(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 107547514 A
(43)申请公布日 2018.01.05

(21)申请号 201710583852.1

(22)申请日 2017.07.17

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

(72)发明人 侯庭伟 黄丽标 李俊 孙建平 胡辉 林常林

(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 赵东阳

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/31(2013.01)
H04L 9/32(2006.01)

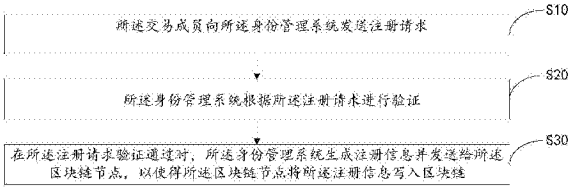
权利要求书2页 说明书13页 附图5页

(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，包括：所述交易成员向所述身份管理系统发送注册请求；所述身份管理系统根据所述注册请求进行验证；在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。本发明还公开了一种身份认证证系统、计算机可读存储介质。本发明能够简化身份认证系统设计和身份认证过程。



CN 107547514 A

1.一种身份认证方法，其特征在于，所述身份认证方法应用于身份认证系统，所述系统包括区块链节点、交易成员和身份管理系统，包括以下步骤：

所述交易成员向所述身份管理系统发送注册请求；

所述身份管理系统根据所述注册请求进行验证；

在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。

2.如权利要求1所述的身份认证方法，其特征在于，所述注册请求包括：

所述交易成员身份信息和所述交易成员对应的第一公钥。

3.如权利要求2所述身份认证方法，其特征在于，所述身份管理系统根据所述注册请求进行验证包括：

所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三方对所述身份信息进行验证；

所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果。

4.如权利要求2所述的身份认证方法，其特征在于，所述身份认证方法还包括：

所述交易成员利用所述第一公钥对应的第一私钥签署交易信息，并将所述交易信息发送给所述区块链节点，以使得所述区块链节点根据所述交易成员身份信息利用所述交易成员对应的第一公钥进行解密验证。

5.如权利要求1所述的身份认证方法，其特征在于，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将注册信息写入区块链包括：

所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息；

所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链。

6.一种身份认证系统，其特征在于，所述系统包括区块链节点、交易成员、身份管理系统和身份认证程序，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时实现如下步骤：

所述交易成员向身份管理系统发送注册请求；

所述身份管理系统根据所述注册请求进行验证；

在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。

7.如权利要求6所述的身份认证系统，其特征在于，所述交易成员身份信息和所述交易成员对应的第一公钥，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时，还用以实现如下步骤：

所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三方对所述身份信息进行验证；

所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果。

8.如权利要求6所述的身份认证系统，其特征在于，所述交易成员身份信息和所述交易成员对应的第一公钥，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管

理系统执行时，还用以实现如下步骤：

所述交易成员利用所述第一公钥对应的第一私钥签署交易信息，并将所述交易信息发送给所述区块链节点，以使得所述区块链节点根据所述交易成员身份信息利用所述交易成员对应的第一公钥进行解密验证。

9.如权利要求6所述的身份认证系统，其特征在于，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时，还用以实现如下步骤：

所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息；

所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链。

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5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] 本发明涉及通信技术领域，尤其涉及一种身份认证方法、系统及计算机可读存储介质。

背景技术

[0002] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。

[0003] 区块链按使用受众范围分为公有链、联盟链和私有链，除了公有链，联盟链和私有链需要身份认证，只有授权许可的用户才能加入。目前大多数联盟链和私有链身份认证系统设计繁重，认证过程复杂，间接影响区块链的落地应用。

[0004] 上述内容仅用于辅助理解本发明的技术方案，并不代表承认上述内容是现有技术。

发明内容

[0005] 本发明的主要目的在于提供一种身份认证方法、系统及计算机可读存储介质，旨在解决身份认证系统设计繁重，认证过程复杂的技术问题。

[0006] 为实现上述目的，本发明提供一种身份认证方法，所述身份认证方法包括：

[0007] 所述交易成员向所述身份管理系统发送注册请求；

[0008] 所述身份管理系统根据所述注册请求进行验证；

[0009] 在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。

[0010] 优选地，所述注册请求包括：

[0011] 所述交易成员身份信息和所述交易成员对应的第一公钥。

[0012] 优选地，所述身份管理系统根据所述注册请求进行验证包括：

[0013] 所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三方对所述身份信息进行验证；

[0014] 所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果。

[0015] 优选地，所述身份认证方法还包括：

[0016] 所述交易成员利用所述第一公钥对应的第一私钥签署交易信息，并将所述交易信息发送给所述区块链节点，以使得所述区块链节点根据所述交易成员身份信息利用所述交易成员对应的第一公钥进行解密验证。

[0017] 优选地，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将注册信息写入区块链包括：

[0018] 所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息；

[0019] 所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链。

[0020] 此外，为实现上述目的，本发明还提供一种身份认证系统，所述系统包括区块链节点、交易成员、身份管理系统和身份认证程序，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时实现如下步骤：

[0021] 所述交易成员向身份管理系统发送注册请求；

[0022] 所述身份管理系统根据所述注册请求进行验证；

[0023] 在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。

[0024] 优选地，所述交易成员身份信息和所述交易成员对应的第一公钥，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时，还用以实现如下步骤：

[0025] 所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三方对所述身份信息进行验证；

[0026] 所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果。

[0027] 优选地，所述交易成员身份信息和所述交易成员对应的第一公钥，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时，还用以实现如下步骤：

[0028] 所述交易成员利用所述第一公钥对应的第一私钥签署交易信息，并将所述交易信息发送给所述区块链节点，以使得所述区块链节点根据所述交易成员身份信息利用所述交易成员对应的第一公钥进行解密验证。

[0029] 优选地，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时，还用以实现如下步骤：

[0030] 所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息；

[0031] 所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链。

[0032] 此外，为了实现上述目的，本发明还提供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上所述的身份认证方法的步骤。

[0033] 本发明提供一种身份认证方法、系统和计算机可读存储介质。所述身份认证方法应用于身份认证系统，所述系统包括区块链节点、交易成员和身份管理系统。在本方法中，所述交易成员向所述身份管理系统发送注册请求；

[0034] 所述身份管理系统根据所述注册请求进行验证；在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。通过上述方式，交易成员先向身份管理系统发送注册请求，然后身份管理系统对交易成员身份进行验证，验证通过后身份管理系统再签署交易成员注册信息并发送给区块链节点，以使得区块链节点把交易信息写入区块链。通过设置身份管理系统对交易成员进行注册管理，简化了身份认证系统，使得在身份管理系统中注册过的交易成员签

署的交易发送给区块链节点通过验证，将交易成员的非对称密作为身份的标识，实现了简化了身份认证过程。

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\装置结构示意图；

[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一实施例和身份认证系统各实施例相关的银行直连清算区块链报文平台示意图；

[0038] 图4为本发明身份认证方法第二实施例的流程示意图；

[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] 图6为本发明身份认证方法第四实施例的流程示意图。

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] 由于现有技术中大多数联盟链和私有链身份认证系统设计太重，认证系统比链上业务应用都复杂，特别对应安全性要求高的系统，会设置多层认证，这种方式容易导致整个系统无法运行，间接影响区块链的落地应用。

[0043] 为了解决上述技术问题，本发明提出一种身份认证方法，通过所述交易成员向所述身份管理系统发送注册请求，所述身份管理系统根据所述注册请求进行验证，在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链，简化了身份认证系统和认证过程。

[0044] 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。

[0045] 本发明实施例终端可以是PC，也可以是智能手机、平板电脑、电子书阅读器、MP3(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面3)播放器、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面3)播放器、便携计算机等具有显示功能的可移动式终端设备。

[0046] 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。

[0047] 可选地，终端还可以包括摄像头、RF(Radio Frequency，射频)电路，传感器、音频电路、Wi-Fi模块等等。其中，传感器比如光传感器、运动传感器以及其他传感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节显示屏的亮度，接近传感器可在移动终端移动到耳边时，关闭显示屏和/或背光。作为运动传感器的一种，重力加速度传感器可检测各个方向上(一般为三轴)加速度的大小，静止时可检测出重力的大小及方向，可用于识别移动终端姿态的应用(比如横竖屏切换、相关

游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等;当然,移动终端还可配置陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器,在此不再赘述。

[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] 所述交易成员向身份管理系统发送注册请求;

[0052] 所述身份管理系统根据所述注册请求进行验证;

[0053] 在所述注册请求验证通过时,所述身份管理系统生成注册信息并发送给所述区块链节点,以使得所述区块链节点将所述注册信息写入区块链。

[0054] 进一步地,处理器1001可以调用存储器1005中存储的网络操作控制应用程序,还执行以下操作:

[0055] 所述注册请求包括:

[0056] 所述交易成员身份信息和所述交易成员对应的第一公钥。

[0057] 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:

[0058] 所述身份管理系统将所述注册请求中的身份信息发送至第三方,以使得第三方对所述身份信息进行验证;

[0059] 所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果。

[0060] 进一步地,处理器1001可以调用存储器1005中存储的网络操作控制应用程序,还执行以下操作:

[0061] 所述交易成员利用所述第一公钥对应的第一私钥签署交易信息,并将所述交易信息发送给所述区块链节点,以使得所述区块链节点根据所述交易成员身份信息利用所述交易成员对应的第一公钥进行解密验证。

[0062] 进一步地,处理器1001可以调用存储器1005中存储的网络操作控制应用程序,还执行以下操作:

[0063] 所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求,生成注册信息;

[0064] 所述身份管理系统将所述注册信息发送给所述区块链节点,以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份,并在所述身份管理系统身份验证通过时,将所述注册信息写入区块链。

[0065] 基于上述硬件结构,提出本发明身份认证方法实施例。

[0066] 参照图2,图2为本发明身份认证方法第一实施例流程示意图,所述身份认证方法包括:

[0067] 步骤S10,所述交易成员向所述身份管理系统发送注册请求;

[0068] 在发明实施案中,该身份认证方法可以应用于银行或者证券等行业,本实施例以

银行行业为例。为保证系统安全，银行的业务处理系统一般包括核心系统和前置系统。银行核心系统，是银行的数据处理中心，集中了银行客户的账务信息，是银行运营的重中之重。核心系统包括核心账务处理系统和核心数据库，两者的交互可以完成各种业务的账务信息处理。可以进行完整的银行交易和事务处理的交易系统，银行核心是一个单独的、可运行的交易系统。

[0069] 前置系统，是中间业务交换平台，可以进行报文转换、报文的加解密处理、通讯协议转换，以及，通过这个平台上的路由功能进行通讯报文的转入或转出处理。

[0070] 交易成员需要通过身份认证才可以加入由各个银行组成的区块链，本实施例中的交易成员通过该交易成员中的前置系统与区块链进行通信进行身份认证。如图3所示，图3是与本发明身份认证方法实施例有关的银行直连清算区块链报文平台示意图，本实施例身份认证方法所应用的身份认证系统与传统认证系统的一个重要区别在于设置了身份管理系统。在各个银行多个交易成员组成的区块链节点中，所述身份管理系统与所述交易成员和区块链节点相连，用于交易成员的注册登记并把交易成员的注册信息发给区块链。图三系统共有4个地位对等的区块链节点，实际实施中区块链节点数目并不局限4个，众多节点共同构成一个端到端的网络。每个区块链节点都允许获得一份完整的数据拷贝。节点间基于一套共识机制通过共同计算共同维护整个区块链。节点之间数据交换通过数字签名技术进行验证。身份管理系统的公钥作为配置信息配置在区块链节点中，在通信过程中，所述身份管理系统通过自身的私钥签署交易与区块链节点进行通信，所述区块链节点则可以采用预先配置的公钥进行验证，从而实现对应的通信。直连清算区块链报文平台还包括监控平台，监控平台独立于身份管理系统，对区块链里的交易信息进行公开以便读取，把所有的交易信息展示出来，给交易成员读取。在本发明的身份认证方法步骤中，交易成员需要向身份管理系统发送注册请求，所述注册请求包括注册需要的信息，只有在身份管理系统中注册的交易成员才能与区块链节点通信。在本实施例中，所述交易成员指的是银行前置机，由所述银行前置机发送注册请求。

[0071] 步骤S20，所述身份管理系统根据所述注册请求进行验证；

[0072] 当所述身份管理系统收到所述交易成员发送的注册请求后，根据所述注册请求进行验证。在步骤S10中向交易成员发送注册请求的交易成员可以分为两种情况：所述交易成员属于组成所述区块链的中的任一个银行的交易成员和不属于组成所述区块链中任一个银行的交易成员。需要验证的内容可以包括：所述交易成员发送的注册请求包括的信息是否准确；所述交易成员是否属于区块链中任一银行的交易处理系统。

[0073] 只有属于区块链中的银行交易处理系统并且发送的信息准确的注册请求才能通过。

[0074] 例如，某个第一区块链由且A,B和C三个银行及其支行组成，只有A,B 和C三个银行及其支行的交易处理系统发送的注册请求的信息准确才能通过验证。以下2种情况均不通过：

[0075] 1)不属于区块链的组成银行的交易系统发送的注册请求。

[0076] 例如，银行D不属于如上所述的第一区块链，银行D的某个前置机1发送了注册请求1，但由于D银行不属于区块链的成员，前置机1发送的注册请求1验证不通过。

[0077] 2)属于区块链的组成银行发送的注册请求包含的信息不准确。

[0078] 例如，银行A属于所述第一区块链，银行A的前置机2发送了注册请求 2，但所述注册请求2包含的信息内容缺失或者信息有误，前置机2发送的注册请求2验证不通过。

[0079] 步骤S30，在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。

[0080] 身份管理系统有把签署的交易发给区块链节点以使得区块链接节点写入区块链的权限，而交易成员需要在身份管理系统中注册并由区块链节点将注册信息写入区块链后才可以与区块链节点通信。身份管理系统自身随机产生一对非对称密钥，所述身份管理系统的非对称密钥中的私钥用于签署交易信息，身份管理系统的非对称密钥中的公钥配置在区块链节点。当所述身份管理系统根据所述注册请求进行验证完成时，所述身份管理系统会得到一个验证结果，所述验证结果可以是第三方根据身份管理系统提供的交易成员身份信息进行验证后发来的验证结果，也可以是身份管理系统根据自身存档的由第三方提供的交易成员的身份证书与所述交易成员注册请求中的身份信息对比得到的验证结果。如果验证结果为通过，身份管理系统则根据注册请求利用自身的私钥对注册请求包含的信息进行加密生成注册信息，身份管理系统把所述注册信息发送给区块链节点，以使得其中区块链节点将所述注册信息写入区块链中，并使得交易成员可以与区块链节点进行通信。

[0081] 例如，在步骤S20中的所述第一区块链中，银行A的前置机3的注册请求3验证通过后，所述身份管理系统得到根据所述注册请求3的验证通过的结果。身份管理系统根据所述注册请求3和注册结果生成对应的注册信息，并把所述注册信息发送给区块链节点，以使得所述区块链节点将所述注册信息写到区块链中。

[0082] 在本实施例中，所述交易成员向所述身份管理系统发送注册请求；所述身份管理系统根据所述注册请求进行验证；在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。通过上述方式，交易成员先向身份管理系统发送注册请求，然后身份管理系统对交易成员身份进行验证，验证通过后身份管理系统再签署交易成员注册信息并发送给区块链节点，以使得区块链节点把交易信息写入区块链。通过设置身份管理系统对交易成员进行注册管理，简化了身份认证系统，使得在身份管理系统中注册过的交易成员签署的交易发送给区块链节点通过验证，将交易成员的非对称密作为身份的标识，实现了简化了身份认证过程。

[0083] 进一步的，基于上述本发明身份认证方法实施例，参照图4，提出本发明身份认证方法的第二实施例。

[0084] 在本实施例中，步骤S20所述注册请求所述交易成员的身份信息和所述交易成员对应的第一公钥，所述的份管理系统根据所述注册请求进行验证可以包括：

[0085] S21，所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三方对所述身份信息进行验证；

[0086] S22，所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果。

[0087] 在本实施例中，采用非对称密钥作为所述交易成员的身份标识，非对称加密算法需要两个密钥：公开密钥和私有密钥，这里分别简称为公钥和私钥。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥

并将其中的一把作为公用密钥向其它方公开;得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方;甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。

[0088] 非对称密钥,特别是ECC密钥,计算速度快,破解难度随密钥长度的增加达到指数级别,安全性高。如果将某个一定长度的非对称密钥和某个组织或者个体保密关联,通过密钥的身份冒用理论上几乎不可能。根据非对称密钥的算法特点,通过鉴别某个非对称密钥是否满足身份认证算法,可以判断持有密钥的个体和对象是否获得系统注册授权。

[0089] 本实施例中所述交易成员的非对称密钥由交易成员随机产生,这里把所述交易成员的非对称密钥称为第一非对称密钥,第一非对称密钥中的公钥称为第一公钥,对应私钥为第一私钥。交易所述交易成员发送注册请求时把交易成员都身份信息和所述交易成员对应的第一公钥捆绑一起。所述交易成员的身份信息包括但不限于所述交易成员所属银行结构名称和在所属银行中的交易成员名称和编码等信息。第一私钥由各个交易成员独自持有,用来签署加密交易信息。对应的第一公钥在注册时和身份信息捆绑,在所述身份管理系统注册并由所述区块链节点将所述注册信息写入区块链后,所述区块链节点就可以利用所述交易成员第一公钥对所述交易成员利用所述第一公私钥签署的交易进行解密和验证,从而保证交易信息的安全。

[0090] 所述身份认证系统接收到所述交易成员发来的注册请求后,根据注册请求将其中交易成员的身份信息发送至第三方。第三方可以是除了身份认证系统和交易成员之外的第三方权威身份认证机构。

[0091] 比如,如第一实施例的第一区块链中的银行A所属的前置机4向所述的身份管理系统发送了注册请求4,所述注册请求4的信息准确,包括所述前置机4的身份信息和所述前置机4的公钥。所述身份认证系统把前置机4的身份信息发给所述第三方,所述第三方对所述前置机4的身份验证通过时,把所述前置机4身份验证通过的结果发给身份管理系统。当不属于所述第一区块链的所述银行D的前置机1发送了注册请求1,由于所述银行D不属于所述所述第一区块链,故第三方对所述前置机1的身份验证不通过,并把所述前置机1身份认证不通过的结果发给身份管理系统。

[0092] 进一步地,所述份管理系统根据所述注册请求进行验证还可以包括,身份管理系统利用自身存档内由第三方提供的交易成员的身份证书与交易成员注册请求里的身份信息进行对比得到结果。所述领域的计数人员应当理解,此处列举的两个身份验证的结果得到的方式只是起到说明作用,而不是限定作用。

[0093] 在本实施例中,所述注册请求包括所述交易成员的身份信息和所述交易成员的第一公钥,充分的包括了身份认证和后续交易验证所需的信息。利用非对称密钥作为交易成员的身份标识,密钥长度可确保产生的密钥不可能碰撞。拥有密钥的个体和组织可以确认。换句话说,密钥是个体和组织的唯一标示。另外,非对称密钥算法是认证中心CA的基本算法,几乎拥有和CA发放的电子证书同等的安全机制。所述身份管理系统将所述注册请求中的身份信息发送至第三方,以使得第三方对所述身份信息进行验证,然后所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果,有效的保证了所述交易成员身份信息的准确性和可靠性。

[0094] 进一步地,基于上述本发明提示的身份认证方法实施例,参照图5,提出本发明的

第三实施例。

[0095] 在本实施例中，在所述区块链节点将交易信息写入区块链后，所述交易成员的交易步骤如下：

[0096] 步骤S40，所述交易成员利用所述第一公钥对应的第一私钥签署交易信息，并将所述交易信息发送给所述区块链节点，以使得所述区块链节点根据所述交易成员身份信息利用所述交易成员对应的第一公钥进行解密验证。

[0097] 所述交易成员身份认证完成后，所述交易成员的身份信息和对应的第一公钥已写入区块链。所述交易成员在交易时，利用所述的第一公钥对应的第一私钥加密交易信息，并把交易信息发送给区块链节点。所述区块链节点收到加密的交易信息后，根据所述交易成语的身份信息找到对应的第一私钥，对所述的交易信息进行解密和验证。当解密成功时，把对应的交易信息写入区块链。在本实施例中，只有注册信息被写入区块链中的交易成员发送的交易信息才能被区块链节点解密和验证，不在身份管理系统中注册的交易成员，其身份信息和对应的公钥没写入到区块链，因而区块链节点无法对其交易信息进行解密和验证，所述交易信息无法写入区块链。

[0098] 进一步的，基于上述本发明提示的身份认证方法实施例，参照图6，提出本发明第四实施例。

[0099] 基于上述所示的实施例，在本实施例中，步骤S30可以包括：

[0100] S31，所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息。

[0101] S32，所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链。

[0102] 为了确保认证过程安全，避免伪造注册信息发送给区块链节点并写入到区块链情况的出现，在本实施例中所述身份管理系统自身生产一对非对称密钥，对应的公钥这里称为第二公钥，对应私钥称为第二私钥。身份管理系统有把签署的交易发给区块链节点以使得区块链接节点写入区块链的权限，身份管理系统的公钥配置在区块链节点。身份管理系统收到所述注册请求验证通过的结果时，利用自身所述的第二私钥注册请求包含的信息进行加密生成注册信息，以便所述区块链节点接收到所述注册信息后利用所述身份管理系统第二私钥对应的第二公钥对所述注册信息进行解密和验证。区块链节点接收到加密的注册信息时，利用所述身份管理系统第二私钥对应的第二公钥对注册信息进行解密。解密成功，则确认所述注册信息由所述身份管理系统发出，所述区块链节点把注册信息写入区块链。解密不成功，则确认加密所述注册信息的密钥并非所述身份管理系统第二公钥对应的第二私钥，所述注册信息并非由所述身份管理系统发出，区块链节点拒绝把所述注册信息写入区块链。

[0103] 在本实施例中，所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息，然后所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链，有效的确保认证过程注册信息的传输和验证的安全。

[0104] 此外，本发明还提供一种身份认证系统。

[0105] 参考图3，提出本发明身份认证系统的第一实施例。

[0106] 在本实施例中，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时可以实现以下步骤：

[0107] 步骤S10，所述交易成员向所述身份管理系统发送注册请求；

[0108] 在发明实施例中，该身份认证系统可以应用于银行或者证券等行业，本实施例以银行行业为例。为保证系统安全，银行的业务处理系统一般包括核心系统和前置系统。银行核心系统，是银行的数据处理中心，集中了银行客户的账务信息，是银行运营的重中之重。核心系统包括核心账务处理系统和核心数据库，两者的交互可以完成各种业务的账务信息处理。可以进行完整的银行交易和事务处理的交易系统，银行核心是一个单独的、可运行的交易系统。

[0109] 前置系统，是中间业务交换平台，可以进行报文转换、报文的加解密处理、通讯协议转换，以及，通过这个平台上的路由功能进行通讯报文的转入或转出处理。

[0110] 交易成员需要通过身份认证才可以加入由各个银行组成的区块链，本实施例中的交易成员通过该交易成员中的前置系统与区块链进行通信进行身份认证。如图3所示，图3是与本发明身份认证系统实施例有关的银行直连清算区块链报文平台示意图，本实施例身份认证系统所应用的身份认证系统与传统认证系统的一个重要区别在于设置了身份管理系统。在各个银行多个交易成员组成的区块链节点中，所述身份管理系统与所述交易成员和区块链节点相连，用于交易成员的注册登记并把交易成员的注册信息发给区块链。图3系统共有4个地位对等的区块链节点，实际实施中区块链节点数目并不局限4个，众多节点共同构成一个端到端的网络。每个区块链节点都允许获得一份完整的数据拷贝。节点间基于一套共识机制通过共同计算共同维护整个区块链。节点之间数据交换通过数字签名技术进行验证。身份管理系统的公钥作为配置信息配置在区块链节点中，在通信过程中，所述身份管理系统通过自身的私钥签署交易与区块链节点进行通信，所述区块链节点则可以采用预先配置的公钥进行验证，从而实现对应的通信。直连清算区块链报文平台还包括监控平台，监控平台独立于身份管理系统，对区块链里的交易信息进行公开以便读取，把所有的交易信息展示出来，给交易成员读取。在本发明的身份认证系统被执行时，交易成员需要向身份管理系统发送注册请求，所述注册请求包括注册需要的信息，只有在身份管理系统中注册的交易成员才能与区块链节点通信。在本实施例中，所述交易成员指的是银行前置机，由所述银行前置机发送注册请求。

[0111] 步骤S20，所述身份管理系统根据所述注册请求进行验证；

[0112] 当所述身份管理系统收到所述交易成员发送的注册请求后，根据所述注册请求进行验证。在步骤S10中向交易成员发送注册请求的交易成员可以分为两种情况：所述交易成员属于组成所述区块链的中的任一个银行的交易成员和不属于组成所述区块链中任一个银行的交易成员。需要验证的内容可以包括：所述交易成员发送的注册请求包括的信息是否准确；所述交易成员是否属于区块链中任一银行的交易处理系统。

[0113] 只有属于区块链中的银行交易处理系统并且发送的信息准确的注册请求才能通过。

[0114] 例如，某个第一区块链由且A,B和C三个银行及其支行组成，只有A,B 和C三个银行

及其支行的交易处理系统发送的注册请求的信息准确才能通过验证。以下2种情况均不通过：

[0115] 1)不属于区块链的组成银行的交易系统发送的注册请求。

[0116] 例如，银行D不属于如上所述的第一区块链，银行D的某个前置机1发送了注册请求1，但由于D银行不属于区块链的成员，前置机1发送的注册请求1验证不通过。

[0117] 2)属于区块链的组成银行发送的注册请求包含的信息不准确。

[0118] 例如，银行A属于所述第一区块链，银行A的前置机2发送了注册请求 2，但所述注册请求2包含的信息内容缺失或者信息有误，前置机2发送的注册请求2验证不通过。

[0119] 步骤S30，在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。

[0120] 身份管理系统有把签署的交易发给区块链节点以使得区块链接节点写入区块链的权限，而交易成员需要在身份管理系统中注册并由区块链节点将注册信息写入区块链后才可以与区块链节点通信。身份管理系统自身随机产生一对非对称密钥，所述身份管理系统的非对称密钥中的私钥用于签署交易信息，身份管理系统的非对称密钥中的公钥配置在区块链节点。当所述身份管理系统根据所述注册请求进行验证完成时，所述身份管理系统会得到一个验证结果，所述验证结果可以是第三方根据身份管理系统提供的交易成员进行验证后发来的验证结果，也可以是身份管理系统根据自身存档的由第三方提供的交易成员的身份证书与所述交易成员注册请求中的身份信息对比得到的验证结果。如果验证结果为通过，身份管理系统则根据注册请求利用自身的私钥对注册请求包含的信息进行加密生成注册信息，身份管理系统把所述注册信息发送给区块链节点，以使得其中区块链节点将所述注册信息写入区块链中，并使得交易成员可以与区块链节点进行通信。

[0121] 例如，在步骤S20中的所述第一区块链中，银行A的前置机3的注册请求3验证通过后，所述身份管理系统得到根据所述注册请求3的验证通过的结果。身份管理系统根据所述注册请求3和注册结果生成对应的注册信息，并把所述注册信息发送给区块链节点，以使得所述区块链节点将所述注册信息写到区块链中。

[0122] 在本实施例中，所述交易成员向所述身份管理系统发送注册请求；所述身份管理系统根据所述注册请求进行验证；在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链。通过上述方式，交易成员先向身份管理系统发送注册请求，然后身份管理系统对交易成员身份进行验证，验证通过后身份管理系统再签署交易成员注册信息并发送给区块链节点，以使得区块链节点把交易信息写入区块链。通过设置身份管理系统对交易成员进行注册管理，简化了身份认证系统，使得在身份管理系统中注册过的交易成员签署的交易发送给区块链节点通过验证，将交易成员的非对称密作为身份的标识，实现了简化了身份认证过程。

[0123] 进一步的，参考图3，提出本发明身份认证系统的第二实施例。

[0124] 在本实施例中，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时可以实现以下步骤：

[0125] 在本实施例中，步骤S20所述注册请求包括所述交易成员的身份信息和所述交易成员对应的第一公钥，所述的份管理系统根据所述注册请求进行验证可以包括：

[0126] S21，所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三

方对所述身份信息进行验证；

[0127] S22，所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果。

[0128] 在本实施例中，采用非对称密钥作为所述交易成员的身份标识，非对称加密算法需要两个密钥：公开密钥和私有密钥，这里分别简称为公钥和私钥。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。

[0129] 非对称密钥，特别是ECC密钥，计算速度快，破解难度随密钥长度的增加达到指数级别，安全性高。如果将某个一定长度的非对称密钥和某个组织或者个体保密关联，通过密钥的身份冒用理论上几乎不可能。根据非对称密钥的算法特点，通过鉴别某个非对称密钥是否满足身份认证算法，可以判断持有密钥的个体和对象是否获得系统注册授权。

[0130] 本实施例中所述交易成员的非对称密钥由交易成员随机产生，这里把所述交易成员的非对称密钥称为第一非对称密钥，第一非对称密钥中的公钥称为第一公钥，对应私钥为第一私钥。交易所述交易成员发送注册请求时把交易成员都身份信息和所述交易成员对应的第一公钥捆绑一起。所述交易成员的身份信息包括但不限于所述交易成员所属银行结构名称和在所属银行中的交易成员名称和编码等信息。第一私钥由各个交易成员独自持有，用来签署加密交易信息。对应的第一公钥在注册时和身份信息捆绑，在所述身份管理系统注册并由所述区块链节点将所述注册信息写入区块链后，所述区块链节点就可以利用所述交易成员第一公钥对所述交易成员利用所述第一私钥签署的交易进行解密和验证，从而保证交易信息的安全。

[0131] 所述身份认证系统接收到所述交易成员发来的注册请求后，根据注册请求将其中交易成员的身份信息发送至第三方。第三方可以是除了身份认证系统和交易成员之外的第三方权威身份认证机构。

[0132] 比如，如第一实施例的第一区块链中的银行A所属的前置机4向所述的身份管理系统发送了注册请求4，所述注册请求4的信息准确，包括所述前置机4的身份信息和所述前置机4的公钥。所述身份认证系统把前置机4的身份信息发给所述第三方，所述第三方对所述前置机4的身份验证通过时，把所述前置机4身份验证通过的结果发给身份管理系统。当不属于所述第一区块链的所述银行D的前置机1发送了注册请求1，由于所述银行D不属于所述所述第一区块链，故第三方对所述前置机1的身份验证不通过，并把所述前置机1身份认证不通过的结果发给身份管理系统。

[0133] 进一步地，所述份管理系统根据所述注册请求进行验证还可以包括，身份管理系统利用自身存档内由第三方提供的交易成员的身份证书与交易成员注册请求里的身份信息进行对比得到结果。所述领域的计数人员应当理解，此处列举的两个身份验证的结果得到的方式只是起到说明作用，而不是限定作用。

[0134] 在本实施例中，所述注册请求包括所述交易成员的身份信息和所述交易成员的第一公钥，充分的包括了身份认证和后续交易验证所需的信息。利用非对称密钥作为交易成

员的身份标识，密钥长度可确保产生的密钥不可能碰撞。拥有密钥的个体和组织可以确认。换句话说，密钥是个体和组织的唯一标示。另外，非对称密钥算法是认证中心CA的基本算法，几乎拥有和CA发放的电子证书同等的安全机制。所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三方对所述身份信息进行验证，然后所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果，有效的保证了所述交易成员身份信息的准确性和可靠性。

[0135] 进一步地，参考图3，提出本发明身份认证系统的第三实施例。

[0136] 在本实施例中，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时可以实现以下步骤：

[0137] 在所述区块链节点将交易信息写入区块链后，所述交易成员的交易步骤如下：

[0138] 步骤S40，所述交易成员利用所述第一公钥对应的第一私钥签署交易信息，并将所述交易信息发送给所述区块链节点，以使得所述区块链节点根据所述交易成员身份信息利用所述交易成员对应的第一公钥进行解密验证。

[0139] 所述交易成员身份认证完成后，所述交易成员的身份信息和对应的第一公钥已写入区块链。所述交易成员在交易时，利用所述的第一公钥对应的第一私钥加密交易信息，并把交易信息发送给区块链节点。所述区块链节点收到加密的交易信息后，根据所述交易成语的身份信息找到对应的第一私钥，对所述的交易信息进行解密和验证。当解密成功时，把对应的交易信息写入区块链。在本实施例中，只有注册信息被写入区块链中的交易成员发送的交易信息才能被区块链节点解密和验证，不在身份管理系统中注册的交易成员，其身份信息和对应的公钥没写入到区块链，因而区块链节点无法对其交易信息进行解密和验证，所述交易信息无法写入区块链。

[0140] 进一步的，参考图3，提出本发明身份认证系统的第四实施例。

[0141] 在本实施例中，所述身份认证程序被所述区块链节点、所述交易成员和所述身份管理系统执行时可以实现以下步骤：

[0142] 基于上述所示的实施例，在本实施例中，步骤S30可以包括：

[0143] S31，所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息。

[0144] S32，所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链。

[0145] 为了确保认证过程安全，避免伪造注册信息发送给区块链节点并写入到区块链情况的出现，在本实施例中所述身份管理系统自身生产一对非对称密钥，对应的公钥这里称为第二公钥，对应私钥称为第二私钥。身份管理系统有把签署的交易发给区块链节点以使得区块链接节点写入区块链的权限，身份管理系统的公钥配置在区块链节点。身份管理系统收到所述注册请求验证通过的结果时，利用自身所述的第二私钥注册请求包含的信息进行加密生成注册信息，以便所述区块链节点接收到所述注册信息后利用所述身份管理系统第二私钥对应的第二公钥对所述注册信息进行解密和验证。区块链节点接收到加密的注册信息时，利用所述身份管理系统第二私钥对应的第二公钥对注册信息进行解密。解密成功，则确认所述注册信息由所述身份管理系统发出，所述区块链节点把注册信息写入区块链。

解密不成功，则确认加密所述注册信息的密钥并非所述身份管理系统第二公钥对应的第二私钥，所述注册信息并非由所述身份管理系统发出，区块链节点拒绝把所述注册信息写入区块链。

[0146] 在本实施例中，所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息，然后所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链，有效的确保认证过程注册信息的传输和验证的安全。

[0147] 此外，本发明实施例还提出一种计算机可读存储介质。

[0148] 本发明计算机可读存储介质上存储有身份认证程序，所述身份认证程序执行时实现如上所述的身份认证方法的步骤。

[0149] 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。

[0150] 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。

[0151] 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。

[0152] 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。

[0153] 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。

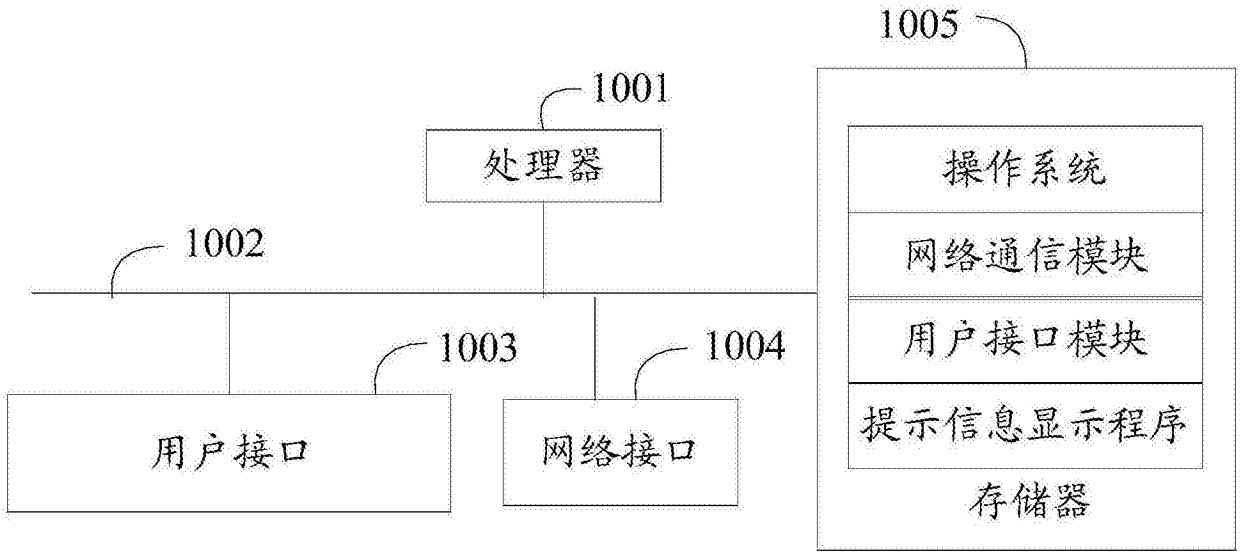

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
提示信息显示程序
1003
1004
用户接口
网络接口
存储器

图1

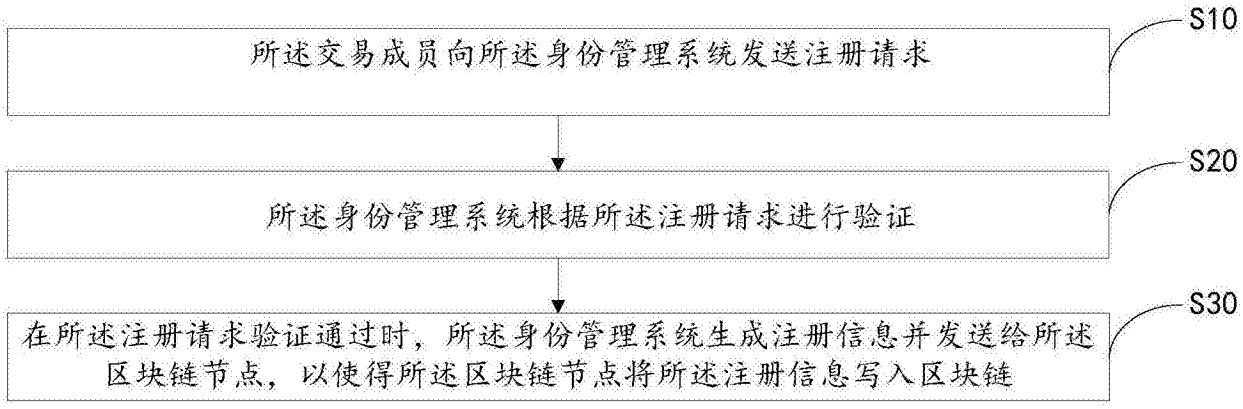

S10
所述交易成员向所述身份管理系统发送注册请求
S20
所述身份管理系统根据所述注册请求进行验证
S30
在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链

图2

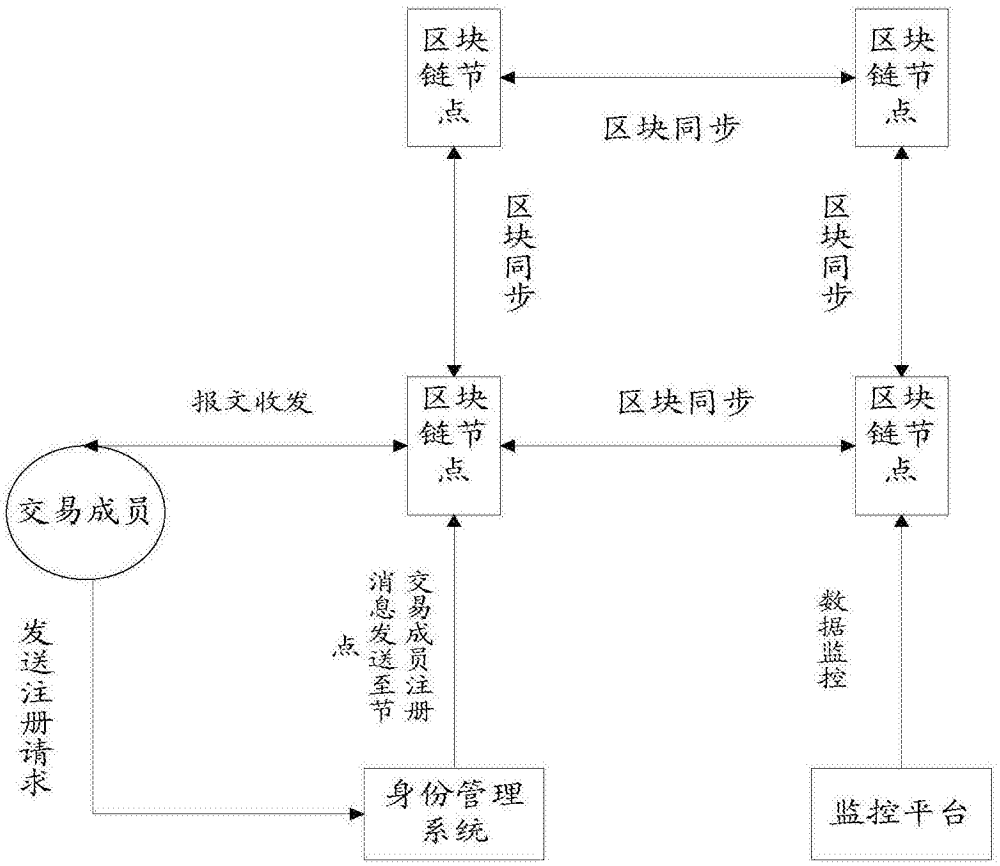

区块链节点
区块链节点
区块同步
区块同步
区块同步
报文收发
区块链节点
区块同步
区块链节点
交易成员
发送注册请求
交易成员注册消息发送至节点
数据监控
身份管理系统
监控平台

图3

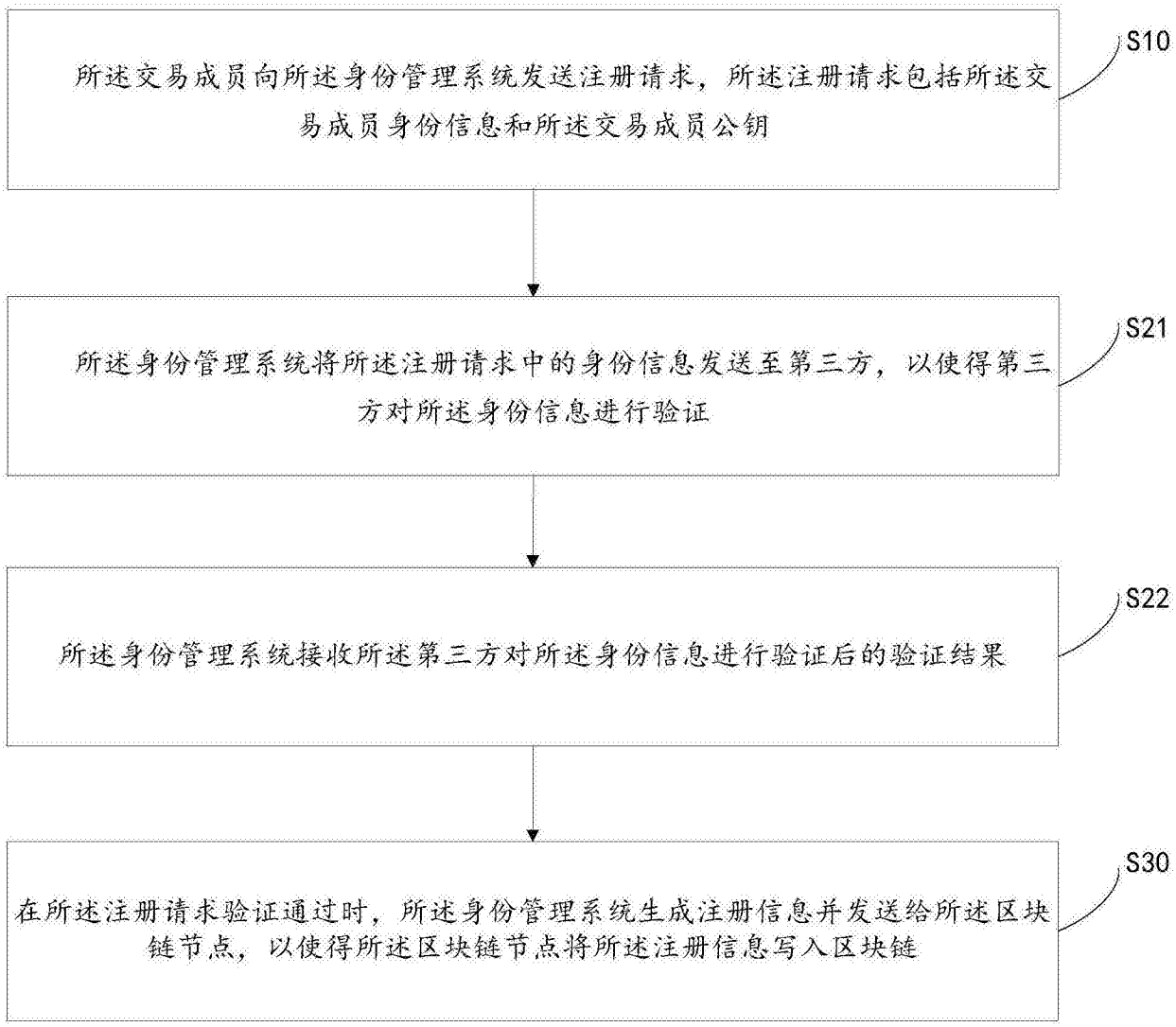

所述交易成员向所述身份管理系统发送注册请求，所述注册请求包括所述交易成员身份信息和所述交易成员公钥
S10
所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三方对所述身份信息进行验证
S21
所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果
S22
在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链
S30

图4

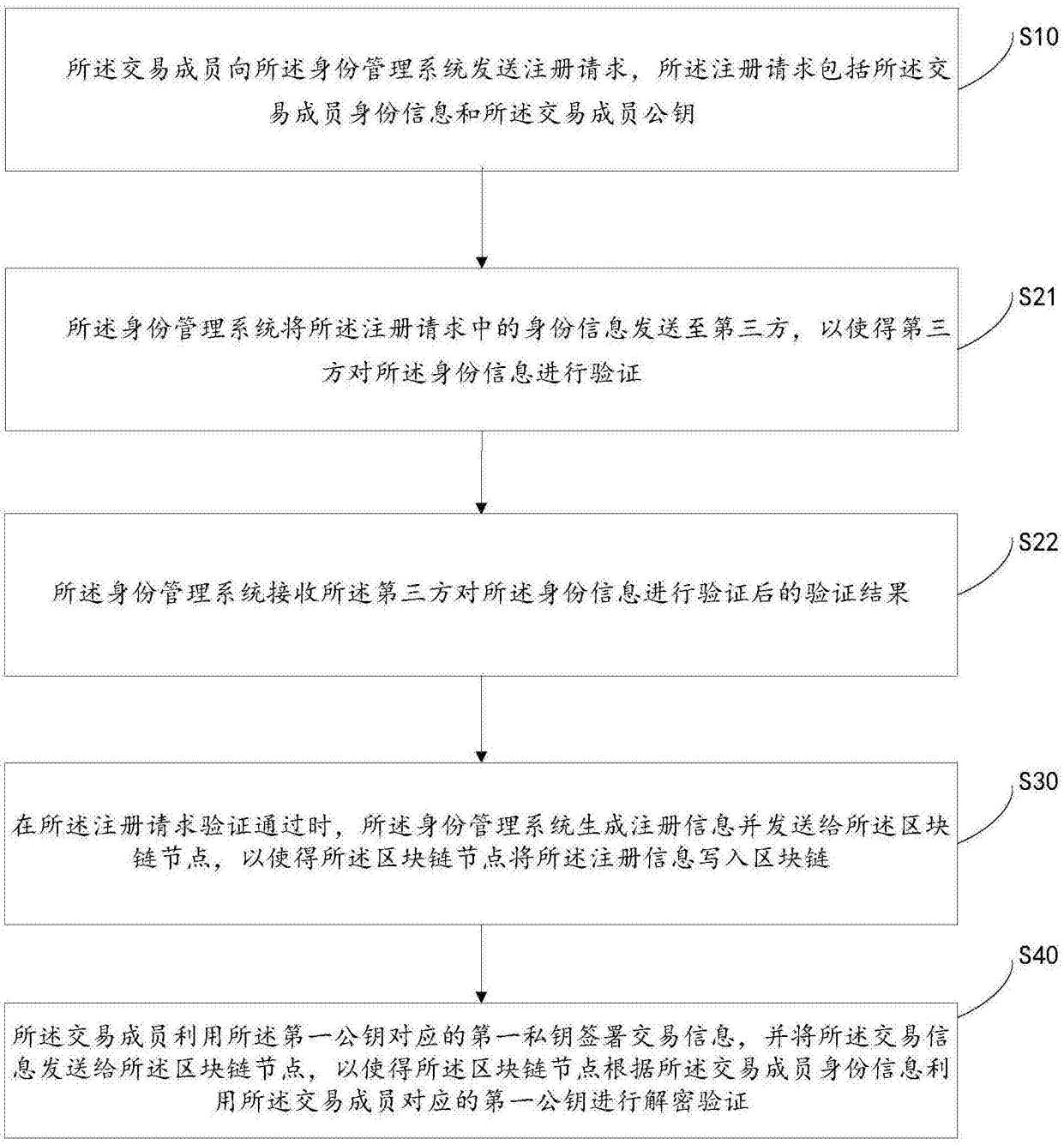

所述交易成员向所述身份管理系统发送注册请求，所述注册请求包括所述交易成员身份信息和所述交易成员公钥
S10
所述身份管理系统将所述注册请求中的身份信息发送至第三方，以使得第三方对所述身份信息进行验证
S21
所述身份管理系统接收所述第三方对所述身份信息进行验证后的验证结果
S22
在所述注册请求验证通过时，所述身份管理系统生成注册信息并发送给所述区块链节点，以使得所述区块链节点将所述注册信息写入区块链
S30
所述交易成员利用所述第一公钥对应的第一私钥签署交易信息，并将所述交易信息发送给所述区块链节点，以使得所述区块链节点根据所述交易成员身份信息利用所述交易成员对应的第一公钥进行解密验证
S40

图5

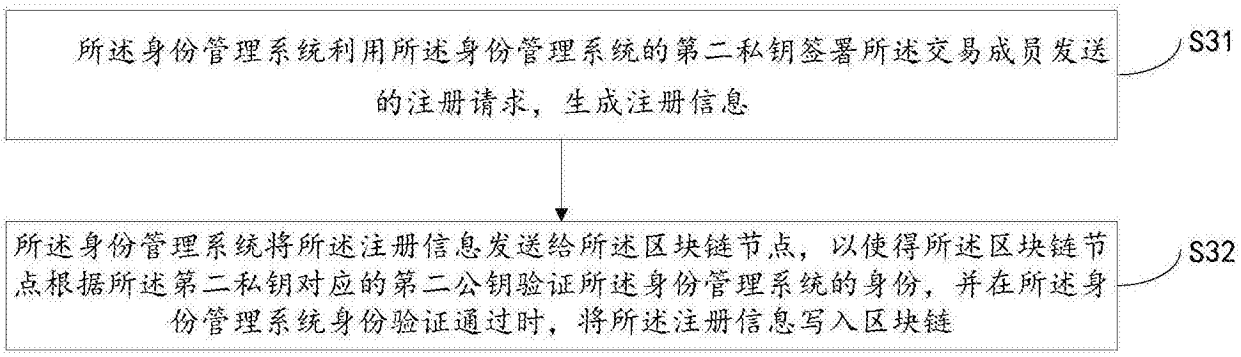

所述身份管理系统利用所述身份管理系统的第二私钥签署所述交易成员发送的注册请求，生成注册信息
S31
所述身份管理系统将所述注册信息发送给所述区块链节点，以使得所述区块链节点根据所述第二私钥对应的第二公钥验证所述身份管理系统的身份，并在所述身份管理系统身份验证通过时，将所述注册信息写入区块链
S32

图6