(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112437938 A
(43)申请公布日 2021.03.02

(21)申请号 201980045178.9

(22)申请日 2019.07.03

(30)优先权数据
62/693,713 2018.07.03 US
62/768,049 2018.11.15 US

(85)PCT国际申请进入国家阶段日
2021.01.20

(86)PCT国际申请的申请数据
PCT/US2019/040646 2019.07.03

(87)PCT国际申请的公布数据
WO2020/010279 EN 2020.01.09

(71)申请人 环玺有限责任公司
地址 新加坡华利街1号国浩大厦25-01A室

(72)发明人 W·努南 L·拉尚斯
L·万德恩布鲁克

(74)专利代理机构 深圳市百瑞专利商标事务所(普通合伙) 44240
代理人 金辉

(51)Int.Cl.
G06Q 20/38(2006.01)

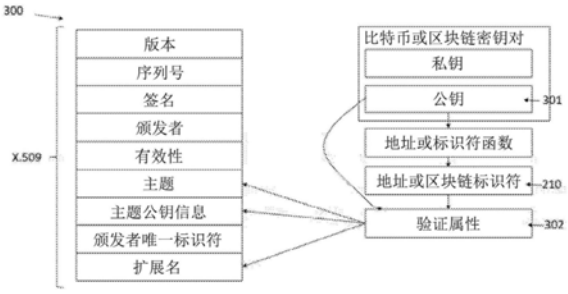
权利要求书1页 说明书9页 附图8页

(54)发明名称

用于区块链地址和所有者验证的系统和方法

(57)摘要

用于保障区块链交易安全的系统和方法,包括通过一个或多个计算设备形成具有多个节点的区块链,每个节点具有区块链地址。向证书服务器请求认证证书。认证证书是一个受信任的证书,它包含一个或多个字段,用于验证与交易相关联的实体的身份,一个地址字段包含一个区块链节点的认证地址。通过确定所述实体已通过受信任的证书认证,并且该认证地址与第一区块链地址相匹配,来验证交易。



CN 112437938 A

1.一种系统,包括:

一个或多个维护区块链的计算设备,所述区块链具有一个或多个节点,每个所述节点包括一个区块链地址,一个或多个所述计算设备能够通过网络彼此通信;

服务器,所述服务器在网络上进行通信,且配置为提供与实体相关联的认证证书,其中所述认证证书包括一地址字段,所述地址字段包含至少一个区块链地址,用以验证所述区块链地址与所述实体相关联。

2.根据权利要求1所述的系统,其中,所述区块链包括比特币区块链。

3.根据权利要求2所述的系统,其中,所述区块链地址是比特币地址。

4.根据权利要求1所述的系统,其中,所述认证证书是X.509证书。

5.根据权利要求4所述的系统,其中,所述地址字段是所述X.509证书的扩展字段。

6.根据权利要求1所述的系统,其中,所述服务器与认证服务相关联。

7.根据权利要求1所述的系统,其中,一个或多个所述计算设备配置为通过从所述服务器中请求认证证书来验证相应实体的身份。

8.根据权利要求7所述的系统,其中,一个或多个所述计算设备配置为在验证相应实体的身份之后与所述相应实体进行金融交易。

9.根据权利要求1所述的系统,其中,所述认证证书与加密公钥相关联。

10.根据权利要求9所述的系统,其中,与所述认证证书中包含的区块链地址相对应的区块链节点与加密公钥相关联。

11.一种安全交易的方法,包括:

通过一个或多个计算设备形成具有多个节点的区块链,每个节点具有区块链地址,其中多个节点中的第一节点具有与交易相关联的第一区块链地址,

从认证服务器请求认证证书,所述认证证书包含一个或多个字段,用于验证与交易相关联的实体的身份,并且认证证书具有包含认证地址的地址字段;以及

通过确定所述认证地址与第一区块链地址相匹配来验证实体与交易相关联。

12.根据权利要求11所述的方法,其中,进一步包括在验证实体与交易相关联后,向第一区块链地址或从第一区块链地址转移资金。

13.根据权利要求11所述的方法,其中,所述区块链包括比特币区块链。

14.根据权利要求13所述的方法,其中,所述区块链地址是比特币地址。

15.根据权利要求11所述的方法,其中,所述认证证书是X.509证书。

16.根据权利要求15所述的方法,其中,所述地址字段是所述X.509证书的扩展字段。

17.根据权利要求11所述的方法,其中,所述服务器与认证服务相关联。

18.根据权利要求11所述的方法,其中,一个或多个所述计算设备配置为通过从服务器中请求认证证书来验证相应实体的身份。

19.根据权利要求18所述的方法,其中,一个或多个所述计算设备配置为在验证相应实体的身份之后与所述相应的实体进行金融交易。

20.根据权利要求11所述的方法,其中,所述认证证书与加密公钥相关联。

21.根据权利要求20所述的方法,其中,与所述认证证书中包含的区块链地址相对应的区块链节点与加密公钥相关联。

用于区块链地址和所有者验证的系统和方法

技术领域

[0001] 本发明涉及区块链,更具体地说,涉及具有身份验证的区块链。

背景技术

[0002] 区块链是一个不断增长的记录列表,称为区块,这些记录使用加密技术(包括密码散列)链接在一起。区块链中的每个区块都可以包含前一区块的密码散列、时间戳和交易数据。一旦将一个区块记录在该链中,在不改变所有后续区块的情况下,任何给定区块中的数据都不能追溯更改。因此,区块链相对不易被修改且设计上相对安全。

[0003] 一些区块链可能与价值单位是根深蒂固的,例如“硬币”或“代币”,它们与系统之间有着密不可分的联系。区块链也可以存储价值,而仅为一本账本就提供了价值核算。比特币区块链(The Bitcoin blockchain)是新一代互联网协议中第一个也是运行时间最长的存储价值的协议。

[0004] 比特币基于一个工作量证明系统,该系统需要能量和计算资源(更普遍而言是劳动力)来生产新的区块以及获取区块奖励。生产每个比特币所需的这些计算资源会使代表价值所需的信任值最小化,这是由于每一个比特币都是“牺牲”的衡量标准(ameasure of sacrifice)。

[0005] 交易的每一方都可以确信,一个特定的单位是通过维护和保障系统的工作而建立的,而不是通过许可或任何法令,或投机性的债务义务来创建。至少从这种意义上讲,比特币不可伪造的特性和生产所需的资源赋予了其价值。换句话说,挖掘比特币区块的工作就是通过使其不可伪造来保护区块链。

[0006] 具体地,挖掘工作是创建一个数据结构,以使在面临安全威胁和网络故障时保持其完整性。即使比特币网络中的所有计算机都处于离线状态,且所有私钥都遭到泄露,攻击者也只能通过重新创建最初区块链创建所需的所有工作来伪造区块链的数据结构。对于大多数攻击者来说,即使有时间,这也是不可行的。

[0007] 此外,随着时间的推移,从系统中获得的效益可以弥补通过挖掘来保护区块链的成本。

[0008] 不可伪造的昂贵商品通过有利的财产转移来不断地提升价值。每当一笔交易成为可能或交易成本降低时,产生比特币的成本就会得到更多补偿。该成本在许多交易中摊销。贵金属的货币价值基于这一原则。这也适用于收藏品,其越稀有越珍贵,且这种稀有性使其难以伪造。这也适用于在产品中加入具有证实存在的技术性且独特性的人类劳动,如艺术。

[0009] 因此,挖掘比特币的工作确保了区块链的安全,并在许多交易中摊销,在这些交易中,所述工作被获得的效益所抵消。

[0010] 尽管区块链具有其所有优点,但与集中式和基于信任的系统相比,其计算效率并不一定高。这主要是因为,在其最底层,区块链以计算效率与可伸缩性换取了社会的可伸缩性、安全性和不可伪造性。也就是说,区块链用一个高度可管理和容易使用的计算平台来换取一个开放的、冗余的和强大的计算平台。

发明内容

[0011] 在一个实施例中，一个系统包括维护区块链的一个或多个计算设备，所述区块链具有一个或多个节点(例如，交易)，每个节点包括一个区块链地址，一个或多个计算设备能够通过网络彼此通信。在网络上通信的服务器配置为提供与实体相关联的认证证书，其中所述认证证书包括包含至少一个区块链地址的地址字段，以验证区块链地址是否与该实体相关联。

[0012] 可能包含以下一项或多项功能。

[0013] 区块链可以是比特币区块链。

[0014] 区块链地址可以是比特币地址。

[0015] 认证证书可以是X.509证书。

[0016] 地址字段可以是X.509证书的扩展字段。

[0017] 服务器可以与认证服务相关联。

[0018] 一个或多个计算设备可配置为通过从服务器中请求认证证书来验证相应实体的身份。

[0019] 一个或多个计算设备可配置为在验证各个实体的身份之后与相应实体进行金融交易。

[0020] 认证证书可以与加密公钥相关联。

[0021] 与认证证书中包含的区块链地址相对应的区块链节点也可以与加密公钥相关联。

[0022] 在另一实施例中，一种用于安全交易的方法，包括通过一个或多个计算设备形成具有多个节点的区块链，每个节点具有区块链地址，其中多个节点中的第一节点具有与交易相关联的第一区块链地址。从认证服务器中请求认证证书，该认证证书包含一个或多个字段，用于验证与交易相关联的实体的身份，并且具有包含认证地址的地址字段。通过确定认证地址与第一区块链地址的匹配来验证与交易相关联的实体。

[0023] 可能包含以下一项或多项功能。

[0024] 在验证实体与交易相关联后，资金可以转移到第一区块链地址，或从第一区块链地址中转移。

[0025] 区块链可以包括比特币区块链。

[0026] 区块链地址可以是比特币地址。

[0027] 认证证书可以是X.509证书。

[0028] 地址字段可以是X.509证书的扩展字段。

[0029] 服务器可以与认证服务相关联。

[0030] 一个或多个计算设备可配置为通过从服务器中请求认证证书来验证相应实体的身份。

[0031] 一个或多个计算设备可配置为在验证各个实体的身份之后与相应实体进行金融交易。

[0032] 认证证书可以与加密公钥相关联。

[0033] 与认证证书中包含的区块链地址相对应的区块链节点也可以与加密公钥相关联。

附图说明

[0034] 从以下附图的描述可以更充分地理解上述特征。所述附图有助于解释和理解所公开的技术。由于图示和描述每个可能的实施例通常是不切实际的或不可能的，因此所提供的附图描述一个或多个示例性实施例。相应地，所述附图不旨在限制本发明的范围。图中相似的数字表示相似的元素。

[0035] 图1是包括认证服务器的计算系统的框图。

[0036] 图2是区块链的框图。

[0037] 图3是认证证书的框图。

[0038] 图3A是包括QR码的系统图。

[0039] 图4是验证与区块链交易相关联的实体身份的过程的流程图。

[0040] 图5是验证与区块链传输相关联的实体身份的过程的流程图。

[0041] 图6是验证与区块链取款相关联的实体身份的过程的流程图。

[0042] 图7是验证与闪电网络相关联的实体身份的过程的流程图。

[0043] 图8是计算装置的框图。

具体实施方式

[0044] 本文所讨论的方法和系统的示例不限于应用在以下描述中阐述或附图中示出的构件细节和组件的配置。本领域技术人员将理解，所述方法和系统能够在其他实施例中实施并且能够以各种方式被实践或执行。本文提供的特定实施方式的示例仅出于说明性目的，并不旨在限制。同样，本文所使用的措词和术语是出于描述的目的，并且不应被视为限制。对本文中以单数形式提及的系统和方法的示例、实施例、组件、元件或行为的任何引用也可以包含包括复数的实施例，并且本文以复数形式对任何实施例、组件、元件或行为的任何引用也可以包含仅包括单数的实施例。单数或复数形式的引用并不旨在限制当前公开的系统或方法、其组件、行为或元件。本文中使用的“包括”、“包含”、“具有”、“组成”、“涉及”及其变体意在涵盖其后列出的项目及其等同物以及其他项目。对“或”的引用可解释为包括在内，使得使用“或”描述的任何术语可以表示单个、多个和所有所述术语中的任何一个。

[0045] 本领域技术人员将认识到，当描述区块链时，术语“块”通常用于指代区块链中的区块，而术语“节点”通常用于指代闪电网络中的节点。然而，在本发明中，术语“块”和“节点”可互换地用于指代区块链中的区块、闪电网络中的节点或两者兼具。术语“块”和“节点”也可被解释为表示在本申请公开的上下文中合适的任何区块或节点。

[0046] 参见图1，计算系统100包括在网络106上通信的计算设备102和104。计算设备102和106可以是能够执行软件指令的任何类型的计算设备，包括但不限于诸如台式计算机、手提式计算机、移动电话、服务器、物联网(IoT)传感器、嵌入式设备等，网络106可以是允许计算设备彼此通信的任何类型的网络，包括但不限于WAN、LAN、因特网等。

[0047] 系统100还可以包括能够与认证服务相关联的一个或多个服务器108。认证服务可以是发布或提供数字证书的服务，所述数字证书提供地址、身份、交易、签名等的安全认证(例如，与公钥基础设施(PKI)相对应的认证机构(CA))。认证服务还可以使用非对称加密(例如，使用公钥/私钥对的公钥加密)来提供身份验证，以建立数据或交易的来源或实体与之的关联(例如，通过见证或授权数字签名或交易)。

[0048] 系统100还可以包括与实体112相关联的服务器110。实体112可以是能够由服务器108进行身份认证的公司、个人或任何其他法律实体。例如，CA可以验证实体的名称、通信地址、Internet域名和比特币地址。可选地，也例如，CA可以通过要求实体证明与区块链标识符对应的私钥的所有权(例如，通过提供使用与比特币地址相对应的私钥所构造的数字签名)，来建立区块链标识符(例如，比特币地址)的所有权。

[0049] 系统100被示为相对最小的系统，其具有两个计算设备102和104、与认证服务相关联的服务器108以及与通过网络106进行通信的实体112相关联的服务器110。然而，附加设备也可以通过网络106进行通信，并且与系统100交互或者为系统100的一部分。为了便于说明，图中未显示这些设备。

[0050] 此外，参见图2，区块链200可以与系统100相关联。区块链200可以全部或部分地由计算设备102和104以及由服务器110进行存储。未示出的其他设备也可以存储区块链200的全部或部分。在实施例中，区块链200可以是比特币区块链、闪电网络等(注意，尽管闪电网络不一定是区块链，但本申请公开中描述的系统和技术可以在闪电网络上操作或与闪电网络结合操作)。区块链200可以是允许任何实体或个人参与的公共区块链，例如比特币区块链或以太坊区块链(the Ethereum blockchain)。在其他实施例中，区块链200可以是具有封闭的用户组和私人交易的私有区块链，或者可以是由组或联营管理的混合型区块链。

[0051] 不管区块链200的类型如何，各种实体均可以与区块链中的交易相关联。例如，区块链200可以包括将资金从一个实体转移到另一个实体的比特币交易。可选地，交易可以与一个或多个源地址(与授权交易输入的实体相关联)和/或目标地址(与潜在地能够对交易的输出行使权利的实体相关联)相关联。由于金融(和其他)交易的安全性，如果交易的各方可以验证交易其他各方的身份，则可能会是有益的。例如，如果接收者是银行，而转让人认证收件人的地址与适当的银行相关，这对于转让人而言可能是有益的。

[0052] 区块链200可以由诸如设备102和104之类的计算设备来创建、维护和扩展。区块链200可以包括一系列的区块(在本申请中也被称为节点)，如源区块202。术语“区块链”可以指整个区块链200结构或可以指该结构内最长的不间断链。(例如，区块204)。区块链200还可以包括从主区块链分支的节点(例如区块206)。

[0053] 每个区块可包含与该区块相关联并用于接受和发送区块链交易的地址210，以及数据交易的散列树(hash tree)212。在实施例中，区块可以与特定实体相关联。因此，区块的地址210也可以与特定实体相关联。例如，如果资金被转移到地址210，那么这些资金可以被与区块214相关联的实体使用。

[0054] 闪电网络是建立在底层区块链(如比特币)之上的第二层协议。成对的用户签订协议，通过抵押品进行善意协商。这些协议称为通道，可以记录在区块链200中(例如，作为“资金”交易)。

[0055] 每一对都通过使用正在进行的谈判和部分签署但未记录的合同(即“链外”)来更新通道，以调整通道抵押品的分配并推迟区块链上的结算。

[0056] 为了转移资金，发送者更新与另一方的未记录合同，而另一方又更新其与另一方的合同，依此类推，直到该进程到达接收者为止。结果可能是一系列的合同更新。

[0057] 各方必须真诚地进行谈判(包括通过取消过去已撤销或更新的合同)，否则就有可能失去闪电网络中的抵押品。如果谈判破裂且没有争议或违约，可以根据最新合同更新中

的约定分配退还抵押品。

[0058] 通过将记录推迟到区块链，闪电网络可以实现更高的交易量和近乎即时的确认：

[0059] 区块链本身的速度和容量限制并不直接限制闪电交易。自动和近乎即时的谈判和合同更新可能不需要立即记录在区块链中，即，它们可以在链外进行。然而，在某些情况下，区块链限制了解决纠纷和结算的速度和数量。只要纠纷和结算比日常交易少得多，那么闪电网络就可以实现非常高的交易可伸缩性。

[0060] 标准比特币交易通常不被接受为最终或不可撤销的交易(例如，“已确认”)，除非它被包括在区块链中，即，除非比特币交易被包括在一个区块中，并且在该区块之后链接了一些额外的区块。在交易进入区块之前，它还不是区块链的一部分且可能依旧容易出现双重支出。区块链的工作量证明不能保护未经确认的交易。

[0061] 在闪电网络中，尽管对区块链的结算是延迟的，但它是以信任最小化(trust-minimized)的方式延迟的。闪电支付完成后，它可能会立即收到闪电网络交易附带的信托最小化保护，即，如果交易对方违反未记录的合同，她将丧失抵押品。因此，虽然在链外进行和技术上未经证实，但闪电支付实际上是最终的、几乎即时的。

[0062] 在闪电网络中，比特币可能在每个单独的通道中来回振荡。在闪电交易中，单个比特币可能不会在单个交易中从最初的发送方一直移动到最终的接收方。相反，闪电网络可能会形成一个庞大的振荡比特币网络，每个比特币只在一个通道内来回移动。

[0063] 与交流变压器一样，闪电网络中的节点可以维护不同值的通道，与其他“大功率”节点创建大通道，同时与其他用户直接维护任意小的通道。这样，这些节点就可以充当转换器，将非常大的流量转换为非常适合日常消费者交易的可管理的小流量。同样，此类节点可以聚集在相似方向上传播的小流量，以便在更高容量的通道上进行捆绑传输。在端点节点具有有限的网络连接性或计算资源的情况下，此类高容量节点也可能能够处理某些路由和通道监视任务。例如，低容量节点可以潜在地安全地将路由测定(route-determination)外包给受信任的、经过身份验证的高容量节点或连接良好的节点。

[0064] 此外，由于闪电通道必须获得资金支持，节点可能拥有大量可用资金，并可能维护更多(且价值更高)的通道。

[0065] 随着高度连接的集线器出现在闪电网络中，它们仍然会被信任最小化。通道受闪电网络规则所保护，且节点可以单方面关闭通道。

[0066] 尽管闪电网络上的身份基本上是静态的和公开的，但交易可能只有交易对方知道——例如，一些部分信息可供交易中的中间节点使用，且一些概要信息可在公共区块链上使用。闪电网络上的节点标识可以选择与公钥相关联。

[0067] 因此，在闪电网络中，身份和信誉对于交易而言可能很重要。例如，在寻找合同和交易对方时，信誉很重要。信誉使各方能够更有效地评估潜在的交易对方是否会遵守有关可用性、连通性和费用的声明。信誉可以基于客观可观察的网络指标，如正常运行时间、通道数量和容量、以及违规和非相互结算的数量。这样的信息可以使用经过认证证书进行身份验证的可信实体来传播。

[0068] 公共身份允许对收款人和商户进行身份验证。例如，在进行购买时，经过身份验证的身份(例如，使用与实体和公钥相关联的认证证书)允许用户验证是否正在向预期的商家付款，并验证发票和收据。经过验证和认证的身份尤其重要，因为它可以有效地防止中间人

攻击(man-in-the-middle attacks),而在没有预先存在信任的匿名数字环境中,中间人攻击是很难防止的。

[0069] 公钥基础设施(PKI)可以提供一个高效且封闭的信任点,它可以在不损害区块链的信任最小化性质的情况下解决信誉和身份这两个需求。

[0070] 例如,在闪电网络上,节点可以由其公钥和网络标识符(例如,IP地址或其他端点标识符)表示。该公钥可以对应于公开信任的X.509数字证书中的公钥(或另一字段中的相应信息,例如,主体属性或X.509扩展)。例如,再次参考图1,提供认证证书的服务器108可以提供上述认证证书(例如,作为X.509证书)。相反,该数字证书可用于认证由认证机构(CA)或注册机构(RA)验证或确认的节点的身份(例如,通过公司或域名)。例如,使用经过身份验证的闪电节点,用户可以确保实际支付给预期的商户。

[0071] 在一些实施例中,为第二层区块链协议(例如,闪电网络)交易的认证而颁发的证书(例如,X.509证书)可以包括发票字段,其中包含与潜在交易相关的数据(例如,目标、金额、时间、目标或经授权方的签名,或一个或多个参与者的地理位置)。例如,如果商户在商品或服务销售交易中请求客户付款,则X.509证书可以包括发票字段(例如,作为主体属性或在X.509扩展中),该字段包括与潜在交易相关的信息(例如,标准闪电网络发票)。

[0072] 参考图3,服务器108可以颁发能够验证与实体相关联的某些身份信息的认证证书300。可选地,认证证书300可以符合X.509格式并且可以是X.509证书。可选地,认证证书300还可以由第三方授权或验证,例如,可以用认证机构(CA)的私钥(例如,对应于受信任的或以其他方式授权的数字证书的私钥)对该证书的数据的一些部分或全部进行签名。在实施例中,地址210和/或公钥301可以包括、用作或用于导出验证属性302,并且可选地可以包括在认证证书300的一部分签署或验证,例如,经认证机构(CA)签署或验证的(例如,在认证证书300颁发期间由CA的私钥签署的)。认证机构用于签署认证证书300的私钥可以由可信源提供,例如由可以与公共认证服务相关联的服务器108提供。

[0073] 认证证书300可以包括各种字段,例如包括包含、用作或用于导出验证属性302的字段。例如,认证证书300可以包括公钥,从该公钥可以导出经验证的比特币地址或区块链标识符。可选地,证书中的一个或多个字段可以包含一个或多个经验证的区块链地址(例如,比特币地址)。这些地址可以在区块链块214中找到相同的地址210。认证证书300还可以包括标识实体的信息,例如序列号、颁发者名称、有效性、公钥、唯一ID和其他信息,其包括但不限于,作为认证证书300的一部分显示的字段中所包含的信息。可选地,部分或全部此类信息可包括、用作或用于导出一个或多个验证属性(例如,公钥可包括实体的验证属性,其中该实体已验证是否拥有相应的私钥)。因此,认证证书300可以将地址210和/或公钥301与受信任实体相关联并认证。

[0074] 认证证书300中包括的验证属性302不限于区块链地址或公钥。例如,验证属性可以是IP地址、另一类型的网络地址、与区块链200内交易相关联的另一唯一标识符、在区块链200内交易中转移的金额,或可与区块链交易和/或区块链交易中涉及的实体相关联的任何其他数据。在实施例中,所述验证属性可以是地址引用。例如,验证属性302可以通过X.509证书的公钥间接引用地址。因此,认证证书300可以保证其中列出的实体确实是与验证属性302相关联的区块链交易所涉及的实体。

[0075] 尽管在X.509证书中显示为一个单独的字段,但是验证属性302可以存储在X.509

证书中的任何位置。此外，在实施例中，验证属性302可以与X.509证书分开存储，但与之相关联。

[0076] 参考图3A，认证证书300可以用QR码350进行编码。作为示例，例如，QR码可以以DER或PEM形式对证书进行编码。然后，QR码350可由诸如352的计算设备扫描，该计算设备可包括硬件或软件钱包。计算设备可以验证认证证书，以建立交易对方的身份(例如，比特币交易中受让人的身份)。计算设备可以在验证认证证书之后通知用户，例如，通过显示认证证书中包含的身份信息以及证书有效的指示。

[0077] QR码中的认证证书可向钱包提供与QR码相关实体的验证身份，或提供认证证书，或提供一个或多个潜在或现有加密货币或区块链地址，或提供一个或多个潜在或现有加密货币或区块链交易(例如，链上比特币交易引用或包含比特币地址)，例如，通过包括加密货币或区块链地址，或对应于该地址的公钥来实现。

[0078] 可选地，然后该钱包可以基于认证证书来验证信息的真实性。另外，可选地，例如，钱包还可以通过请求服务器108认证QR码中包含的认证证书来验证QR码中的证书。然后，该钱包可以与该地址进行交易，并确信他们正在与被验证的实体进行交易。

[0079] 例如，QR码350可以对认证证书和发票两者进行编码。在某些情况下，发票可能包含在认证证书中。另外，或者备选地，QR码350可以对包含除加密货币地址或标识符之外信息的证书进行编码。例如，QR码可包含包括URL、账户标识符、用户标识符或滚动或周期性改变的标识符的认证证书(例如，AliPayTM、LineTM或WeChatPayTM的付款URL或帐号)。

[0080] 因此，例如，当实体扫描QR码时，实体可以验证证书以及证书或QR码中包含的信息，以确保QR码(以及QR码中的信息)与正确的源相关联。

[0081] 可选地，QR码可以对在线位置(例如，URL)或接口(例如，因特网可访问API)进行编码，其中可以检索认证证书。然后，硬件设备或软件程序(例如，硬件比特币钱包)可以检索认证证书(例如，通过从指定的URL下载证书)并验证证书。例如，用户可以使用移动设备上的比特币钱包扫描QR码编码或以其他方式引用URL，从URL中检索认证证书，并验证检索到的认证证书，包括例如验证身份信息和包含在证书中或从证书导出的比特币地址。

[0082] 可选地，除了可以从中检索证书的位置之外，该QR码还可以包括或编码信息。例如，QR码可以包括目标区块链或加密货币地址，以及可以从中检索认证证书的URL。可选地，证书可用于建立与加密货币或区块链地址相对应的身份，并确保此类加密货币或区块链地址与编码或包含在QR码中的地址相匹配。可选地，检索到的证书可用于检查包括在QR码中、附属于QR码或以其他方式与QR码中包含信息相关的数字签名(例如，检查QR码中包含的数据已通过与证书对应的私钥进行有效签名)。

[0083] 参考图4，流程图描述对区块链交易的一方进行身份验证的一般过程400。过程400可由想要向交易的其他方证明其身份的实体使用，或由想要获得交易其他方的身份保证的实体使用。

[0084] 在步骤402中，一方从服务器108请求证明某个实体(请求方本身或与交易相关联的另一方)不是冒名顶替者。可选地，该请求可以包括关于实体的识别信息，包括但不限于：设备指纹、域验证、生物特征数据、视频验证2FA令牌(2FA token)、质询问题和/或答案、街道地址、电话号码、网络地址、唯一标识符、加密密钥等。认证服务机构也可以通过电话或短信联系来确定识别信息，以验证实体的身份。识别信息也可以通过联系、通过认证服务、通

过电话或短信来验证实体的身份。

[0085] 在步骤404中，请求认证的一方将地址(即地址210)发送到服务器108。该地址可包括区块链标识符，例如，公钥或区块链或加密货币地址(例如，比特币地址)。又例如，区块链内的交易，或实体参与的任何其他类型的区块链活动。

[0086] 在步骤406中，服务器108认证实体的身份。在一些情况下，例如，如果地址是静态的，则服务器108还可以认证所提供的地址是否与实体相关联。这可以通过解密地址、对照数据库检查地址，或者通过数据关联以其他方式将地址链接到实体来实现。例如，服务器108可以验证与地址或与地址对应公钥相对应的私钥的占有权(例如，加密货币地址所在的，或从中可以导出的公钥)。也例如，实体与公钥或地址的关联可以全部或部分地基于以下一个或多个来建立或假设：(1)在请求服务器108时，要求通过与公钥或地址对应的私钥进行签名，(2)要求通过与公钥或地址对应的私钥在其对应的公钥上进行签名，(3)要求在对应于其的公钥的地址上，通过与公钥或地址对应的私钥对地址进行签名对应于其公钥，或(4)要求提出请求的实体参与交互式签名协议，例如，通过提供一个nonce值(nonce value)并要求通过与公钥或地址对应的私钥对该nonce值进行签名。

[0087] 如果实体和地址经过身份认证，则服务器108可以向将实体与所提供地址相关联的请求者颁发和发送认证证书(例如认证证书300)。然后，该证书可以提供给交易的其他各方，以保证涉及交易的实体实际上是认证证书中列出的实体。

[0088] 参考图5，该流程图描述了用于通过区块链交易进行请求和/或接收资金的过程500。在步骤502中，交易的一方通过向另一方(即第二方)请求资金来启动资金转移。在步骤504中，交易的第一方生成一个接收地址(例如，地址210)，所述资金可以转移到该地址。

[0089] 在步骤506中，交易的第一方(或另一方)向服务器108发送请求，请求获得认证证书，该证书验证了第一方的身份。该请求包括关于第一方的识别信息以及在步骤504中生成的接收地址。在步骤510中，服务器108验证第一方的身份(例如，使用上述一种或多种技术)。

[0090] 如果服务器108可以验证第一方的身份，则生成认证证书并将接收地址与该认证证书相关联。然后，认证证书可以发送给资金的转让方，在步骤514中，通过认证证书确认所提供的地址确实是与第一方相关的地址。在步骤516中，可以启动资金转移。

[0091] 参考图6，该流程图描述了用于通过区块链交易进行资金提取的过程600。在步骤602中，提款方发起提款，并且在步骤604中，产生一个资金应该转移到的地址。在步骤606中，提款方(或另一方)向服务器108发送请求以证明提款方的身份。认证请求包括在步骤604中所生成的接收地址。

[0092] 在步骤608中，例如，服务器108通过上述讨论的身份验证方法来验证提款方的身份。如果服务器108可以识别提款方的身份，则服务器108可以在步骤610中生成认证证书。认证证书可以包括在步骤604中所生成的接收地址。因此，认证证书可以提供验证，证明接收地址与正确的提款方相关联。

[0093] 然后，在步骤612中，认证证书可以提供给转让方，用以验证接收地址与正确的提款方相关联。核实后，在步骤614中，转让方可以授权和/或发起提款。

[0094] 参考图7，该流程图描述了用于在闪电网络中建立通道的过程700。在步骤702中，生成具有闪电ID的新的闪电节点。在步骤704中，新的闪电节点的实体可以请求服务器108

生成认证证书。该请求可能包括新的节点ID。

[0095] 在步骤706中，服务器108可以通过使用如上述讨论的技术来验证请求验证的实体的身份。如果验证了身份，则在步骤708中，服务器108可以生成认证证书，该认证证书验证与新的闪电节点相关联的实体的身份，并将新的闪电节点ID与经验证的实体相关联。

[0096] 在步骤710中，认证证书可以提供给其他闪电节点，然后在步骤712中，验证新的闪电节点的标识。在步骤714中，其他闪电节点可以打开与新的闪电节点的通道，并且在步骤716中，通过通道发起与新的闪电节点的交易。

[0097] 参考图8，示例性的计算系统800可以用于执行上述过程和方法的一些、全部或部分。例如，计算设备102和104以及服务器108可以包括计算系统800的变体。例如，如上所述，这些设备可以维护和创建区块链，执行区块链交易，并执行验证身份和地址的方法。

[0098] 计算系统800包括处理器802(可能与处理器110相同或类似)、随机存取存储器(RAM)804和存储设备806，存储设备806可能是硬盘驱动器、CD、DVD、闪存驱动器或任何其他类型的非易失性存储器。软件指令可以存储在RAM804和/或存储设备806中。处理器802可以耦合到存储设备806和/或RAM704中，以便处理器802可以读取软件指令。

[0099] 当处理器802读取软件指令时，软件指令可使处理器802执行如上所述的用于计算磁性目标的位置的操作。尽管未示出，处理器802和/或系统800可包括其它输入和输出，例如用于接收来自传感元件的信号的输入、GPIO、电源输入或诸如USB、SATA、HDMI等其它接口。

[0100] 上述系统和技术可用于验证任何区块链交易中所涉及的实体。例如，一个公共信任的X.509数字证书将允许用户(以及软件和硬件钱包)验证特定的区块链地址实际上是由预期接收人而不是中间人控制的。软件或硬件钱包也可以使用X.509数字证书来验证接收人的身份。

[0101] 上述的系统、设备和方法是为了理解和说明的目的而示出的示例系统、设备和方法。这些系统、设备和方法的变型在本申请公开的范围内。同样，等效的系统、设备和方法也在本申请公开的范围内。附图中所示和本公开中所述的流程图不一定要求任何特定的步骤顺序。而且，可以根据需要添加、移除、重新布置和重新排序各种步骤，以产生相同或相似的结果，并且仍然保持在本申请公开的范围内。

[0102] 在该专利中描述了各种实施例。然而，该专利的范围不应限于所描述的实施例，而应仅由所附权利要求的精神和范围来限定。本专利中引用的所有参考文献全部通过引用合并。

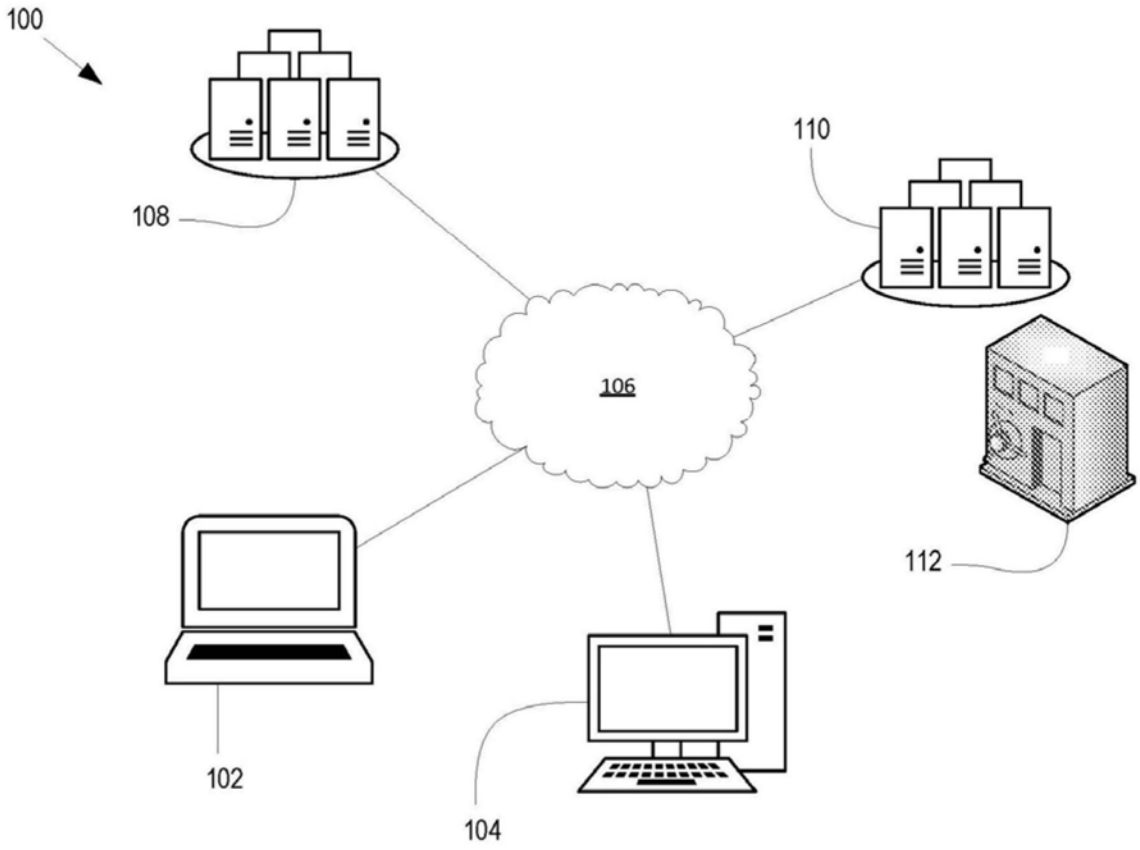


图1

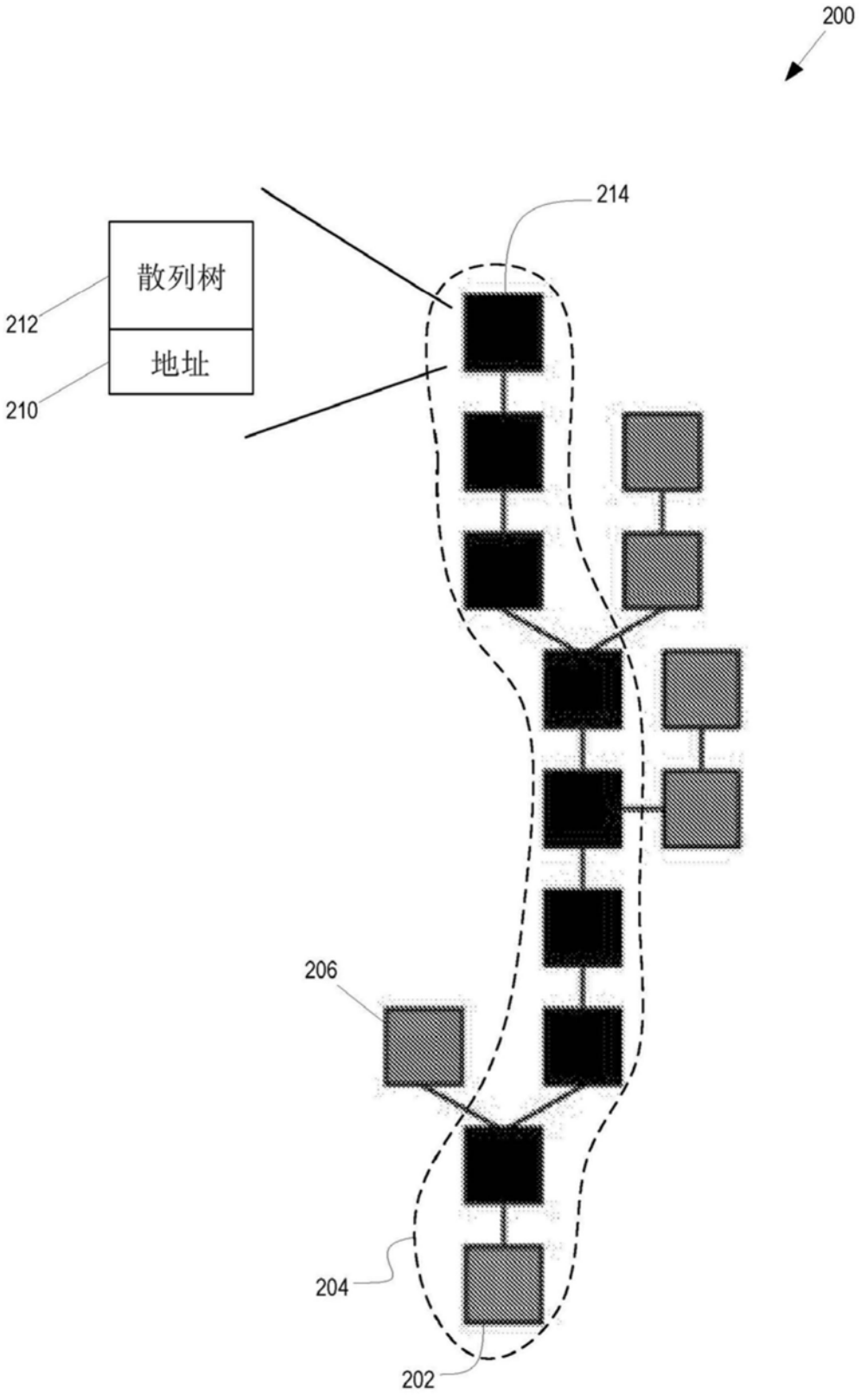


图2

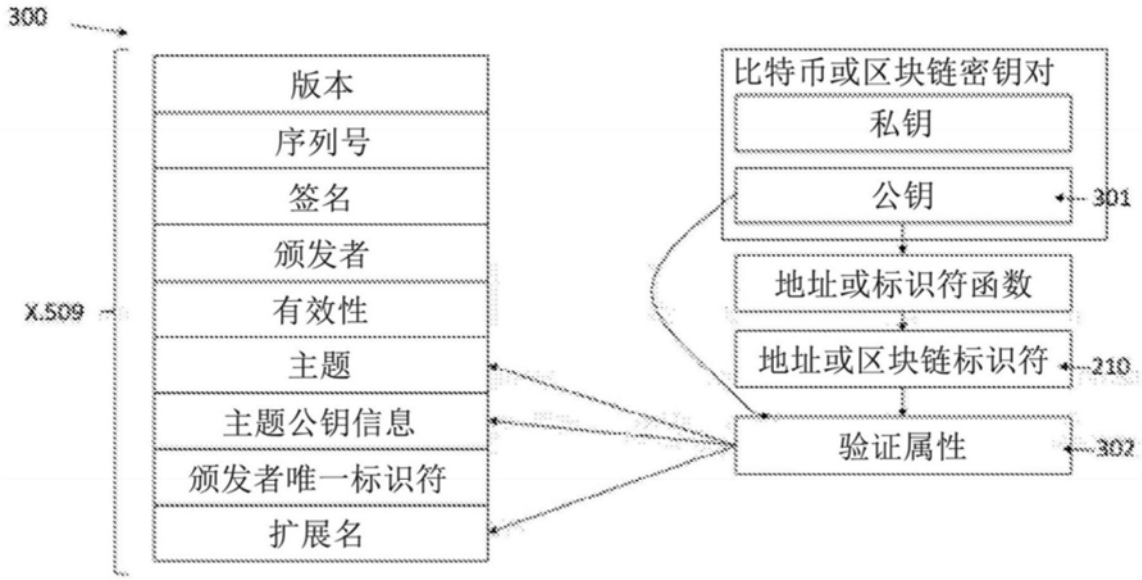

300
X.509
版本
序列号
签名
颁发者
有效性
主题
主题公钥信息
颁发者唯一标识符
扩展名
比特币或区块链密钥对
私钥
公钥
301
地址或标识符函数
地址或区块链标识符
210
验证属性
302

图3

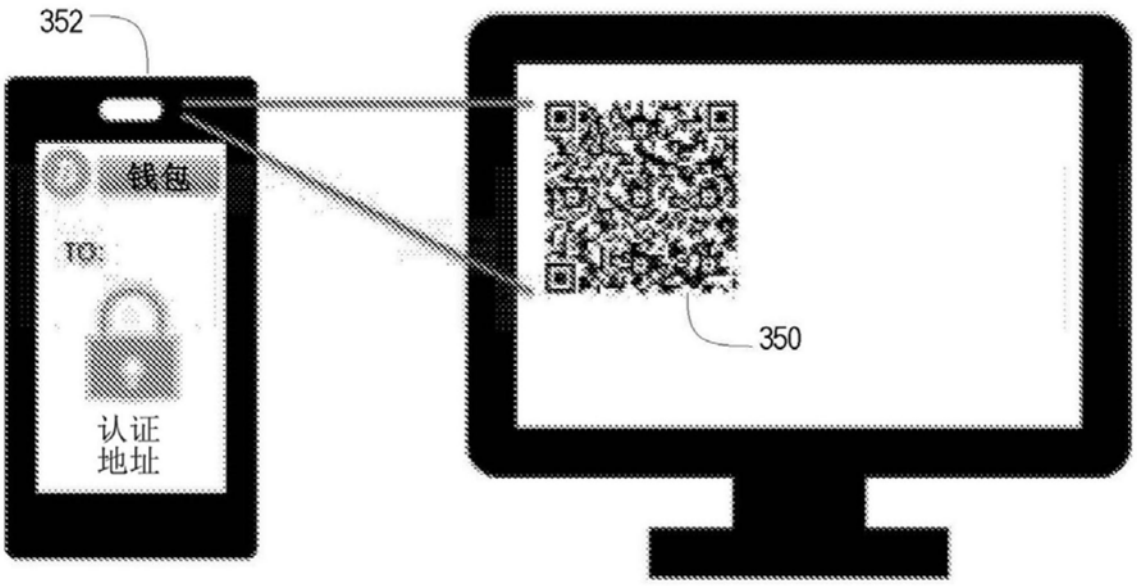

352
钱包
TO:
认证
地址
350

图3A

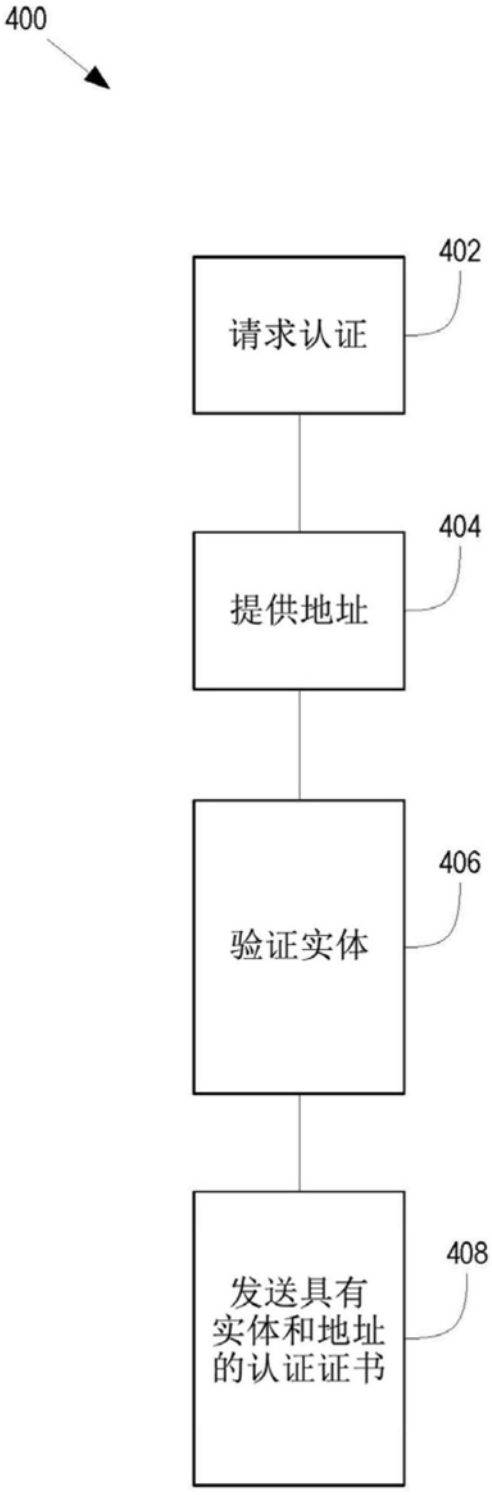


图4

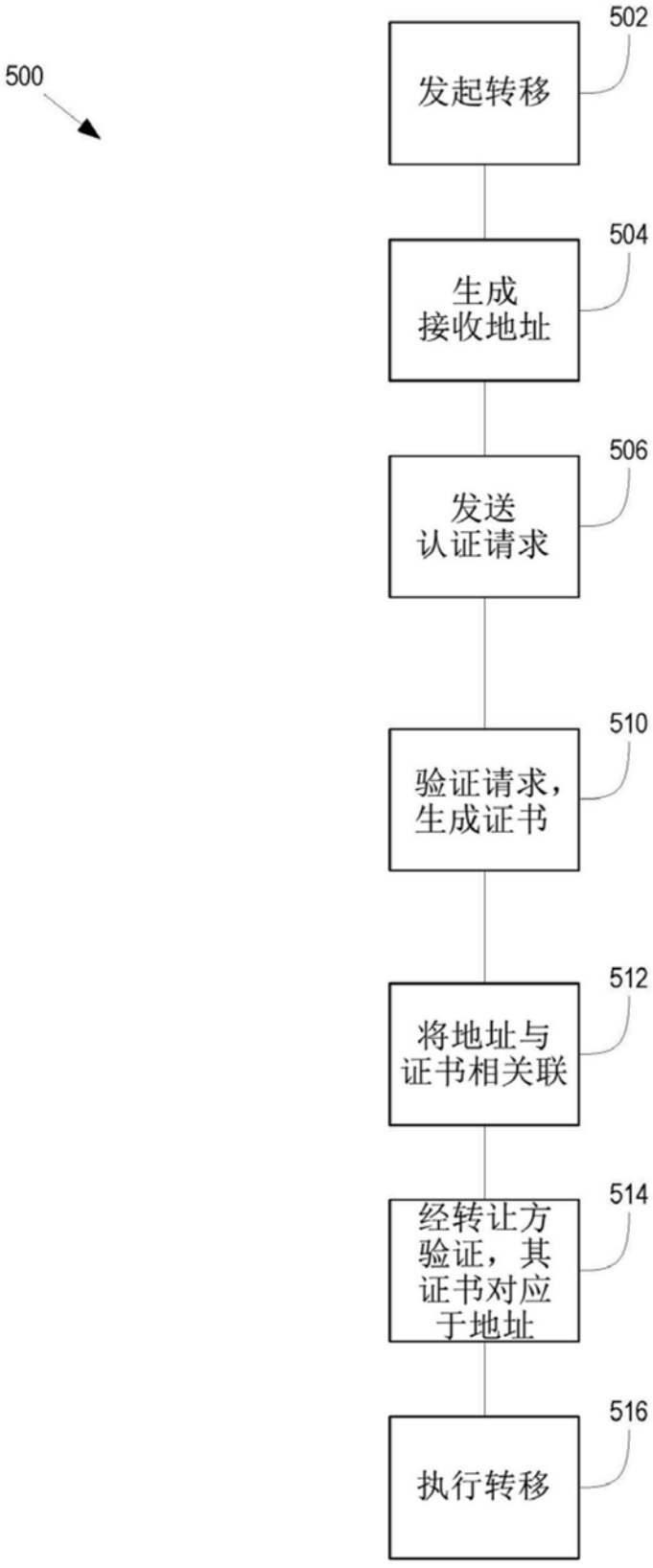

500
502
发起转移
504
生成
接收地址
506
发送
认证请求
510
验证请求，
生成证书
512
将地址与
证书相关联
514
经转让方
验证，其
证书对应
于地址
516
执行转移

图5

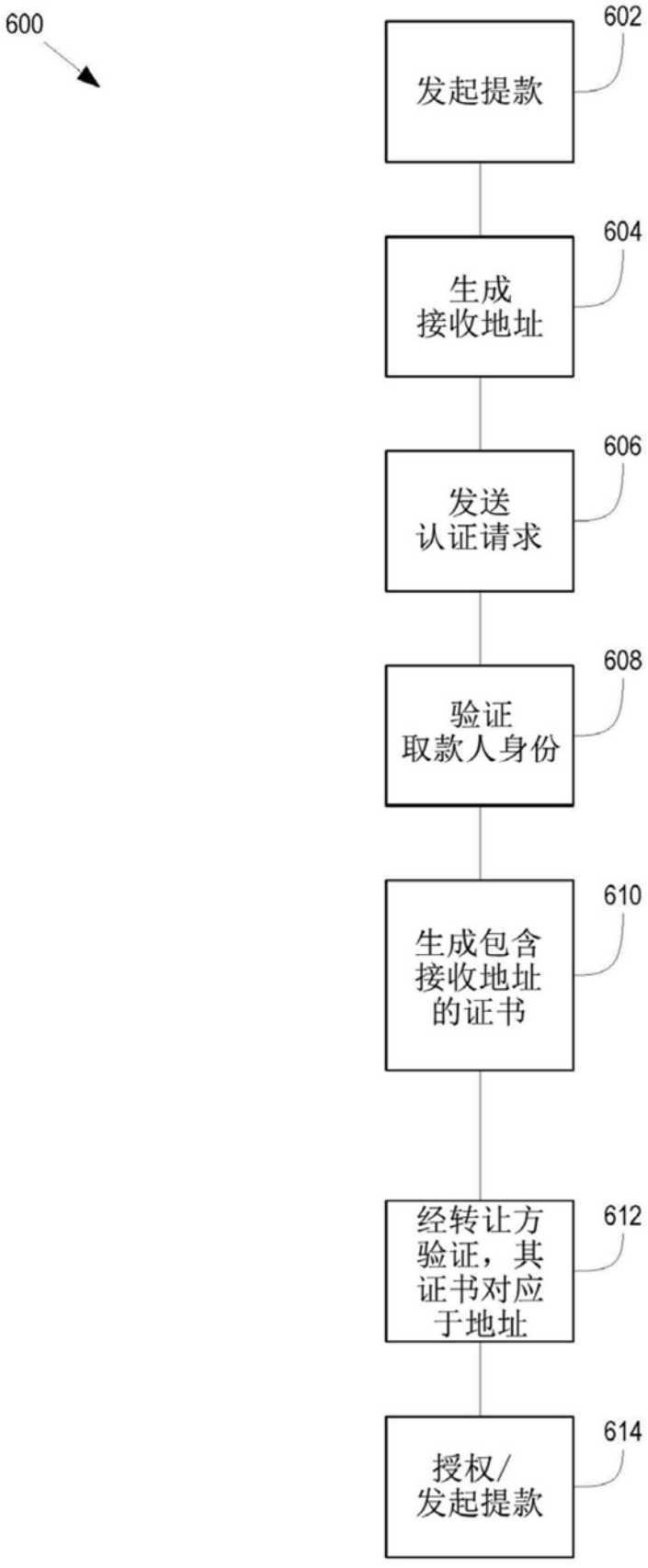

600
602
发起提款
604
生成
接收地址
606
发送
认证请求
608
验证
取款人身份
610
生成包含
接收地址
的证书
612
经转让方
验证，其
证书对应
于地址
614
授权/
发起提款

图6

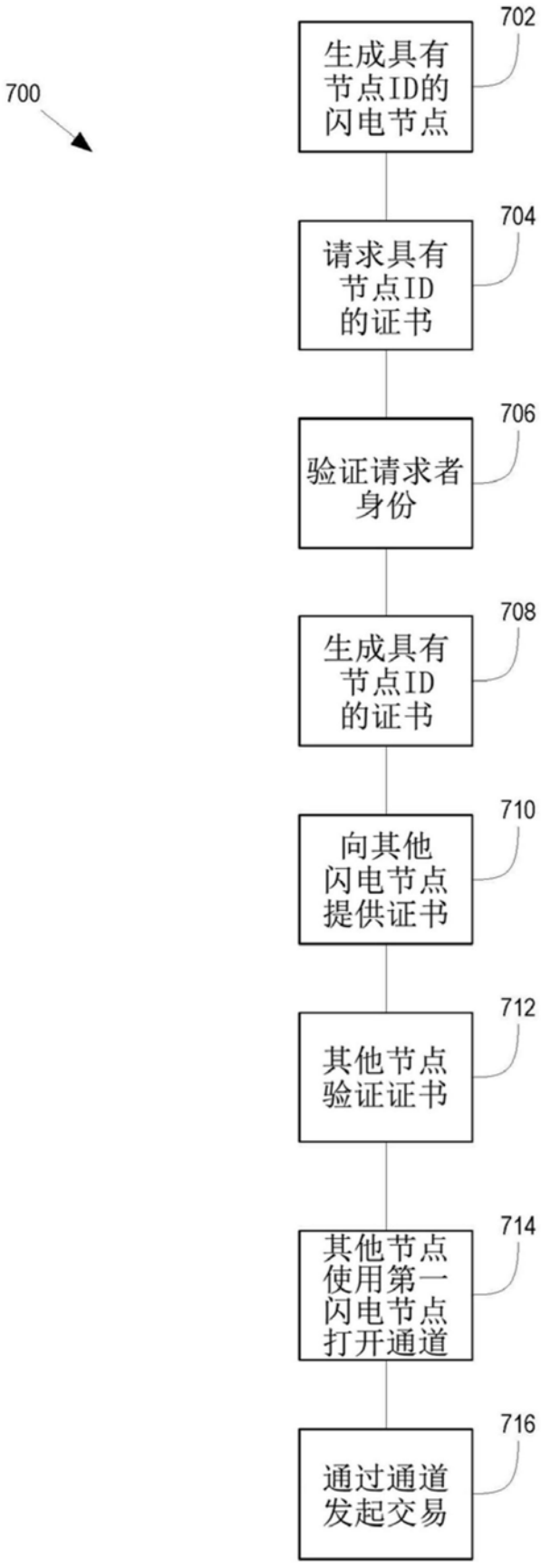

700
生成具有节点ID的闪电节点
702
请求具有节点ID的证书
704
验证请求者身份
706
生成具有节点ID的证书
708
向其他闪电节点提供证书
710
其他节点验证证书
712
其他节点使用第一闪电节点打开通道
714
通过通道发起交易
716

图7

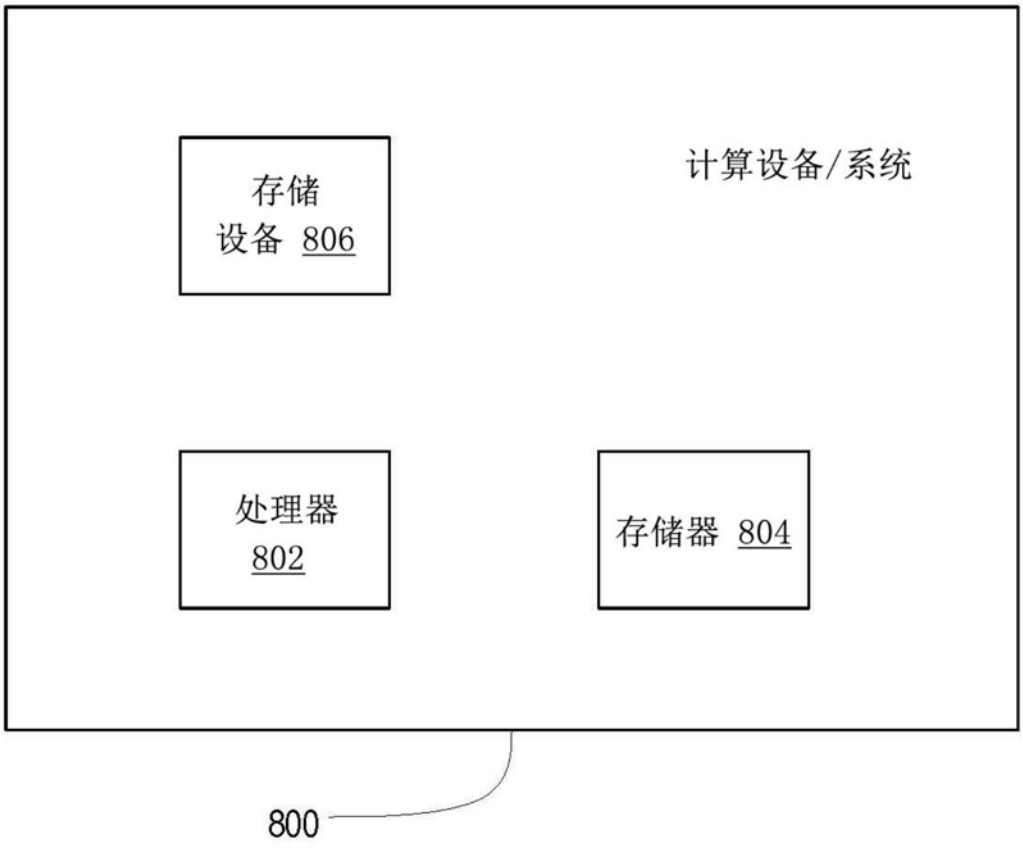


图8