(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 108777684 A
(43)申请公布日 2018.11.09

(21)申请号 201810543425.5

(22)申请日 2018.05.30

(71)申请人 招商银行股份有限公司
地址 518000 广东省深圳市福田区深南大道7088招商银行大厦

(72)发明人 张育明 潘海清 陈鹏

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G06Q 20/38(2012.01)

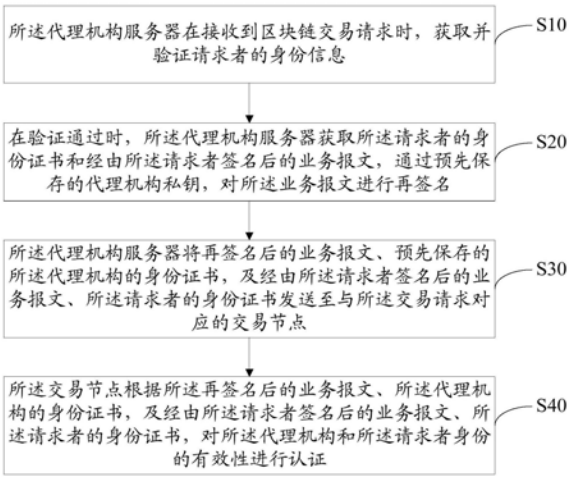
权利要求书2页 说明书9页 附图4页

(54)发明名称

身份认证方法、系统及计算机可读存储介质

(57)摘要

本发明公开了一种身份认证方法，应用于身份认证系统，所述身份认证系统包括代理机构服务器和交易节点，该方法包括：代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息；在验证通过时，获取请求者的身份证书和经由请求者签名后的业务报文，通过预先保存的代理机构私钥，对业务报文进行再签名；将再签名后的业务报文、预先保存的代理机构的身份证书，及经由请求者签名后的业务报文、请求者的身份证书发送至与交易请求对应的交易节点；交易节点对代理机构和请求者身份的有效性进行认证。本发明还公开了一种身份认证系统和一种计算机可读存储介质。本发明能够实现对区块链参与者进行安全有效的身份认证。



CN 108777684 A

1.一种身份认证方法，其特征在于，应用于身份认证系统，所述身份认证系统包括代理机构服务器和交易节点，所述身份认证方法包括如下步骤：

所述代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息；

在验证通过时，所述代理机构服务器获取所述请求者的身份证书和经由所述请求者签名后的业务报文，通过预先保存的代理机构私钥，对所述业务报文进行再签名；

所述代理机构服务器将再签名后的业务报文、预先保存的所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书发送至与所述交易请求对应的交易节点；

所述交易节点根据所述再签名后的业务报文、所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书，对所述代理机构和所述请求者身份的有效性进行认证。

2.如权利要求1所述的身份认证方法，其特征在于，所述代理机构服务器获取并验证请求者的身份信息的步骤包括：

所述代理机构服务器获取所述交易请求中携带的请求者的身份信息；

所述代理机构服务器判断预设的身份信息数据库中是否存在所述请求者的身份信息，若是，则判定所述请求者的身份信息验证通过。

3.如权利要求2所述的身份认证方法，其特征在于，所述请求者的身份信息包括访问口令、设备标识和生物特征中的至少一种。

4.如权利要求1所述的身份认证方法，其特征在于，所述交易节点根据所述再签名后的业务报文、所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书，对所述代理机构和所述请求者身份的有效性进行认证的步骤包括：

所述交易节点判断所述代理机构的身份证书是否有效；

若所述代理机构的身份证书有效，则所述交易节点根据所述代理机构的身份证书和所述再签名后的业务报文，对所述代理机构身份的有效性进行认证；

当所述代理机构的身份被认证为有效时，所述交易节点判断所述请求者的身份证书是否有效；

若所述请求者的身份证书有效，则所述交易节点根据所述请求者的身份证书和经由所述请求者签名后的业务报文，对所述请求者身份的有效性进行认证。

5.如权利要求4所述的身份认证方法，其特征在于，所述交易节点判断所述代理机构的身份证书是否有效的步骤包括：

所述交易节点判断所述代理机构的身份证书是否在预设的有效期内；

若所述代理机构的身份证书在预设的有效期内，则所述交易节点获取预置的信任根证书，并判断所述代理机构的身份证书是否由所述信任根证书对应的证书颁发机构所颁发；

若所述代理机构的身份证书是由所述信任根证书对应的证书颁发机构所颁发，则所述交易节点从证书颁发机构站点下载证书吊销列表，并判断所述代理机构的身份证书是否存在于所述证书吊销列表中；

若所述代理机构的身份证书不存在于所述证书吊销列表中，则判定所述代理机构的身份证书是有效的。

6.如权利要求4所述的身份认证方法，其特征在于，所述交易节点根据所述代理机构的

身份证书和所述再签名后的业务报文，对所述代理机构身份的有效性进行认证的步骤包括：

所述交易节点从所述代理机构的身份证书中读取所述代理机构的公钥；

所述交易节点根据所述代理机构的公钥对所述再签名后的业务报文进行验签，若验证通过，则判定所述代理机构的身份是有效的。

7.如权利要求1至6中任一项所述的身份认证方法，其特征在于，所述身份认证系统还包括证书颁发机构服务器，所述代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息的步骤之前，还包括：

所述代理机构服务器向所述证书颁发机构服务器发起身份证书申请请求；

所述证书颁发机构服务器获取所述身份证书申请请求中携带的申请者的身份信息和申请者的公钥，并对所述申请者的身份信息作匿名化处理；

所述证书颁发机构服务器将匿名化处理后的所述申请者的身份信息和所述申请者的公钥进行绑定，以生成所述申请者的身份证书，并将所述申请者的身份证书下发给所述代理机构服务器。

8.如权利要求7所述的身份认证方法，其特征在于，所述申请者包括所述代理机构和触发所述区块链交易请求的请求者。

9.一种身份认证系统，其特征在于，所述身份认证系统包括：代理机构服务器、交易节点和身份认证程序，所述身份认证程序被所述代理机构服务器和所述交易节点执行时实现如权利要求1至6中任一项所述的身份认证方法的步骤。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有身份认证程序，所述身份认证程序被处理器执行时实现如权利要求1至6中任一项所述的身份认证方法的步骤。

身份认证方法、系统及计算机可读存储介质

技术领域

[0001] 本发明涉及互联网技术领域，尤其涉及身份认证方法、系统及计算机可读存储介质。

背景技术

[0002] 近年来，随着互联网金融的不断发展，区块链技术被逐渐引入银行等金融机构的业务交易中。所谓区块链技术，是一种将传统加密技术和互联网分布式技术相结合形成的一种全新的网络应用技术，在基于区块链技术的互联网交易过程中，区块链中成员身份的认证是保障区块链交易真实性和安全性的重要步骤之一。

[0003] 目前金融区块链具有参与者较多，身份复杂，且并不完全可信的特点，因而如何对区块链参与者进行安全有效的身份认证，从而保障区块链交易的真实性和安全性是目前亟待解决的问题。

发明内容

[0004] 本发明的主要目的在于提出一种身份认证方法、系统及计算机可读存储介质，旨在实现对区块链参与者进行安全有效的身份认证。

[0005] 为实现上述目的，本发明提供一种身份认证方法，应用于身份认证系统，所述身份认证系统包括代理机构服务器和交易节点，所述身份认证方法包括如下步骤：

[0006] 所述代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息；

[0007] 在验证通过时，所述代理机构服务器获取所述请求者的身份证书和经由所述请求者签名后的业务报文，通过预先保存的代理机构私钥，对所述业务报文进行再签名；

[0008] 所述代理机构服务器将再签名后的业务报文、预先保存的所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书发送至与所述交易请求对应的交易节点；

[0009] 所述交易节点根据所述再签名后的业务报文、所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书，对所述代理机构和所述请求者身份的有效性进行认证。

[0010] 优选地，所述代理机构服务器获取并验证请求者的身份信息的步骤包括：

[0011] 所述代理机构服务器获取所述交易请求中携带的请求者的身份信息；

[0012] 所述代理机构服务器判断预设的身份信息数据库中是否存在所述请求者的身份信息，若是，则判定所述请求者的身份信息验证通过。

[0013] 优选地，所述请求者的身份信息包括访问口令、设备标识和生物特征中的至少一种。

[0014] 优选地，所述交易节点根据所述再签名后的业务报文、所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书，对所述代理机构和所述请

求者身份的有效性进行认证的步骤包括：

[0015] 所述交易节点判断所述代理机构的身份证书是否有效；

[0016] 若所述代理机构的身份证书有效，则所述交易节点根据所述代理机构的身份证书和所述再签名后的业务报文，对所述代理机构身份的有效性进行认证；

[0017] 当所述代理机构的身份被认证为有效时，所述交易节点判断所述请求者的身份证书是否有效；

[0018] 若所述请求者的身份证书有效，则所述交易节点根据所述请求者的身份证书和经由所述请求者签名后的业务报文，对所述请求者身份的有效性进行认证。

[0019] 优选地，所述交易节点判断所述代理机构的身份证书是否有效的步骤包括：

[0020] 所述交易节点判断所述代理机构的身份证书是否在预设的有效期内；

[0021] 若所述代理机构的身份证书在预设的有效期内，则所述交易节点获取预置的信任根证书，并判断所述代理机构的身份证书是否由所述信任根证书对应的证书颁发机构所颁发；

[0022] 若所述代理机构的身份证书是由所述信任根证书对应的证书颁发机构所颁发，则所述交易节点从证书颁发机构站点下载证书吊销列表，并判断所述代理机构的身份证书是否存在于所述证书吊销列表中；

[0023] 若所述代理机构的身份证书不存在于所述证书吊销列表中，则判定所述代理机构的身份证书是有效的。

[0024] 优选地，所述交易节点根据所述代理机构的身份证书和所述再签名后的业务报文，对所述代理机构身份的有效性进行认证的步骤包括：

[0025] 所述交易节点从所述代理机构的身份证书中读取所述代理机构的公钥；

[0026] 所述交易节点根据所述代理机构的公钥对所述再签名后的业务报文进行验签，若验证通过，则判定所述代理机构的身份是有效的。

[0027] 优选地，所述身份认证系统还包括证书颁发机构服务器，所述代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息的步骤之前，还包括：

[0028] 所述代理机构服务器向所述证书颁发机构服务器发起身份证书申请请求；

[0029] 所述证书颁发机构服务器获取所述身份证书申请请求中携带的申请者的身份信息和申请者的公钥，并对所述申请者的身份信息作匿名化处理；

[0030] 所述证书颁发机构服务器将匿名化处理后的所述申请者的身份信息和所述申请者的公钥进行绑定，以生成所述申请者的身份证书，并将所述申请者的身份证书下发给所述代理机构服务器。

[0031] 优选地，所述申请者包括所述代理机构和触发所述区块链交易请求的请求者。

[0032] 此外，为实现上述目的，本发明还提供一种身份认证系统，所述身份认证系统包括：代理机构服务器、交易节点和身份认证程序，所述身份认证程序被所述代理机构服务器和所述交易节点执行时实现如上所述的身份认证方法的步骤。

[0033] 此外，为实现上述目的，本发明还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有身份认证程序，所述身份认证程序被处理器执行时实现如上所述的身份认证方法的步骤。

[0034] 本发明提出的身份认证方法，通过采用代理机构的外部认证和交易节点内部认证

相结合的双层认证方式，即，代理机构服务器在接收到区块链交易请求时，首先对请求者的身份信息进行外部验证，验证通过后，再在区块链交易节点上进行代理机构和请求者身份的内部认证。这种双层认证方式保证了参与区块链交易的代理机构和区块链交易请求者的身份是真实有效的，有利于保障区块链交易的真实性和安全性。

附图说明

[0035] 图1是本发明实施例方案涉及的硬件运行环境的终端结构示意图；

[0036] 图2为本发明身份认证方法第一实施例的流程示意图；

[0037] 图3为本发明身份认证方法第二实施例中步骤S40的细化步骤示意图；

[0038] 图4为图3中步骤S41的细化步骤示意图；

[0039] 图5为本发明身份认证方法第三实施例的流程示意图。

[0040] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0041] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0042] 本发明实施例的主要解决方案是：代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息；在验证通过时，代理机构服务器获取请求者的身份证书和经由请求者签名后的业务报文，通过预先保存的代理机构私钥，对业务报文进行再签名；代理机构服务器将再签名后的业务报文、预先保存的代理机构的身份证书，及经由请求者签名后的业务报文、请求者的身份证书发送至与交易请求对应的交易节点；交易节点根据再签名后的业务报文、代理机构的身份证书，及经由请求者签名后的业务报文、请求者的身份证书，对代理机构和请求者身份的有效性进行认证。

[0043] 目前金融区块链具有参与者较多，身份复杂，且并不完全可信的特点，因而如何对区块链参与者进行安全有效的身份认证，从而保障区块链交易的真实性和安全性是目前亟待解决的问题。

[0044] 本发明提出的身份认证方法，通过采用代理机构的外部认证和交易节点内部认证相结合的双层认证方式，即，代理机构服务器在接收到区块链交易请求时，首先对请求者的身份信息进行外部验证，验证通过后，再在区块链交易节点上进行代理机构和请求者身份的内部认证。这种双层认证方式保证了参与区块链交易的代理机构和区块链交易请求者的身份是真实有效的，有利于保障区块链交易的真实性和安全性。

[0045] 如图1所示，图1是本发明实施例方案涉及的硬件运行环境的终端结构示意图。

[0046] 本发明实施例终端为代理机构服务器和交易节点，该交易节点可以是PC，也可以是智能手机、平板电脑、便携计算机等具有显示功能的可移动式终端设备。

[0047] 如图1所示，该终端可以包括：处理器1001，例如CPU，网络接口1004，用户接口1003，存储器1005，通信总线1002。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard)，可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器，也可以是稳定的存储器(non-volatile memory)，例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器

1001的存储装置。

[0048] 本领域技术人员可以理解，图1中示出的终端结构并不构成对终端的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0049] 如图1所示，作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及身份认证程序。

[0050] 在图1所示的终端中，网络接口1004主要用于连接后台服务器，与后台服务器进行数据通信；用户接口1003主要用于连接客户端(用户端)，与客户端进行数据通信；而处理器1001可以用于调用存储器1005中存储的身份认证程序，并执行以下操作：

[0051] 所述代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息；

[0052] 在验证通过时，所述代理机构服务器获取所述请求者的身份证书和经由所述请求者签名后的业务报文，通过预先保存的代理机构私钥，对所述业务报文进行再签名；

[0053] 所述代理机构服务器将再签名后的业务报文、预先保存的所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书发送至与所述交易请求对应的交易节点；

[0054] 所述交易节点根据所述再签名后的业务报文、所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书，对所述代理机构和所述请求者身份的有效性进行认证。

[0055] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0056] 所述代理机构服务器获取所述交易请求中携带的请求者的身份信息；

[0057] 所述代理机构服务器判断预设的身份信息数据库中是否存在所述请求者的身份信息，若是，则判定所述请求者的身份信息验证通过。

[0058] 进一步地，所述请求者的身份信息包括访问口令、设备标识和生物特征中的至少一种。

[0059] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0060] 所述交易节点判断所述代理机构的身份证书是否有效；

[0061] 若所述代理机构的身份证书有效，则所述交易节点根据所述代理机构的身份证书和所述再签名后的业务报文，对所述代理机构身份的有效性进行认证；

[0062] 当所述代理机构的身份被认证为有效时，所述交易节点判断所述请求者的身份证书是否有效；

[0063] 若所述请求者的身份证书有效，则所述交易节点根据所述请求者的身份证书和经由所述请求者签名后的业务报文，对所述请求者身份的有效性进行认证。

[0064] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0065] 所述交易节点判断所述代理机构的身份证书是否在预设的有效期内；

[0066] 若所述代理机构的身份证书在预设的有效期内，则所述交易节点获取预置的信任根证书，并判断所述代理机构的身份证书是否由所述信任根证书对应的证书颁发机构所颁

发；

[0067] 若所述代理机构的身份证书是由所述信任根证书对应的证书颁发机构所颁发，则所述交易节点从证书颁发机构站点下载证书吊销列表，并判断所述代理机构的身份证书是否存在于所述证书吊销列表中；

[0068] 若所述代理机构的身份证书不存在于所述证书吊销列表中，则判定所述代理机构的身份证书是有效的。

[0069] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0070] 所述交易节点从所述代理机构的身份证书中读取所述代理机构的公钥；

[0071] 所述交易节点根据所述代理机构的公钥对所述再签名后的业务报文进行验签，若验证通过，则判定所述代理机构的身份是有效的。

[0072] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0073] 所述代理机构服务器向所述证书颁发机构服务器发起身份证书申请请求；

[0074] 所述证书颁发机构服务器获取所述身份证书申请请求中携带的申请者的身份信息和申请者的公钥，并对所述申请者的身份信息作匿名化处理；

[0075] 所述证书颁发机构服务器将匿名化处理后的所述申请者的身份信息和所述申请者的公钥进行绑定，以生成所述申请者的身份证书，并将所述申请者的身份证书下发给所述代理机构服务器。

[0076] 进一步地，所述申请者包括所述代理机构和触发所述区块链交易请求的请求者。

[0077] 基于上述硬件结构，提出本发明身份认证方法各个实施例。

[0078] 参照图2，图2为本发明身份认证方法第一实施例的流程示意图。本实施例身份认证方法应用于身份认证系统，该身份认证系统包括代理机构服务器和交易节点，实际应用中，代理机构可以为商业银行或其他金融服务提供商，交易节点为区块链参与方进行交易时所涉及的区块链节点。所述身份认证方法包括：

[0079] 步骤S10，所述代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息；

[0080] 该步骤中，代理机构服务器首先接收区块链交易请求，正常情况下，该区块链交易请求由区块链参与者触发；然后，代理机构服务器对接收到的区块链交易请求进行解析，以获取到其中携带的请求者的身份信息，当然代理机构服务器也可以在接收到区块链交易请求后，提示请求者输入自己的身份信息；之后，代理机构服务器对获取到的请求者的身份信息进行验证。

[0081] 在一实施方式中，所述请求者的身份信息包括访问口令、设备标识和生物特征中的至少一种，其中，访问口令包括但不限于用户名、密码、动态口令、短信验证码等，设备标识包括但不限于设备的MAC(Media Access Control，媒体访问控制)地址、唯一标识号码等，生物特征包括但不限于指纹、声纹、虹膜等。具体地，可以基于访问口令、设备标识和生物特征中的一种身份信息进行验证，如仅采用用户名+密码的验证方式，也可以结合多种身份信息进行验证，如采用用户名+密码+指纹的验证方式，具体实施时可灵活设置。

[0082] 上述步骤S10可以进一步包括：所述代理机构服务器获取所述交易请求中携带的

请求者的身份信息;所述代理机构服务器判断预设的身份信息数据库中是否存在所述请求者的身份信息,若是,则判定所述请求者的身份信息验证通过。

[0083] 在进行请求者身份验证时,代理机构服务器可以获取交易请求中携带的请求者的身份信息,然后判断预设的身份信息数据库中是否存在请求者的身份信息,其中身份信息数据库记录了所有已在代理机构注册的区块链参与者的身份信息;若身份信息数据库中存在请求者的身份信息,说明请求者已在代理机构注册,此时代理机构服务器即可判定请求者的身份信息验证通过。

[0084] 步骤S20,在验证通过时,所述代理机构服务器获取所述请求者的身份证书和经由所述请求者签名后的业务报文,通过预先保存的代理机构私钥,对所述业务报文进行再签名;

[0085] 在请求者的身份信息验证通过后,代理机构服务器进一步对交易请求进行解析,以获取到其中携带的请求者的身份证书和经由请求者签名后的业务报文。其中,请求者的身份证书是由证书颁发机构(CA,Certificate Authority)所颁发,CA是负责发放和管理数字证书的权威机构。

[0086] 在区块链交易中,请求者具备自己的非对称密钥,即公钥和私钥,请求者通过自己的私钥对业务报文进行签名后,将签名后的业务报文发送给代理机构服务器;代理机构服务器也具备自己的非对称密钥,当代理机构服务器接收到经由请求者签名后的业务报文后,通过预先保存的自身私钥对该业务报文进行再签名,经再签名后发送的业务报文可以看做是请求者和代理机构无法抵赖的行为。

[0087] 步骤S30,所述代理机构服务器将再签名后的业务报文、预先保存的所述代理机构的身份证书,及经由所述请求者签名后的业务报文、所述请求者的身份证书发送至与所述交易请求对应的交易节点;

[0088] 该步骤中,代理机构服务器将再签名后的业务报文、预先保存的所述代理机构的身份证书,及经由所述请求者签名后的业务报文、所述请求者的身份证书一并发送至与上述交易请求对应的交易节点。其中,与交易请求对应的交易包括但不限于同业签约、转账、汇款、清算及快捷支付等;代理机构的身份证书同样由证书颁发机构CA颁发。

[0089] 步骤S40,所述交易节点根据所述再签名后的业务报文、所述代理机构的身份证书,及经由所述请求者签名后的业务报文、所述请求者的身份证书,对所述代理机构和所述请求者身份的有效性进行认证。

[0090] 该步骤中,交易节点根据接收到的上述再签名后的业务报文、所述代理机构的身份证书,及经由所述请求者签名后的业务报文、所述请求者的身份证书,对所述代理机构和所述请求者身份的有效性进行认证。

[0091] 在对代理机构和所述请求者身份的有效性进行认证时,可以采用基于PKI的身份认证技术,首先验证代理机构的身份证书和再签名后的业务报文的有效性,再验证请求者的身份证书和经由所述请求者签名后的业务报文的有效性,当两者均验证通过时,说明代理机构为真实的代理机构,且请求者为真实的区块链参与者。由于在网络数据传输中,攻击者可能伪造或截取请求者及代理机构发送的信息,从而进行非法交易,因此,对代理机构和请求者进行双重身份认证,能够保证参与交易的代理机构和请求者是合法的,从而保证了区块链交易的安全性。

[0092] 在代理机构和请求者身份均被认证为有效时，交易节点即执行与所述区块链交易请求对应的交易操作，在此过程中，代理机构服务器还可以记录交易节点基于数字资产钱包进行相关操作的详细日志信息，以为后期追踪盗刷犯罪、反洗钱等非法活动提供辅助证据支撑。

[0093] 本实施例提出的身份认证方法，通过采用代理机构的外部认证和交易节点内部认证相结合的双层认证方式，即，代理机构服务器在接收到区块链交易请求时，首先对请求者的身份信息进行外部验证，验证通过后，再在区块链交易节点上进行代理机构和请求者身份的内部认证。这种双层认证方式保证了参与区块链交易的代理机构和区块链交易请求者的身份是真实有效的，有利于保障区块链交易的真实性和安全性。

[0094] 进一步地，基于本发明身份认证方法第一实施例，提出本发明身份认证方法第二实施例。

[0095] 参照图3，图3为本发明身份认证方法第二实施例中步骤S40的细化步骤示意图。基于上述图2所示的实施例，步骤S40可以包括：

[0096] 步骤S41，所述交易节点判断所述代理机构的身份证书是否有效；

[0097] 若所述代理机构的身份证书有效，则执行步骤S42，所述交易节点根据所述代理机构的身份证书和所述再签名后的业务报文，对所述代理机构身份的有效性进行认证；

[0098] 当所述代理机构的身份被认证为有效时，执行步骤S43，所述交易节点判断所述请求者的身份证书是否有效；

[0099] 若所述请求者的身份证书有效，则执行步骤S44，所述交易节点根据所述请求者的身份证书和经由所述请求者签名后的业务报文，对所述请求者身份的有效性进行认证。

[0100] 在本实施例中，交易节点在接收到再签名后的业务报文、代理机构的身份证书，及经由所述请求者签名后的业务报文、请求者的身份证书后，需要依次对代理机构和请求者的身份的有效性进行认证。

[0101] 首先，交易节点判断代理机构的身份证书是否有效。

[0102] 在一判断方式中，参照图4，图4为图3中步骤S41的细化步骤示意图，上述步骤S41可以进一步包括：

[0103] 步骤S411，所述交易节点判断所述代理机构的身份证书是否在预设的有效期内；

[0104] 若所述代理机构的身份证书在预设的有效期内，则执行步骤S412，所述交易节点获取预置的信任根证书，并判断所述代理机构的身份证书是否由所述信任根证书对应的证书颁发机构所颁发；

[0105] 若所述代理机构的身份证书是由所述信任根证书对应的证书颁发机构所颁发，则执行步骤S413，所述交易节点从证书颁发机构站点下载证书吊销列表，并判断所述代理机构的身份证书是否存在于所述证书吊销列表中；

[0106] 若所述代理机构的身份证书不存在于所述证书吊销列表中，则执行步骤S414，判定所述代理机构的身份证书是有效的。

[0107] 具体地，交易节点可以首先从代理机构的身份证书中读取该证书的有效期，若当前时间在该有效期内，则说明该证书未过期，此时交易节点通过自身浏览器获取预置在浏览器中的信任根证书，并判断代理机构的身份证书是否由所述信任根证书对应的证书颁发机构所颁发，其中，证书颁发机构可以是信任根，也可以是信任根下的二级证书颁发机构，

若判断代理机构的身份证书是由所述信任根证书对应的证书颁发机构所颁发，则交易节点进一步从对应的证书颁发机构站点下载证书吊销列表(CRL，Certificate Revocation List)，并判断代理机构的身份证书是否存在于该证书吊销列表中，若不存在，则说明代理机构的身份证书未被吊销，此时即判定代理机构的身份证书是有效的。通过这种判断方式，实现了对代理机构的身份证书的有效性的准确判断。

[0108] 当然，在更多的判断方式中，也可以选择证书的有效期、证书颁发机构的合法性以及证书是否存在于证书吊销列表中的一种或两种进行判断，具体实施时可灵活设置。

[0109] 当判断代理机构的身份证书有效时，交易节点进一步根据代理机构的身份证书和再签名后的业务报文，对代理机构身份的有效性进行认证，具体认证方式为：交易节点从代理机构的身份证书中读取代理机构的公钥，并通过该公钥对再签名后的业务报文进行验签，若验证通过，说明该再签名后的业务报文是由该代理机构所发送，此时判定代理机构的身份是有效的，反之判定代理机构的身份是无效的，当判定代理机构的身份为无效时，终止本次区块链交易并向代理机构服务器返回身份无效信息。

[0110] 当代理机构的身份被认证为有效时，交易节点进一步判断请求者的身份证书是否有效，若请求者的身份证书有效，则再根据请求者的身份证书和经由所述请求者签名后的业务报文，对请求者身份的有效性进行认证。其中，判断请求者的身份证书是否有效以及对请求者身份的有效性进行认证的具体方式可参照上述对代理机构的认证方式，此处不作赘述。

[0111] 进一步地，参照图5，图5为本发明身份认证方法第三实施例的流程示意图。基于上述的实施例，所述身份认证系统还包括证书颁发机构服务器，在步骤S10之前，还可以包括：

[0112] 步骤S50，所述代理机构服务器向所述证书颁发机构服务器发起身份证书申请请求；

[0113] 步骤S60，所述证书颁发机构服务器获取所述身份证书申请请求中携带的申请者的身份信息和申请者的公钥，并对所述申请者的身份信息作匿名化处理；

[0114] 步骤S70，所述证书颁发机构服务器将匿名化处理后的所述申请者的身份信息和所述申请者的公钥进行绑定，以生成所述申请者的身份证书，并将所述申请者的身份证书下发给所述代理机构服务器。

[0115] 进一步地，申请者包括代理机构和触发所述区块链交易请求的请求者。

[0116] 在本实施例中，在进行区块链交易之前，交易发起者和代理机构都需要向证书颁发机构申请身份证书，以为后续身份认证提供前提准备。当代理机构申请自身的身份证书时，直接向证书颁发机构服务器发起身份证书申请请求，当交易发起者申请自身的身份证书时，可以委托代理机构向证书颁发机构申请身份证书，此时代理机构需要对申请者的真实身份信息进行验证，验证通过后，再向证书颁发机构服务器发起身份证书申请请求，其中，身份证书申请请求中携带申请者的身份信息和申请者的公钥。

[0117] 当证书颁发机构服务器接收到代理机构服务器发送的身份证书申请请求时，获取该身份证书申请请求中携带的申请者的身份信息和申请者的公钥，并对申请者的身份信息作匿名化处理，该匿名化处理表现为一个真实身份到身份标识的映射，如ID→ID'，匿名化映射关系只有证书颁发机构自己知道，从而达到“前台自愿，后台实名”的目的；然后，证书颁发机构服务器将匿名化处理后的申请者的身份信息和申请者的公钥进行绑定，以生成申

请者的身份证书，并将申请者的身份证书下发给代理机构服务器，由此完成身份证书的颁发。

[0118] 本发明还提供一种身份认证系统。

[0119] 本发明身份认证系统包括：代理机构服务器、交易节点和身份认证程序，所述身份认证程序被所述代理机构服务器和所述交易节点执行时实现如上所述的身份认证方法的步骤。

[0120] 其中，身份认证程序被执行时所实现的方法可参照本发明身份认证方法各个实施例，此处不再赘述。

[0121] 本发明还提供一种计算机可读存储介质。

[0122] 本发明计算机可读存储介质上存储有身份认证程序，所述身份认证程序被处理器执行时实现如上所述的身份认证方法的步骤。

[0123] 其中，在所述处理器上运行的身份认证程序被执行时所实现的方法可参照本发明身份认证方法各个实施例，此处不再赘述。

[0124] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0125] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0126] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0127] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

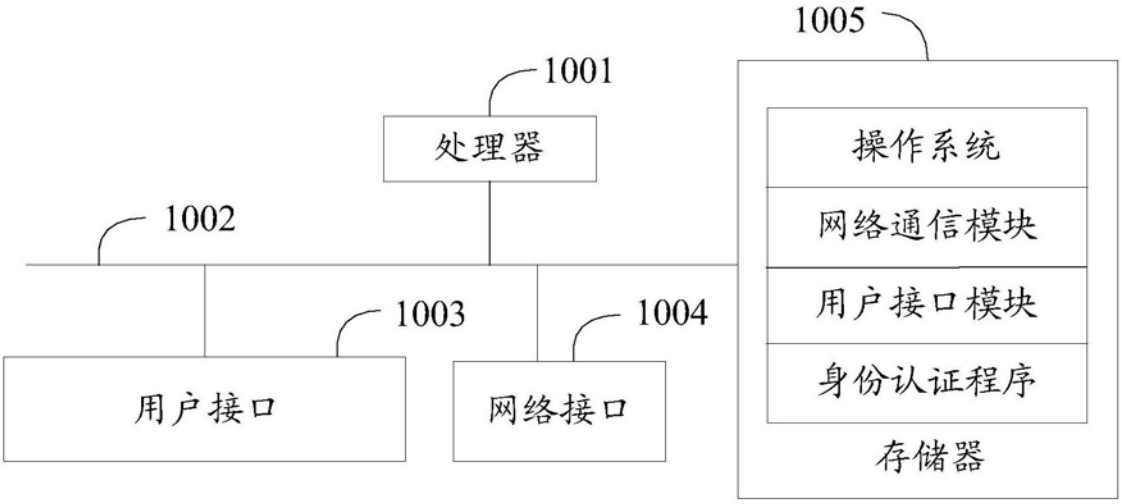

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
1003
1004
身份认证程序
用户接口
网络接口
存储器

图1

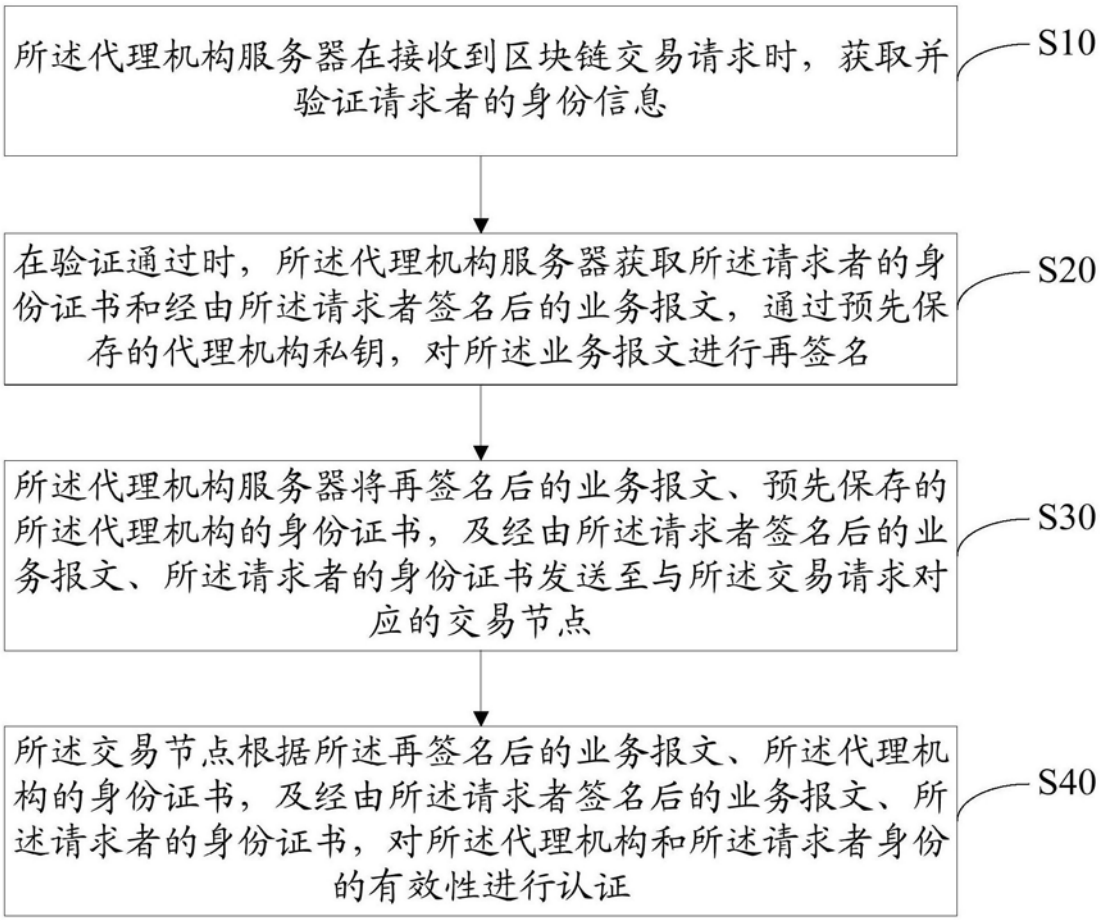

所述代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息
S10
在验证通过时，所述代理机构服务器获取所述请求者的身份证书和经由所述请求者签名后的业务报文，通过预先保存的代理机构私钥，对所述业务报文进行再签名
S20
所述代理机构服务器将再签名后的业务报文、预先保存的所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书发送至与所述交易请求对应的交易节点
S30
所述交易节点根据所述再签名后的业务报文、所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书，对所述代理机构和所述请求者身份的有效性进行认证
S40

图2

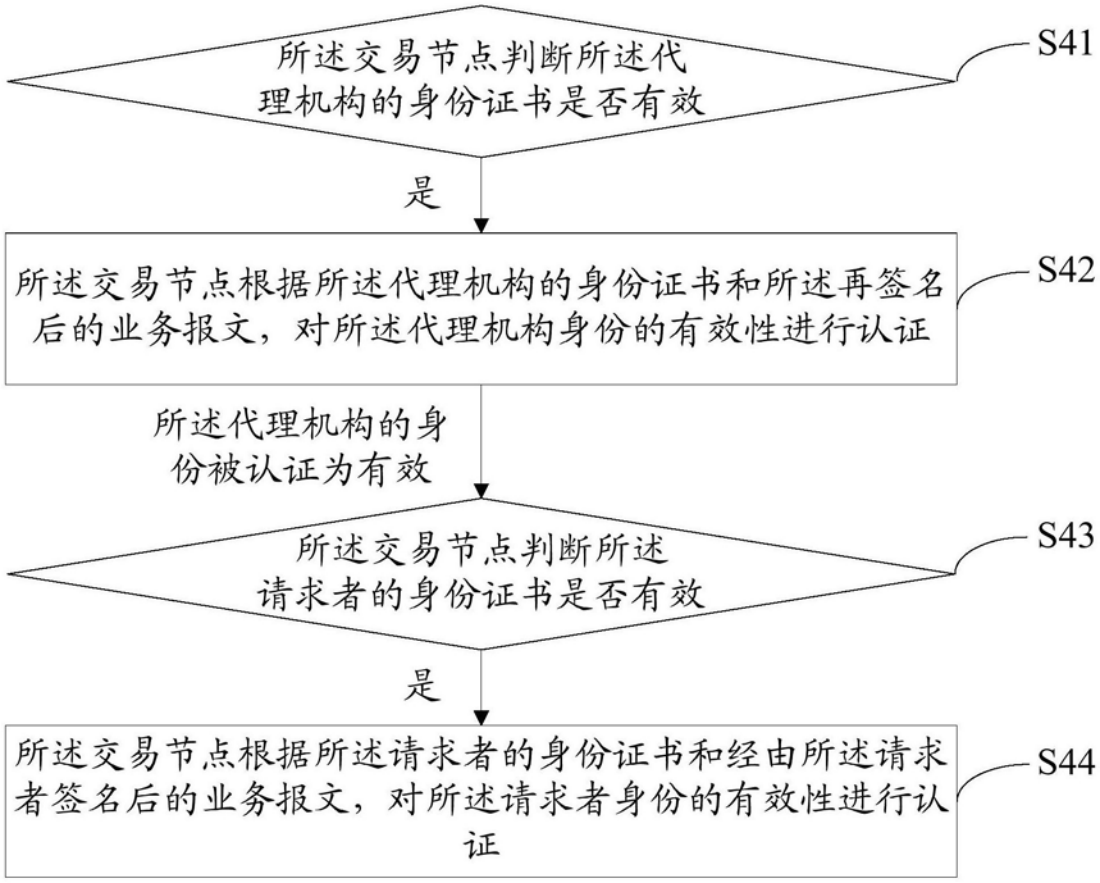

所述交易节点判断所述代理机构的身份证书是否有效
S41
是
所述交易节点根据所述代理机构的身份证书和所述再签名后的业务报文，对所述代理机构身份的有效性进行认证
S42
所述代理机构的身份被认证为有效
所述交易节点判断所述请求者的身份证书是否有效
S43
是
所述交易节点根据所述请求者的身份证书和经由所述请求者签名后的业务报文，对所述请求者身份的有效性进行认证
S44

图3

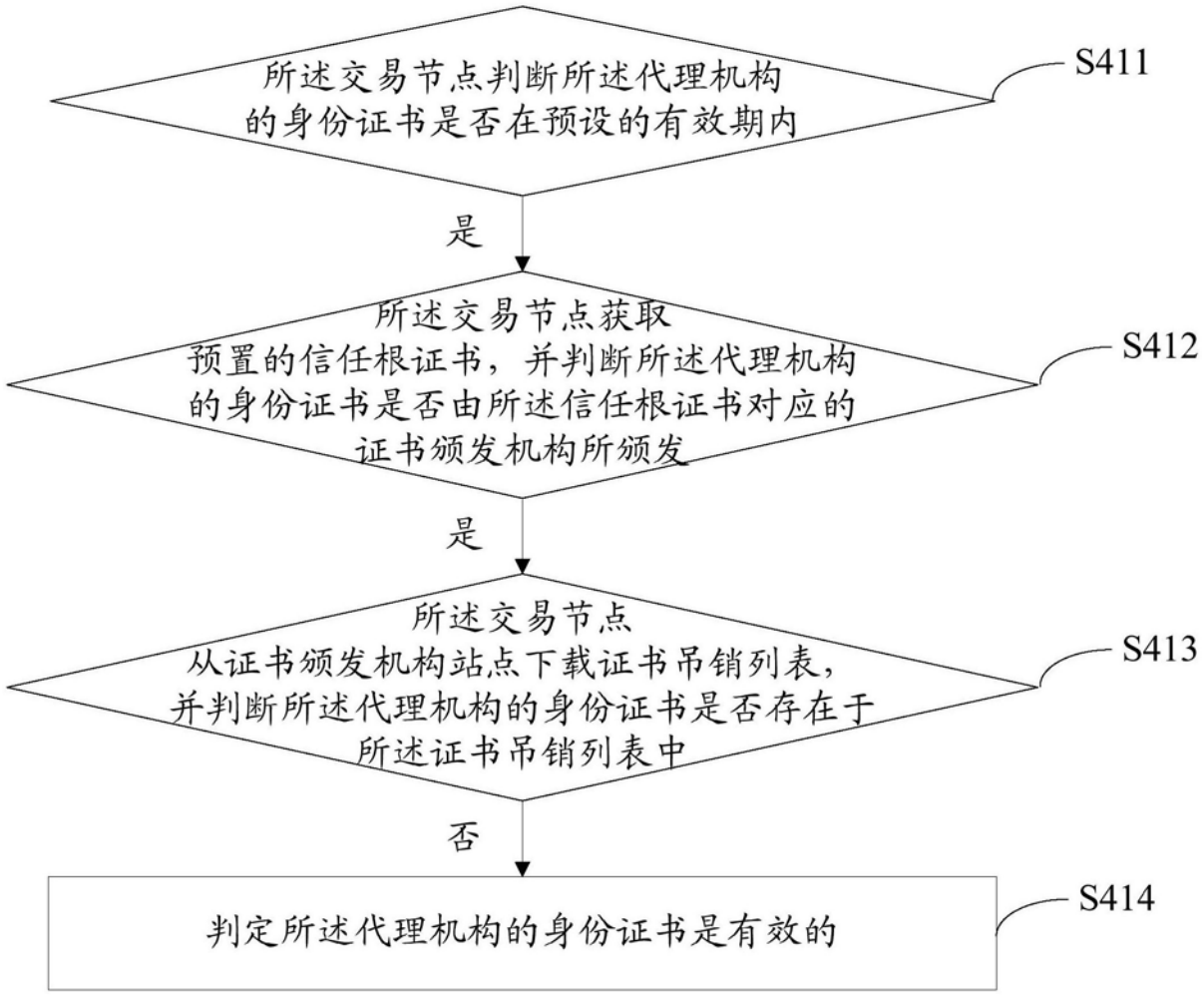

所述交易节点判断所述代理机构的身份证书是否在预设的有效期内
S411
是
所述交易节点获取预置的信任根证书，并判断所述代理机构的身份证书是否由所述信任根证书对应的证书颁发机构所颁发
S412
是
所述交易节点从证书颁发机构站点下载证书吊销列表，并判断所述代理机构的身份证书是否存在于所述证书吊销列表中
S413
否
判定所述代理机构的身份证书是有效的
S414

图4

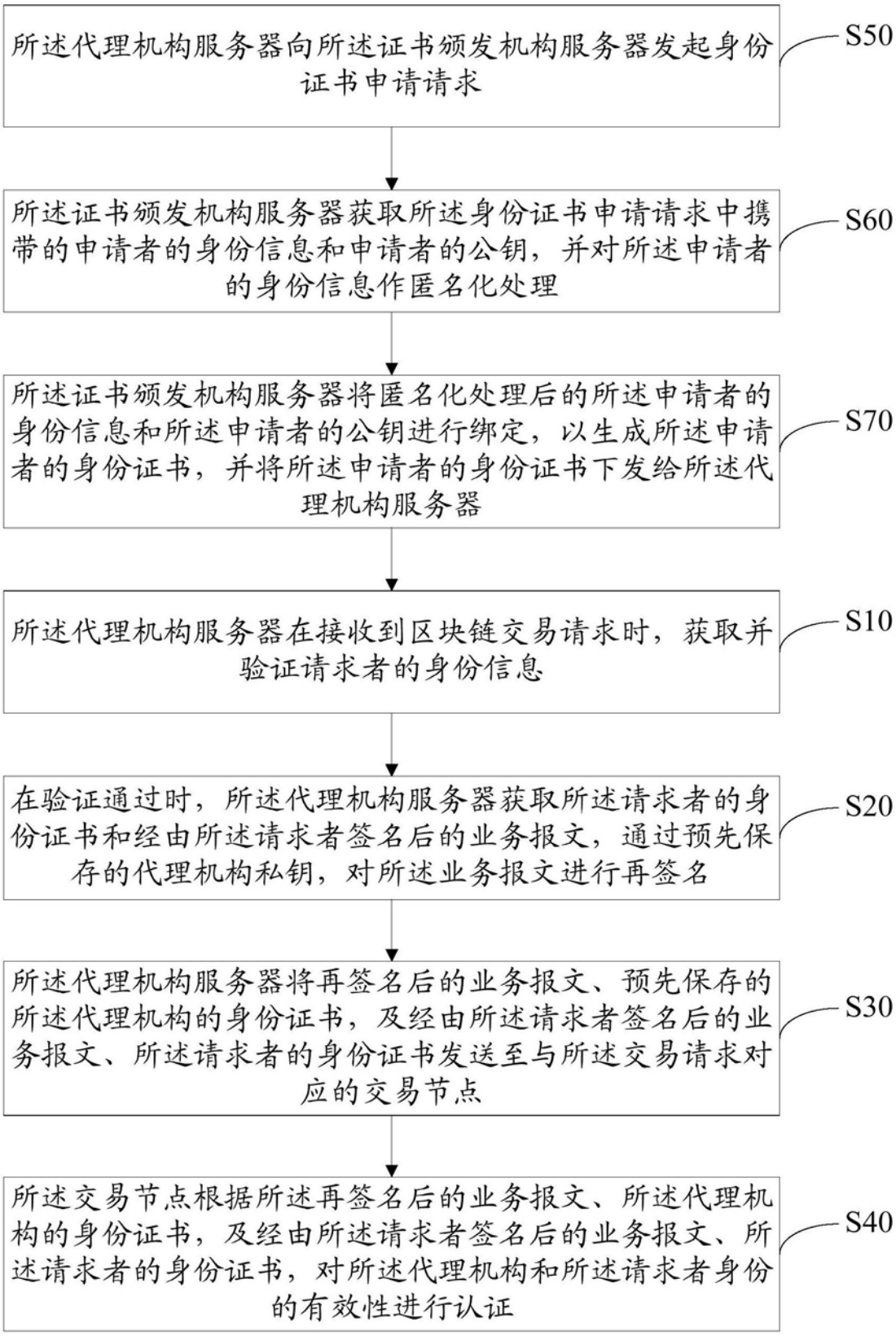

所述代理机构服务器向所述证书颁发机构服务器发起身份证书申请请求
S50
所述证书颁发机构服务器获取所述身份证书申请请求中携带的申请者的身份信息和申请者的公钥，并对所述申请者的身份信息作匿名化处理
S60
所述证书颁发机构服务器将匿名化处理后的所述申请者的身份信息和所述申请者的公钥进行绑定，以生成所述申请者的身份证书，并将所述申请者的身份证书下发给所述代理机构服务器
S70
所述代理机构服务器在接收到区块链交易请求时，获取并验证请求者的身份信息
S10
在验证通过时，所述代理机构服务器获取所述请求者的身份证书和经由所述请求者签名后的业务报文，通过预先保存的代理机构私钥，对所述业务报文进行再签名
S20
所述代理机构服务器将再签名后的业务报文、预先保存的所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书发送至与所述交易请求对应的交易节点
S30
所述交易节点根据所述再签名后的业务报文、所述代理机构的身份证书，及经由所述请求者签名后的业务报文、所述请求者的身份证书，对所述代理机构和所述请求者身份的有效性进行认证
S40

图5