含的指令序列的执行可以促使处理器1904执行这里描述的处理步骤。在替代实施例中，可以使用硬连线电路代替软件指令或与软件指令组合。

[0202] 主存储器1906、ROM 1908和/或存储设备1910可以包括非暂时性存储介质。这里使用的术语“非暂时性介质”和类似术语是指存储促使机器以特定方式操作的数据和/或指令的介质，所述介质不包括暂时性信号。这种非暂时性介质可以包括非易失性介质和/或易失性介质。非易失性介质包括例如光盘或磁盘，例如存储设备1910。易失性介质包括动态存储器，例如主存储器1906。常规形式的非暂时性介质包括，例如，软磁盘、软盘、硬盘、固态驱动器、磁带或任何其他磁数据存储介质、CD-ROM、任何其他光学数据存储介质、具有孔图案的任何物理介质、RAM、PROM和EPROM、FLASH-EPROM、NVRAM、任何其他存储器芯片或盒式磁带以及它们的网络版本。

[0203] 计算机系统1900还可以包括耦接到总线1902的网络接口1918。网络接口1918可以提供耦接到一个或多个网络链路的双向数据通信，所述一个或多个网络链路连接到一个或多个本地网络。例如，网络接口1918可以是综合业务数字网(ISDN)卡、电缆调制解调器、卫星调制解调器或调制解调器，以提供与相应类型的电话线的数据通信连接。作为另一示例，网络接口1918可以是局域网(LAN)卡，以提供与兼容LAN(或WAN组件以与WAN通信)的数据通信连接。还可以实现无线链路。在任何这样的实施方式中，网络接口1918可以发送和接收携

带表示各种类型的信息的数字数据流的电信号、电磁信号或光信号。

[0204] 计算机系统1900可以通过网络、网络链路和网络接口1918发送消息和接收数据，包括程序代码。在因特网示例中，服务器可以通过因特网、ISP、本地网络和网络接口1918发送用于应用程序的请求代码。

[0205] 所接收的代码当被接收时可以由处理器1904执行，和/或存储在存储设备1910或其他非易失性存储器中以用于稍后执行。

[0206] 前面部分中描述的每个处理、方法和算法可以体现在由包括计算机硬件的一个或多个计算机系统或者计算机处理器执行的代码模块中并且被其完全或部分自动化地实现。处理和算法可以部分或全部地在专用电路中实现。

[0207] 上述各种特征和处理可以彼此独立地使用，或者可以以各种方式组合。所有可能的组合和子组合都旨在落入本文的范围内。另外，在一些实施方式中可以省略某些方法或处理框。本文描述的方法和处理也不限于任何特定顺序，与其相关的框或状态可以以适当的其他顺序执行。例如，所描述的框或状态可以以不同于具体公开的顺序执行，或者多个框或状态可以在单个框或状态中组合。框或状态的示例可以串行、并行或以某种其他方式执行。可将框或状态添加到所公开的实施例中或从所公开的实施例中移除。这里描述的系统和组件的示例可与所描述的不同地被配置。例如，与所公开的实施例相比，可添加、移除或重新布置元件。

[0208] 本文描述的方法的各种操作可以至少部分地由被临时配置(例如，通过软件)或被永久配置为执行相关操作的一个或多个处理器执行。无论是临时配置还是永久配置，这样的处理器可以构成处理器实现的引擎，所述处理器实现的引擎用于执行本文描述的一个或多个操作或功能。

[0209] 类似地，这里描述的方法可以至少部分地由处理器实现，其中特定处理器是硬件的示例。例如，所述方法的至少一些操作可以由一个或多个处理器或处理器实现的引擎执行。此外，一个或多个处理器还可操作以支持“云计算”环境中的相关操作的性能，或作为“软件即服务”(SaaS)操作。例如，至少一些操作可以由一组计算机(作为包括处理器的机器的示例)执行，这些操作可以经由网络(例如，因特网)经由一个或多个适当的接口(例如，应用编程接口(API))被访问。

[0210] 某些操作的性能可以在处理器之间分配，不仅驻留在单个机器中，而且跨多个机器被部署。在一些实施例中，处理器或处理器实现的引擎可以位于单个地理位置(例如，在家庭环境、办公室环境或服务器群内)。在其他实施例中，处理器或处理器实现的引擎可以分布在多个地理位置。

[0211] 在本文中，多个实例可实现作为单个实例所描述的组件、操作或结构。尽管一个或多个方法的各个操作被示出并描述为独立的操作，但是可以同时执行一个或多个独立的操作，并且不需要以所示的顺序执行所述操作。在配置中作为独立组件呈现的结构和功能可以实现为组合结构或组件。类似地，作为单个组件呈现的结构和功能可以实现为独立的组件。这些和其他变化、修改、添加和改进都落入本文中的主题的范围内。

[0212] 尽管已经参考具体实施例描述了主题的概述，但是在不脱离本文的实施例的较宽范围的情况下，可以对这些实施例进行各种修改和改变。具体实施方式不应被视为具有限制意义，并且各种实施例的范围仅由所附权利要求以及这些权利要求所赋予的等同物的全

部范围限定。此外，这里使用的相关术语(诸如“第一”、“第二”、“第三”等)不表示任何顺序、高度或重要性，而是用于将一个元件与另一元件区分开。此外，术语“一”、“一个”和“多个”在本文中并不表示对数量的限制，而是表示存在至少一个所述的物品。另外，在本文中，“或”是包括性的而不是排他性的，除非另外明确指出或通过上下文另外指出。因此，在本文中，“A或B”是指“A、B或两者”，除非另外明确指出或通过上下文另外指出。此外，“和”既是连接性的又是数量性的，除非另外明确指出或通过上下文另外指出。因此，在本文中，“A和B”是在连接性上或者数量性上指“A和B”，除非另外明确指出或通过上下文另外指出。

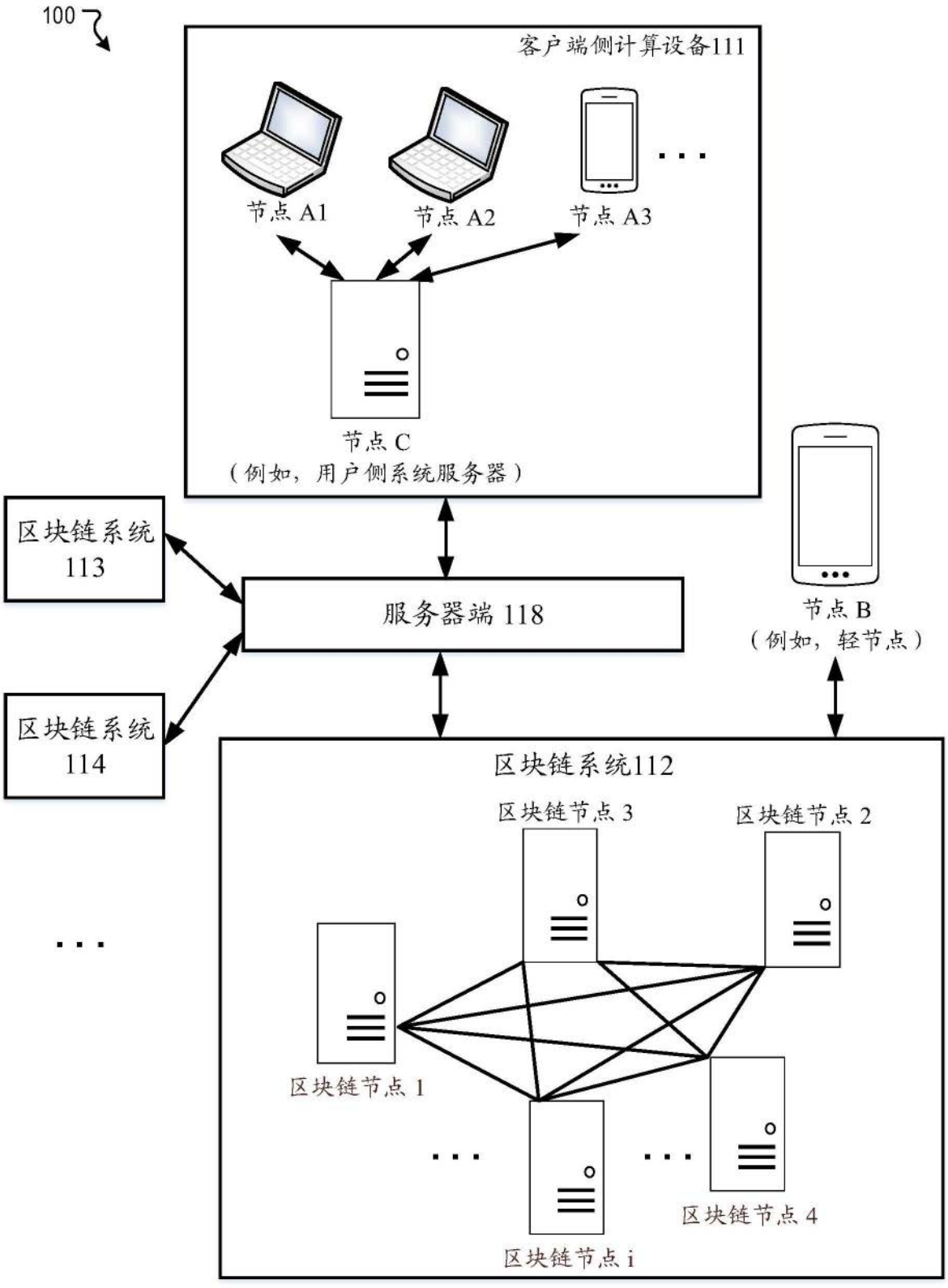

100
客户端侧计算设备111
节点 A1
节点 A2
节点 A3
节点 C
（例如，用户侧系统服务器）
区块链系统
113
服务器端 118
节点 B
（例如，轻节点）
区块链系统
114
区块链系统112
区块链节点 3
区块链节点 2
区块链节点 1
区块链节点 4
区块链节点 i

图1

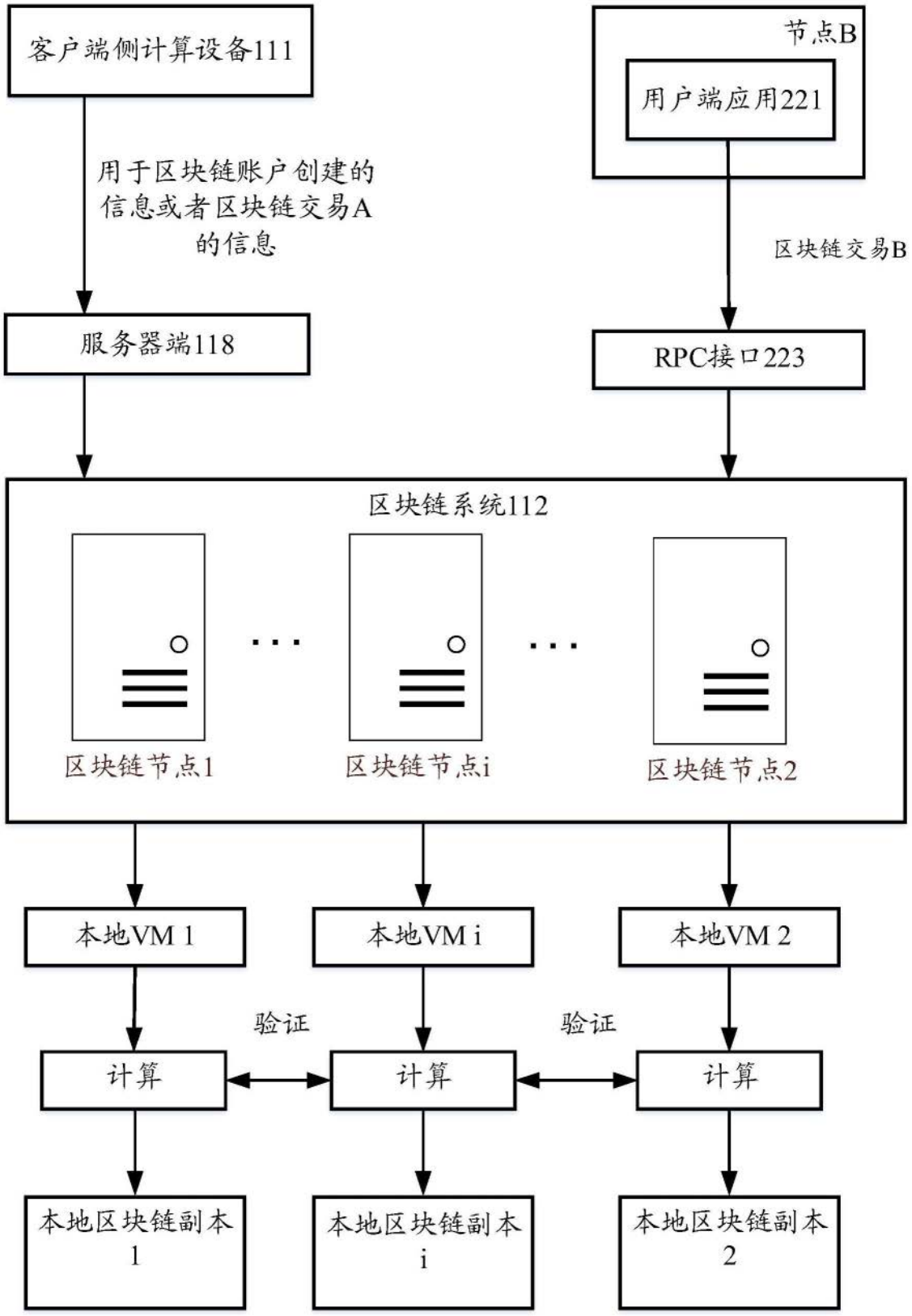

客户端侧计算设备111
节点B
用户端应用221
用于区块链账户创建的信息或者区块链交易A的信息
区块链交易B
服务器端118
RPC接口223
区块链系统112
区块链节点1
区块链节点i
区块链节点2
本地VM 1
本地VM i
本地VM 2
验证
验证
计算
计算
计算
本地区块链副本1
本地区块链副本i
本地区块链副本2

图2

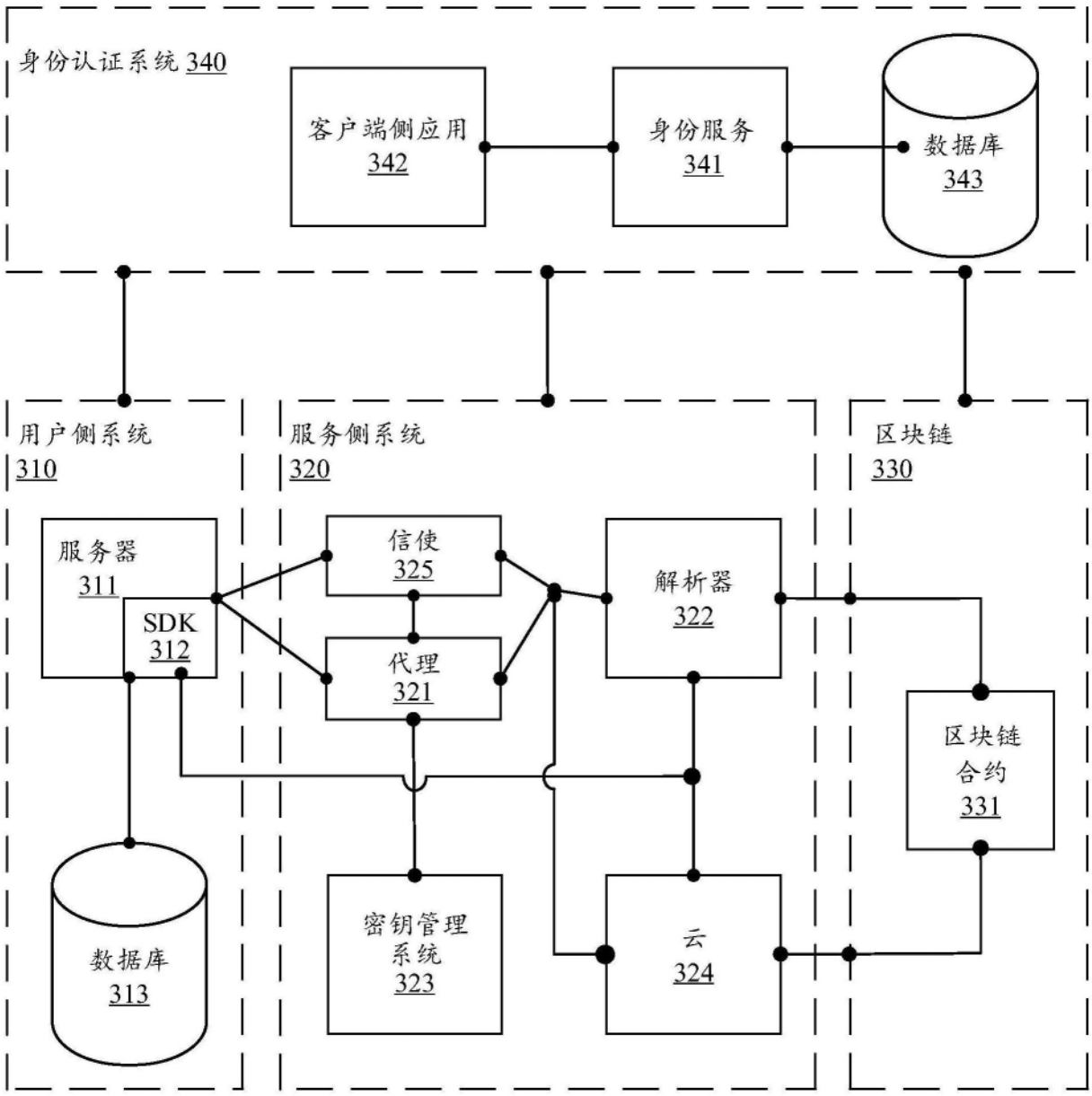

身份认证系统 340
客户端侧应用
342
身份服务
341
数据库
343
用户侧系统
310
服务侧系统
320
区块链
330
服务器
311
SDK
312
信使
325
代理
321
解析器
322
区块链
合约
331
数据库
313
密钥管理
系统
323
云
324

图3

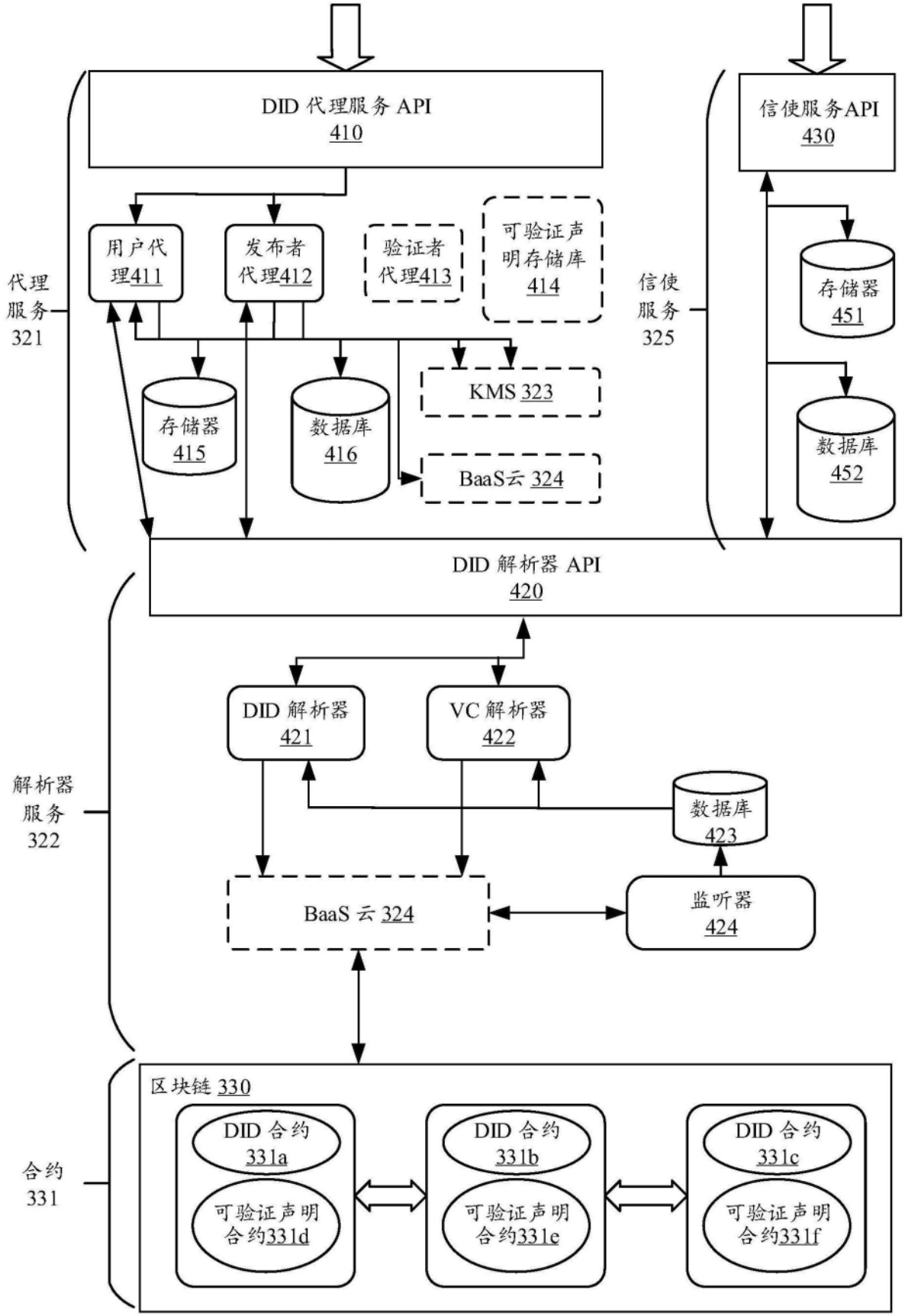

DID 代理服务 API
410
信使服务API
430
用户代理411
发布者代理412
验证者代理413
可验证声明存储库
414
代理服务
321
信使服务
325
存储器
451
KMS 323
存储器
415
数据库
416
数据库
452
BaaS云 324
DID 解析器 API
420
DID 解析器
421
VC 解析器
422
解析器服务
322
数据库
423
BaaS 云 324
监听器
424
区块链 330
DID 合约
331a
DID 合约
331b
DID 合约
331c
可验证声明合约331d
可验证声明合约331e
可验证声明合约331f
合约
331

图4

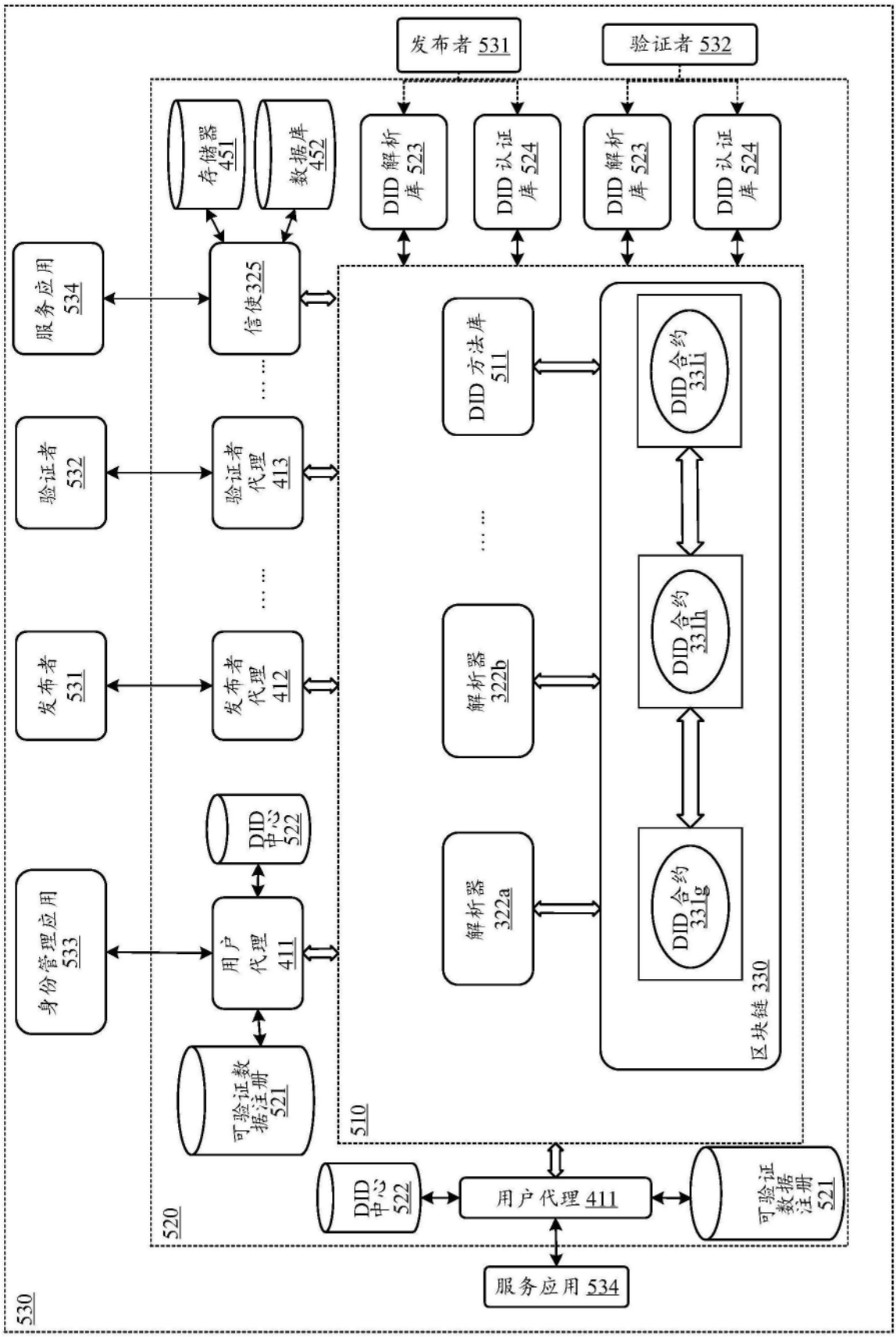

530
520
510
发布者 531
验证者 532
存储器 451
数据库 452
DID 解析库 523
DID 认证库 524
DID 解析库 523
DID 认证库 524
服务应用 534
信使325
DID 方法库 511
DID 合约 331i
验证者 532
验证者代理 413
DID 合约 331h
发布者 531
发布者代理 412
解析器 322b
DID 合约 331g
身份管理应用 533
用户代理 411
DID 中心 522
解析器 322a
区块链 330
可验证数据注册 521
DID 中心 522
用户代理 411
可验证数据注册 521
服务应用 534

图5

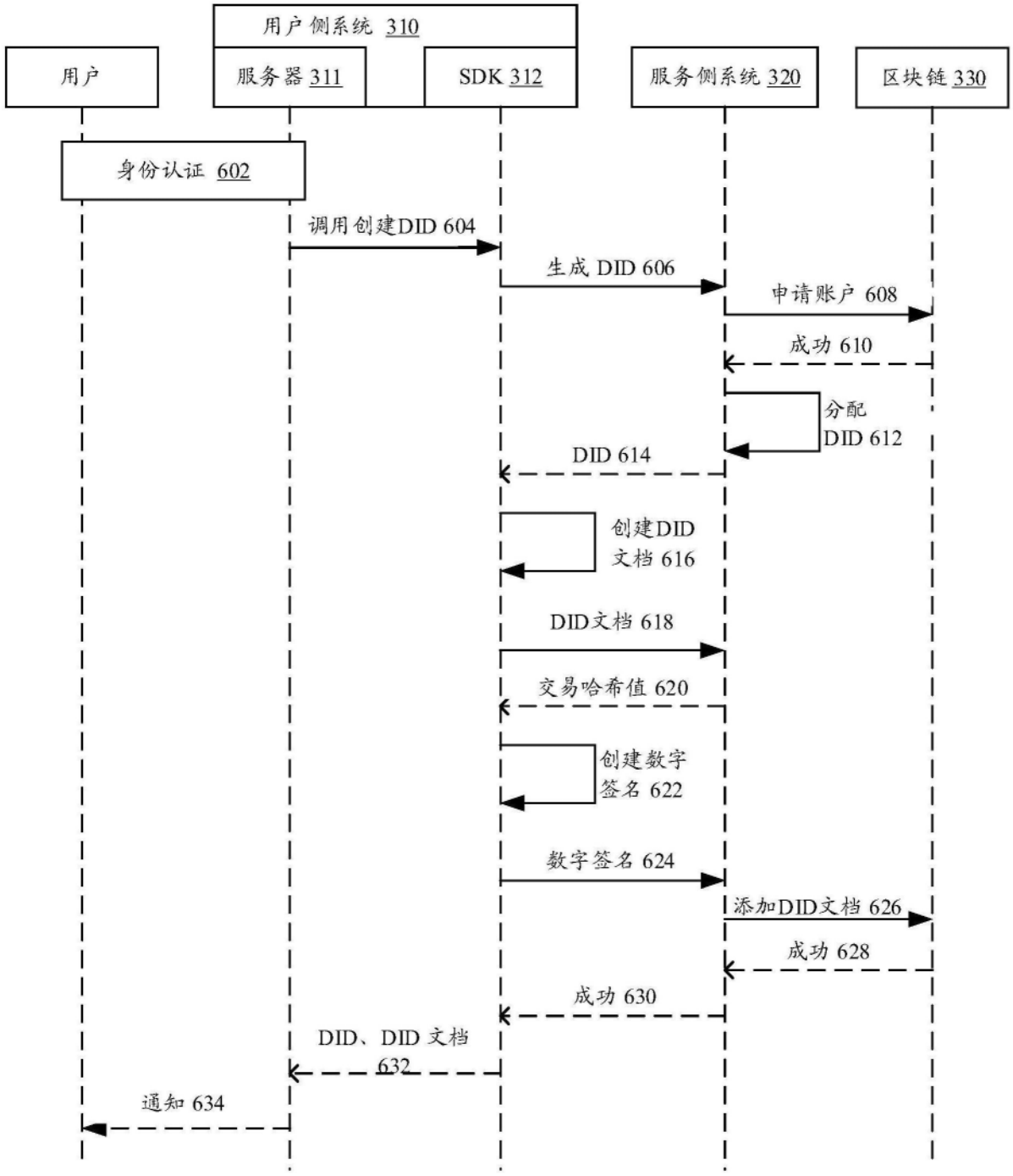

用户侧系统 310
用户
服务器 311
SDK 312
服务侧系统 320
区块链 330
身份认证 602
调用创建DID 604
生成 DID 606
申请账户 608
成功 610
分配 DID 612
DID 614
创建DID 文档 616
DID文档 618
交易哈希值 620
创建数字 签名 622
数字签名 624
添加DID文档 626
成功 628
成功 630
DID、DID 文档 632
通知 634

图6A

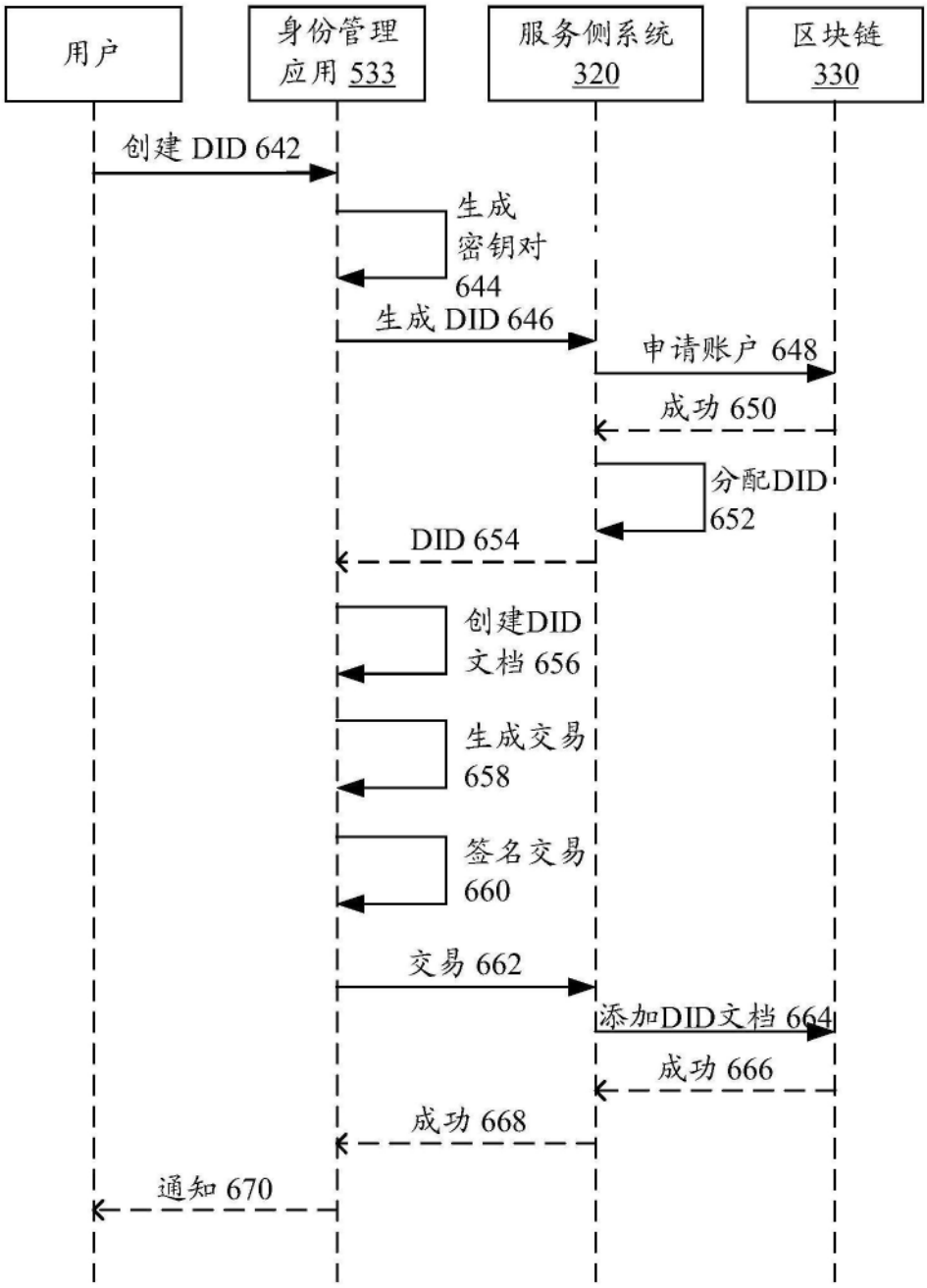

用户
身份管理应用 533
服务侧系统 320
区块链 330
创建 DID 642
生成密钥对 644
生成 DID 646
申请账户 648
成功 650
分配DID 652
DID 654
创建DID文档 656
生成交易 658
签名交易 660
交易 662
添加DID文档 664
成功 666
成功 668
通知 670

图6B

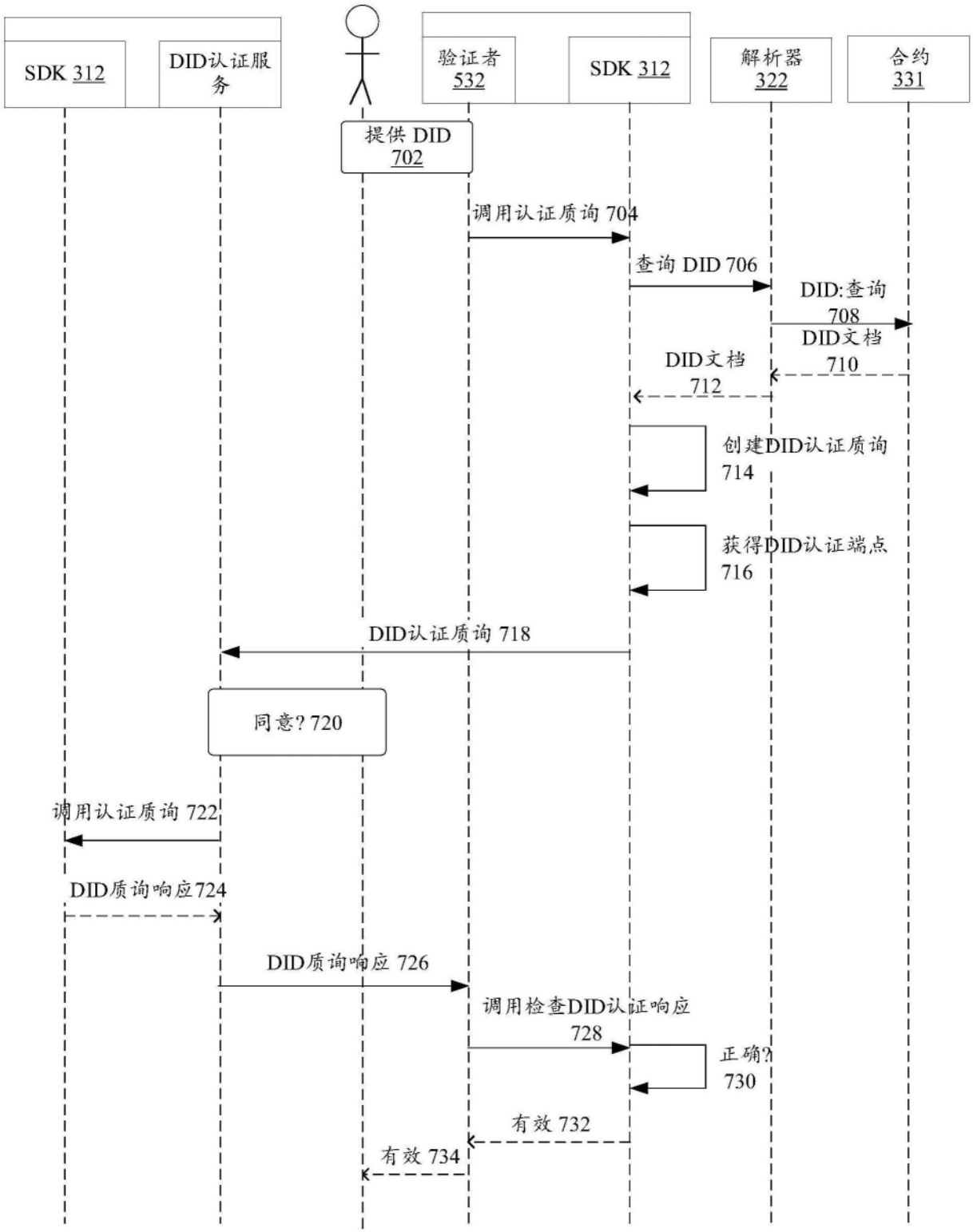

SDK 312
DID认证服务
验证者 532
SDK 312
解析器 322
合约 331
提供 DID 702
调用认证质询 704
查询 DID 706
DID:查询 708
DID文档 710
DID文档 712
创建DID认证质询 714
获得DID认证端点 716
DID认证质询 718
同意? 720
调用认证质询 722
DID质询响应724
DID质询响应 726
调用检查DID认证响应 728
正确? 730
有效 732
有效 734

图7

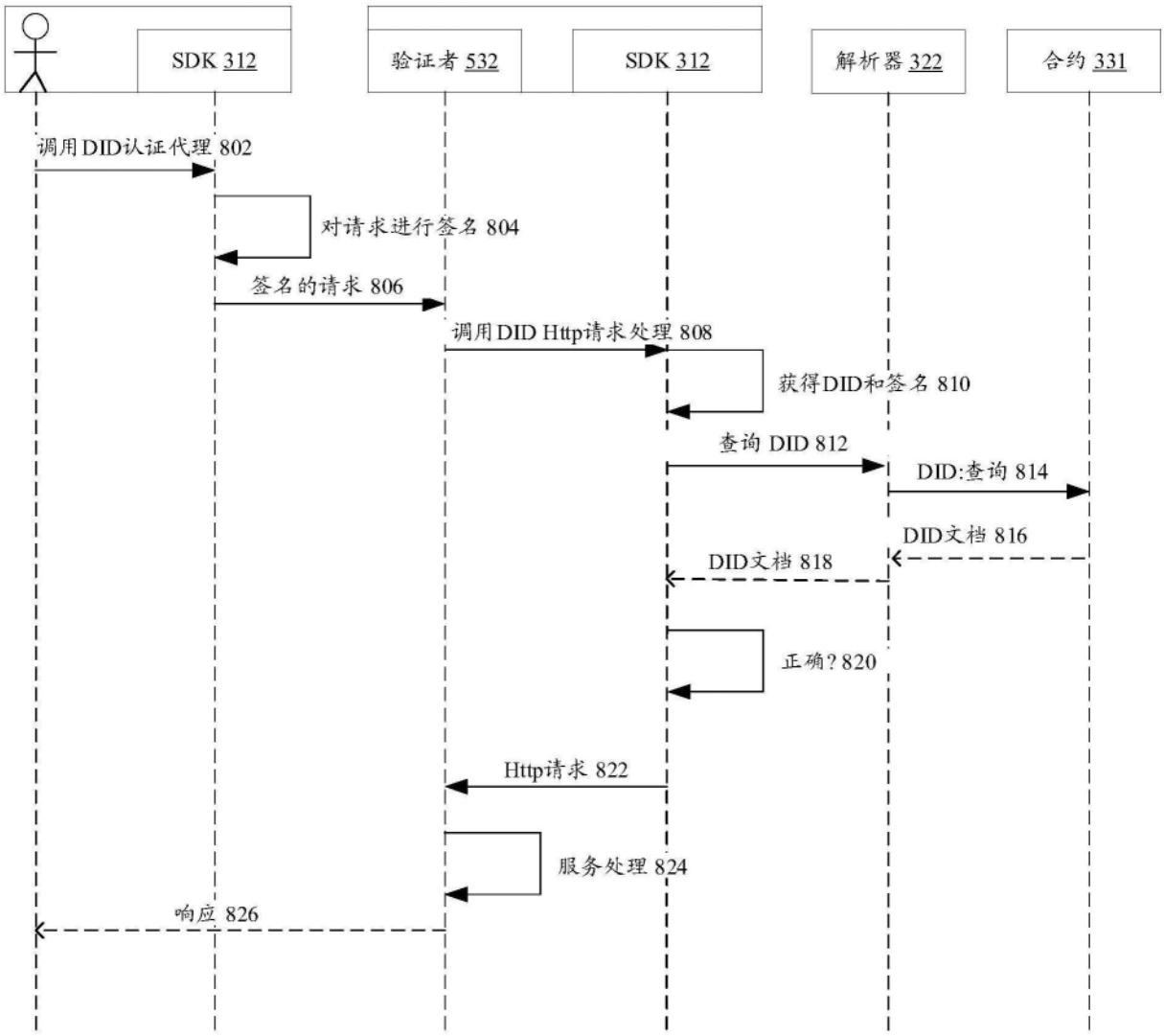

SDK 312
验证者 532
SDK 312
解析器 322
合约 331
调用DID认证代理 802
对请求进行签名 804
签名的请求 806
调用DID Http请求处理 808
获得DID和签名 810
查询 DID 812
DID:查询 814
DID文档 816
DID文档 818
正确? 820
Http请求 822
服务处理 824
响应 826

图8

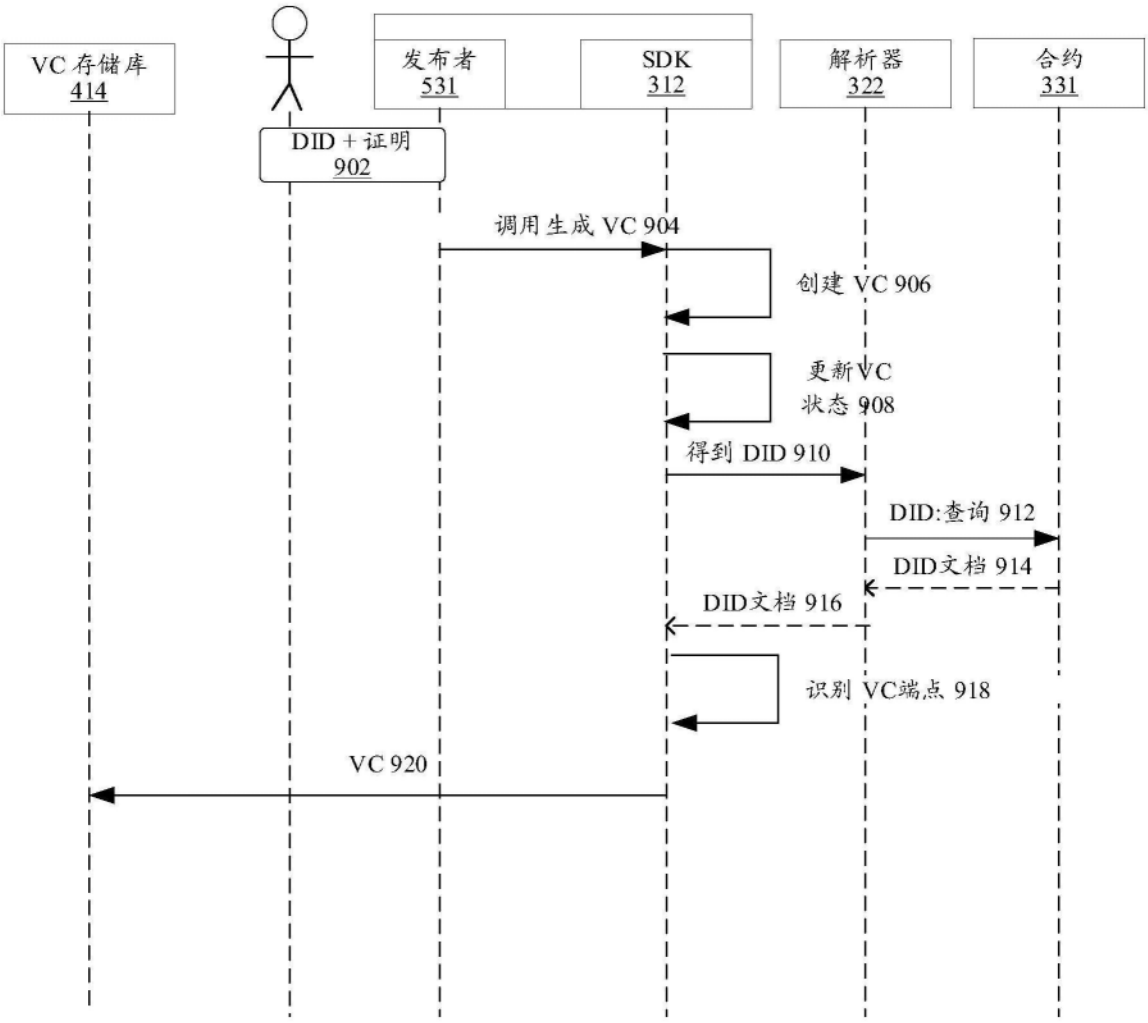

VC 存储库
414
发布者
531
SDK
312
解析器
322
合约
331
DID + 证明
902
调用生成 VC 904
创建 VC 906
更新VC
状态 908
得到 DID 910
DID:查询 912
DID文档 914
DID文档 916
识别 VC端点 918
VC 920

图9

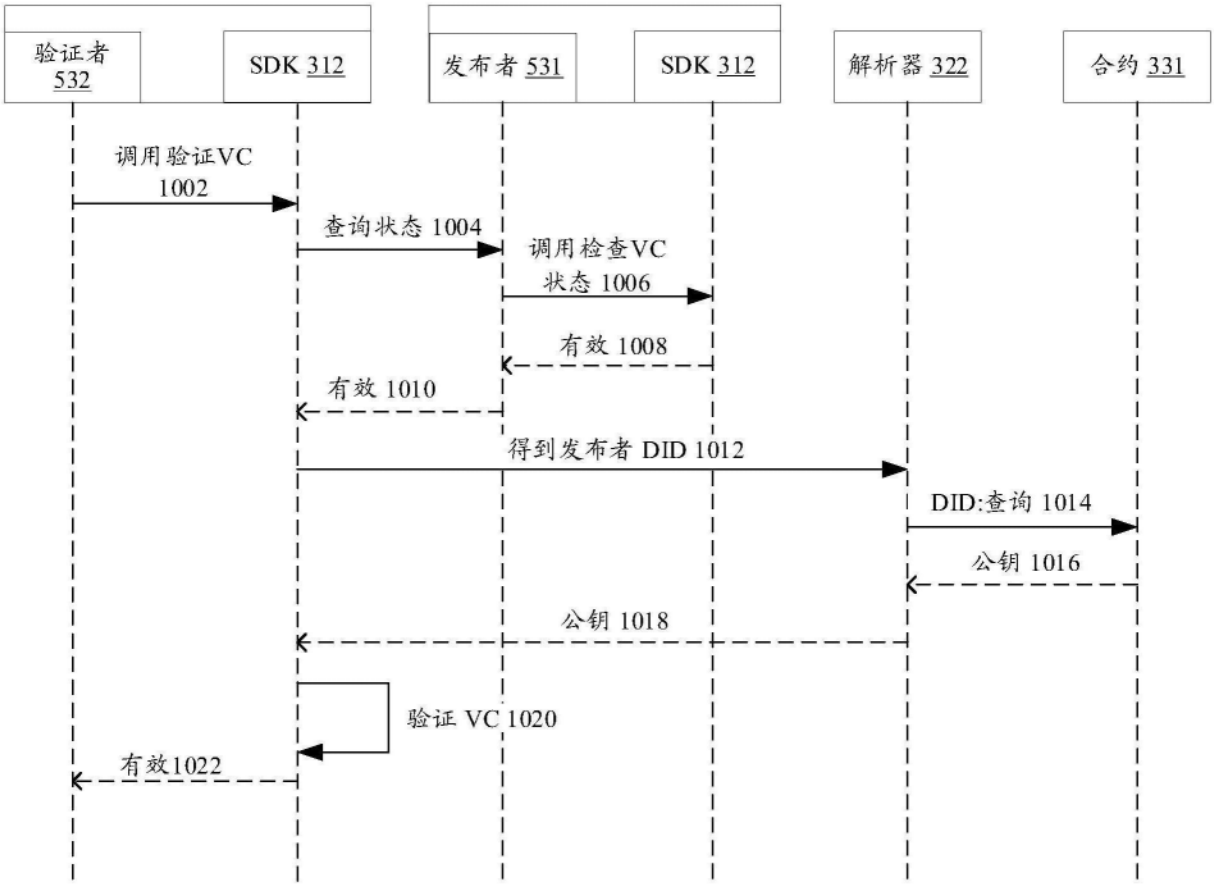

验证者 532
SDK 312
发布者 531
SDK 312
解析器 322
合约 331
调用验证VC 1002
查询状态 1004
调用检查VC 状态 1006
有效 1008
有效 1010
得到发布者 DID 1012
DID:查询 1014
公钥 1016
公钥 1018
验证 VC 1020
有效1022

图10

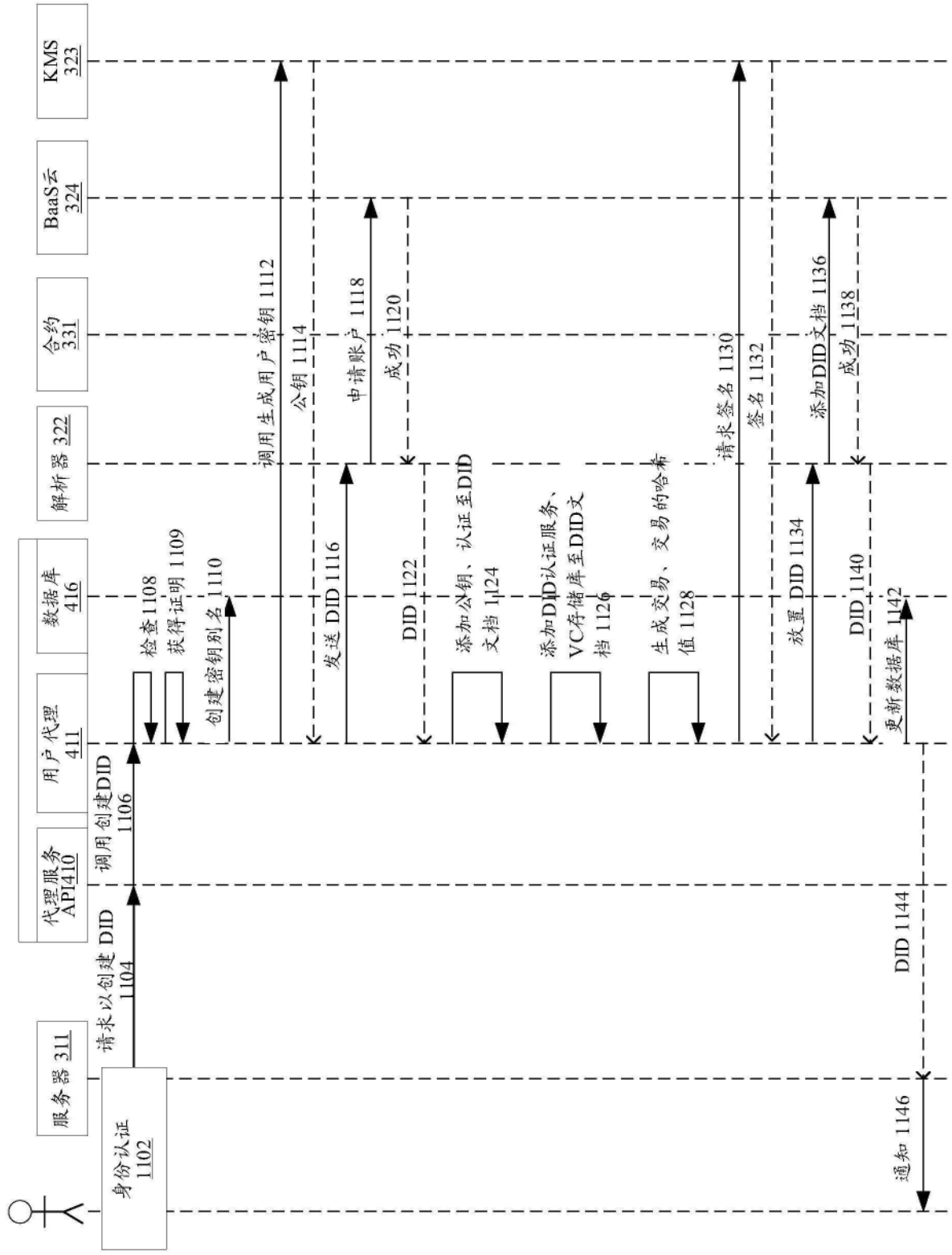

身份认证 1102
服务器 311
代理服务 API410
用户代理 411
数据库 416
解析器 322
合约 331
BaaS云 324
KMS 323
请求以创建 DID 1104
调用创建DID 1106
检查1108
获得证明 1109
创建密钥别名 1110
调用生成用户密钥 1112
公钥 1114
发送 DID 1116
申请账户 1118
成功 1120
DID 1122
添加公钥、认证至DID文档 1124
添加DID认证服务、VC存储库至DID文档 1126
生成交易、交易的哈希值 1128
请求签名 1130
签名 1132
放置 DID 1134
添加DID文档 1136
成功 1138
DID 1140
更新数据库 1142
DID 1144
通知 1146

图11

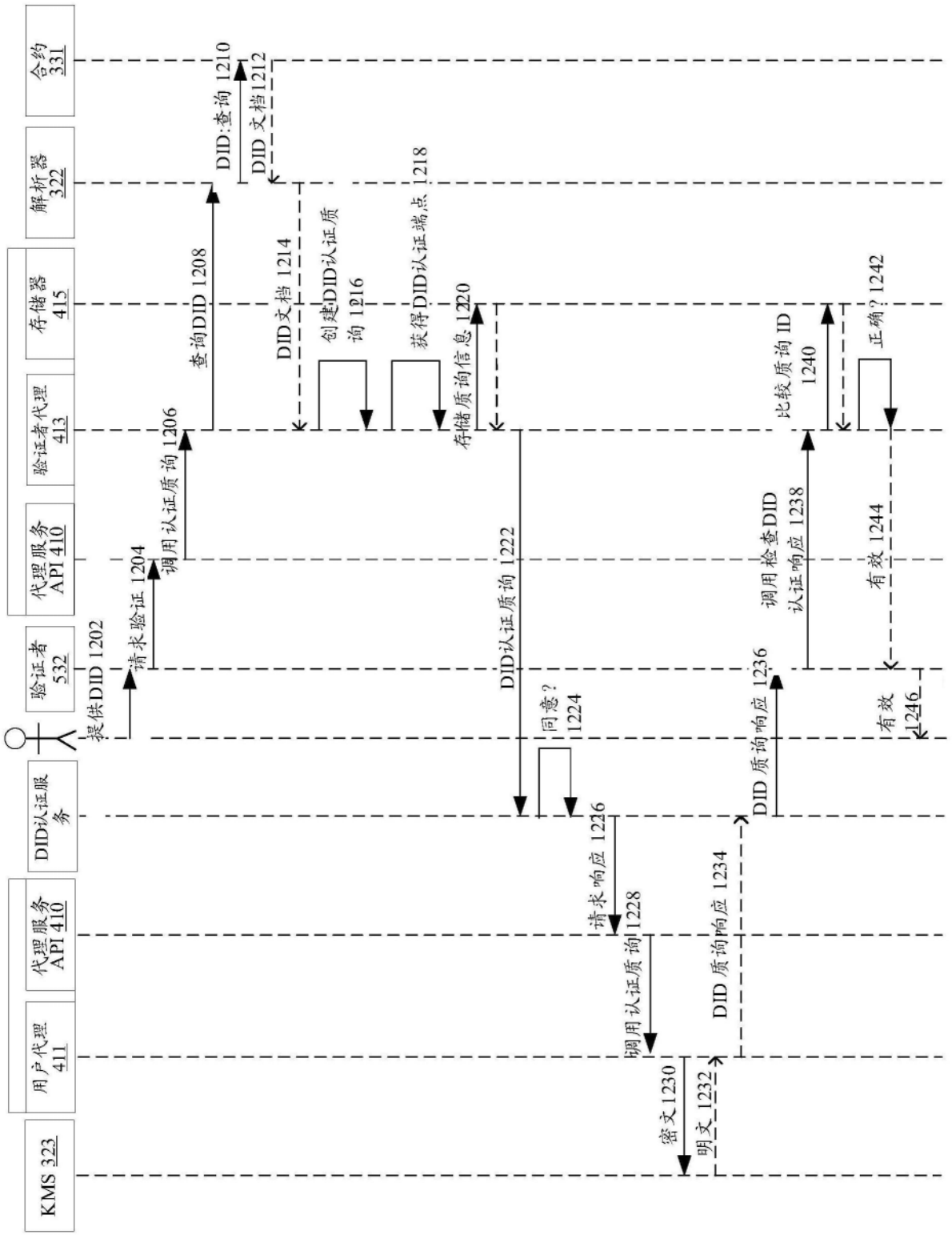

KMS 323
用户代理 411
代理服务 API 410
DID认证服务
验证者 532
代理服务 API 410
验证者代理 413
存储器 415
解析器 322
合约 331
提供DID 1202
请求验证 1204
调用认证质询 1206
查询DID 1208
DID:查询 1210
DID文档1212
DID文档 1214
创建DID认证质询 1216
获得DID认证端点 1218
存储质询信息 1220
DID认证质询 1222
同意? 1224
请求响应 1226
调用认证质询 1228
密文1230
明文 1232
DID 质询响应 1234
DID 质询响应 1236
调用检查DID认证响应 1238
比较质询 ID 1240
正确? 1242
有效 1244
有效 1246

图12

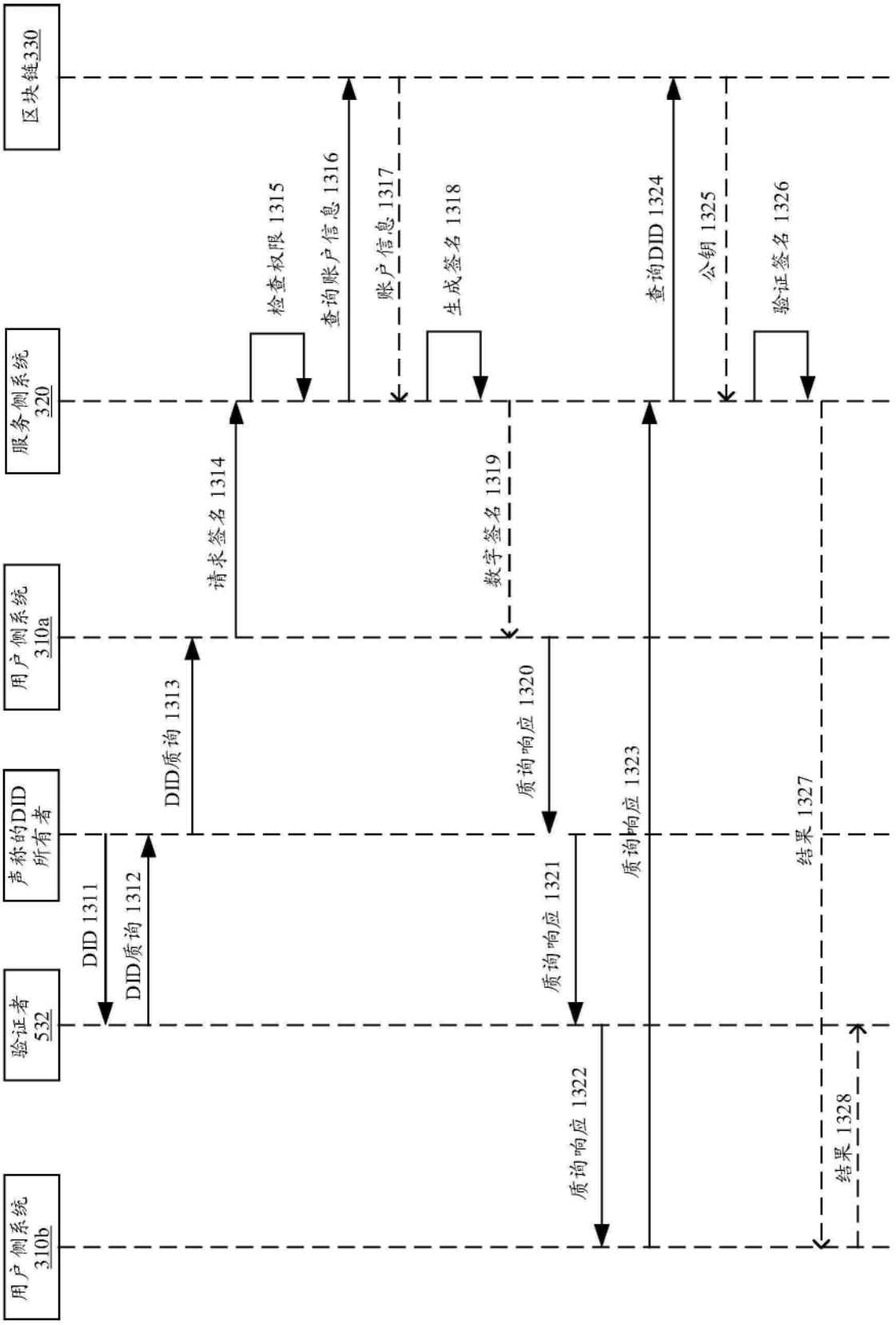

区块链330
服务侧系统320
用户侧系统310a
声称的DID所有者
验证者532
用户侧系统310b
检查权限 1315
查询账户信息 1316
账户信息 1317
生成签名 1318
查询DID 1324
公钥 1325
验证签名 1326
请求签名 1314
数字签名 1319
DID质询 1313
质询响应 1320
质询响应 1323
结果 1327
DID 1311
DID质询 1312
质询响应 1321
质询响应 1322
结果 1328

图13

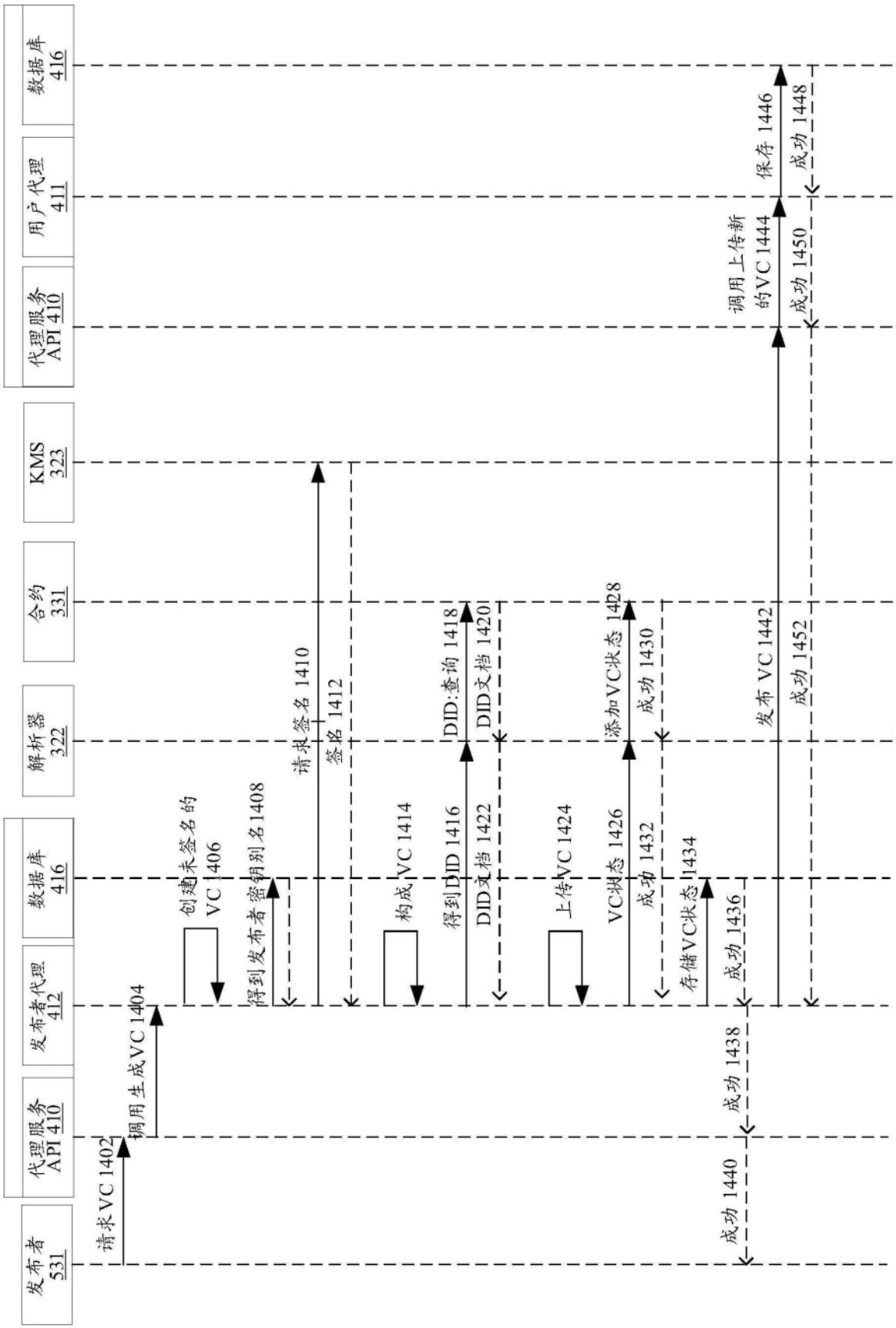

发布者 531
代理服务 API 410
发布者代理 412
数据库 416
解析器 322
合约 331
KMS 323
代理服务 API 410
用户代理 411
数据库 416
请求VC 1402
调用生成VC 1404
创建未签名的 VC 1406
得到发布者密钥别名1408
请求签名 1410
签名 1412
构成VC 1414
得到DID 1416
DID:查询 1418
DID文档 1420
DID文档 1422
上传VC 1424
VC状态 1426
添加VC状态 1428
成功 1430
成功 1432
存储VC状态 1434
成功 1436
成功 1438
成功 1440
发布 VC 1442
调用上传新的VC 1444
保存 1446
成功 1448
成功 1450
成功 1452

图14

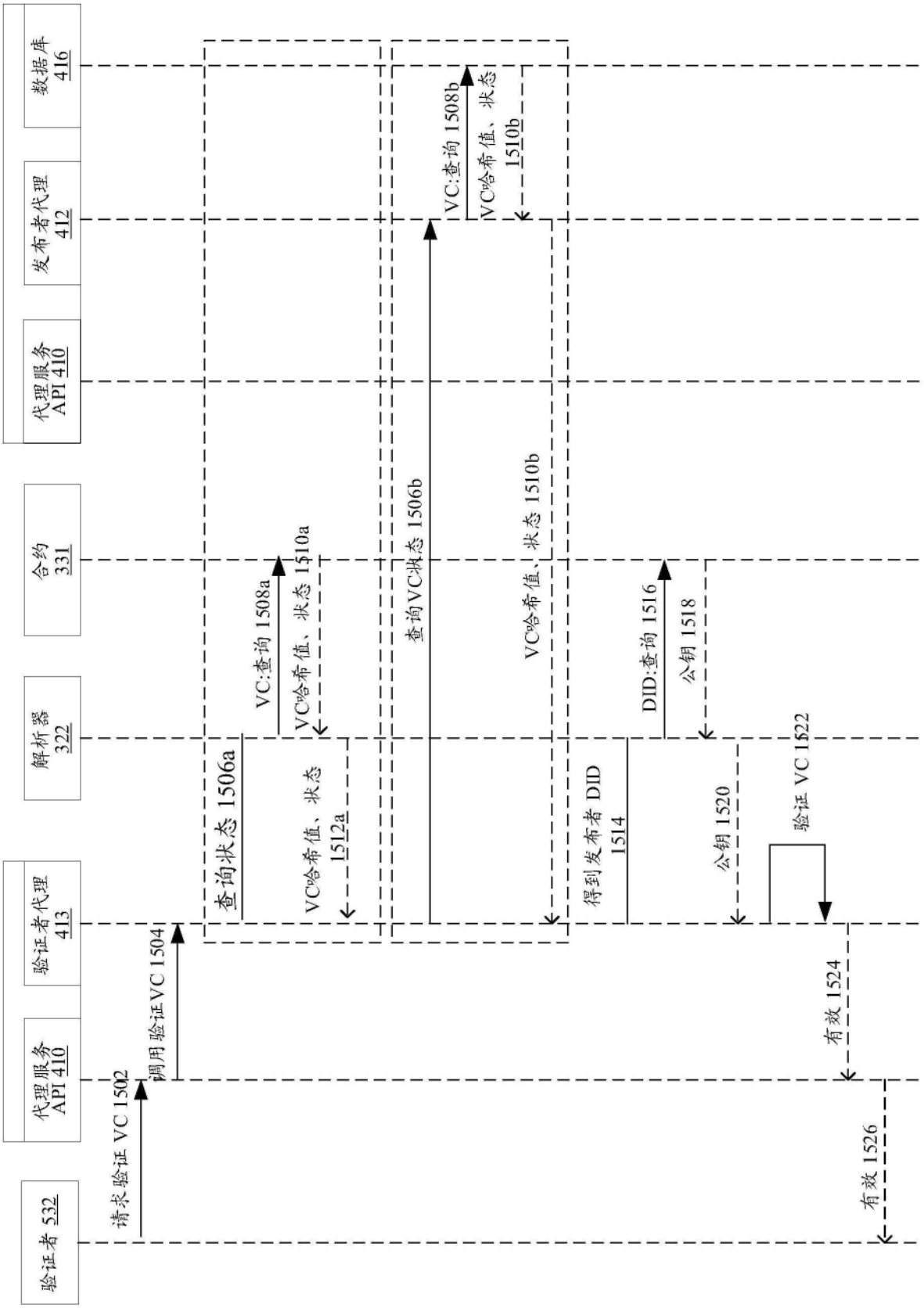

验证者 532
代理服务 API 410
验证者代理 413
解析器 322
合约 331
代理服务 API 410
发布者代理 412
数据库 416
请求验证 VC 1502
调用 验证VC 1504
查询状态 1506a
VC:查询 1508a
VC哈希值、状态 1510a
VC哈希值、状态 1512a
查询VC状态 1506b
VC:查询 1508b
VC哈希值、状态 1510b
VC哈希值、状态 1510b
得到发布者 DID 1514
DID:查询 1516
公钥 1518
公钥 1520
验证 VC 1522
有效 1524
有效 1526

图15

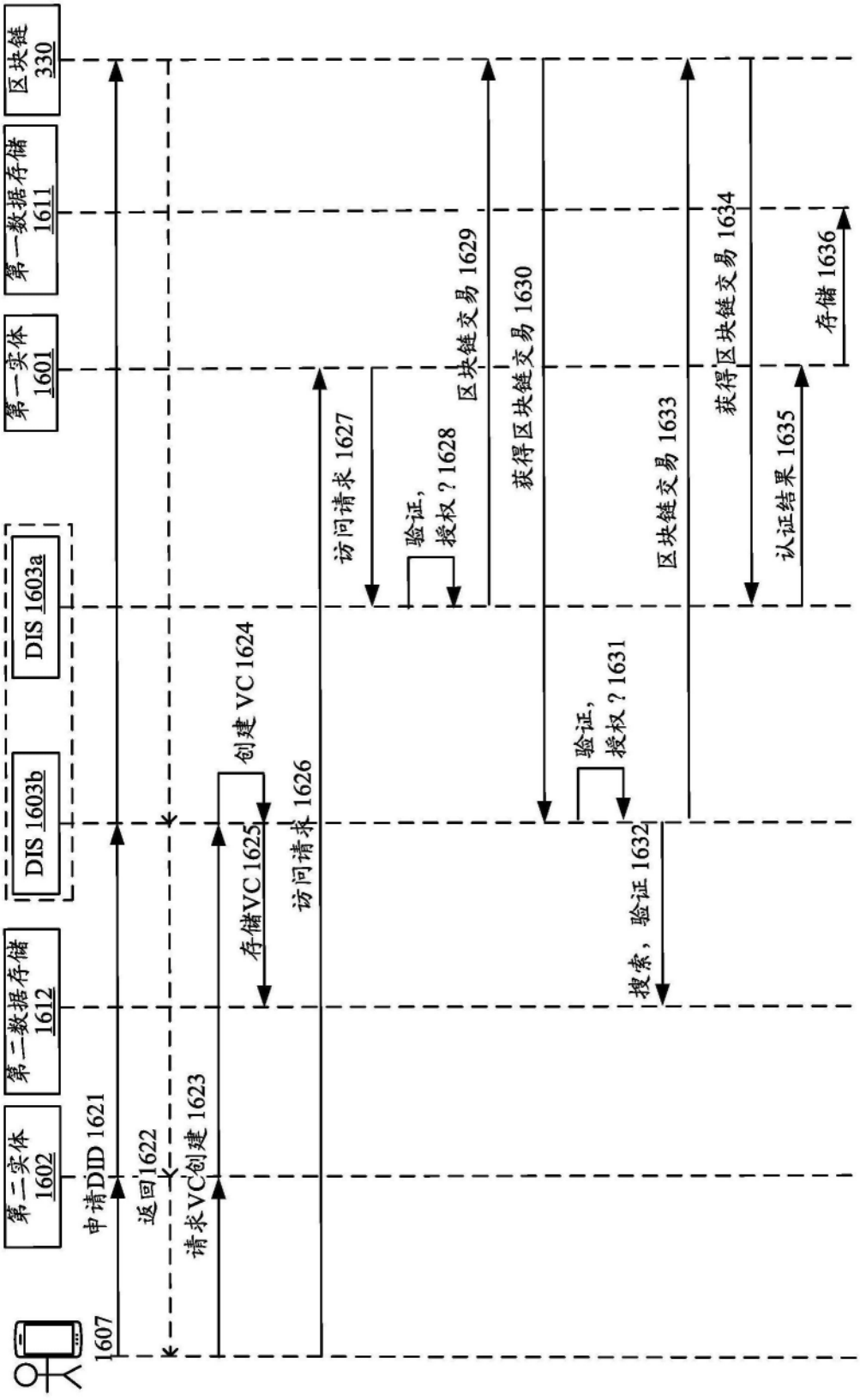

第二实体 1602
第二数据存储 1612
DIS 1603b
DIS 1603a
第一实体 1601
第一数据存储 1611
区块链 330
1607
申请DID 1621
返回1622
请求VC创建 1623
存储VC 1625
创建 VC 1624
访问请求 1626
访问请求 1627
验证，授权？1628
区块链交易 1629
获得区块链交易 1630
验证，授权？1631
搜索，验证 1632
区块链交易 1633
获得区块链交易 1634
认证结果 1635
存储 1636

图16

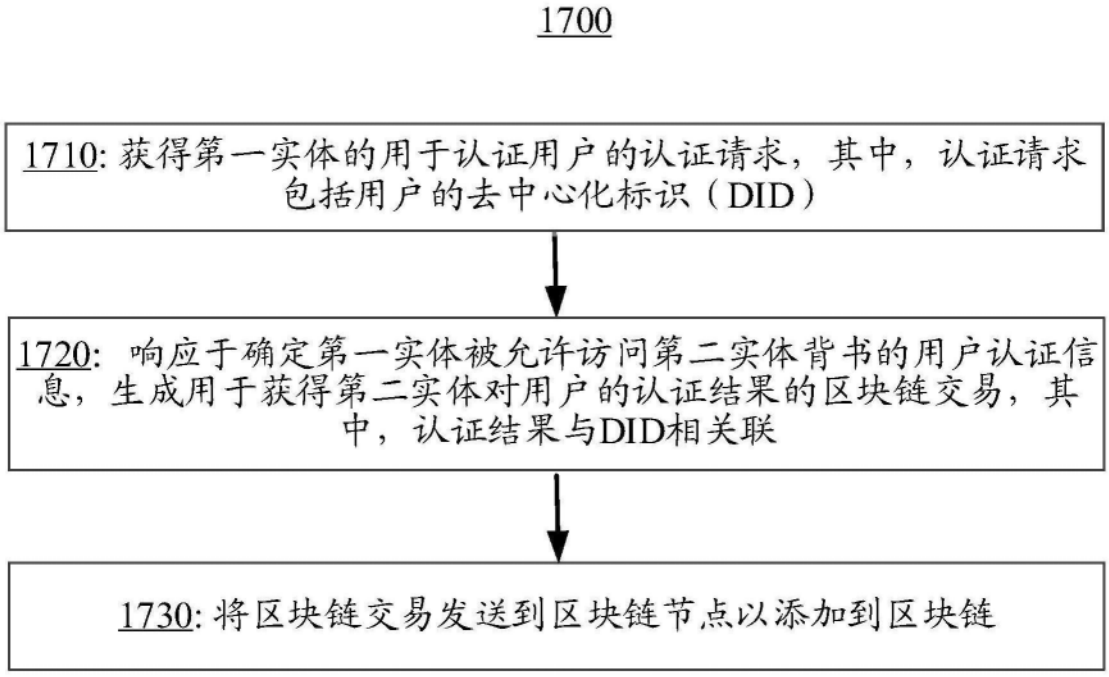

1700
1710: 获得第一实体的用于认证用户的认证请求，其中，认证请求包括用户的去中心化标识（DID）
1720: 响应于确定第一实体被允许访问第二实体背书的用户认证信息，生成用于获得第二实体对用户的认证结果的区块链交易，其中，认证结果与DID相关联
1730: 将区块链交易发送到区块链节点以添加到区块链

图17A

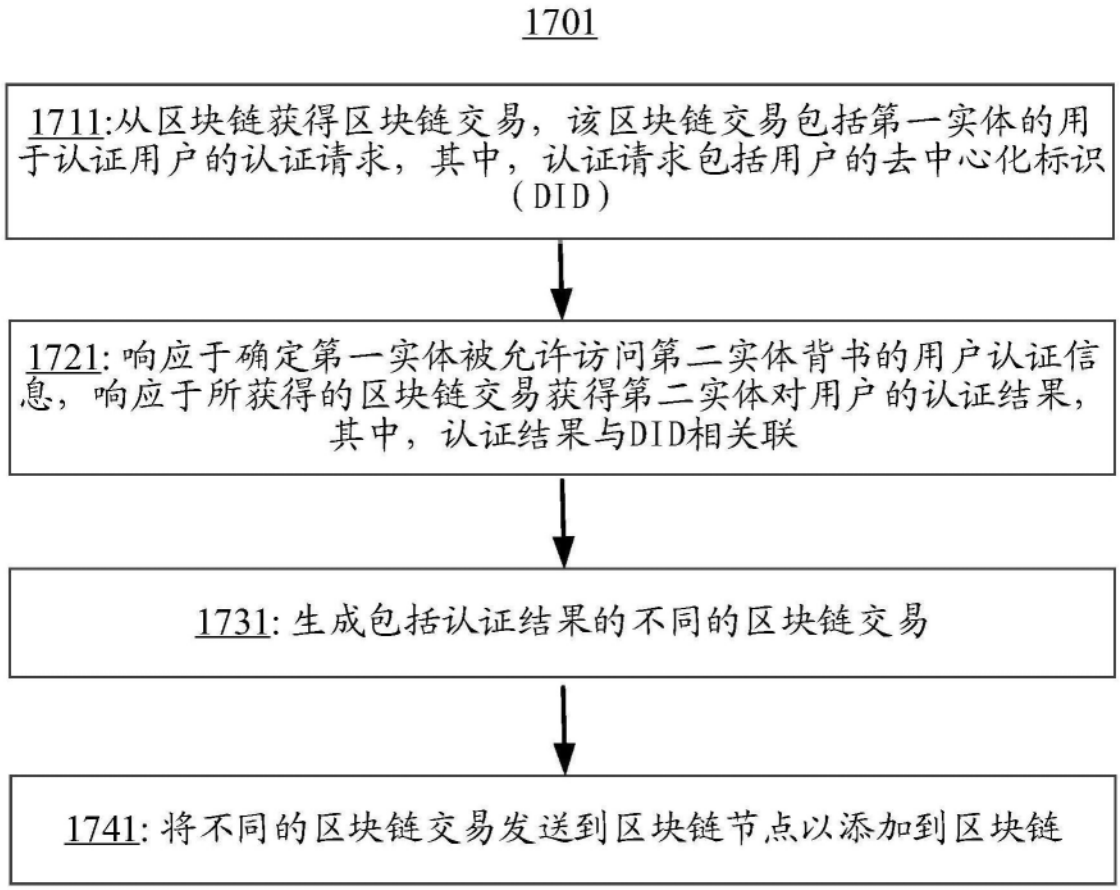

1701
1711:从区块链获得区块链交易，该区块链交易包括第一实体的用于认证用户的认证请求，其中，认证请求包括用户的去中心化标识（DID）
1721: 响应于确定第一实体被允许访问第二实体背书的用户认证信息，响应于所获得的区块链交易获得第二实体对用户的认证结果，其中，认证结果与DID相关联
1731: 生成包括认证结果的不同的区块链交易
1741: 将不同的区块链交易发送到区块链节点以添加到区块链

图17B

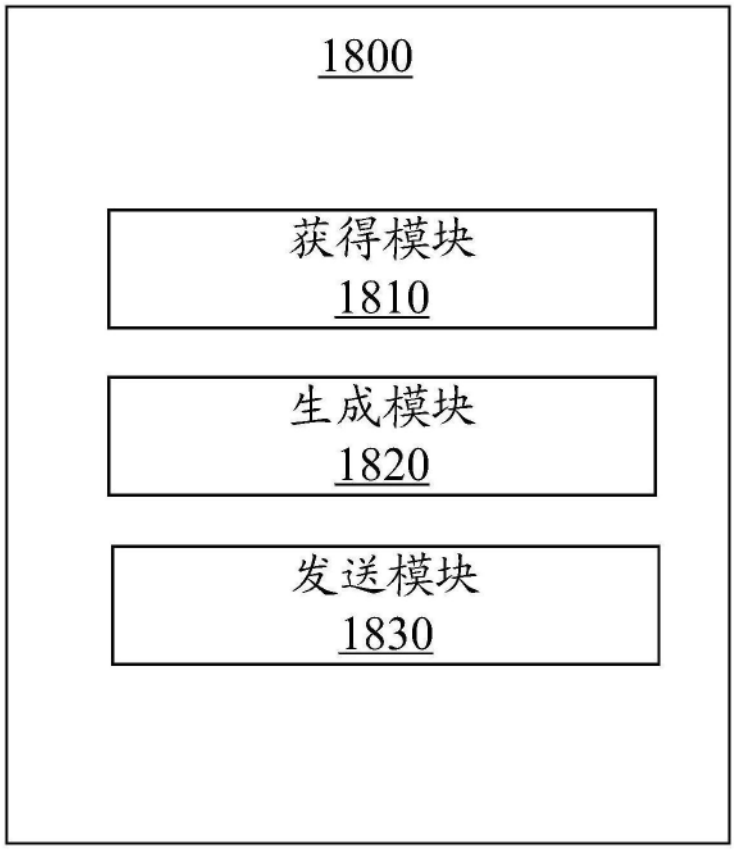



图18A

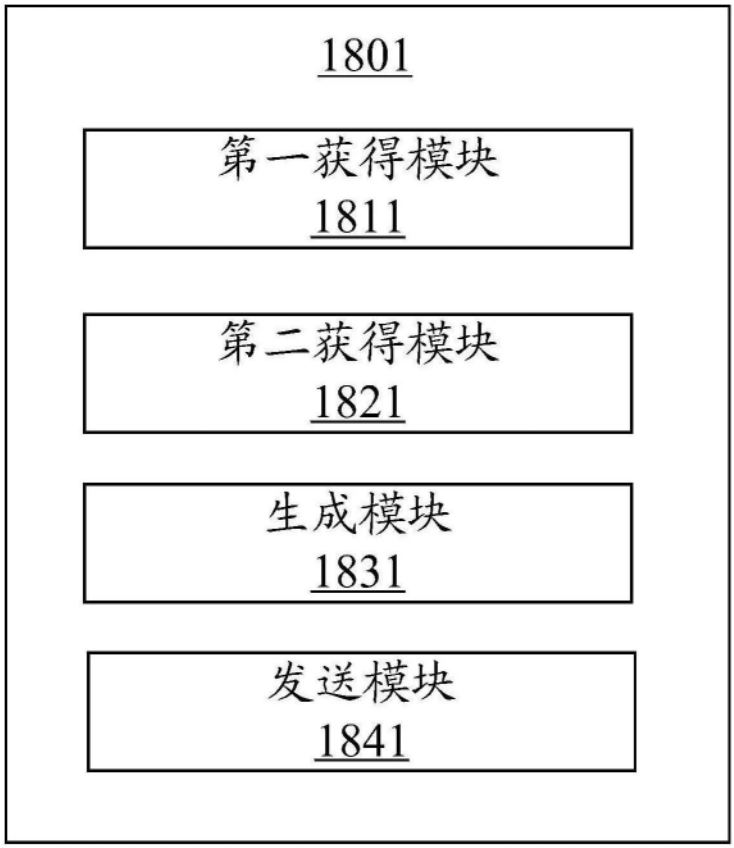

1801
第一获得模块
1811
第二获得模块
1821
生成模块
1831
发送模块
1841

图18B

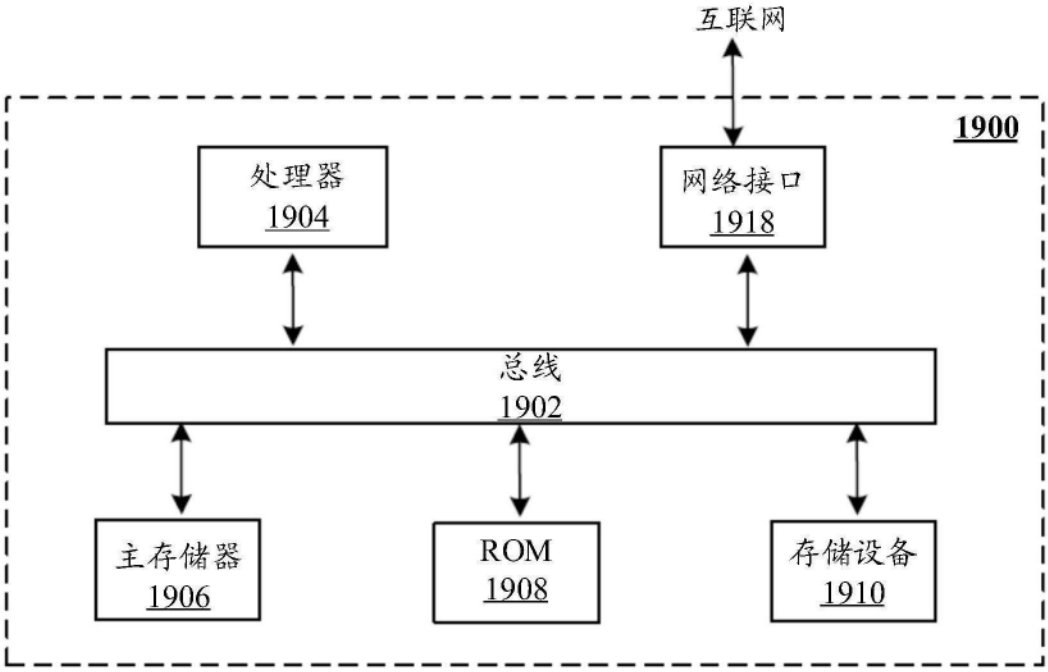

互联网
1900
处理器
1904
网络接口
1918
总线
1902
主存储器
1906
ROM
1908
存储设备
1910

图19