(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117579281 A
(43)申请公布日 2024.02.20

(21)申请号 202311291288.8

(22)申请日 2018.06.04

(30)优先权数据
62/514,109 2017.06.02 US

(62)分案原申请数据
201880036586.3 2018.06.04

(71)申请人 维萨国际服务协会
地址 美国加利福尼亚州

(72)发明人 M·诺西埃 A·索马尼 Q·王

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

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/00(2022.01)

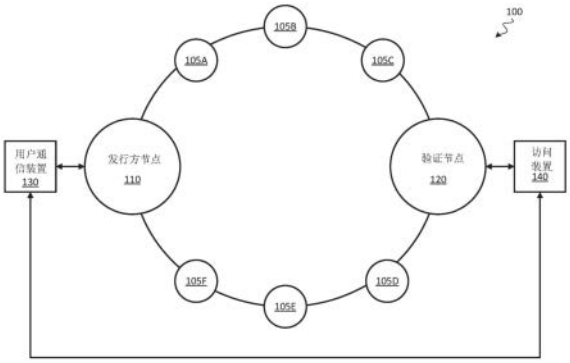
权利要求书3页 说明书15页 附图8页

(54)发明名称

用于使用区块链的所有权验证的方法和系统

(57)摘要

一种用于所有权验证的区块链系统可包括一个或多个发行方网络节点和一个或多个验证网络节点。发行方网络节点可配置成接收用以发行凭证的包括公共密钥的请求、将所述凭证预配到通信装置、生成从对所述凭证和所述公共密钥进行散列导出的有效负载、将所述有效负载存储在区块链的记录中,及将所述记录同步到所述区块链上的其它网络节点。验证网络节点可配置成接收所述凭证、所述公共密钥和由所述通信装置生成的签名以请求访问资源、使用所述公共密钥验证所述签名、基于所述凭证和所述公共密钥生成散列值、确定所述散列值存储在所述区块链中,及认证所述通信装置以用于访问所请求资源。



CN 117579281 A

1.一种计算机实现的方法,包括:

由凭证发行方计算机接收用以向通信装置发行凭证的请求,所述请求包括与所述通信装置相关联的通信装置公共密钥;

由所述凭证发行方计算机确定将发行到所述通信装置的所述凭证;

由所述凭证发行方计算机将所述凭证预配到所述通信装置;

由所述凭证发行方计算机生成从对所述凭证和所述通信装置公共密钥进行散列导出的有效负载;

由所述凭证发行方计算机将所述有效负载存储在区块链的记录中,所述区块链包括多个区块,每个区块包含一个或多个记录;以及

由所述凭证发行方计算机将所述记录同步到所述区块链上的其它网络节点。

2.根据权利要求1所述的计算机实现的方法,其中所述记录包括运用签名密钥生成的签名。

3.根据权利要求2所述的计算机实现的方法,其中所述签名密钥是与所述凭证发行方计算机相关联的发行方密钥。

4.根据权利要求2所述的计算机实现的方法,其中所述签名密钥是与证书颁发中心相关联的证书颁发中心密钥。

5.根据权利要求1所述的计算机实现的方法,其中所述记录包括:运用与所述凭证发行方计算机相关联的发行方密钥生成的第一签名;和运用与证书颁发中心相关联的证书颁发中心密钥生成的第二签名。

6.根据权利要求1所述的计算机实现的方法,其中所述有效负载是进一步从所述区块链的先前区块的散列导出的。

7.根据权利要求1所述的计算机实现的方法,其中将所述凭证预配到所述通信装置包括:将标识所述区块链中的哪一区块包含所述记录的区块标识符提供到所述通信装置。

8.根据权利要求1所述的计算机实现的方法,其中所述凭证是账户标识符或令牌,所述令牌是所述账户标识符的替代。

9.一种凭证发行方计算机,包括:

处理器;以及

非瞬态计算机可读介质,所述非瞬态计算机可读介质存储可由所述处理器执行以执行处理的指令,所述处理包括:

接收用以向通信装置发行凭证的请求,所述请求包括与所述通信装置相关联的通信装置公共密钥;

确定将发行到所述通信装置的所述凭证;

将所述凭证预配到所述通信装置;

生成从对所述凭证和所述通信装置公共密钥进行散列导出的有效负载;

将所述有效负载存储在区块链的记录中;以及

将所述记录同步到所述区块链上的其它网络节点。

10.根据权利要求9所述的凭证发行方计算机,其中所述记录包括运用签名密钥生成的签名。

11.根据权利要求10所述的凭证发行方计算机,其中:

所述签名密钥是与所述凭证发行方计算机相关联的发行方密钥,或与证书颁发中心相关联的证书颁发中心密钥。

12.根据权利要求9所述的凭证发行方计算机,其中所述记录包括:运用与所述凭证发行方计算机相关联的发行方密钥生成的第一签名;和运用与证书颁发中心相关联的证书颁发中心密钥生成的第二签名。

13.根据权利要求9所述的凭证发行方计算机,其中所述有效负载是进一步从所述区块链的先前区块的散列导出的。

14.根据权利要求9所述的凭证发行方计算机,其中将所述凭证预配到所述通信装置包括:将标识所述区块链中的哪一区块包含所述记录的区块标识符提供到所述通信装置。

15.一种计算机实现的方法,包括:

由通信装置获得通信装置密钥对,所述通信装置密钥对包括与所述通信装置相关联的通信装置公共密钥;

由所述通信装置向凭证发行方计算机传输用以向所述通信装置发行凭证的请求,所述请求包括所述通信装置公共密钥;

响应于所述请求,由所述通信装置从所述凭证发行方计算机接收区块链中包含所述凭证的记录的区块的区块标识符,所述记录被同步到所述区块链上的网络节点的集合;以及

将所述凭证和所述区块标识符存储到与所述通信装置公共密钥相关联的所述通信装置的安全存储器。

16.根据权利要求15所述的计算机实现的方法,还包括:

由所述通信装置将所述凭证和所述通信装置公共密钥提供到访问装置以请求对资源的访问;

由所述通信装置从所述访问装置接收密码质询;

由所述通信装置提供对所述密码质询的响应;以及

由所述通信装置基于由所述访问装置对所述密码质询的认证和由验证节点计算机对所述凭证的认证而从所述访问装置接收对所述资源的访问,其中对所述凭证的所述认证基于对散列值的验证,所述散列值基于所述凭证和所述通信装置公共密钥并且存储在所述区块链的所述记录中。

17.根据权利要求16所述的计算机实现的方法,其中所述通信装置进一步运用所述凭证和公共密钥将所述区块标识符提供到所述访问装置,其中所述区块标识符用于对所述凭证的所述认证中。

18.根据权利要求15所述的计算机实现的方法,其中获得所述通信装置密钥对包括:由安装在所述通信装置上的应用程序生成所述通信装置密钥对。

19.根据权利要求18所述的计算机实现的方法,其中:

所述应用程序与资源提供方相关联,并且

所述资源提供方的账户的标识符进一步存储到与所述通信装置公共密钥相关联的所述通信装置的所述安全存储器。

20.根据权利要求15所述的计算机实现的方法,其中所述凭证是账户标识符或令牌,所述令牌是所述账户标识符的替代。

21.一种通信装置,包括:

处理器;以及

非瞬态计算机可读介质,所述非瞬态计算机可读介质存储指令,所述指令可由所述处理器执行以执行根据权利要求15至20中任一项所述的方法。

用于使用区块链的所有权验证的方法和系统

[0001] 本发明申请是国际申请号为PCT/US2018/035844,国际申请日为2018年6月4日,进入中国国家阶段的申请号为201880036586.3,名称为“用于使用区块链的所有权验证的方法和系统”的发明专利申请的分案申请。

[0002] 相关申请交叉引用

[0003] 本申请要求2017年6月2日申请的美国临时申请第62/514,109号的优先权,所述申请出于所有目的以全文引用的方式并入本文中。

背景技术

[0004] 计算机安全的第一道防线是确保提交凭证以申请对服务或资源的访问的实体是凭证的适当所有者。举例来说,用户可通过互联网提供账户标识符以请求对与账户相关联的服务或资源的访问。验证凭证所有权的一项技术是请求用户另外提交个人标识信息(PII)(例如,地址、电话号码、电子邮件、生物标识技术等)。然而,此类技术会减少用户隐私性,并且许多用户对提供PII感到不舒服,尤其是在信息会被提供到第三方的情况下。另一技术是使用带外通信来验证凭证所有权。举例来说,一次性代码可发送到用户的注册装置或电子邮件,并且用户可提交一次性代码来证明用户的身份。另一实例可能需要用户致电凭证发行方,或单独登录到另一账户或装置。然而,此类技术可能导致用户摩擦并且降低用户体验的质量。

[0005] 本发明的实施例单独地且共同地解决这些问题和其它问题。

发明内容

[0006] 描述用以使用区块链和公共-专用密钥密码学验证凭证(例如,账户标识符等)或其它敏感资产或信息的所有权的技术。用户起初可将公共-专用密钥对的公共密钥传输到发行方,并请求发行方提供凭证。发行方可将公共密钥与分配给用户的凭证相关联,并生成详述公共密钥与凭证之间的相关联性的数据有效负载。数据有效负载接着可被发布或存储在区块链中。当用户稍后尝试使用凭证访问服务或资源时,用户可提供凭证、公共密钥和用公共-专用密钥对的专用密钥生成的签名。所述签名可用于验证公共密钥,并且可查询区块链以确定是否存在公共密钥与凭证之间的相关联性的记录。此记录在区块链中的存在验证了用户是凭证的适当所有者,因为用户拥有最初用于获取凭证的公共-专用密钥对。

[0007] 根据一些实施例,一种区块链系统可包括一个或多个发行方网络节点和一个或多个验证网络节点。发行方网络节点可配置成接收用以发行用于通信装置的凭证的包括通信装置公共密钥的请求、确定将发行到通信装置的凭证、将凭证预配到通信装置、生成从对凭证和通信装置公共密钥进行散列导出的有效负载、将有效负载存储在区块链的记录中,及将记录同步到区块链上的其它网络节点。验证网络节点可配置成接收凭证、通信装置公共密钥和由通信装置生成的通信装置签名以请求访问资源。验证网络节点可进一步配置成使用通信装置公共密钥验证通信装置签名,及响应于验证通信装置签名,基于凭证和通信装置公共密钥生成散列值。验证网络节点可进一步配置成确定散列值存储在区块链中,及响

应于确定散列值存储在区块链中,认证通信装置以用于访问所请求资源。

[0008] 根据一些实施例,一种计算机实施的方法可包括由凭证发行方计算机接收用以发行用于通信装置的凭证的请求,所述请求包括与通信装置相关联的通信装置公共密钥。所述方法还可包括确定将发行到通信装置的凭证、将凭证预配到通信装置、生成从对凭证和通信装置公共密钥进行散列导出的有效负载、将有效负载存储在区块链的记录中,及将记录同步到区块链上的其它网络节点。

[0009] 根据一些实施例,一种计算机实施的方法可包括由与区块链相关联的网络节点接收凭证、与通信装置相关联的通信装置公共密钥和通信装置签名以请求访问资源。所述方法可进一步包括使用通信装置公共密钥来验证通信装置签名,及响应于验证通信装置签名,基于凭证和通信装置公共密钥生成散列值。所述方法还可包括确定散列值存储在区块链的记录中、验证与区块链的记录相关联的记录签名,及响应于确定散列值存储在区块链中及验证记录的记录签名,认证通信装置以用于访问所请求资源。

附图说明

[0010] 图1说明根据一些实施例的区块链系统。

[0011] 图2说明根据一些实施例的发行方节点计算机的框图。

[0012] 图3说明根据一些实施例的验证节点计算机的框图。

[0013] 图4说明根据一些实施例的通信装置的框图。

[0014] 图5说明根据一些实施例的与区块链系统的交互的通信流程图。

[0015] 图6说明根据一些实施例的区块链的一部分。

[0016] 图7说明根据一些实施例的用于将记录添加到区块链的过程的流程图。

[0017] 图8说明根据一些实施例的用于验证凭证的所有权的过程的流程图。

[0018] 图9说明根据一些实施例的高级区块链架构。

具体实施方式

[0019] 本发明的各个实施例提供了使用区块链和公共-专用密钥密码学来验证凭证(例如,账户标识符等)或其它敏感资产或信息的所有权的技术。用户起初可将公共-专用密钥对的公共密钥传输到发行方,并请求发行方提供凭证。发行方可将公共密钥与分配给用户的凭证相关联,并生成详述公共密钥与凭证之间的相关联性的数据有效负载。数据有效负载接着可被发布或存储在区块链中。当用户稍后尝试使用凭证访问服务或资源时,用户可提供凭证、公共密钥和用公共-专用密钥对的专用密钥生成的签名。所述签名可用于验证公共密钥,并且可查询区块链以确定是否存在公共密钥与凭证之间的相关联性的记录。此记录在区块链中的存在验证了用户是凭证的适当所有者,因为用户拥有最初用于获取凭证的公共-专用密钥对。

[0020] 在论述本发明的各种实施例之前,下文提供了对各个术语的解释。

[0021] “区块链”可指分布式数据库。区块链可用于维护不断增长的称为区块的记录列表。区块链可用于以难以伪造的方式维护各方之间的交易或事件的记录。区块链中的每一区块可包括若干记录以及区块链中的先前区块的散列。如果先前区块中的记录改变,那么任何以下区块中的散列可被破坏。结果是为了伪造给定记录,黑客必须伪造所述记录以及

所有后续记录使得散列最终相同。这在实践中极其困难。另外,区块链可分布在大量实体之间。可通过比较区块链与多个个别记录来验证区块链的任何改变。

[0022] “记录”可指一个或多个交互的证据。数字记录可以是交互的电子文档。记录可包括记录标识符和记录信息。举例来说,记录信息可包括描述一个或多个交互的信息和/或与交互相关联的信息(例如,数字签名)。记录信息还可包括多个数据包,其中的每一个包括描述不同交互的不同数据。记录标识符可以是用于标识记录的数字、标题或其它数据值。记录标识符可能是非描述性的,因为它可能不会提供关于记录中的记录信息的任何有意义的信息。记录的实例包括医疗记录、学术记录、交易记录、凭证发行记录等。在一些实施例中,记录可存储在区块链的区块中。个别区块可包括个别记录或预定数目的记录,并且区块链可以是组织成区块的一系列记录。

[0023] “节点”或“网络节点”可指通信网络中的连接点。网络节点可以是物理电子装置,其能够创建、接收或传输数据。在一些实施例中,网络节点可以是记录保存网络(例如,区块链网络)内的计算装置。网络节点可能够创建数据包(例如,数据有效负载)、转移数据包、接收数据包、认证数据包、访问中心记录和/或执行任何其它合适的功能。不同类型的网络节点可能够执行记录网络中的不同组的功能。在一些实施例中,网络节点可与例如在线服务提供商、内容提供商的资源提供商、证书颁发中心、金融机构(例如,银行)、商家、交易处理网络或任何其它合适的实体相关联和/或由其操作。

[0024] “密钥”可指用于加密算法中以将输入数据变换成另一表示的一条信息。密码算法可以是将原始数据变换成替代表示的加密算法,或将加密信息变换回原始数据的解密算法。密码算法的实例可包括三重数据加密标准(TDES)、数据加密标准(DES)、高级加密标准(AES)等。

[0025] “密钥对”可包括一对相联系的加密密钥。举例来说,密钥对可包括公共密钥和对应的专用密钥。在密钥对中,第一密钥(例如,公共密钥)可用于对消息进行加密,而第二密钥(例如,专用密钥)可用于对经过加密的消息进行解密。另外,公共密钥可能够验证用对应的专用密钥创建的数字签名。公共密钥可分布在网络中,以便允许验证使用对应的专用密钥签名的消息。公共密钥和专用密钥可以是任何合适格式,包括基于RSA或椭圆曲线密码学(ECC)的格式。在一些实施例中,可使用非对称密钥对算法来生成密钥对。

[0026] “数字证书”可指用于显示所有权的电子文档。数字证书可包括公共密钥或关于公共密钥的信息,连同公共密钥的所有者的身份,以及数字签名(例如,指示验证了所列举的所有者实际上拥有公共密钥的实体的数据)。此数字签名可以是使用验证实体的专用密钥加密的消息。实体可使用验证实体的公共密钥对消息进行解密,以标识验证实体。

[0027] “证书颁发中心”可指向其它实体颁发证书以证明身份的受信实体。举例来说,证书颁发中心可颁发数字证书,其包括关于密码密钥的信息和关于密钥所有者的身份的信息。数字证书可由证书颁发中心签名以证明证书的内容的有效性。证书颁发中心的实例可包括网络运营商、网络域提供商、交易处理器或处理网络等。

[0028] “签名”可指消息或一些数据的电子签名。数字签名可以是数字数据值、字母数字数据值或包括图形指示的任何其它类型的数据。数字签名可以是使用加密算法从消息和专用密钥生成的唯一数据值。在一些实施例中,可使用采用公共密钥的认证算法来验证签名。

[0029] “用户”可指实体,例如人、组织或与出于某一目的利用资源的人或组织相关联或

由其操作的装置或系统。用户可具有可用于访问资源的一个或多个账户。根据一些实施例，用户还可被称作账户持有人、消费者、订户，或持卡人等。

[0030] “资源”可指服务、项目、位置、数据、信息，或帮助用户实现某一目的的有价值的物品。一些资源可能受限，且可能需要用户具有访问资源的账户。资源的实例可包括：软件应用程序和相关功能；包括云服务的在线服务；与交易有关的商品(虚拟和/或物理对象)或服务；可兑换其它资源的积分、分数和/或货币；电子装置，例如服务器、计算机、移动装置、游戏系统等等；例如运输工具或运送服务的运输，例如无线服务的通信能力；受限区域；介质内容；等。

[0031] “资源提供商”可指可提供资源的实体。资源提供商的实例可包括服务提供商，例如网络服务提供商、社交网络、发行方、银行、商家、政府机构、交易处理网络等。

[0032] “凭证”可指可用于访问资源的一条数据。凭证可链接到账户，并且可能需要验证凭证才能访问与账户相关联的资源。凭证的实例可包括例如主账号的账户标识符、可用作账户标识符的替代的令牌、用户名或用户标识符、口令、密码、PIN、密码密钥、数字证书、生物标识数据等。在一些实施例中，凭证还可以是数字资产，前提是存在可证明资产的所有权的受信保管人。举例来说，数字资产可以是机动车辆管理局颁发的驾驶执照或车辆标识号(VIN)，或住房管理局颁发的以标识用户拥有的土地的地号、文档记录服务发行的文档编号等。

[0033] “通信装置”可指包括一个或多个电子组件的装置(例如，集成芯片)，所述一个或多个电子组件可与另一装置或实体通信。举例来说，通信装置可以是计算装置，其包括耦合到存储供处理器执行的指令或代码的存储器的至少一个处理器，并且所述通信装置可包括允许通信装置与其它实体交互的通信接口。通信装置可以是可由用户运输和操作的便携式通信装置。便携式通信装置可将远程通信能力提供给网络。便携式通信装置可配置成将数据或通信传输到其它装置且从其它装置接收数据或通信。便携式通信装置可呈例如移动电话(例如，智能电话、蜂窝电话等)的移动装置、平板计算机、便携式介质播放器、个人数字助理装置(PDA)、可穿戴式装置(例如，手表、手镯、戒指、眼镜、例如健身跟踪器的健康监测装置等)、电子读取器装置等形式，或呈卡(例如，智能卡)或挂件等形式。便携式通信装置的实例还可包括便携式计算装置(例如，笔记本电脑、上网本、超级本等)。便携式通信装置还可呈车辆(例如，汽车)的形式，或者集成为车辆的一部分(例如，车辆的信息系统)。通信装置的其它实例可包括物联网(IoT)装置、智能设备和电子装置、游戏机等。通信装置还可包括多个装置或组件(例如，当装置通过系链到另一装置而能远程访问网络时—两个装置在一起可被视为通信装置)。

[0034] “服务器计算机”可指功能强大的计算机或计算机集群。举例来说，服务器计算机可以是大型主机、小型计算机集群或充当单元的一组服务器。在一个实例中，服务器计算机可以是连接到网络服务器的数据库服务器。服务器计算机可连接到数据库，并且可包括用于服务于来自一个或多个客户端计算机的请求的任何硬件、软件、其它逻辑或前述内容的组合。服务器计算机可包括一个或多个计算设备并且可使用各种计算结构、布置和编译中的任何计算结构、布置和编译来服务于来自一个或多个客户端计算机的请求。

[0035] “发行方”或“凭证发行方”可指维护用户的账户的实体。发行方可给用户提供或发行凭证，并且所述凭证可用于访问账户或与账户相关联的资源。所述账户可与通信装置相

关联,所述账户例如在安装在通信装置上的应用程序中注册的账户。发行方还可与主机系统相关联,所述主机系统代表发行方来执行发行方的一些或全部功能。发行方的实例可包括服务提供商、银行、商家、政府机构、交易处理器等。

[0036] “访问装置”可指用于与资源提供商通信的合适装置。在一些实施例中,访问装置可以是可与用户通信装置交互的网络服务器、商家计算机或交易处理网络。访问装置一般可位于任何合适位置中,例如位于服务提供商或商家的位置处,或可在远程位置处(例如,在云中)。访问装置的一些实例包括POS装置、蜂窝电话、PDA、个人计算机(PC)、平板电脑、手持式专用读取器、机顶盒、电子收款机(ECR)、自动取款机(ATM)、虚拟收款机(VCR)、查询一体机、安全系统、访问系统、网站等。访问装置可使用任何合适的接触或非接触式操作模式以运用通信装置发送或接收数据。在一些实施例中,访问装置可包括读取器、处理器和计算机可读介质。读取器可包括任何合适的接触或非接触式操作模式。举例来说,示例性读卡器可包括用于与通信装置交互的射频(RF)天线、光学扫描器、条形码读取器或磁条读取器。

[0037] “实账户标识符”可指与账户相关联的原始账户标识符。举例来说,实账户标识符可以是由发行方针对卡账户(例如,信用卡、借记卡等)发行的主账号(PAN)。举例来说,在一些实施例中,实账户标识符可包括十六位数值,例如,“4147 0900 0000 1234”。实账户标识符的前六位(例如,“414709”)可表示可标识与实账户标识符相关联的发行方的实际发行方标识符(BIN)。

[0038] “令牌”可指一些信息的替代标识符。举例来说,令牌可包括账户的标识符,所述标识符是实账户标识符的替代,例如,主账号(PAN)。举例来说,令牌可包括可用作原始账户标识符的替代的一系列字母数字字符(例如,令牌“4900 0000 0000 0001”可用于代替PAN“4147 0900 0000 1234”)。在一些实施例中,令牌可以是保留格式的,并且可具有与现有交易处理网络中使用的账户标识符一致的数字格式(例如,ISO 8583金融交易消息格式)。在一些实施例中,令牌可用于代替PAN,以发起、授权、结算或解决交易。在通常提供原始凭证的其它系统中,令牌还可用于表示原始凭证。在一些实施例中,可生成令牌值,使得不可以通过计算方式从令牌值导出原始PAN或其它账户标识符的恢复。此外,在一些实施例中,令牌格式可配置成允许接收令牌的实体将其标识为令牌,并辨识发行令牌的实体。

[0039] “授权请求消息”可指请求对交易的授权的电子消息。在一些实施例中,授权请求消息被发送给交易处理计算机和/或支付卡的发行方,以请求对交易进行授权。根据一些实施例的授权请求消息可符合ISO 8583,ISO 8583是用于交换与用户使用支付装置或支付账户进行的支付相关联的电子交易信息的系统的标准。授权请求消息可包括可与支付装置或支付账户相关联的发行方账户标识符。授权请求消息还可包括与“标识信息”对应的额外数据元素,包括(只作为实例):服务代码、卡验证值(CVV)、动态卡验证值(dCVV)、主账号或“账号”(PAN)、支付令牌、用户名、到期日期等等。授权请求消息还可包括交易信息,例如与当前交易相关联的任何信息,例如交易金额、商家标识符、商家位置、收单方银行标识号(BIN)、卡接受器ID、标识正购买的项目的信息等,以及可用于确定是否标识和/或授权交易的任何其它信息。

[0040] “授权响应消息”可指响应授权请求的消息。在一些状况下,授权响应消息可以是由发行金融机构或交易处理计算机生成的对授权请求消息的电子消息应答。授权响应消息可包括例如以下状态指示符中的一个或多个:批准-交易被批准;拒绝-交易未被批准;或呼

叫中心-响应未决的更多信息,商家必须呼叫免费授权电话号码。授权响应消息还可包括授权代码,所述授权代码可以是信用卡发行银行响应于电子消息中的授权请求消息(直接地或者通过交易处理计算机)返回给商家的访问装置(例如POS设备)的指示对交易的批准的代码。所述代码可充当授权的证据。

[0041] “散列”可指由散列函数(例如,可用于将具有任意大小的数据映射到具有固定大小的数据的函数)返回的数据。散列可用于唯一地标识机密信息。在许多状况下,两个不同输入数据值具有相同散列在统计学上不太可能。散列算法的实例可包括MD5、MD6、SHA变型等。

[0042] “认证”可指证明或验证某些信息和/或验证所述信息的来源的身份的过程。举例来说,用户可提供认证数据(例如,凭证),其是唯一的或仅用户已知以证明用户的身份。不同类型的认证数据的实例可包括生物标识技术、口令、密码、PIN、安全问题的答案、质询的加密响应、人和/或装置签名等。

[0043] 图1说明根据一些实施例的区块链系统100。系统100可包括通过通信网络彼此以通信方式连接的多个网络节点105A到105F、110及120,所述通信网络例如:互联网;局域网(LAN);城域网(MAN);广域网(WAN);无线网络;交易处理网络;或其组合。网络节点105A到105F、110和120中的每一个可维护区块链的副本,其含有由系统100发行或记录的凭证的记录。区块链系统100中的网络节点中的每一个可充当发行方节点、验证节点或其组合。在一些实施例中,区块链系统100中的每一节点可充当验证节点,而节点的子集还可充当发行方节点。在一些实施例中,区块链系统100可以是仅已知或受信任实体可成会成员的许可系统。这与开放式区块链系统相反,所述开放式区块链系统中,任何人可以是参与者。在一些实施例中,区块链系统100的成员可包括资源提供商,包括在线服务提供商、凭证发行方、商家、交易处理器,或可维护和/或验证用户账户的其它实体等。

[0044] 区块链系统100可包括与凭证发行方相关联或由其操作的一个或多个发行方节点110。发行方节点110可处理来自用户的请求以获得用户可用来访问资源的凭证。举例来说,当用户向资源提供商注册或开设账户时,发行方节点110可发行账户标识符。作为另一实例,例如令牌或密码密钥的一些凭证可具有有限的使用期限,并且发行方节点110可在所述凭证到期时补给此类凭证。当发行方节点110给用户发行凭证时,发行方节点110可将凭证发行的记录发布到发行方节点110处的区块链。在一些实施例中,所述凭证可由用户提供,并且发行方节点110可用于将用户提供的凭证的记录发布到发行方节点110处的区块链。

[0045] 凭证的记录也同步到区块链系统100的其它网络节点。举例来说,发行方节点110可将记录广播到网络节点105A到105F和120中的一个或多个以将记录添加到相应网络节点处的区块链的副本。在一些实施例中,与区块链系统100中的发行方相关联的一个或多个证书颁发中心可用于使记录同步。换句话说,发行方节点110可将记录提供到证书颁发中心,并且证书颁发中心可将记录发布到区块链系统110中的每一网络节点。

[0046] 区块链系统100还可包括与系统中的资源提供商相关联或由其操作的一个或多个验证节点120。验证节点120可处理来自用户的请求以访问资源。举例来说,验证节点120可从用户接收凭证以请求访问与凭证相关联的资源。验证节点120可通过查询验证节点120处的区块链以确定凭证的记录是否存在于区块链中而验证凭证。如果凭证的记录存在于区块链中,那么验证节点120可认证用户并且授权用户访问所请求的资源。

[0047] 为了与区块链系统100交互,由用户操作的通信装置130可将对凭证的请求发送到发行方节点110。所述凭证可与资源提供商相关联,并且可用于请求访问资源。发行方节点110可为用户确定发行到通信装置130的凭证,将凭证预配到通信装置130,并且将凭证发布到由区块链系统100维护的区块链。在一些实施例中,用户可选择他/她自己的凭证,并且通信装置130可将凭证提供到发行方节点110以请求发行方节点110将用户提供的凭证记录到区块链。

[0048] 一旦所述凭证已经预配到通信装置130并且被记录到区块链,那么通信装置130可提交凭证以请求访问资源。所述凭证可包括标识与资源提供商相关联的用户的账户的账户信息,或用于认证用户和/或通信装置130的其它认证信息。在一些实施例中,通信装置130可将凭证提供到访问装置140以请求访问资源。可被请求的资源的实例可包括对受限内容或信息的访问、对用户的在线账户的访问、对网络资源的访问、对受限区域的访问、对与交易有关的商品或服务的访问等。

[0049] 访问装置140可将凭证提交到验证节点120以认证用户和/或通信装置130。在接收到凭证后,验证节点120可查询区块链以确定凭证的记录是否存储在区块链中。如果凭证的记录存在于区块链中,那么验证节点120可向访问装置140指示凭证是有效的并且可授权访问资源。如果凭证的记录不存在于区块链中或被指示已经到期,那么可拒绝访问资源。应注意,在一些实施例中,通信装置130可直接运用验证节点120请求访问资源,而无需通过访问装置。举例来说,验证节点120可以是由资源提供商操作的网络服务器,并且通信装置130可与验证节点120通信以使用网页浏览器或安装在通信装置130上的其它应用程序请求访问资源。

[0050] 图2说明根据一些实施例的发行方节点计算机200的框图。发行方节点计算机200可包括处理器202、网络接口204、记录数据库232、节点数据库234、用户数据库236、密钥数据库238,和存储可由处理器202执行的代码的计算机可读存储器210。

[0051] 记录数据库232可存储由发行方节点计算机200发行的凭证以及由系统中的其它发行方发行的凭证的记录。举例来说,由发行方节点计算机200发行的凭证的记录可插入并存储在记录数据库232中。在一些实施例中,所述记录可采取组织成一个或多个记录的区块的区块链的形式。每一记录可含有从对凭证进行散列导出的散列值,以及其它数据,例如与凭证的用户相关联的公共密钥及先前区块的散列。

[0052] 节点数据库234可存储关于维护记录数据库的系统中的网络节点的信息。举例来说,节点数据库234可包括标识符,例如系统中的其它网络节点的IP地址。此信息可由发行方节点计算机200使用以将新的记录提供到其它网络节点以使系统中的记录数据库同步。

[0053] 用户数据库236可存储关于用户和其通信装置的信息,所述用户和其通信装置向与发行方节点计算机200相关联的资源提供商注册。用户信息可包括可用于标识用户的名称、地址、电子邮件、电话号码、生物标识技术,和/或安全问题的答案等。装置信息可包括序列号、装置别名、互联网协议(IP)地址、介质访问控制(MAC)地址、移动用户综合业务数字网(MSISDN)号码或与通信装置相关联的其它通信号码、国际移动用户标识(IMSI)号码、国际移动站设备标识(IMEI)号码,或其它可变或非可变装置标识字符。当处理来自用户的对凭证的请求时,用户数据库236中的信息可用于验证用户和他/她的通信装置的身份。

[0054] 密钥数据库238可存储由发行方节点计算机200使用的密码密钥。举例来说,密钥

数据库238可存储与其它发行方或证书颁发中心相关联的公共密钥,使得发行方节点计算机200可验证由这些其它实体签署的签名。密钥数据库238可存储发行方节点计算机200可用来生成签名的发行方专用密钥。在一些实施例中,密钥数据库238可使用硬件安全模块(HSM)来实施。

[0055] 计算机可读存储器210可包括记录更新模块212、签名模块214、预配模块216、验证模块218和/或其它合适的软件模块。一个或多个这些软件模块可包括可由处理器202执行以执行包括以下操作的功能的代码:处理用以发行用于通信装置的与资源相关联的凭证的请求、确定将发行到通信装置的凭证、将凭证预配到通信装置、生成从对凭证和通信装置公共密钥进行散列导出的有效负载、将有效负载存储在记录数据库的记录中,及将记录同步到其它网络节点。

[0056] 预配模块216可提供功能以确定将发行到用户的凭证并且将所述凭证预配到用户的通信装置。举例来说,预配模块216可包括随机数生成器或其它算法以生成用于用户的凭证,或可将功能提供给分配到用户或账户或与其映射的查找凭证。预配模块216还可实施用于将凭证预配或存储到用户通信装置的通信协议。在一些实施例中,所述凭证可存储在用户通信装置的安全存储器中,并且预配模块216可实施用于访问安全存储器的协议。

[0057] 签名模块214可提供功能以生成数字签名。举例来说,签名模块214可实施逻辑以使用发行方密钥(例如,发行方专用密钥)生成用于数据有效负载的数字签名。数字签名可提供来自发行方的证明以指示数据有效负载的真实性。

[0058] 验证模块218可提供功能以验证记录数据库232中的记录的存在和有效性。举例来说,验证模块218可实施逻辑以从被查询的数据生成散列值,并搜索记录数据库232以确定是否存在含有散列值的记录。验证模块218还可通过验证与记录相关联的一个或多个数字签名来验证所述记录的真实性,并且验证记录的内容是否已到期。

[0059] 记录更新模块212可提供功能以维护并更新一组记录,例如记录数据库232中的记录。举例来说,记录更新模块212可提供逻辑以从数据有效负载生成散列值以作为记录存储在记录数据库232中。记录更新模块212还可将更新通知发送到其它网络节点以使其它网络节点处的记录与新的记录同步。记录更新模块212还可从其它网络节点接收更新通知以将新的记录添加到记录数据库232。记录更新模块212可在将新的记录添加到记录数据库232之前请求验证模块218验证从其它网络节点接收的新的记录的签名。

[0060] 图3说明根据一些实施例的验证节点计算机300的框图。验证节点计算机300可包括处理器302、网络接口304、记录数据库332、密钥数据库338,和存储可由处理器302执行的代码的计算机可读存储器310。计算机可读存储器310可包括记录更新模块312、验证模块318和/或其它合适的软件模块。一个或多个这些软件模块可包括可由处理器302执行以执行功能的代码,所述功能包括接收凭证、通信装置公共密钥、由通信装置生成的通信装置签名以请求访问资源。所述功能还可包括使用通信装置公共密钥来验证通信装置签名、基于凭证和通信装置公共密钥生成散列值、确定散列值存储在记录数据库332中,及认证通信装置以用于访问所请求资源。

[0061] 验证节点计算机300的各个组件类似于上文所描述的发行方节点计算机200的组件,且因此无需重复所述组件的细节描述。验证节点计算机300与发行节点计算机200的不同之处可在于验证节点计算机300可能缺乏发行及预配凭证的能力,并且因此可能缺乏生

成新的记录的能力。尽管如此,验证节点计算机300仍可从系统中的其它网络节点接收新的记录,并相应地更新记录数据库332。

[0062] 图4说明根据一些实施例的通信装置400的框图。通信装置400可包括连接到存储器402的装置硬件404。装置硬件404可包括处理器405、通信子系统406、用户接口406、显示器屏幕407(其可以是用户接口406的部分),和非接触式接口408。处理器405可实施为一个或多个集成电路(例如,一个或多个单核或多核微处理器和/或微控制器),且被用来控制通信装置400的操作。处理器405可响应于存储在存储器402中的程序代码或计算机可读代码而执行各种程序,并且可维持多个同时执行的程序或过程。通信子系统409可包括可由通信装置400用于与其它装置通信和/或与外部网络连接的一个或多个RF收发器和/或连接器。用户接口406可包括输入和输出元件的任何组合,以允许用户与通信装置400交互并调用通信装置400的功能。在一些实施例中,显示器屏幕407可以是用户接口406的部分。

[0063] 非接触式接口408可包括一个或多个RF收发器以与访问装置的非接触式读取器交互以进行交易(例如,支付交易、访问交易、信息交换等)。在一些实施例中,非接触式接口408可由操作系统420访问。在一些实施例中,显示器407也可以是非接触式接口408的部分并被用于例如使用QR码、条形码等执行交易。

[0064] 存储器402可使用任何数目的非易失性存储器(例如,闪存器)和易失性存储器(例如,DRAM、SRAM)的任何组合、或任何其它非暂时性存储介质、或其组合介质来实施。存储器402可存储操作系统420和实施应用程序功能414的一个或多个应用程序412驻留其中的应用程序环境410。应用程序412可包括用于访问来自资源提供商的资源的提供商特定应用程序、例如网络浏览器的通用应用程序,或其它合适的应用程序。应用程序的实例可包括钱包或银行应用程序、支付应用程序、商家应用程序等。在一些实施例中,应用程序功能可包括生成通信装置公共-专用密钥对、使用通信装置专用密钥生成通信装置签名、与发行方通信以发起对凭证的请求、将凭证存储在通信装置400上,及与网络节点交互以请求访问资源。

[0065] 图5说明根据一些实施例的与区块链系统交互以用于凭证发行及所有权验证的通信流程图。操作552到562涉及发行方的凭证发行,且操作572到584在用户请求访问与凭证相关联的资源时涉及验证凭证。应注意,在一些实施例中,发行方节点510和验证节点520可以是相同的网络节点。

[0066] 在操作552处,用户可操作通信装置530以生成或以其它方式获得通信装置公共-专用密钥对。在一些实施例中,通信装置公共-专用密钥对可预加载到通信装置上或由安装在通信装置530上的应用程序生成。应用程序可以是由资源提供商提供以允许通信装置530访问与资源提供商相关联的一个或多个资源的应用程序,或例如可用于与各个资源提供商通信或访问各个资源提供商的网络浏览器的通用应用程序。

[0067] 在一些实施例中,通信装置公共-专用密钥对可以是特定于凭证的,使得不同密钥对针对于每一凭证生成,或可以是特定于账户的,使得不同密钥对针对用户的每一账户生成,但同一公共-专用密钥对用于与同一账户相关联的多个凭证(例如,多个令牌)。通信装置公共-专用密钥对还可以是特定于资源提供商的,使得不同密钥对针对不同资源提供商生成,但同一密钥对用于用户的与同一资源提供商相关联的多个凭证和/或账户。通信装置公共-专用密钥对还可以是特定于通信装置的,使得同一密钥对用于预配给同一通信装置的用于各个账户和资源提供商的凭证。通信装置公共-专用密钥对还可以是特定于以上的

任何组合的。通信装置公共-专用密钥对可使用例如整数分解或离散对数的合适算法来生成。在一些实施例中,通信装置公共-专用密钥对可由远程服务器生成并且被提供到通信装置530。

[0068] 在操作554处,通信装置530可将请求发送到发行方节点510以请求发行方节点510发行与资源相关联的凭证。所述请求可包括在操作552中生成或获得的通信装置公共-专用密钥对的通信装置公共密钥。所述请求还可包括发行方节点510可用来验证用户的身份和/或账户的其它使用标识信息。举例来说,在一些实施例中,被请求的凭证可以是用作账户标识符的替代的令牌,并且所述请求可包括信息标识账户。在一些实施例中,当用户登录与发行方节点510相关联的应用程序或网站时,可传输所述请求。在一些实施例中,通信装置530可提供其自身的凭证,并且可请求发行方节点510将凭证记录到区块链。举例来说,这在用户具有选择他/她的自身的例如用户名和/或口令的凭证的选择的情况下可能发行。

[0069] 在操作556处,发行方节点510可验证用户的身份和/或账户,并且为用户确定将发行到通信装置530的凭证。在一些实施例中,所述凭证可由发行方节点510随机生成或根据预定算法生成。在所请求凭证是令牌的实施例中,发行方节点510可通过查询令牌库来确定将发行的令牌,所述令牌库存储账户标识符和分配给账户标识符的令牌的映射。发行方节点510接着可生成数据有效负载,所述数据有效负载从通信装置530提供的凭证和通信装置公共密钥导出。举例来说,数据有效负载可包括凭证和通信装置公共密钥的散列。在一些实施例中,数据有效负载可通过对凭证、通信装置公共密钥和区块链的先前区块的散列进行散列来导出。包括先前区块的散列可降低记录被伪造的风险,因为区块链中的每一区块取决于区块链的先前区块。发行节点510接着可通过将数据有效负载作为记录存储在区块链的当前区块中来将数据有效负载发布到区块链。

[0070] 根据一些实施例,区块链可组织成区块,并且每一区块可含有一个或多个记录。每一记录可表示凭证与通信装置公共密钥之间的相关联性。每一区块可包括区块标识符,其可用于针对记录查询区块链。区块标识符可以是序列号、随机数,或区块链的先前区块的散列等。在一些实施例中,来自不同发行方的凭证可被维护在单独的区块链中,或组合成由系统维护的单个区块链。

[0071] 在一些实施方案中,除了数据有效负载之外,每一记录还可包括一个或多个数字签名。举例来说,数据有效负载可由发行方节点510使用签名密钥来签署以生成用于记录的记录签名。签名密钥可以是特定于凭证发行方的发行方密钥。在一些实施例中,发行方节点510可将数据有效负载提供到证书颁发中心,并且证书颁发中心可使用证书颁发中心密钥来签署数据有效负载以生成记录签名。每一记录还可由对应的发行方和证书颁发中心来签署。举例来说,数据有效负载可由发行方运用发行方密钥来签署,并且由证书颁发中心运用证书颁发中心密钥来单独地签署以生成记录的两个签名。作为另一实例,数据有效负载可由发行方运用发行方密钥来签署,并且数据有效负载连同由发行方生成的签名可由证书颁发中心运用证书颁发中心密钥来签署。

[0072] 包括数据有效负载和任何签名的记录接着可同步到区块链系统中的其它网络节点。举例来说,在操作558处,发行方节点510可将通知发送到验证节点520以及其它网络节点以更新验证节点520处的区块链的副本。所述通知可包括将添加到区块链的记录(例如,数据有效负载和任何签名)。在一些实施例中,发行方节点510可将记录提供到一个或多个

证书颁发中心,且所述证书颁发中心可将更新通知发送到区块链系统的其它网络节点。

[0073] 在操作562处,发行方节点510将所请求凭证预配到通信装置530。发行节点510还可将区块链中含有凭证的记录的区块的区块标识符提供到通信装置530。举例来说,发行方节点510可将凭证和区块标识符存储在通信装置530的安全存储器中,并且使所述凭证和所述区块标识符与资源提供商的公共密钥和用户账户相关联。通信装置530接着可使用凭证以请求访问与资源提供商相关联的资源。

[0074] 举例来说,在操作572处,通信装置530可与访问装置540交互以请求访问资源。举例来说,访问装置540可以是为用户提供对资源的访问的计算装置(例如,网络服务器)、销售点终端、运送或受限区域门等。通信装置530可将凭证和通信装置公共密钥提供到访问装置540以请求访问资源。在一些实施例中,通信装置530还可将区块标识符提供到访问装置540,所述区块标识符标识区块链中含有凭证的记录的区块。

[0075] 访问装置540可在操作574处通过将密码质询提供到通信装置530来验证通信装置公共密钥,并且通信装置530可在操作576处提供对密码质询的响应。举例来说,访问装置540可将数值提供到通信装置530,且通信装置530可使用通信装置公共-专用密钥对的通信装置专用密钥对数值进行加密或签署数值以生成通信装置签名,并将通信装置签名发送回到访问装置540。如果访问装置540可使用通信装置公共密钥对通信装置签名进行恰当解密以检索数值,那么可验证在操作572处接收的通信装置公共密钥。在一些实施例中,数值可以是由访问装置540或区块链系统的验证节点生成的随机数、随机数字符串或不可预测的数字。在一些实施例中,数值可以是与运用访问装置540进行的交易相关联的交易数据(例如,交易金额等)。

[0076] 通信装置签名可替代地从通信装置530上已经可用的可验证数据生成,且因此数值无需由访问装置540提供。在此类实施例中,通信装置签名可被提供到访问装置540作为操作572的一部分。举例来说,数值可以是区块链中含有凭证的记录的区块的区块标识符。通信装置签名可使用通信装置公共密钥进行解密,并且所述结果可用于针对记录查询区块链。数值还可以是凭证本身和/或通信装置公共密钥。在一些实施例中,数值还可以是资源提供商需要的其它数据,例如账单地址或其它用户标识数据等。在一些实施例中,访问装置540可不验证通信装置签名本身,并且可将通信装置签名传输到验证节点以供验证。

[0077] 在操作578处,访问装置540可将从通信装置530接收的凭证和通信装置公共密钥发送到验证节点520以确定区块链是否含有凭证与通信装置公共密钥之间的相关联性的记录。在一些实施例中,在访问装置540验证了通信装置签名之后执行操作578。在一些实施例中,通信装置签名与凭证和通信装置公共密钥一起发送到验证节点520。在此类实施例中,在查询区块链之前,验证节点520可验证通信装置签名。举例来说,验证节点520可使用通信装置公共密钥对通信装置签名进行解密以获得区块标识符,且接着使用经过解密的区块标识符查询区块链。

[0078] 在操作582处,验证节点520可查询区块链以确定凭证的记录是否存在于区块链中。举例来说,验证节点520可生成所接收的凭证和通信装置公共密钥的散列,并且检查散列值是否存储于区块链中。在一些实施例中,如果通信装置530提供区块标识符(例如,可在通信装置签名中进行解密,或连同凭证和通信装置公共密钥一起发送等),那么验证节点520可查询由区块标识符标识的区块,并确定散列值是否存储在所述区块中。在记录是进一

步从区块链中的先前区块的散列导出的实施例中,验证节点520可使用区块标识符查询先前区块的散列。验证节点520可从所接收的凭证、公共密钥和先前区块的散列生成散列值,并确定散列值是否存储在与区块标识符相关联的区块中。在一些实施例中,区块标识符可以是先前区块的散列,且区块标识符可直接用作散列函数的输入。

[0079] 如果散列值存在于区块链中,那么验证节点520可确定公共密钥的所有者也是凭证的所有者,并且因此通信装置530和其用户可被认证以用于访问所请求资源。在一些实施例中,如果记录包括任何签名(例如,由发行方和/或证书颁发中心生成的签名),那么在可认证通信装置530和其用户之前还验证签名。验证记录签名提供了所述凭证是由有效来源发行的额外保证。在一些实施例中,凭证可具有有限使用期限,并且可在预定时间量或预定使用量之后到期。在此类实施例中,区块链中的每一记录还可包括指示与记录相关联的凭证是否已到期的标签。如果与记录相关联的标签指示凭证仍是有效的并且尚未到期,那么可认证通信装置530和其用户。在操作584处,验证节点520将认证结果发送到访问装置520,并且访问装置540可基于认证结果授权用户访问所请求资源。应注意,在一些实施例中,访问装置540和验证节点520可以是同一网络节点的部分或是同一装置的部分。在一些实施例中,访问装置540的功能中的一些可由验证节点520执行,或反之亦然。

[0080] 根据一些实施例,参考图1和5描述的区块链系统和交互可实施于交易系统中。举例来说,区块链系统中的网络节点可包括银行和/或交易处理器,如发行方、商家、管理商家账户的收单方、交易处理网络(例如,威士卡、万事达卡等等),和/或第三方交易服务提供商,例如移动钱包提供商等。

[0081] 由用户操作并且用作支付装置的便携式通信装置(例如,移动电话、智能卡等)可将通信装置公共密钥传输到发行方,例如银行或交易处理器,其发行例如充当账户标识符的替代的PAN或令牌的账户标识符。在一些实施例中,可通过用户登录到在线银行应用程序、移动钱包应用程序、商家应用程序或由发行方管理或与发行方相关联的网站等来实现传输通信装置公共密钥。发行方可验证用户的身份,并且确定将发行方到用户的账户标识符(例如,PAN、令牌等)。这可涉及发行方检查用户的数据库和/或发行方管理的账户及确定与用户相关联或与用户的通信装置相关联的账户标识符。

[0082] 发行方接着可创建包括由用户提供的通信装置公共密钥和账户标识符的有效负载或消息,并用发行方的专用密钥签署消息。发行方可将此消息传输到交易处理网络。交易处理网络(例如,充当证书颁发中心)接着可将账户标识符和通信装置公共密钥发布到由交易处理网络管理的区块链,并且使系统中的网络节点上的区块链同步。在一些实施例中,发行方可能够将通信装置公共密钥和账户标识符发布到区块链本身,并且使所述通信装置公共密钥和账户标识符同步到其它网络节点,而无需将其发送到交易处理网络。在一些实施例中,发行方可发布账户标识符和通信装置公共密钥的散列而非实际值以保护用户隐私性。被发布的散列可另外通过区块链中的先前区块的散列值来计算。发行方可将区块标识符返回到用户,使得可标识区块链中容纳记录的位置。

[0083] 在一些实施例中,发行方可以数字方式签署其发布到区块链的记录,从而向其它实体证明发行方是发行账户标识符的实体。然而,区块链系统可具有数百或数千个不同发行方,并且使用发行方签名可能需要系统中的每一网络节点将每一发行方都建立为受信任实体。因而,在一些实施例中,交易处理网络可向例如发行方、商家和/或钱包提供商的其它

实体证明其验证了发行账户标识符的发行方的身份。以此方式,交易处理网络可充当发行方证书的根证书颁发中心。通过充当根证书颁发中心,交易处理网络可简化与数字凭证相关联的信托过程。交易处理网络可与发行方建立信任且接着商家仅需要信任交易处理网络,而非每一商家需要与每一发行方建立信任。交易处理网络可签署发行方的证书,在本质上证明发行方应受信任。这允许商家仅信任交易处理网络而非相对大量的发行方。

[0084] 在一些实施例中,交易处理网络可进一步将其自身的签名添加在发布在区块链上的记录上。这可充当增加的置信量度。交易处理网络实际上在声明发布记录的发行方实际上是与记录相关联的账户标识符的发行方。这可防止一个发行方错误地发布记录以证明由另一发行方发行的账户标识符的所有权的情境。在一些实施例中,交易处理网络签名可用于代替发行方签名。

[0085] 为了使用所发行的账户标识符进行交易,所述用户可将账户标识符和通信装置公共密钥提供到商家(例如,通过POS终端或网站等)。用户还可提供由通信装置专用密钥签署的质询消息。在一些实施例中,质询消息可由商家提供到用户,且可呈随机数或随机产生的数字序列的形式。在一些实施例中,商家所需的区块标识符或其它支付数据,例如账单地址,可用作质询消息。商家可首先验证所提供的通信装置公共密钥能够对运用通信装置专用密钥签署的质询消息进行恰当解密。商家接着可检查由交易处理网络管理的区块链中的记录。如果商家能够找到指示通信装置公共密钥和账户标识符彼此相关联的记录,那么商家可将用户认证为通信装置公共密钥和账户标识符的所有者,并且因此验证账户标识符的所有权。

[0086] 本文中所描述的技术可使得用户能够证明其对凭证(例如,PAN或令牌)的所有权,而不必放弃凭证数据之外的任何PII信息。相比于常规的技术,这明显增加了消费者隐私性。此外,根据一些实施例的区块链系统为发行方产生了较低的集成成本。不需要每当用户需要验证发行方的凭证所有权时都涉及发行方。相反,在需要凭证所有权验证之前,发行方仅需要与用户进行单次交互。另外,相较于常规的技术,本文中所描述的技术还减少了消费者摩擦。虽然消费者仍可能需要在凭证所有权验证期间采取某些措施,但所述过程比常规的技术容易得多且更顺畅。举例来说,用户将不必输入大量的PII或被重新导向到发行方网页以便被认证。

[0087] 此外,在商家是区块链网络的成员的实施方案中,凭证验证可在商家处本地执行,而不必将凭证传输到发行方。这可以是有利的,例如,在不可获得商家与发行方之间的连续网络连接性的环境中。凭证所有权验证过程还可较快执行,因为验证可在本地进行,而不必通过网络传输凭证。这在例如大众运输系统的环境中可以是有利的,在所述环境中,尽可能地降低交易处理速度是有利的。

[0088] 图6说明根据一些实施例的区块链600的一部分。图6中展示的区块链600的部分包括两个区块—区块(n)和区块(n+1)。所述区块中的每一个可包括一个或多个记录,例如如所展示的‘x’记录数。每一记录可包括有效负载。因此,区块(n)中的记录可包括有效负载(n)(1)到有效负载(n)(x),且区块(n+1)中的记录可包括有效负载(n+1)(1)到有效负载(n+1)(x)。每一记录还可具有一个或多个签名。举例来说,含有有效负载(n+1)(2)的记录可包括第一签名SIG_i(n+1)(2)和第二签名SIG_{ca}(n+1)(2)。

[0089] 根据一些实施例,区块链600可用于存储例如主账号(PAN)的凭证或例如令牌的其

它账户标识符的记录。作为实例,有效负载(n+1)(2)中的数据可包括通过将散列函数应用于PAN导出的散列值、与请求PAN的通信装置相关联的公共密钥,和先前区块的散列值(例如,区块(n)的散列值)。记录的第一签名可以是由发行方(例如,发行PAN的银行)使用发行方专用密钥生成的发行方签名,并且第二签名可以是由证书颁发中心(例如,交易处理网络)使用证书颁发中心专用密钥生成的证书颁发中心签名。在一些实施例中,签名中的一个或多个可从记录省去。

[0090] 图7说明根据一些实施例的用于将记录添加到区块链的过程700的流程图。过程700可例如由凭证发行方计算机或发行方网络节点等执行。在框702处,过程700可通过接收用以发行用于通信装置的凭证的请求来进行。所述请求可包括与通信装置相关联的通信装置公共密钥。在框704处,过程700可确定将发行到通信装置的凭证。举例来说,所述凭证可随机生成、使用预定算法生成,或从数据存储区检索。在一些实施例中,所述凭证可以是账户标识符或令牌,所述令牌是账户标识符的替代。在框706处,例如可通过将凭证存储到通信装置上,而将凭证预配到通信装置。在一些实施例中,将凭证预配到通信装置可包括将区块标识符提供到通信装置,所述区块标识符标识区块链中的哪一区块将用于存储凭证的记录。

[0091] 在框708处,过程700可生成从对凭证和通信装置公共密钥进行散列导出的有效负载。在一些实施例中,有效负载可进一步从区块链的先前区块的散列导出的。在框710处,有效负载可存储在区块链的记录中。在一些实施例中,记录可包括运用签名密钥生成的签名。签名密钥可以是与凭证发行方计算机相关联的发行方密钥,或与证书颁发中心相关联的证书颁发中心密钥。在一些实施例中,记录可包括分别运用发行方密钥和证书颁发中心密钥生成的两个签名。在框712处,将记录同步到区块链上的其它网络节点。

[0092] 图8说明根据一些实施例的用于验证凭证的所有权的过程800的流程图。举例来说,过程800可由验证计算机或验证网络节点等执行。过程800可在框802处通过接收凭证、与通信装置相关联的通信装置公共密钥和用以请求访问资源的通信装置签名来进行。可通过使用对应于通信装置公共密钥的通信装置专用密钥对数值进行加密而生成通信装置签名。在一些实施例中,数值可以是从网络节点提供到通信装置的数字、标识区块链中的哪一区块含有凭证的记录的区块标识符、区块链中含有凭证的记录的区块的先前区块的散列中的一个,或其某一组合。在框804处,可使用通信装置公共密钥来验证通信装置签名,作为认证通信装置的一部分。在框806处,响应于验证通信装置签名,可基于凭证和通信装置公共密钥生成散列值。在框808处,过程800可确定散列值存储在区块链的记录中。在框810处,过程800可验证与含有散列值的区块链的记录相关联的记录签名。在框812处,响应于确定散列值存储在区块链中及验证记录的记录签名,可认证通信装置以用于访问所请求资源。

[0093] 图9说明根据一些实施例的可用于实施本文中所描述的技术的高级区块链架构904。举例来说,区块链架构904可以是超级分类账结构(Hyperledger Fabric),并且可包括成员服务软件区块904A、区块链服务软件区块904B、链码服务软件区块904C和世界状态数据库904D。在一些实施例中,链码服务软件区块904C含有应用程序的核心逻辑。所述链码服务软件区块可从网络中的不同参与者,例如发行方,接收请求。链码服务软件区块904C可将这些请求转换成对存储在区块链中的数据执行的操作。链码服务软件区块904C可向发行方公开或授权功能,例如创建指示凭证与公共密钥之间的相关联性的新的记录或将所述新的

记录发布到区块链的能力。链码服务软件区块904C还可使得发行方能够去除凭证与公共密钥之间的相关联性,或将记录标记为到期或变得无效。链码服务软件区块904C可进一步允许例如商家的第三方订户针对记录或凭证与公共密钥之间的相关联性查询区块链。

[0094] 现将描述可用于实施本文中所描述的实体或组件中的任一个的计算机系统。计算机系统中的子系统通过系统总线互连。额外子系统包括可连接到显示器适配器的打印机、键盘、固定磁盘和监视器。外围装置和输入/输出(I/O)装置可连接到I/O控制器,且可通过本领域已知的任何数量的构件(例如串行端口)连接到计算机系统。举例来说,串行端口或外部接口可用于将计算机设备连接到例如互联网的广域网、鼠标输入装置或扫描器。通过系统总线的互连允许中央处理器与每个子系统通信,且控制来自系统存储器或固定磁盘的指令的执行以及子系统之间的信息交换。系统存储器和/或固定磁盘可体现计算机可读介质。

[0095] 本文中所描述的技术可涉及实施一个或多个功能、过程、操作或方法步骤。在一些实施例中,由于通过适当编程的计算装置、微处理器、数据处理器等执行指令集或软件代码,可实施功能、过程、操作或方法步骤。指令集或软件代码可存储在由计算装置、微处理器等访问的存储器或其它形式的数据存储元件中。在其它实施例中,功能、过程、操作或方法步骤可由固件或专用处理器、集成电路等实施。

[0096] 本文中所描述的方法和过程本质上是示例性的,并且根据一些实施例的方法和过程可按与本文中所描述的次序不同的次序执行步骤中的一个或多个、包括没有具体描述的一个或多个额外步骤、省略一个或多个步骤、将一个或多个步骤组合成单个步骤、将一个或多个步骤分割成多个步骤,和/或其任何组合。

[0097] 本申请中描述的任何软件组件或功能可使用例如常规的或面向对象的技术并使用任何合适的计算机语言,例如Java、C++或Perl,实施为由处理器执行的软件代码。软件代码可被存储为计算机可读介质,例如,随机存取存储器(RAM)、只读存储器(ROM)、例如硬盘驱动器或软盘的磁性介质,或例如CD-ROM的光学介质上的一系列指令或命令。任何此类计算机可读介质可驻留在单个计算设备上或单个计算设备内,并且可存在于系统或网络内的不同计算设备上或不同计算设备内。

[0098] 在不偏离本发明的范围的情况下,任何实施例的一个或多个特征可与任何其它实施例的一个或多个特征组合。

[0099] 除非明确指示为相反情况,否则“一”或“所述”的叙述旨在表示“一个或多个”。

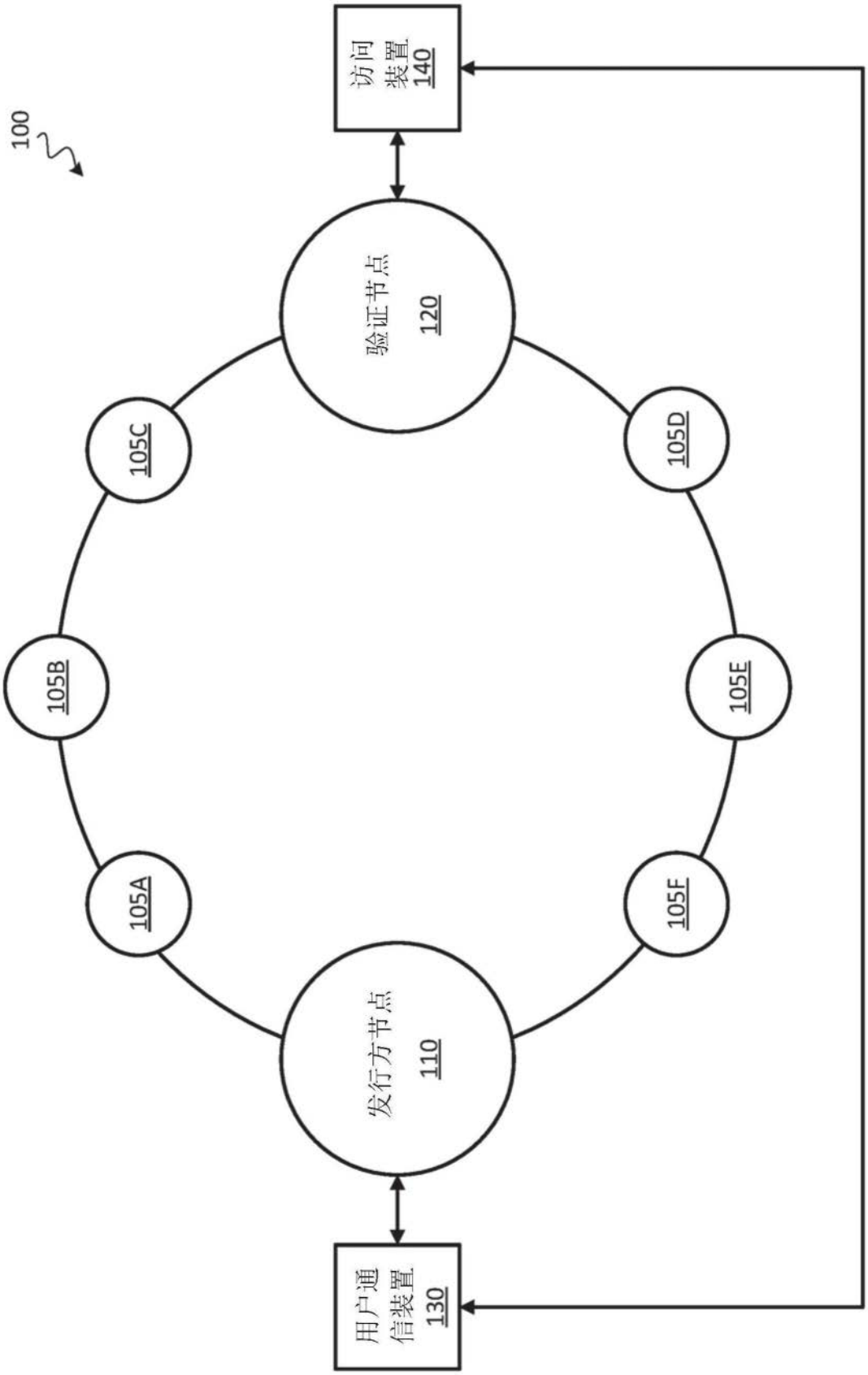

100
访问装置 140
验证节点 120
105C
105D
105B
105E
105A
105F
发行方节点 110
用户通信装置 130

图1

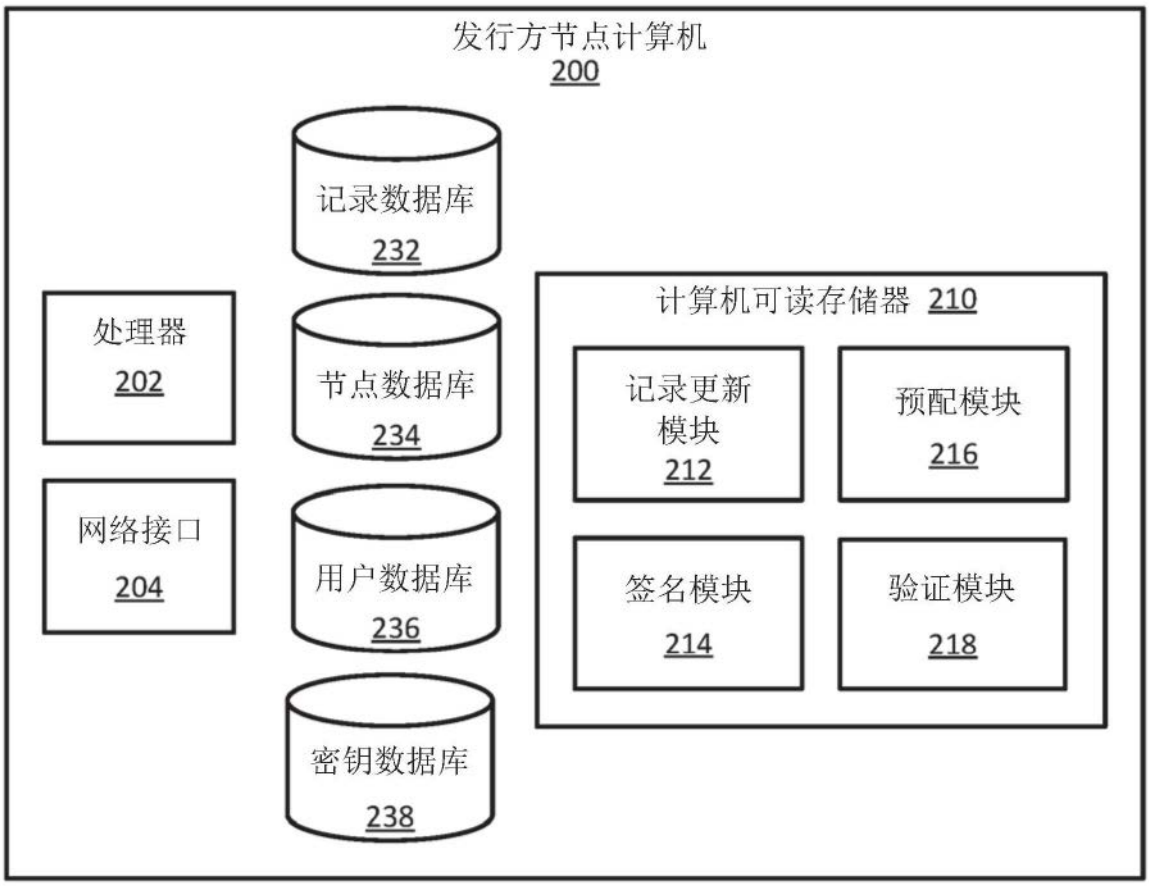

发行方节点计算机
200
记录数据库
232
处理器
202
节点数据库
234
网络接口
204
用户数据库
236
密钥数据库
238
计算机可读存储器 210
记录更新模块
212
预配模块
216
签名模块
214
验证模块
218

图2

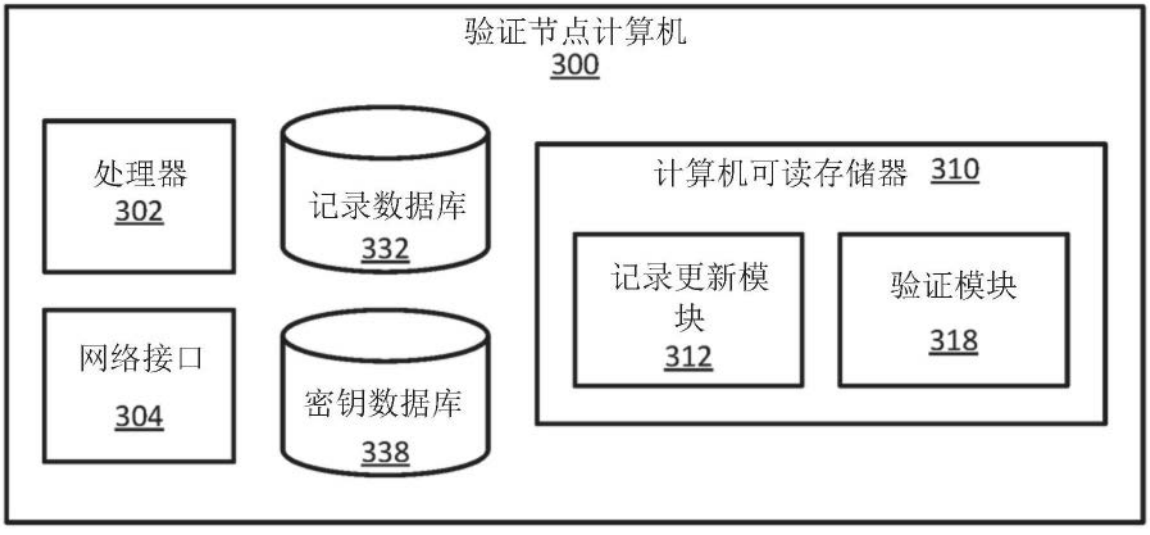

验证节点计算机
300
处理器
302
记录数据库
332
网络接口
304
密钥数据库
338
计算机可读存储器 310
记录更新模块
312
验证模块
318

图3

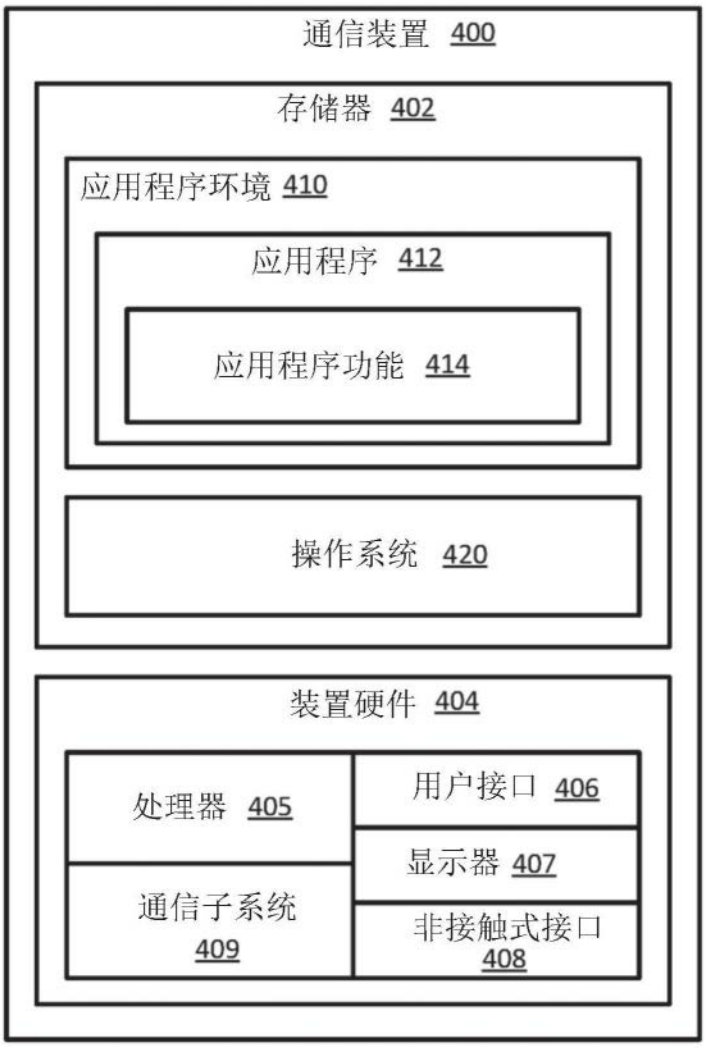

通信装置 400
存储器 402
应用程序环境 410
应用程序 412
应用程序功能 414
操作系统 420
装置硬件 404
处理器 405
用户接口 406
显示器 407
通信子系统 409
非接触式接口 408

图4

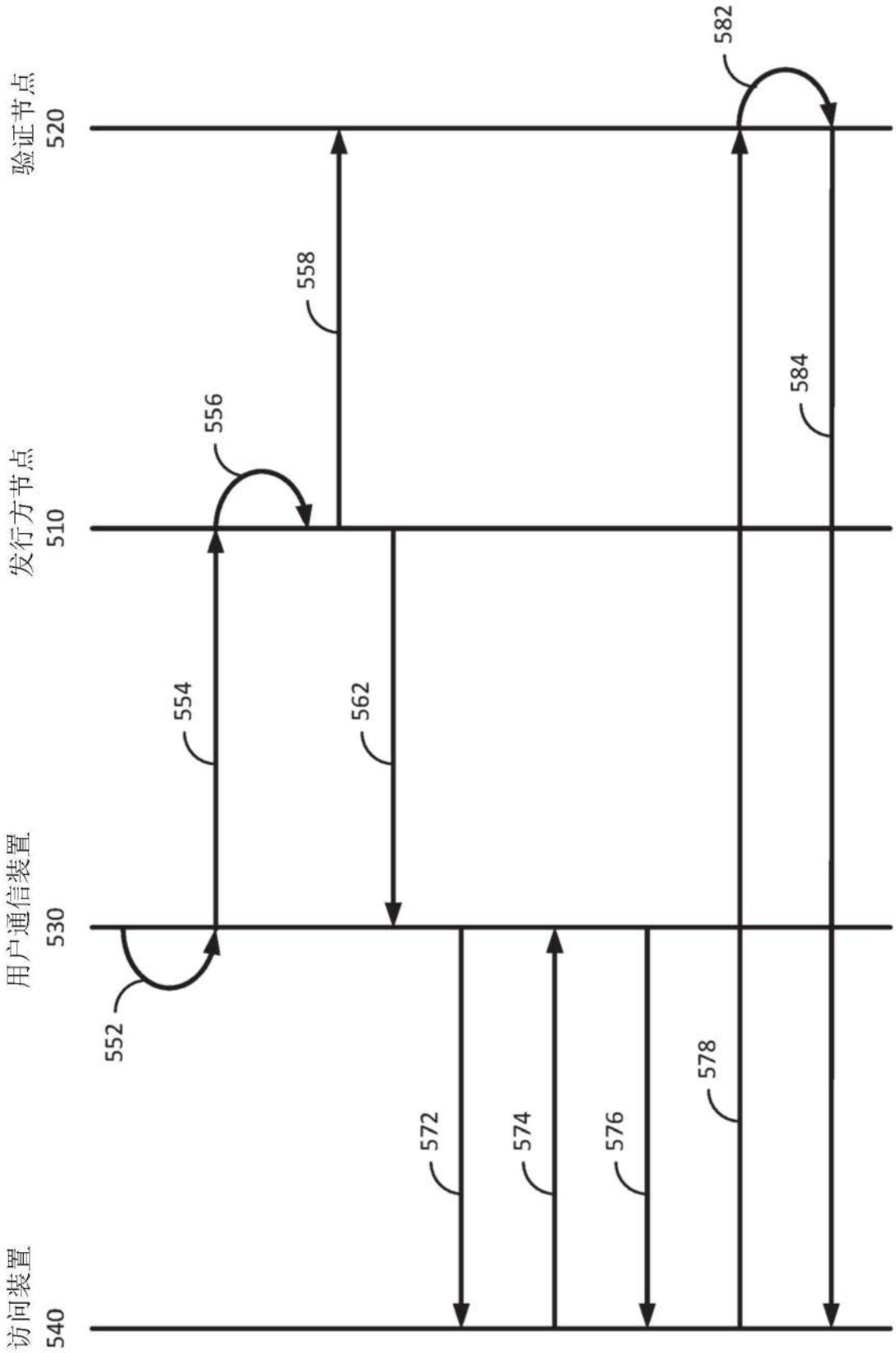

验证节点
520
发行方节点
510
用户通信装置
530
访问装置
540
552
554
556
558
562
572
574
576
578
582
584

图5

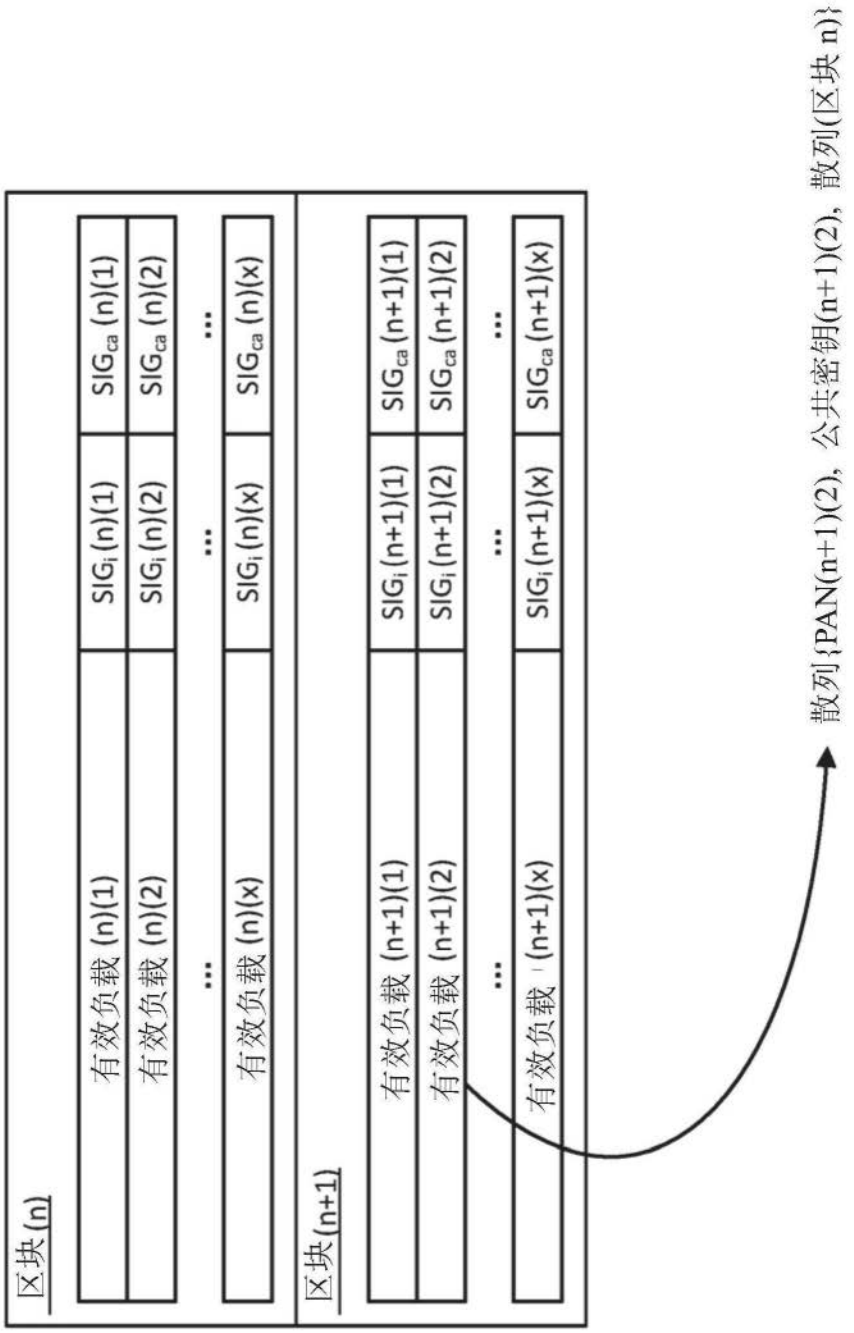

区块(n)
有效负载 (n)(1)
有效负载 (n)(2)
...
有效负载 (n)(x)
SIGi (n)(1)
SIGi (n)(2)
...
SIGi (n)(x)
SIGca (n)(1)
SIGca (n)(2)
...
SIGca (n)(x)
区块(n+1)
有效负载 (n+1)(1)
有效负载 (n+1)(2)
...
有效负载 (n+1)(x)
SIGi (n+1)(1)
SIGi (n+1)(2)
...
SIGi (n+1)(x)
SIGca (n+1)(1)
SIGca (n+1)(2)
...
SIGca (n+1)(x)
散列{PAN(n+1)(2)，公共密钥(n+1)(2)，散列(区块 n)}

图6

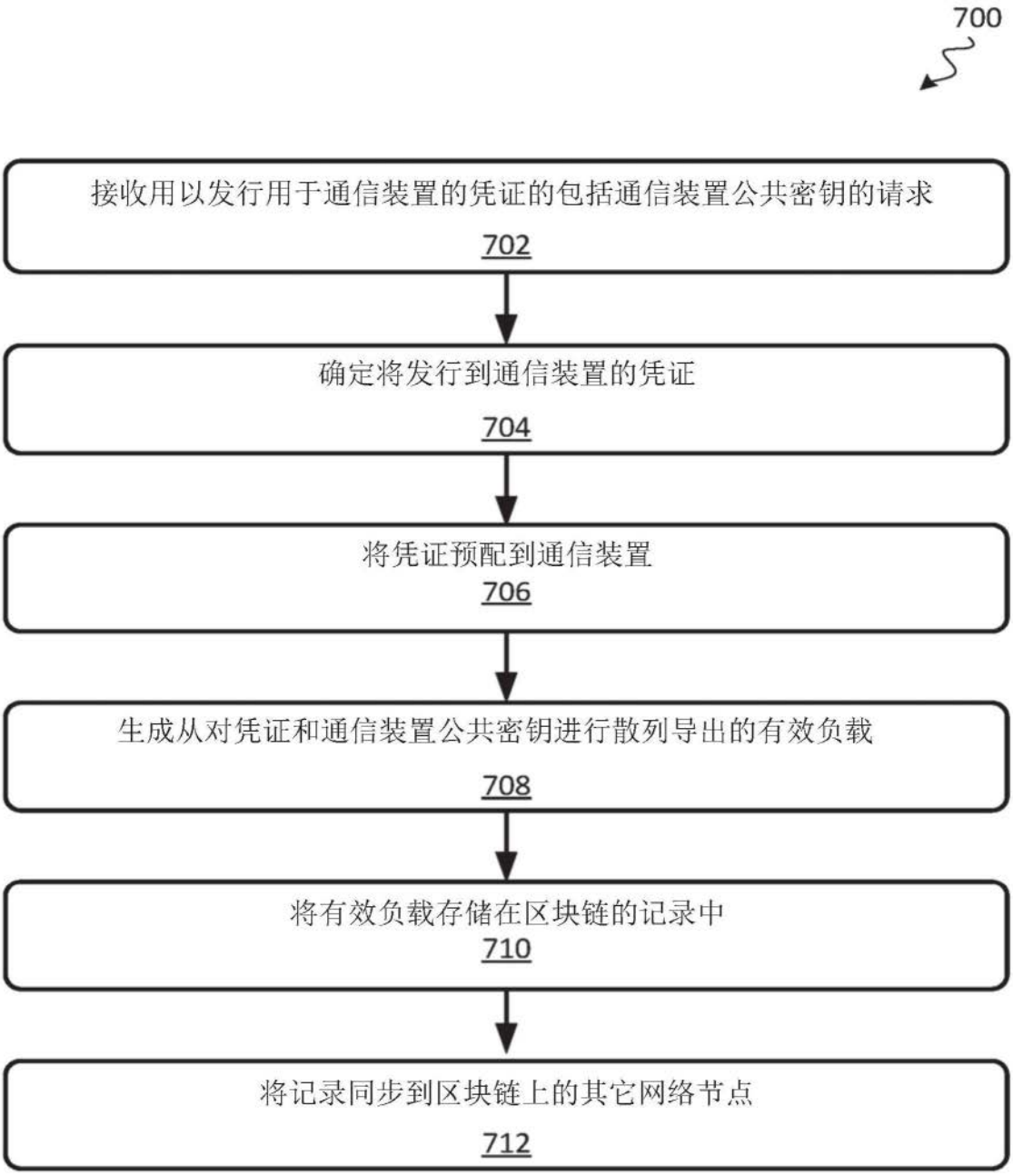

700
接收用以发行用于通信装置的凭证的包括通信装置公共密钥的请求
702
确定将发行到通信装置的凭证
704
将凭证预配到通信装置
706
生成从对凭证和通信装置公共密钥进行散列导出的有效负载
708
将有效负载存储在区块链的记录中
710
将记录同步到区块链上的其它网络节点
712

图7

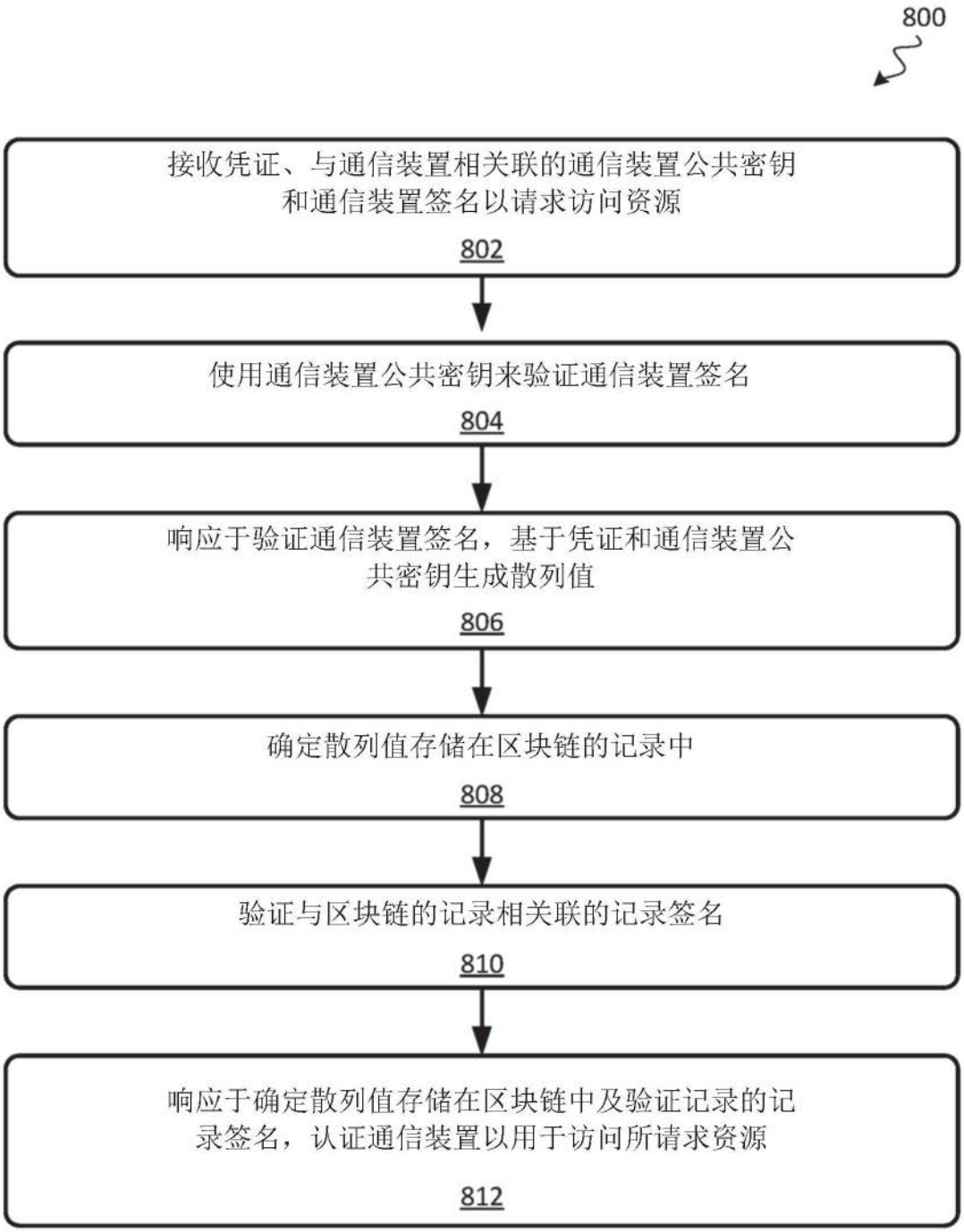

800
接收凭证、与通信装置相关联的通信装置公共密钥和通信装置签名以请求访问资源
802
使用通信装置公共密钥来验证通信装置签名
804
响应于验证通信装置签名，基于凭证和通信装置公共密钥生成散列值
806
确定散列值存储在区块链的记录中
808
验证与区块链的记录相关联的记录签名
810
响应于确定散列值存储在区块链中及验证记录的记录签名，认证通信装置以用于访问所请求资源
812

图8

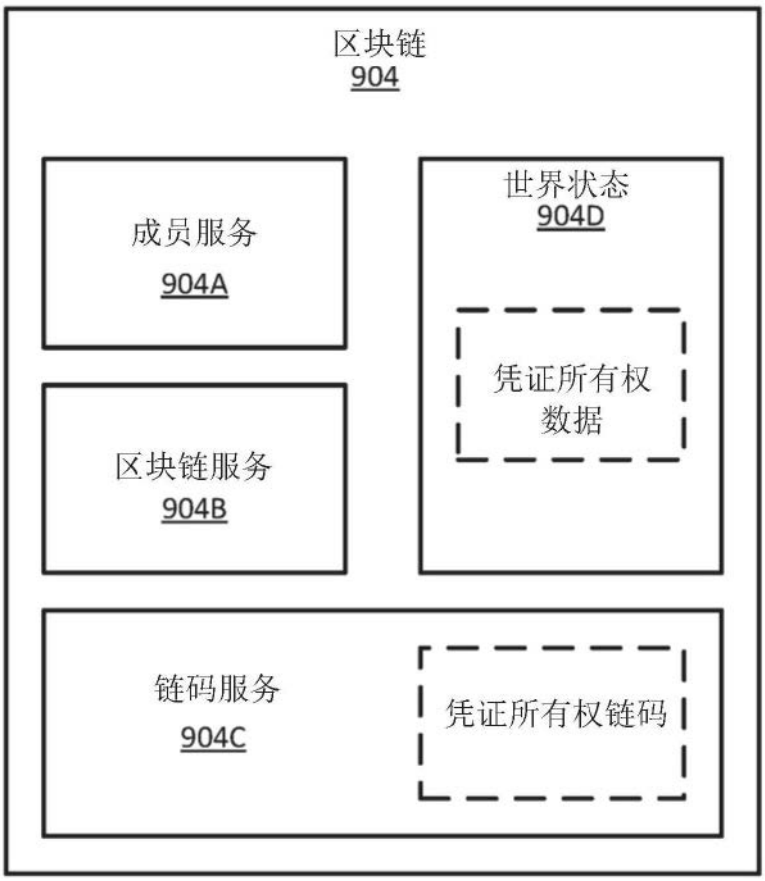

区块链
904
成员服务
904A
区块链服务
904B
世界状态
904D
凭证所有权
数据
链码服务
904C
凭证所有权链码

图9