(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 110915183 B
(45)授权公告日 2022.03.22

(21)申请号 201880047373.0
(22)申请日 2018.07.24
(65)同一申请的已公布的文献号
申请公布号 CN 110915183 A
(43)申请公布日 2020.03.24
(30)优先权数据
15/660,756 2017.07.26 US
(85)PCT国际申请进入国家阶段日
2020.01.16
(86)PCT国际申请的申请数据
PCT/EP2018/070023 2018.07.24
(87)PCT国际申请的公布数据
WO2019/020616 EN 2019.01.31
(73)专利权人 国际商业机器公司
地址 美国纽约
(72)发明人 L·A·巴腾 G·马德尔
R·劳特拉伊
(74)专利代理机构 北京市中咨律师事务所 11247
代理人 刘都 于静
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 101543107 A,2009.09.23
CN 1922585 A,2007.02.28
US 2017046638 A1,2017.02.16
WO 2017008084 A1,2017.01.12
US 2007110062 A1,2007.05.17
CN 106295401 A,2017.01.04
CN 106503994 A,2017.03.15
Damiano等.Blockchain Based Access Control.《MEDICAL IMGAE COMPUTING AND COMPUTER-ASSISTED INTERNATIONAL -MICCAI 2015》.2017,

审查员 程杰

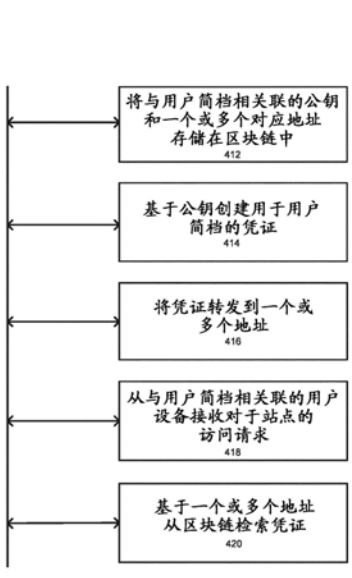
权利要求书2页 说明书7页 附图7页

(54)发明名称

经由硬/软令牌验证的区块链认证

(57)摘要

示例操作可以包括以下各项中的一项或多项:将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中;基于所述公钥创建用于所述用户简档的凭证;将所述凭证转发到所述一个或多个地址;从与所述用户简档相关联的用户设备接收对站点的访问请求;以及基于所述一个或多个地址从所述区块链检索所述凭证。



CN 110915183 B

1.一种认证方法,包括:

将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中;

基于所述公钥创建用于所述用户简档的基于智能合同的凭证;

将所述基于智能合同的凭证转发到所述一个或多个地址;

从与所述用户简档相关联的用户设备接收对站点的访问请求;以及

执行与基于智能合同的凭证对应的智能合同,以基于区块链上的所述地址确定访问所述站点所需的基于智能合同的凭证。

2.如权利要求1的方法,其中,所述凭证是访问控制列表(ACL)。

3.如权利要求1的方法,其中,所述基于智能合同的凭证是在有限的时间窗口内创建的。

4.如权利要求3的方法,其中所述一个或多个地址包括在多个访问尝试迭代中对应于多个凭证的多个地址位置。

5.如权利要求4的方法,其中所述请求包括所述多个地址位置。

6.如权利要求1的方法,进一步包括:

响应于接收到所述请求,将加密消息传输到所述用户设备;以及

基于所述加密消息接收解密消息。

7.如权利要求6的方法,进一步包括:

将所述解密的消息的解密消息内容与所述加密的消息的加密消息内容进行比较;以及

当所述解密消息内容与所述加密消息内容相匹配时,则验证所述基于智能合同的凭证是有效的,并且如果是,则授权对所述用户设备的访问。

8.一种认证装置,包括:

处理器,被配置为:

将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中;

基于所述公钥创建用于所述用户简档的基于智能合同的凭证;

将所述基于智能合同的凭证转发到所述一个或多个地址;

接收器,被配置为从与所述用户简档相关联的用户设备接收对站点的访问请求;以及

其中,所述处理器被进一步配置为执行与基于智能合同的凭证对应的智能合同,以基于区块链上的所述地址确定访问所述站点所需的基于智能合同的凭证。

9.如权利要求8的装置,其中,所述凭证是访问控制列表(ACL)。

10.如权利要求8的装置,其中,所述基于智能合同的凭证是在有限的时间窗口内创建的。

11.如权利要求10的装置,其中所述一个或多个地址包括在多个访问尝试迭代中对应于多个凭证的多个地址位置。

12.如权利要求11的装置,其中所述请求包括该多个地址位置。

13.如权利要求8的装置,其中该处理器进一步配置为:

响应于接收到所述请求,将加密消息转发到所述用户设备,且其中所述接收器进一步配置为基于所述加密消息接收解密消息。

14.如权利要求13的装置,其中该处理器被进一步配置为:

将所述解密的消息的解密消息内容与所述加密的消息的加密消息内容进行比较;以及

当所述解密消息内容与所述加密消息内容相匹配时，则验证所述基于智能合同的凭证是有效的，并且如果是，则授权对所述用户设备的访问。

15.一种非暂态计算机可读存储介质，其配置为存储指令，所述指令在被执行时致使处理器执行：

将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中；

基于所述公钥创建用于所述用户简档的凭证；

将所述基于智能合同的凭证转发到所述一个或多个地址；

从与所述用户简档相关联的用户设备接收对站点的访问请求；以及

执行与基于智能合同的凭证对应的智能合同，以基于区块链上的所述地址确定访问所述站点所需的基于智能合同的凭证。

16.如权利要求15所述的非暂态计算机可读存储介质，其中所述凭证是访问控制列表(ACL)。

17.如权利要求15所述的非暂态计算机可读存储介质，其中所述基于智能合同的凭证是在有限的时间窗口内创建的。

18.如权利要求17所述的非暂态计算机可读存储介质，其中所述一个或多个地址包括在多个访问尝试迭代中对应于多个凭证的多个地址位置。

19.如权利要求18的非暂态计算机可读存储介质，其中所述请求包括所述多个地址位置。

20.如权利要求15的非暂时性计算机可读存储介质，其中该处理器被进一步配置为执行：

响应于接收到所述请求，将加密消息传输到所述用户设备；

基于所述加密消息接收解密消息；

将所述解密的消息的解密消息内容与所述加密的消息的加密消息内容进行比较；以及

当所述解密消息内容与所述加密消息内容相匹配时，则验证所述基于智能合同的凭证是有效的，并且如果是，则授权对所述用户设备的访问。

经由硬/软令牌验证的区块链认证

技术领域

[0001] 本申请总体上涉及授权访问的管理，并且更具体地涉及经由硬/软令牌验证的区块链认证。

背景技术

[0002] 区块链是一种类型的计算架构，该计算架构使得对等分布式(共享和复制)数据库或分类账能够不受单个组织或实体控制，而是受许多不同的组织或实体控制。通过跨独立机器的网络，该配置允许节点可靠地跟踪和维持系统中的信息状态。这样一来，区块链使得能够经济高效地创建商用网络而不需要中心控制点。这种配置与传统的面向数据库的系统操作相反，在传统的面向数据库的系统中，独立的各方维护自己的记录系统，并在效率低下，有时甚至复杂的组织间流程之间相互协调更新，这需要独立，可信赖的第三方管理员的服务。

[0003] 双要素认证是由大多数主要政府机构(如国防部(DoD))批准的事实上的认证类型。通过使用公共访问卡(CAC)和/或硬件的软件狗(诸如安全识别密钥‘fob’)来执行双要素认证。CAC依赖于用于验证卡中存在的ID/EDIPI号的集中式服务器。硬件令牌不需要与后端服务器通信，因为它们具有生成一次性代码(例如，一次性密码)以访问系统所需的必要组件。这样的令牌需要被验证，因为后端系统将需要验证由用户提供的令牌匹配。

[0004] 双要素认证是应用于不同计算系统和网络的公知类型的安全过程。社交媒体站点和电子邮件提供商使用移动设备作为第二形式的认证(例如，发送到移动电话的密码+访问代码)。DoD已经指定所有DoD网络必须受到CAC保护。为了使用CAC，系统需要支持DoD PKI，DoD PKI是创建、管理、分发、使用、存储和撤销数字证书和管理公钥加密所需的一组角色、策略和过程。PKI在假设系统在DoD网络内的情况下工作。当试图在不访问DoD网络(例如，战术环境)的情况下认证用户时，这成为挑战。DoD/DoJ能够通过CAC卡及其相应的PKI通过使用桥来交叉认证用户。部署这种基础设施可能很复杂。鉴于大多数硬件令牌是防篡改的，它们通常比移动设备更可信，然而，管理这些设备是另一个挑战。

[0005] 在常规认证机制中，认证过程可以使用CAC卡或硬件令牌。这种方法将允许专用网络内部的用户使用CAC卡进行认证，因为该内部用户在网络内。专用网络外的用户可以具有有效的CAC，并且可以尝试向附属于专用网络的第三方站点注册，然而，由于外部用户不在专用网络内，因此请求将被拒绝并且外部用户将被拒绝访问专用网络。

发明内容

[0006] 一个示例性实施例可以包括一种方法，该方法提供了以下各项中的一项或多项：将与用户简档相关联的公钥和对应地址存储在区块链中；基于公钥创建用于用户简档的一组凭证；将凭证转发到一个或多个地址；从与用户简档相关联的用户设备接收对站点的访问请求；以及基于基于一个或多个地址从区块链检索凭证。该过程可以被随机化以提高安全性，并且系统管理员可以定义请求要素的策略。

[0007] 另一个示例性实施例可以包括一种装置，该装置包括处理器，该处理器被配置为执行以下各项中的一项或多项：将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中；基于公钥创建用于用户简档的凭证；将凭证转发至一个或多个地址；接收器，该接收器被配置为从与用户简档相关联的用户设备接收对于站点的访问请求；并且该处理器被进一步被配置为基于一个或多个地址从区块链检索凭证。

[0008] 又一个示例性实施例可以包括非瞬态计算机可读存储介质，该非瞬态计算机可读存储介质被配置为存储指令，这些指令在被执行时使处理器执行以下各项中的一项或多项：将与用户简档相关联的公钥和对应地址存储在区块区块链中；基于公钥创建用于用户简档的一组凭证；将凭证转发到一个或多个地址；从与用户简档相关联的用户设备接收对站点的访问请求；以及基于一个或多个地址从区块链检索凭证。该过程可以被随机化以提高安全性，并且系统管理员可以定义请求要素的策略。

附图说明

[0009] 现在将参照附图仅通过举例来描述本发明的实施例，在附图中：

[0010] 图1A示出根据示例实施例的利用区块链的密钥生成程序；

[0011] 图1B示出了根据示例性实施例的利用区块链系统配置的公开地址认证方案；

[0012] 图2示出了根据示例性实施例的区块链架构配置；

[0013] 图3示出了根据示范性实施例的用户设备、安全实体和区块区块链之间的交互的系统消息交互图；

[0014] 图4A示出根据示例性实施例的管理区块链中的认证的示例性方法的流程图；

[0015] 图4B示出根据示范性实施例的管理区块链中的认证的示例方法的另一流程图；

[0016] 图5示出了被配置为支持一个或多个示例性实施例的示例性网络实体。

具体实施方式

[0017] 将容易理解的是，如本文的附图中一般性描述和示出的，即时组件可以以多种不同的配置来布置和设计。因此，如附图所示，对方法、设备、非暂时性计算机可读介质和系统中的至少一个的实施例的以下详细描述并非旨在限制所要求保护的本申请的范围，而是仅代表所选实施例。

[0018] 在整个说明书中描述的即时特征、结构或特性可以在一个或多个实施例中以任何合适的方式组合。例如，在整个说明书中，短语“示例实施例”、“一些实施例”或其他类似语言的使用是指以下事实：结合该实施例描述的特定特征、结构或特性可以包括在至少一个实施例中。因此，在整个说明书中，短语“示例实施例”、“在一些实施例中”、“在其他实施例中”或其他类似语言的出现不一定都指同一组实施例，并且所描述的特征、结构或特性可以在一个或多个实施例中，以任何合适的方式组合。

[0019] 此外，虽然术语“消息”可能已经在实施例的描述中使用，该应用可以应用于许多类型的网络数据，如数据包、帧、数据报文等。术语“消息”还包括分组、帧、数据报文及其任何等效物。此外，尽管在示例性实施例中可以描述特定类型的消息和信令，但是它们不限于特定类型的消息，并且应用不限于特定类型的信令。

[0020] 在一个实施例中，本申请涉及授权访问的管理，并且在另一个实施例中，涉及基于

分散式多要素认证过程来管理授权方对数据的访问，该分散式多要素认证过程包括用于经由硬/软令牌验证执行的区块链认证的软件和硬件令牌验证。

[0021] 示例性实施例提供了使用区块链来支持分散式多要素认证来验证密码、支持CAC系统、硬件令牌、和/或通过发出软令牌来使用生物测定数据。使用区块链技术来提供多要素认证提供了对验证协议的支持，这允许分散式验证授权。该方法支持高可用性、高容错性、高冗余性等，因此基础设施可以承受网络攻击。

[0022] 软件令牌的发布提供了一种通过区块链技术证明似有信息的所有权的方法。该方法允许跨不同组织/区块链发布验证令牌，并且支持将以分散配置操作的战术云访问控制部署。其他特征包括经由区块链中的公钥的私有数据的所有权证明的区块链地址和从密码、EPID、硬件令牌代码、生物测定数据和/或其他类型的认证的密钥导出。

[0023] 根据示例性实施例，软件令牌验证与使用区块链作为分发基础设施的硬件令牌结合使用。该方法允许经由区块链发出令牌/访问控制，同时允许跨不同组织的用户认证，而不需要访问后端DoD PKI(例如，私有PKI系统)。这是通过扩展CAC卡中的基本逻辑来提供然后被推送到区块链的区块链地址/公钥来执行的，该区块链用于验证卡的用户以及验证签名。类似地，每个用户将具有专用的地址集合，其中以与它们的硬件令牌相同的速率生成的软件令牌被生成。软件令牌被发送至地址以证明令牌的所有权。每个令牌是服务认证用户所需的访问控制规则的形式。通过使用区块链中的数据来验证硬件令牌代码，不需要集中式后端服务器来管理认证过程。由区块链方法提供的验证为没有中央授权的生物测定数据信息的验证、没有中央授权的CAC卡的验证、硬件令牌的验证和/或公共网络中的专用网络访问控制列表(ACL)的发布提供支持。一种方法是使用‘M’个总认证要素中的任何随机‘N’个认证要素。例如，考虑一种系统，其中认证要素包括口令、PIN、图片口令、指纹和CAC，其在该示例中是总共5个要素。该配置将通过向区块链验证服务注册与要素相关联的公钥来实现所有5个要素的注册。当需要认证用户时，认证服务将通过要求对m个认证要素中的n个认证要素(n个要素)的回答来质询用户。例如，给定上述5个要素，系统将需要5个要素中的3个要素进行认证。这允许用户在要素丢失或损坏的情况下按需添加/移除认证要素。

[0024] 图1A展示了根据示例性实施例的利用区块链的密钥生成过程。参见图1A，配置100包括用于认证的多于一个选项，包括CAC 112、生物测定数据114和/或硬件(HW)令牌116。密钥生成可以来自那些源的任何一个。密钥可以包括密钥SK1、公钥PK1和存储该信息的区块链地址A1，根据一个实例，可使用‘n’个操作的任何组合。例如，为了使能多要素认证提供商，将需要拥有密码并且用作‘种子’以生成公钥/私钥对。接下来，公钥将被发布并用于认证。此外，区块链地址将从公钥导出，该公钥将允许任何人经由建立的地址向集中授权(例如，公司PKI 120)发送ACL/软件令牌，该ACL/软件令牌可用于注册他们的设备，该集中授权随后将生成ACL或访问令牌并将其发送到区块链140中的特定地址130。访问控制可以是静态的、或动态的，通过使用智能合同/链码来实施。例如，代替ACL，智能合同散列将与在区块链结构中执行智能合同所需的必要参数一起被发送。

[0025] 图1B展示了根据示例性实施例的利用区块链系统配置的公开地址认证方案。参见图1B，配置150提供使用区块链中的公共地址来认证用户设备。在任何给定时间，如果用户‘A’152想要认证和接入网络系统，一旦用户已注册他/她的公钥/地址并且它们已被公布在区块链140中，ACL也被生成并且被发送至用户A在区块链中的地址。在硬件令牌的情况下，

将根据所需时间窗发布这些ACL，并且因为令牌代码用于导出用户A的下一个地址，所以不需要将其注册到系统，因为传统的基础设施允许硬件令牌与其归属服务器保持同步。

[0026] 认证操作可以提供从移动设备或其他计算设备提交请求的用户A152以尝试访问站点170(172)。该请求可以包括与设备相关联的不同地址，例如A1、A2和Ai，其中‘i’是硬件令牌的当前迭代。站点170然后将向区块链140请求该数据。该网站将利用一次码向用户设备发送质询，并且将选择n种随机认证方式中的一种(174)。例如，如果选择了PK1，其属于用户设备的CAC卡，则设备将接收密文并且使用私钥(SK1)对其进行解密。该过程要求用户A150输入PIN或其他秘密字或短语，然后从该EPID导出SK，或者其已经存储在用户设备150的CAC卡内。然后，卡使用SK来解密密文，并接收回一次码2(176)。站点170将验证一次码1是否等于一次码2(182)。接着，如果上述检查通过，则下一步操作是验证用户A拥有的ACL(184)。如果ACL是有效的(例如，用户A具有权限特权)，则准许访问(186)，否则，拒绝用户A授权。类似的方法用于生物测定数据和硬件令牌。一个差异在于生物测定数据将需要用户A提供生物测定数据，从中在运行时生成密钥对。然后，生物测定逻辑将使用此来对数据进行签名/加密/解密。在使用生物测定数据的情况下，我们可以具有两个实施例。一种是使用随机的公钥/私钥对，其通过使用生物测定数据来解锁以向受信设备进行认证(例如，移动设备内的注册/认证)。第二实施例将是使用生物测定信号提取(例如，模板提取)以及量化以便生成种子，当与随机盐组合时，该种子然后可以用于导出公钥/私钥对。该方案可以不限于认证，因为消息可以被签名并且提供非抵赖。

[0027] 图2示出了根据多个示例性实施例的一种区块链系统配置。区块链系统200可包括某些公共区块链元素，诸如参与区块链交易添加和验证过程(共有)和/或可访问区块链的指派的区块链对等节点282-285的组280。任何区块链对等节点组280可发起新交易并寻求写入区块链不可变分类账272，其副本存储在加固的物理基础设施271上。在该配置中，定制的区块链配置可以包括链接到API 276以访问和执行存储的程序/应用代码(例如，链代码和/或智能合同)275的一个或多个应用277，这些代码(例如，链代码和/或智能合同)275是根据参与者寻求的定制的配置创建的并且可以维持他们自己的状态、控制拥有的资产以及接收外部信息。该代码可以被部署为交易并且经由附加到分布式分类账而安装在所有区块链对等节点上。

[0028] 区块链库270包括不同层的区块链数据、服务(例如，加密信任服务、虚拟执行环境)、以及加强的物理计算机基础设施，该计算机基础设施是接收和存储新交易并提供对寻求访问数据条目的审计员的访问所必需的。区块链层272暴露接口，该接口提供对处理程序代码以及参与物理平台271所需的虚拟执行环境的访问。密码信任服务273用于验证交易并且保持信息私密。根据示例性实施例，区块链分类账可以存储地址信息和其他数据，诸如不同用户设备的令牌278。这些令牌和其他认证数据可以用于在这些设备寻求访问第三方安全站点时认证这些设备。图2的区块链配置可以通过由区块链平台270暴露的接口以及提供的服务来处理和执行程序/应用代码175。代码可以控制区块链资产，例如，它可以存储和传输数据，并且可以由区块链以智能合同的形式来执行，该智能合同包括具有条件或受其执行影响的其他代码元素的链代码。

[0029] 图3示出了多个组件或模块之间的交互的系统消息传递图300，这些组件或模块可以包括软件、硬件或两者的组合。根据示例性实施例，组件可以包括第一组件(诸如用户设

备)、第二组件(诸如PKI)和第三组件(诸如区块链)。参见图3,用户设备310可以寻求访问存储在区块链330中的不同用户简档信息。为了接收访问,过程可以包括创建密钥和用于存储密钥的唯一地址(312)。公钥可以基于经由PKI 320做出的密钥被存储(313)并且在区块链330中存储(314)。注册用户设备(316),并且在做出后续访问尝试时(318),可从区块链检索所存储的凭证(322)并将其作为加密的消息转发(324)。解密的消息响应(326)可指示可被验证的合适凭证(328),从而可提供访问(332)。

[0030] 在一个实施例中,第一组件、第二组件和第三组件可以是单独的装置,如服务器、计算机或其他计算装置,或者可以是单个设备。在其他实施例中,第一组件和第二组件可以作为单个设备封闭或执行,第一组件和第三组件可以作为单个设备封闭或执行,并且第二组件和第三组件可以作为单个设备封闭或执行。组件或设备310、320和330可以以有线或无线的方式彼此直接连接或通信地耦合,并且可以驻留在本地和/或远程。

[0031] 图4A示出了根据示例性实施例的管理区块链中的认证的示例方法的流程图400。参见图4A,该方法可以包括:将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中(412);基于公钥创建用于用户简档的凭证(414);将凭证转发到一个或多个地址(416);从与用户简档相关联的用户设备接收对于站点的访问请求(418);以及基于一个或多个地址从区块链检索凭证(420)。

[0032] 该凭证是访问控制列表(ACL)。在有限时间窗口内创建凭证。所述一个或多个地址包括在多个访问尝试迭代中对应于多个凭证的多个地址位置。该请求包括多个地址位置。此外,所述方法还可以包括:响应于接收到所述请求,向用户设备发送加密消息,以及基于加密消息接收解密消息。所述方法还可以包括:将所述解密的消息的解密消息内容与所述加密的消息的加密消息内容进行比较,并且当所述解密消息内容与所述加密消息内容相匹配时,验证所述凭证是有效的,并且如果是,则授权对所述用户设备的访问。

[0033] 图4B展示了根据示例性实施例的管理区块链中的认证的示例方法的另一流程图450。参考图4B,该方法可以包括:将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中(452);接收与用户简档相关联的生物测定数据样本(454);从生物测定数据样本提取一个或多个生物测定元素(456);基于所述公钥和所述一个或多个生物测定元素创建用于所述用户简档的凭证(458);将该凭证存储在区块链中(462);从与用户简档相关联的用户设备接收对站点的访问请求(464);从区块链检索凭证(466);以及授权请求访问站点(468)。

[0034] 注册过程开始于生成包括公钥和私钥的公钥/私钥对。实际上,创建了非对称加密系统,其中公钥旨在通常是已知的和/或对于除了贡献者之外的人是可用的,而私钥旨在保持私有并且仅对于贡献者是已知的。私钥在注册过程中使用以创建标识符之后应当被存储在安全存储设备中、被销毁或以其他方式保持秘密。公钥/私钥对用于对交易请求进行修改和加密。交易请求可以是交易消息或交易分类账中的其他加密条目。接下来,接收生物测定样本并连同PIN或密码或某种其他类型的安全数据。生物测定提取可用于从生物测定样本导出生物测定特征。生物测定元件、私钥和可选的其他数据被用于组合输入并输出嵌入功能,该嵌入功能随后通过密码单向功能被转换,该密码单向功能输出不能由外部方容易地重新创建的组合标识符。

[0035] 以上实施例可以在硬件、由处理器执行的计算机程序、固件、或以上各项的组合中

实现。计算机程序可以嵌入在诸如存储介质的计算机可读介质上。例如，计算机程序可以驻留在随机存取存储器(“RAM”)、闪存、只读存储器(“ROM”)、可擦除可编程只读存储器(“EPROM”)、电可擦除可编程只读存储器(“EEPROM”)、寄存器、硬盘、可移动盘、致密盘只读存储器(“CD-ROM”)、或本领域已知的任何其他形式的存储介质中。

[0036] 示范性存储介质可以耦合至处理器，从而使得处理器可以从存储介质读取信息和向存储介质写入信息。在替代方案中，存储介质可以集成到处理器。处理器和存储介质可以驻留在专用集成电路(“ASIC”)中。在替代方案中，处理器和存储介质可作为分立组件存在。例如，图5示出了示例网络元件500，其可以表示或被集成在任何上述部件等中。

[0037] 如图5中所示，存储器510和处理器520可以是用于执行如在本文所描述的应用或操作集的网络实体500的分立组件。该应用能够以处理器520理解的计算机语言的软件来编码，并且存储在诸如存储器510之类的计算机可读媒质中。计算机可读媒质可以是包括可以存储软件的有形硬件组件(例如存储器)的非瞬态计算机可读媒质。此外，软件模块530可以是另一为网络实体500的一部分的分立实体，并且包含可由处理器520执行以实现一个或多个本文描述的功能的软件指令。除了网络实体500的上述部件之外，网络实体500还可以具有被配置为接收和发送通信信号(未示出)的发送器和接收器对。

[0038] 虽然系统、方法、和非瞬态计算机可读介质中的至少一个的示范性实施例已经在附图中展示并且在前述具体实施方式中进行了描述，但应理解的是，本申请不限于所披露的实施例，而是能够如由以下权利要求书所阐述和定义的许多重新安排、修改、和替换。例如，不同附图的系统的能力可由本文描述的或在分布式架构中的模块或组件中的一个或多个执行，且可包含发射器、接收器或两者的对。例如，由单独模块执行的功能的全部或部分可以由这些模块中的一个或多个来执行。进一步，本文描述的功能可以在不同时间并且关于模块或组件内部或外部的不同事件来执行。此外，在不同模块之间发送的信息可以经由数据网络、互联网、语音网络、互联网协议网络、无线设备、有线设备和/或经由多个协议中的至少一个在模块之间发送。此外，由任意模块发送或接收的消息可以直接和/或经由一个或多个其他模块发送或接收。

[0039] 本领域技术人员将认识到，“系统”可以具体化为个人计算机、服务器、控制台、个人数字助理(PDA)、蜂窝电话、平板计算设备、智能电话或任何其他合适的计算设备、或设备的组合。呈现如由“系统”执行的上述功能不旨在以任何方式限制本申请的范围，而是旨在提供许多实施例的一个示例。实际上，本文公开的方法、系统和装置可以与计算技术一致地以局部和分布式形式来实现。

[0040] 应注意的是，本说明书中描述的一些系统特征已经被呈现为模块，以便更具体地强调其实现方式独立性。例如，模块可以被实现为硬件电路，该硬件电路包括定制超大规模集成(VLSI)电路或门阵列、现成半导体(诸如逻辑芯片、晶体管或其他分立组件)。模块还可以在可编程硬件设备中实现，诸如现场可编程门阵列、可编程阵列逻辑、可编程逻辑设备、图形处理单元等。

[0041] 模块还可以是至少部分地在软件中实现以由不同类型的处理器执行。所标识的可执行代码单元可以例如包括：可以例如被组织为对象、过程或函数的计算机指令的一个或多个物理或逻辑块。然而，所标识的模块的可执行文件不需要物理地定位在一起，而是可以包括存储在不同位置中的不同指令，这些指令在逻辑上结合在一起时包括该模块并且实现

该模块的所陈述的目的。而且，模块可以存储在计算机可读媒质上，计算机可读媒质可以是例如硬盘驱动器、闪存设备、随机存取存储器(RAM)、磁带或用于存储数据的任何其他这样的媒质。

[0042] 实际上，可执行代码的模块可以是单个指令或多个指令，并且甚至可以分布在若干不同代码段上、在不同程序之间、和跨若干存储器设备。类似地，在本文中操作数据可以在模块内识别和示出，并且可以以任何合适的形式体现并在任何合适类型的数据结构内组织。操作数据可以被收集为单个数据集，或者可以分布在不同的位置上，包括在不同的存储设备上，并且可以至少部分地仅仅作为系统或网络上的电子信号而存在。

[0043] 将容易理解的是，本申请的部件，如本文的附图中一般性地描述和展示的，可以多种多样不同的配置被安排和设计。因此，实施例的详细描述不旨在限制所要求保护的本申请的范围，而仅仅是本申请的所选实施例的代表。

[0044] 本领域普通技术人员将容易理解，以上可以用不同顺序的步骤和/或用在配置上与所披露的那些不同的硬件元件来实践。因此，尽管已经基于这些优选实施例描述了本申请，但是对于本领域技术人员显而易见的是，某些修改、变化和替代构造将是显而易见的。

[0045] 尽管已经描述了本申请的优选实施例，但应理解的是，所描述的实施例仅是说明性的，并且当考虑与其完全的等效物和修改(例如，协议、硬件设备、软件平台等)范围时，本申请的范围将仅由所附权利要求书限定。

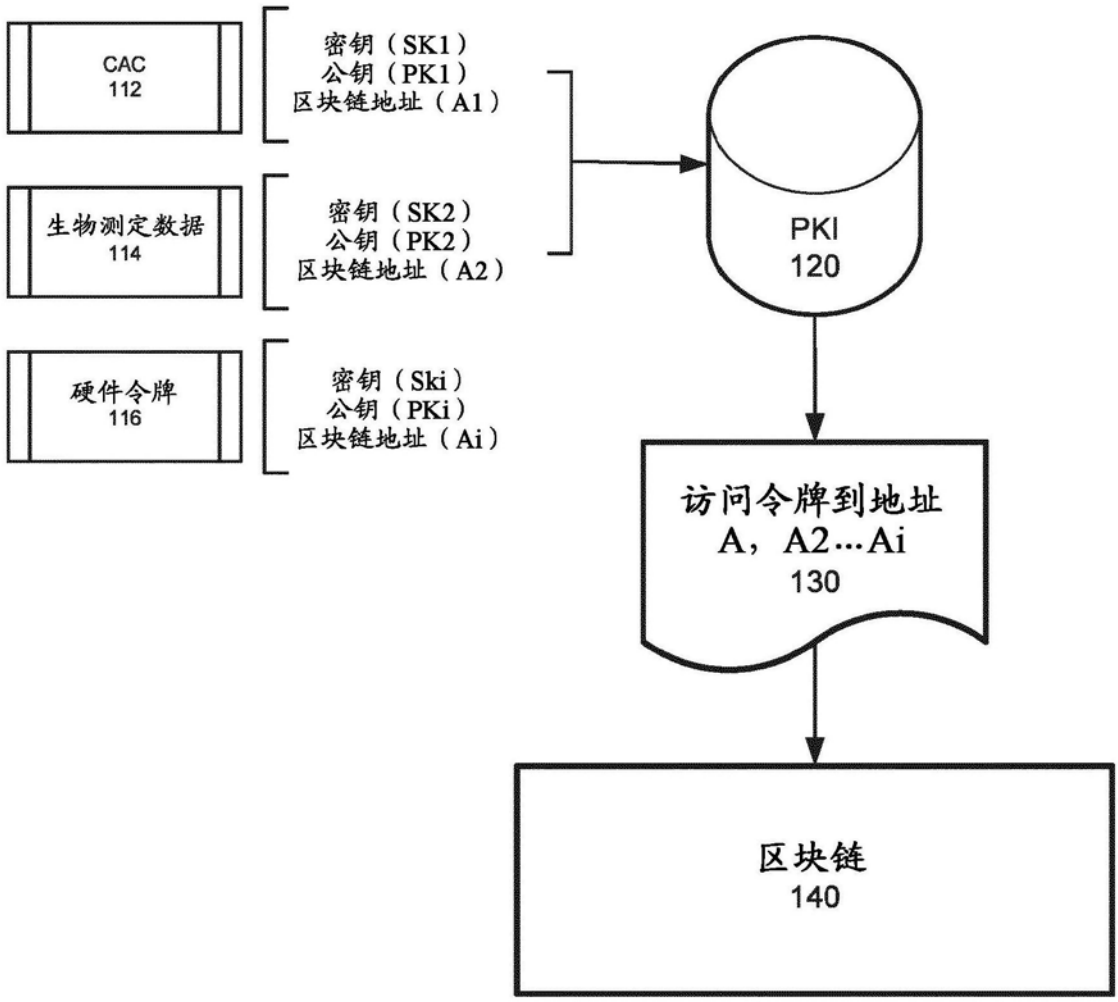

100
CAC
112
密钥（SK1）
公钥（PK1）
区块链地址（A1）
生物测定数据
114
密钥（SK2）
公钥（PK2）
区块链地址（A2）
硬件令牌
116
密钥（Ski）
公钥（PKi）
区块链地址（Ai）
PKI
120
访问令牌到地址
A，A2…Ai
130
区块链
140

图1A

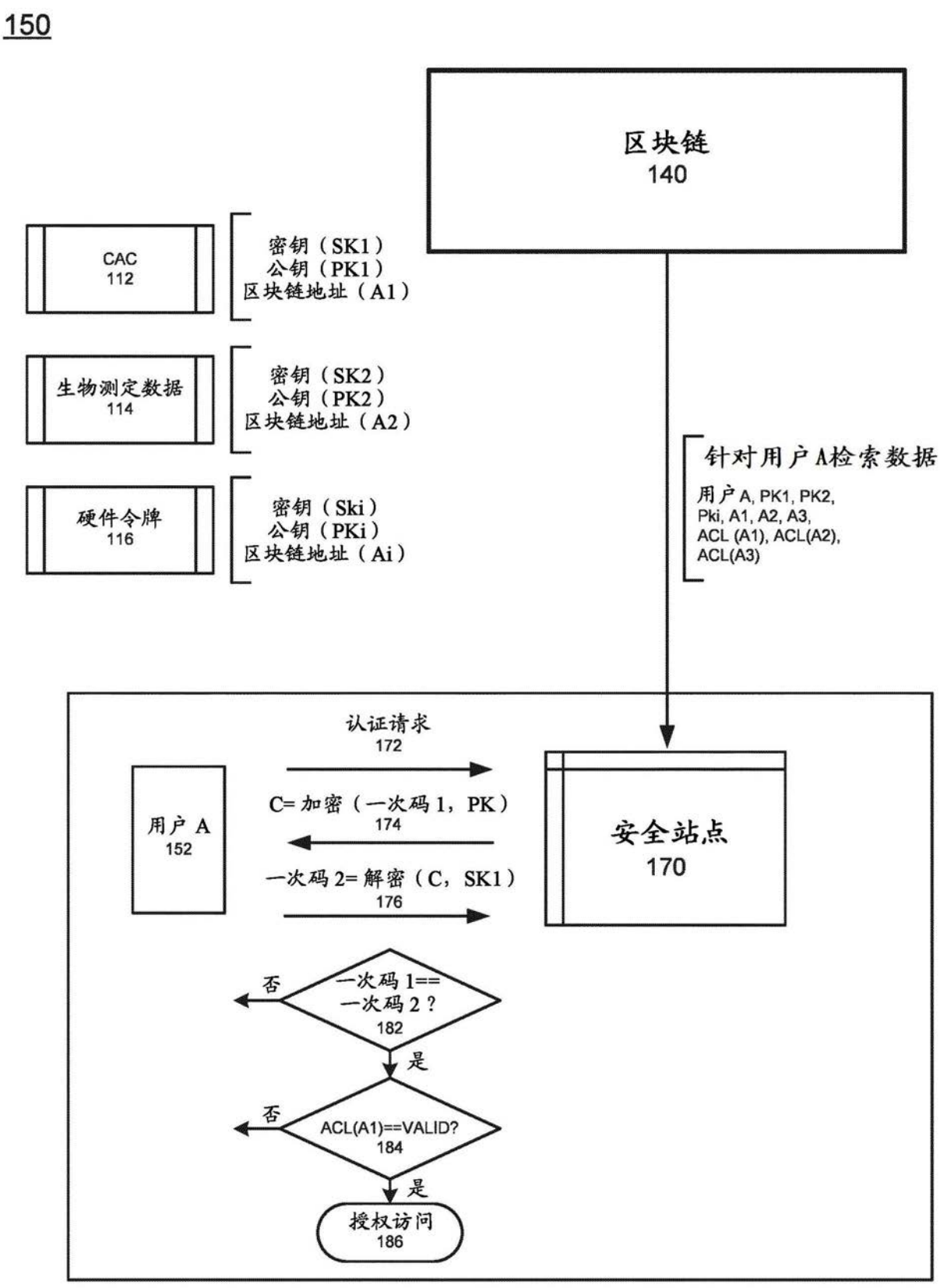

150
区块链
140
CAC
112
密钥（SK1）
公钥（PK1）
区块链地址（A1）
生物测定数据
114
密钥（SK2）
公钥（PK2）
区块链地址（A2）
硬件令牌
116
密钥（Ski）
公钥（PKi）
区块链地址（Ai）
针对用户A检索数据
用户A, PK1, PK2,
Pki, A1, A2, A3,
ACL (A1), ACL(A2),
ACL(A3)
用户 A
152
认证请求
172
C= 加密（一次码 1，PK）
174
一次码 2= 解密（C，SK1）
176
安全站点
170
一次码 1==
一次码 2？
182
否
是
ACL(A1)==VALID?
184
否
是
授权访问
186

图1B

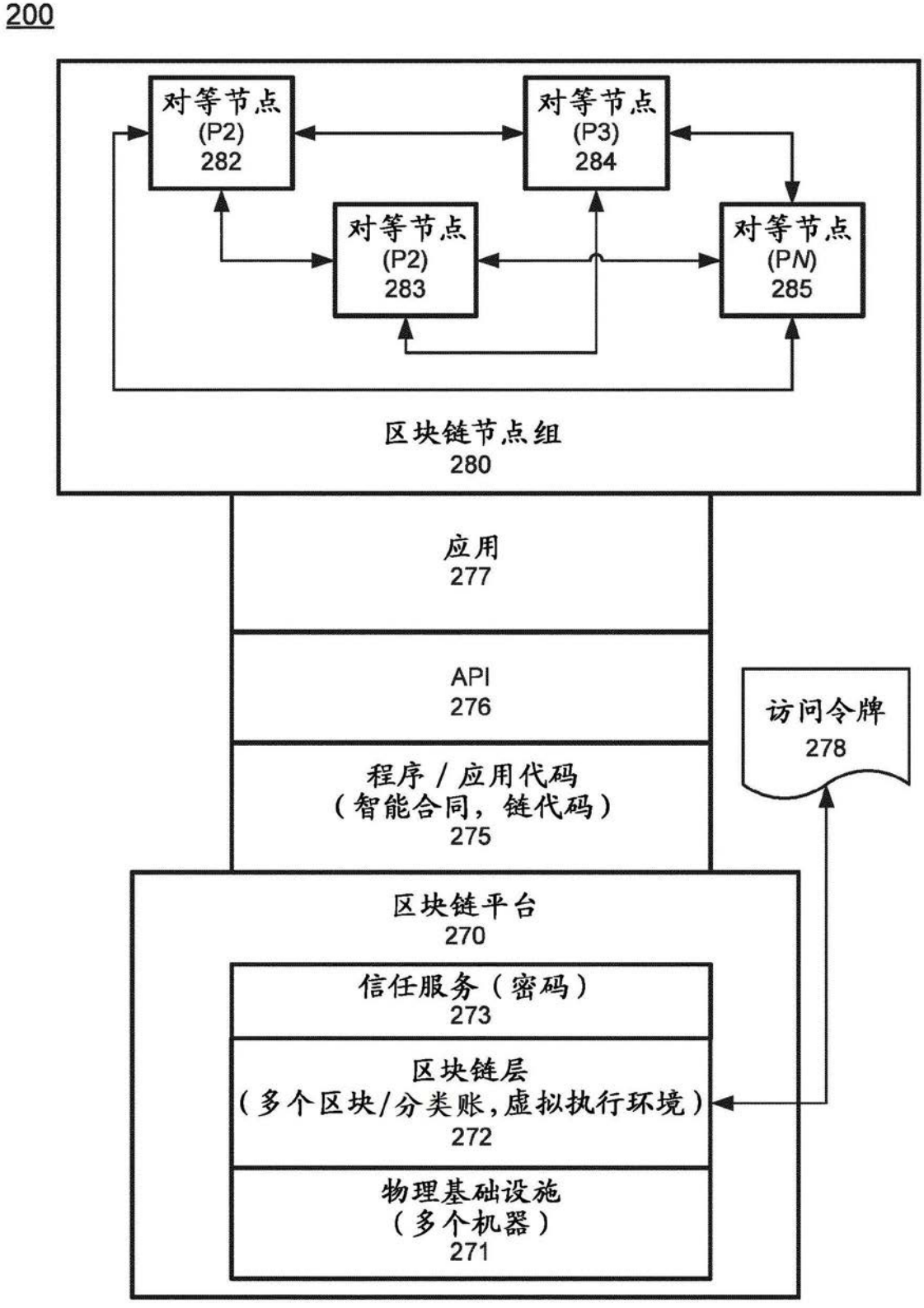

200
对等节点
(P2)
282
对等节点
(P3)
284
对等节点
(P2)
283
对等节点
(PN)
285
区块链节点组
280
应用
277
API
276
程序 / 应用代码
（智能合同，链代码）
275
访问令牌
278
区块链平台
270
信任服务（密码）
273
区块链层
（多个区块/分类账，虚拟执行环境）
272
物理基础设施
（多个机器）
271

图2

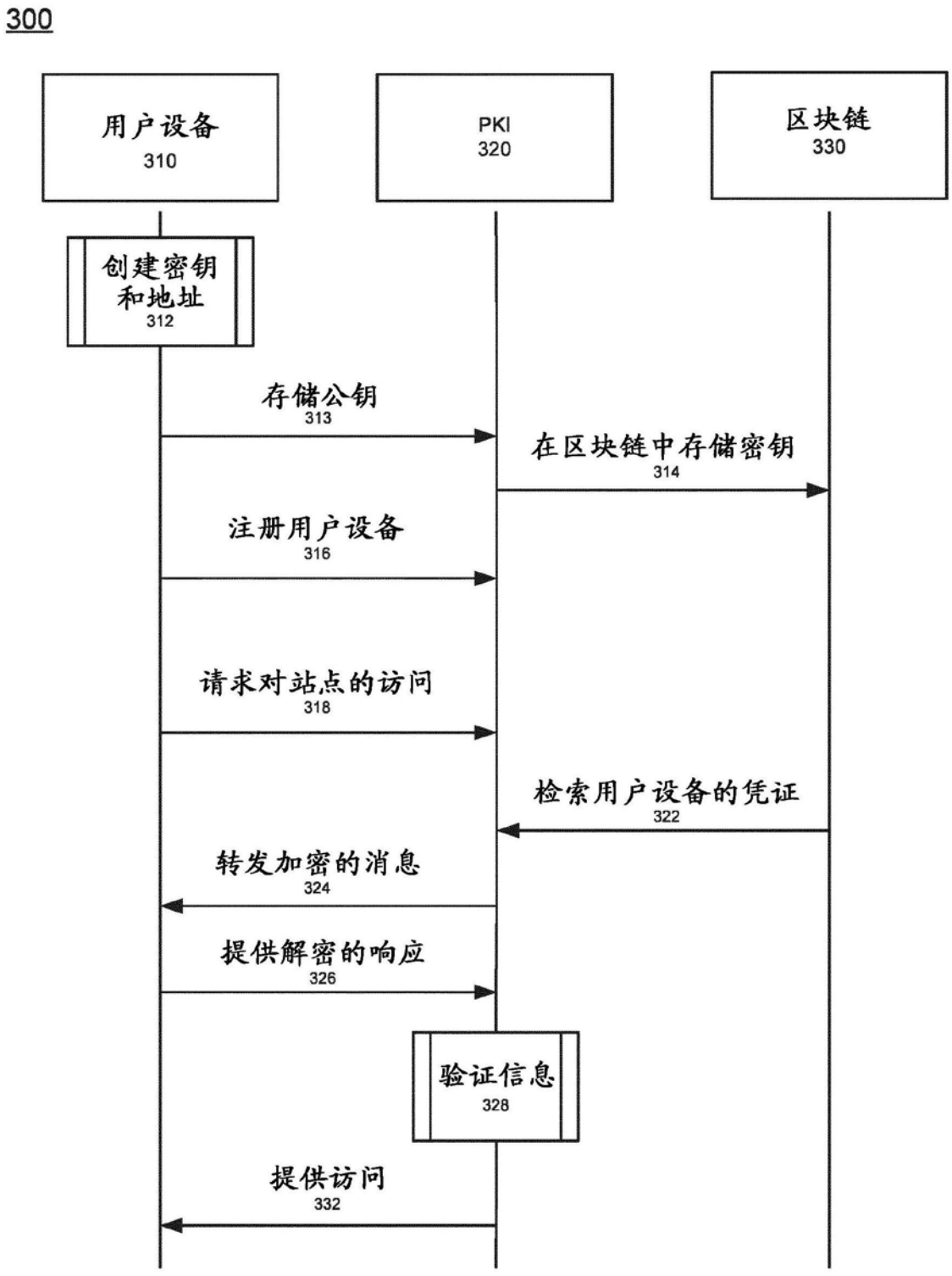

300
用户设备
310
PKI
320
区块链
330
创建密钥和地址
312
存储公钥
313
在区块链中存储密钥
314
注册用户设备
316
请求对站点的访问
318
检索用户设备的凭证
322
转发加密的消息
324
提供解密的响应
326
验证信息
328
提供访问
332

图3

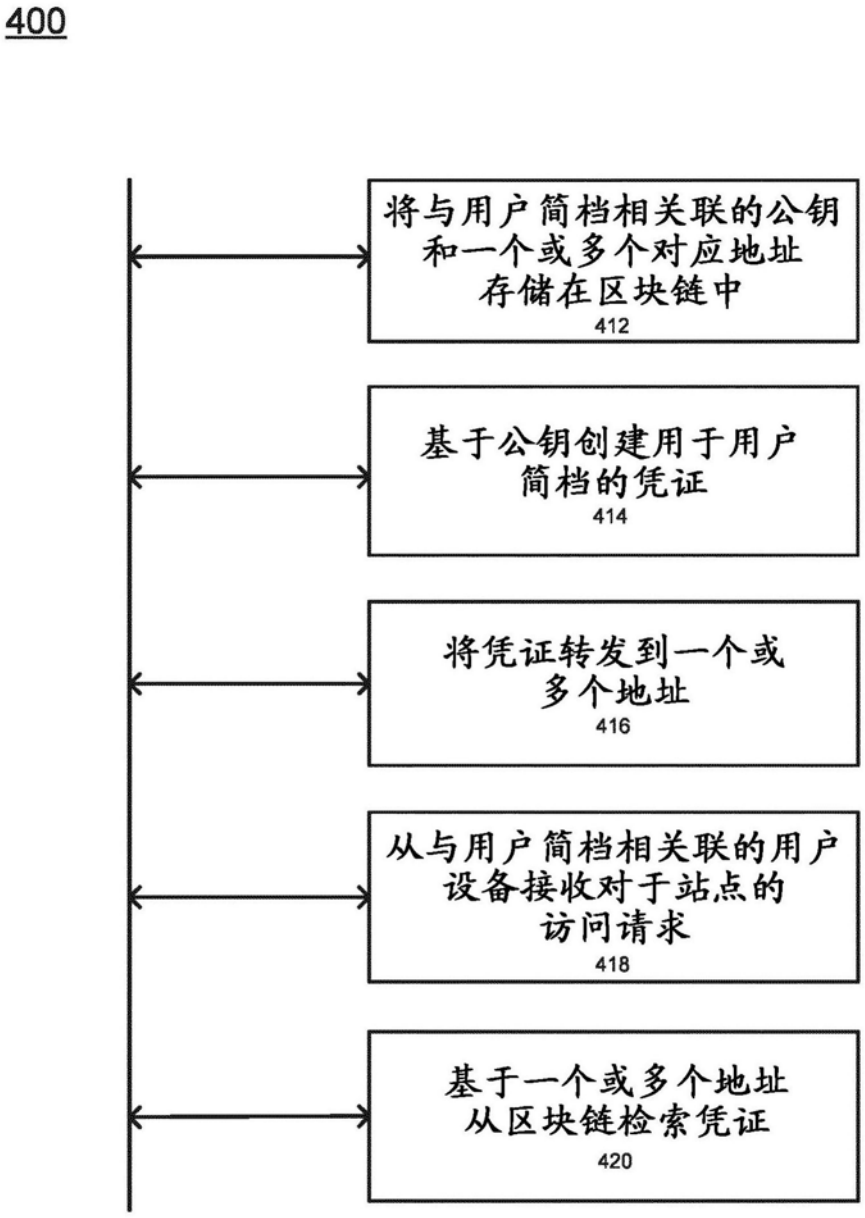

400
将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中
412
基于公钥创建用于用户简档的凭证
414
将凭证转发到一个或多个地址
416
从与用户简档相关联的用户设备接收对于站点的访问请求
418
基于一个或多个地址从区块链检索凭证
420

图4A

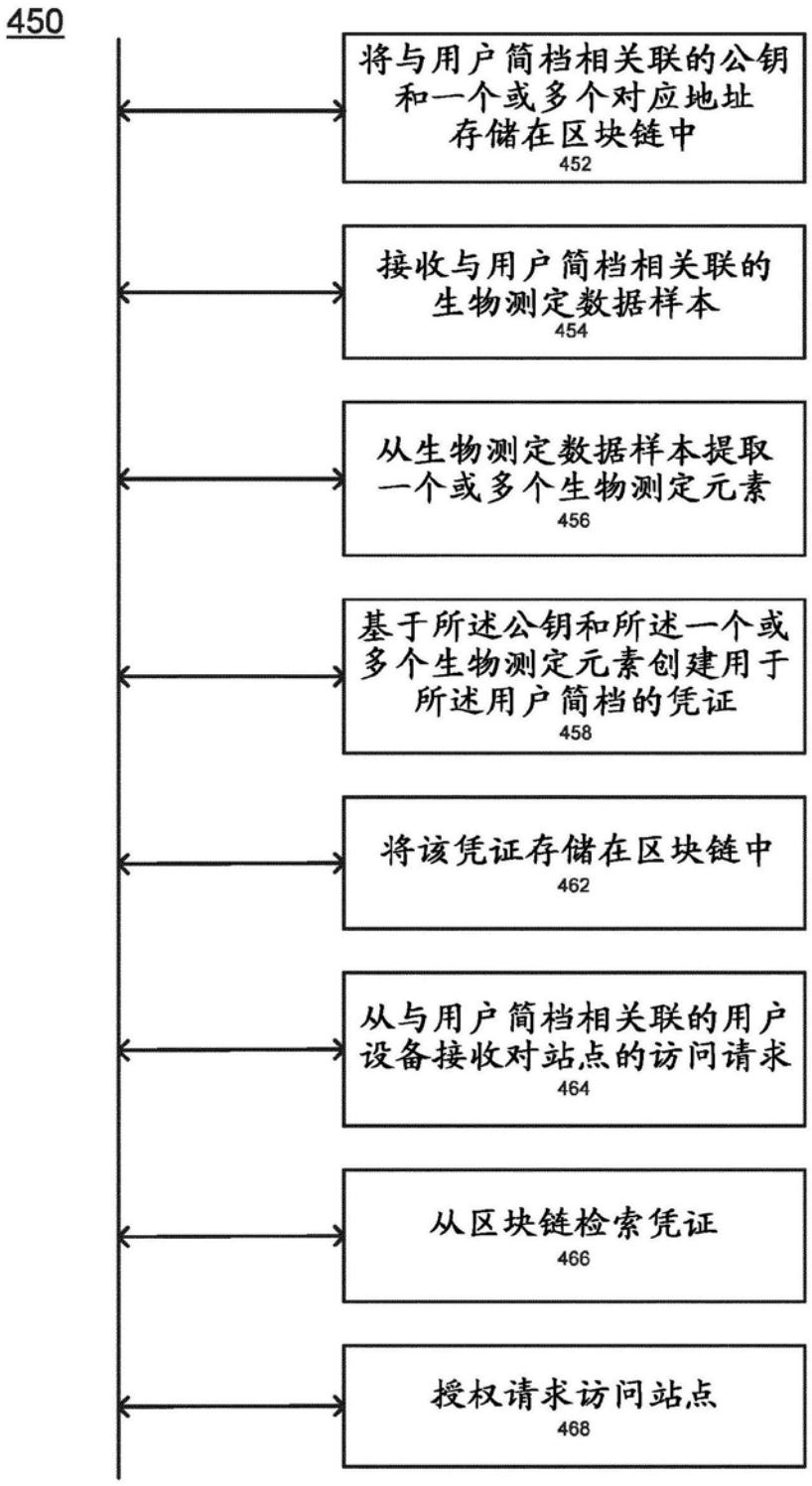

450
将与用户简档相关联的公钥和一个或多个对应地址存储在区块链中
452
接收与用户简档相关联的生物测定数据样本
454
从生物测定数据样本提取一个或多个生物测定元素
456
基于所述公钥和所述一个或多个生物测定元素创建用于所述用户简档的凭证
458
将该凭证存储在区块链中
462
从与用户简档相关联的用户设备接收对站点的访问请求
464
从区块链检索凭证
466
授权请求访问站点
468

图4B

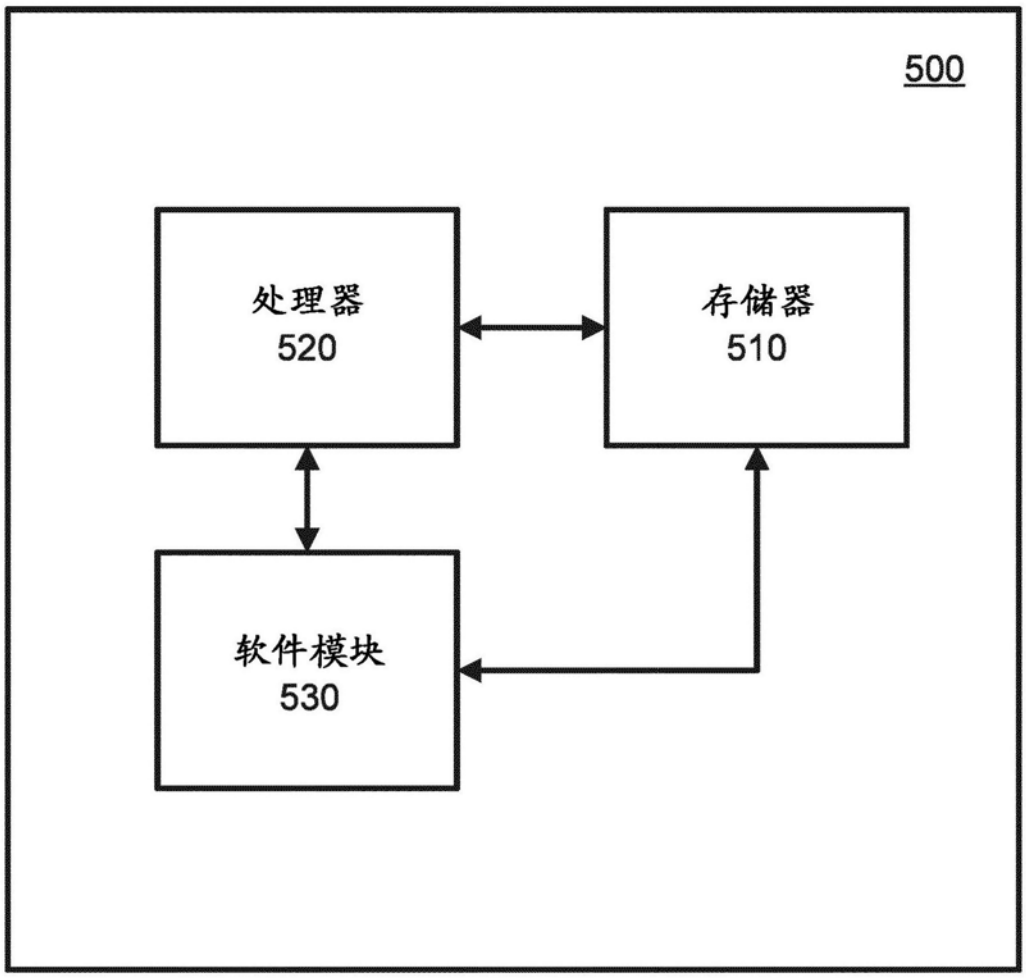


图5