(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 106533696 B
(45)授权公告日 2019.10.01

(21)申请号 201611024371.9

(22)申请日 2016.11.18

(65)同一申请的已公布的文献号
申请公布号 CN 106533696 A

(43)申请公布日 2017.03.22

(73)专利权人 江苏通付盾科技有限公司
地址 215021 江苏省苏州市苏州工业园区东长路88号建屋2.5产业园C2幢4F

(72)发明人 汪德嘉 郭宇 王少凡 柴泉

(74)专利代理机构 北京市浩天知识产权代理事务所(普通合伙) 11276
代理人 宋菲 刘兰兰

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 105701372 A,2016.06.22,
CN 105976231 A,2016.09.28,
CN 105991731 A,2016.10.05,
CN 106096967 A,2016.11.09,
CN 105871867 A,2016.08.17,
CN 105893042 A,2016.08.24,
WO 2016154001 A1,2016.09.29,
CN 105162785 A,2015.12.16,
孙媛媛.基于信任链的P2P可信身份认证模型的研究与设计.《中国优秀硕士学位论文全文数据库 信息科技辑》.2016,(第3期),

审查员 行朝霞

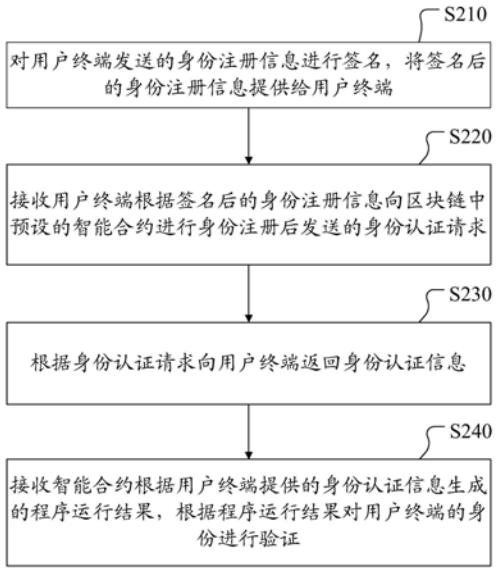
权利要求书3页 说明书9页 附图8页

(54)发明名称

基于区块链的身份认证方法、认证服务器及用户终端

(57)摘要

本申请实施例公开了一种基于区块链的身份认证方法、认证服务器及用户终端，涉及身份识别技术领域，包括：对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给用户终端；接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求；根据身份认证请求向用户终端返回身份认证信息；接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证。由此可见，本申请实施例中的身份认证方式能够兼顾信息的安全性与高效性。



CN 106533696 B

1.一种基于区块链的身份认证方法,其特征在于,包括:

对用户终端发送的身份注册信息进行签名,将签名后的身份注册信息提供给所述用户终端;

接收所述用户终端根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求;

根据所述身份认证请求向所述用户终端返回身份认证信息;

接收所述智能合约根据所述用户终端提供的所述身份认证信息生成的程序运行结果,根据所述程序运行结果对所述用户终端的身份进行验证。

2.根据权利要求1所述的方法,其特征在于,所述根据所述身份认证请求向所述用户终端返回身份认证信息的步骤具体包括:

随机生成所述身份认证信息,将所述身份认证信息返回给所述用户终端;其中,所述身份认证信息包括:随机数和/或随机序列。

3.根据权利要求2所述的方法,其特征在于,所述智能合约根据所述用户终端提供的所述身份认证信息生成的程序运行结果具体包括:

智能合约根据所述身份认证信息执行写入操作后的写入操作结果,以及所述智能合约根据所述身份认证信息以及预存的认证服务器的公钥进行校验后的校验操作结果;

则所述根据所述程序运行结果对所述用户终端的身份进行验证的步骤具体包括:

当所述程序运行结果与所述身份认证信息匹配时,确定所述用户终端的身份验证结果为成功;

当所述程序运行结果与所述身份认证信息不匹配时,确定所述用户终端的身份验证结果为失败。

4.根据权利要求3所述的方法,其特征在于,所述根据所述程序运行结果对所述用户终端的身份进行验证的步骤之后,进一步包括步骤:将身份验证结果发送给所述用户终端。

5.根据权利要求1所述的方法,其特征在于,所述对用户终端发送的身份注册信息进行签名的步骤之前,进一步包括步骤:

将所述预设的智能合约广播到所述区块链中;其中,所述智能合约中预存有认证服务器的公钥,且所述智能合约用于对接收到的数据执行数据写入操作,并根据预存的认证服务器的公钥对已写入的数据执行数据校验操作。

6.根据权利要求1所述的方法,其特征在于,所述用户终端根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册的步骤具体包括:

用户终端将所述签名后的身份注册信息、认证服务器的区块链账户地址以及所述智能合约的区块链账户地址发送给所述智能合约;

所述智能合约根据所述认证服务器的区块链账户地址确定所述认证服务器的公钥,根据所述公钥对所述签名后的身份注册信息进行校验,并将校验结果提供给所述用户终端以及所述认证服务器。

7.根据权利要求1所述的方法,其中,所述身份认证请求包括:登录类型的身份认证请求以及注销类型的身份认证请求。

8.根据权利要求1所述的方法,其中,所述身份注册信息包括:用户终端的区块链账户地址或用户名。

9.一种基于区块链的身份认证方法,其特征在于,包括:

向认证服务器发送身份注册信息,接收所述认证服务器对所述身份注册信息进行签名后返回的签名后的身份注册信息;

根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册;

注册成功后向所述认证服务器发送身份认证请求,接收所述认证服务器返回的身份认证信息;

将所述身份认证信息提供给所述智能合约,以供所述智能合约根据所述身份认证信息生成程序运行结果,所述程序运行结果用于提供给所述认证服务器进行身份验证。

10.根据权利要求9所述的方法,其特征在于,所述根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册的步骤具体包括:

将所述签名后的身份注册信息、认证服务器的区块链账户地址以及所述智能合约的区块链账户地址发送给所述智能合约;

所述智能合约根据所述认证服务器的区块链账户地址确定所述认证服务器的公钥,根据所述公钥对所述签名后的身份注册信息进行校验,并将校验结果提供给用户终端以及所述认证服务器。

11.一种认证服务器,其特征在于,包括:

签名模块,用于对用户终端发送的身份注册信息进行签名,将签名后的身份注册信息提供给所述用户终端;

接收模块,用于接收所述用户终端根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求;

认证模块,用于根据所述身份认证请求向所述用户终端返回身份认证信息;

验证模块,用于接收所述智能合约根据所述用户终端提供的所述身份认证信息生成的程序运行结果,根据所述程序运行结果对所述用户终端的身份进行验证。

12.根据权利要求11所述的认证服务器,其中,所述认证模块具体用于:

随机生成所述身份认证信息,将所述身份认证信息返回给所述用户终端;其中,所述身份认证信息包括:随机数和/或随机序列。

13.根据权利要求12所述的认证服务器,其中,所述智能合约根据所述用户终端提供的所述身份认证信息生成的程序运行结果具体包括:

智能合约根据所述身份认证信息执行写入操作后的写入操作结果,以及所述智能合约根据所述身份认证信息以及预存的认证服务器的公钥进行校验后的校验操作结果;

则所述验证模块具体用于:

当所述程序运行结果与所述身份认证信息匹配时,确定所述用户终端的身份验证结果为成功;

当所述程序运行结果与所述身份认证信息不匹配时,确定所述用户终端的身份验证结果为失败。

14.根据权利要求13所述的认证服务器,其中,所述验证模块进一步用于:将身份验证结果发送给所述用户终端。

15.根据权利要求11所述的认证服务器,其中,所述认证服务器进一步包括:

广播模块,用于将所述预设的智能合约广播到所述区块链中;其中,所述智能合约中预

存有认证服务器的公钥，且所述智能合约用于对接收到的数据执行数据写入操作，并根据预存的认证服务器的公钥对已写入的数据执行数据校验操作。

16.根据权利要求11所述的认证服务器，其中，所述身份认证请求包括：登录类型的身份认证请求以及注销类型的身份认证请求。

17.根据权利要求11所述的认证服务器，其中，所述身份注册信息包括：用户终端的区块链账户地址或用户名。

18.一种用户终端，其特征在于，包括：

签名接收模块，用于向认证服务器发送身份注册信息，接收所述认证服务器对所述身份注册信息进行签名后返回的签名后的身份注册信息；

身份注册模块，用于根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册；

认证请求模块，用于注册成功后向所述认证服务器发送身份认证请求，接收所述认证服务器返回的身份认证信息；

认证信息传递模块，用于将所述身份认证信息提供给所述智能合约，以供所述智能合约根据所述身份认证信息生成程序运行结果，所述程序运行结果用于提供给所述认证服务器进行身份验证。

19.根据权利要求18所述的用户终端，其中，所述身份注册模块具体用于：

将所述签名后的身份注册信息、认证服务器的区块链账户地址以及所述智能合约的区块链账户地址发送给所述智能合约；

所述智能合约根据所述认证服务器的区块链账户地址确定所述认证服务器的公钥，根据所述公钥对所述签名后的身份注册信息进行校验，并将校验结果提供给所述用户终端以及所述认证服务器。

基于区块链的身份认证方法、认证服务器及用户终端

技术领域

[0001] 本申请实施例涉及身份识别技术领域，尤其涉及基于区块链的身份认证方法、认证服务器及用户终端。

背景技术

[0002] 身份认证，是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

[0003] 如图1所示，在传统第三方身份认证系统中，假设应用服务器A需要确认用户B的身份，主要流程如下：1.1、用户B向第三方认证服务器C发送身份认证请求，请求中包含应用服务器A要求的信息；1.2、第三方认证服务器C对收到的请求进行验证，通过后对应用服务器A要求的信息进行签名，然后将认证信息返回给用户B，认证信息包含上述的签名；1.3、用户B向应用服务器A发送认证信息，认证信息中包含上述的签名；1.4、应用服务器A根据签名对用户B的身份进行验证，最后向用户B返回认证结果。

[0004] 但是，发明人在实现本发明的过程中发现，现有技术中的方式至少存在下述问题：在传统第三方身份认证系统中，第三方认证服务器将收到用户登录应用服务器的信息，如果第三方认证服务器出现信息泄露将会对用户和应用服务器造成重大风险。

发明内容

[0005] 鉴于上述问题，提出了本申请实施例以便提供一种解决上述问题的基于区块链的身份认证方法、认证服务器及用户终端。

[0006] 依据本申请实施例的一个方面，提供了一种基于区块链的身份认证方法，包括：对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给用户终端；接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求；根据身份认证请求向用户终端返回身份认证信息；接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证。

[0007] 依据本申请实施例的另一个方面，提供了一种基于区块链的身份认证方法，包括：向认证服务器发送身份注册信息，接收认证服务器对身份注册信息进行签名后返回的签名后的身份注册信息；根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册；注册成功后向认证服务器发送身份认证请求，接收认证服务器返回的身份认证信息；将身份认证信息提供给智能合约，以供智能合约根据身份认证信息生成程序运行结果，程序运行结果用于提供给认证服务器进行身份验证。

[0008] 依据本申请实施例的另一个方面，提供了一种认证服务器，包括：签名模块，用于对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给用户终端；接

收模块，用于接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求；认证模块，用于根据身份认证请求向用户终端返回身份认证信息；验证模块，用于接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证。

[0009] 依据本申请实施例的另一个方面，提供了一种用户终端，包括：签名接收模块，用于向认证服务器发送身份注册信息，接收认证服务器对身份注册信息进行签名后返回的签名后的身份注册信息；身份注册模块，用于根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册；认证请求模块，用于注册成功后向认证服务器发送身份认证请求，接收认证服务器返回的身份认证信息；认证信息传递模块，用于将身份认证信息提供给智能合约，以供智能合约根据身份认证信息生成程序运行结果，程序运行结果用于提供给认证服务器进行身份验证。

[0010] 在本申请实施例提供的一种基于区块链的身份认证方法、认证服务器及用户终端中，能够将用户身份认证信息写入智能合约中，并利用区块链的智能合约来校验用户信息。由此一来，一方面，将认证信息上传区块链中的智能合约，能够有效利用区块链不易篡改、安全性高的优势；另一方面，由于区块链中的智能合约本身是一段可以自动运行的程序，可以根据输入参数自动验证合约中的信息，利用智能合约验证用户信息使得验证结构更为简单高效。由此可见，本申请实施例中的身份认证方式能够兼顾信息的安全性与高效性。

[0011] 上述说明仅是本申请实施例技术方案的概述，为了能够更清楚了解本申请实施例的技术手段，而可依照说明书的内容予以实施，并且为了让本申请实施例的上述和其它目的、特征和优点能够更明显易懂，以下特举本申请的具体实施方式。

附图说明

[0012] 一个或多个实施例通过与之对应的附图中的图片进行示例性说明，这些示例性说明并不构成对实施例的限定，附图中具有相同参考数字标号的元件表示为类似的元件，除非有特别申明，附图中的图不构成比例限制。

[0013] 图1是现有技术中身份认证方法的交互序列图；

[0014] 图2是本申请实施例一提供的一种基于区块链的身份认证方法的流程图；

[0015] 图3是本申请实施例二提供的一种基于区块链的身份认证方法的流程图；

[0016] 图4是本申请实施例三提供的一种基于区块链的身份认证方法的流程图；

[0017] 图5是本申请实施例四提供的一种认证服务器的结构示意图；

[0018] 图6是本申请实施例五提供的一种认证服务器的结构示意图；

[0019] 图7是本申请实施例六提供的一种用户终端的结构示意图；

[0020] 图8是本申请实施例提供的身份认证方法中身份注册流程的交互序列图；

[0021] 图9是本申请实施例提供的身份认证方法中身份认证流程的交互序列图。

具体实施方式

[0022] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围

完整的传达给本领域的技术人员。

[0023] 实施例一

[0024] 图2是本申请实施例一提供的一种基于区块链的身份认证方法的流程图。如图2所示，该方法包括：

[0025] 步骤S210：对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给用户终端。

[0026] 在本实施例中，为了避免用户终端的身份认证请求被劫持或者被冒名顶替，在进行认证操作前，需要将用户终端注册到区块链中的智能合约中。因此，需要对用户终端发送的身份注册信息进行签名，以保证身份注册信息的准确性和真实性，然后将签名后的身份注册信息提供给用户终端，方便其将签名后的身份注册信息发送给区块链中的智能合约。

[0027] 步骤S220：接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求。

[0028] 在步骤S220中，仅接收完成了身份注册的用户终端发送的身份认证请求，由此可以保证发送身份认证请求的用户终端是真实正确的用户终端，而非假冒伪装的用户终端。

[0029] 其中，智能合约是指一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。其中，承诺指的是合约参与方同意的(经常是相互的)权利和义务。这些承诺定义了合约的本质和目的；而数字形式表明智能合约建立的权利和义务，是由一台计算机或者计算机网络执行的。而区块链技术是比特币的底层技术，实质上是一个分布式的数据库账本，记载了所有的交易记录。区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性(防伪)和生成下一个区块。这项技术也因其安全、便捷的特性逐渐得到了银行与金融业的关注。目前越来越多的领域尝试使用区块链技术来解决现有的问题和不足。

[0030] 相应的，与区块链结合的智能合约是一段代码和数据的集合，部署在区块链网络上运行。同时智能合约有自己的区块链账户，在时间或事件的驱动下能自动执行一些功能，如可以在相互之间传递信息，修改区块链的状态比如账户信息等。与区块链结合的智能合约最大的特点是图灵完备，通俗来说可以完全模拟一台计算机所能做的所有事情。

[0031] 步骤S230：根据身份认证请求向用户终端返回身份认证信息。

[0032] 在收到用户终端发送的身份认证请求后，根据身份认证请求中的相关信息生成对应的身份认证信息，并将该身份认证信息返回给发送请求的用户终端。

[0033] 步骤S240：接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证。

[0034] 用户终端将上述身份认证信息发送到区块链中的智能合约中后，智能合约将执行写入数据操作，将上述身份认证信息写入到智能合约中。在智能合约完成写入数据操作后，接收其发送的程序运行结果，对上述程序运行结果进行比对验证，最后将身份验证结果发送给用户终端。由此完成整个身份认证过程。

[0035] 综上所述，本申请实施例提供的一种基于区块链的身份认证方法，一方面，将认证信息上传区块链中的智能合约，能够有效利用区块链不易篡改、安全性高的优势；另一方面，由于区块链中的智能合约本身是一段可以自动运行的程序，可以根据输入参数自动验证合约中的信息，利用智能合约验证用户信息使得验证结构更为简单高效。由此可见，本申

请实施例中的身份认证方式能够兼顾信息的安全性与高效性。

[0036] 实施例二

[0037] 图3是本申请实施例二提供的一种基于区块链的身份认证方法的流程图，该方法的执行主体优选为认证服务器。如图3所示，该方法包括：

[0038] 步骤S310：将预设的智能合约广播到区块链中。

[0039] 具体地，将预设的智能合约以区块链交易的形式广播到区块链网络上，经过多数节点的验证，使该智能合约达成区块链网络上的共识，然后该智能合约便可以运行在区块链网络上。其中，上述智能合约的结构分为四个部分，分别是智能合约区块链账户地址、预存的认证服务器公钥、数据部分和程序部分，且该智能合约的程序部分能够实现两个功能，一是向数据部分写入数据，即用于对接收到的数据执行数据写入操作；二是校验已写入数据部分中的数据，即根据预存的认证服务器的公钥与接收到的签名内容和签名来校验签名真伪。

[0040] 步骤S320：对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给用户终端。

[0041] 在本实施例中，为了避免用户终端的身份认证请求被劫持或者被冒名顶替，在进行认证操作前，需要将用户终端注册到区块链中的智能合约中。因此，需要对用户终端发送的身份注册信息进行签名，以保证身份注册信息的准确性和真实性，然后将签名后的身份注册信息提供给用户终端，方便其将签名后的身份注册信息发送给区块链中的智能合约。其中，上述身份注册信息包括但不限于用户终端的区块链账户或用户名。

[0042] 步骤S330：接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求。

[0043] 其中，用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册的步骤具体包括：用户终端将签名后的身份注册信息、认证服务器的区块链账户地址以及智能合约的区块链账户地址发送给智能合约；智能合约根据认证服务器的区块链账户地址确定认证服务器的公钥，根据公钥对签名后的身份注册信息进行校验，并将校验结果提供给用户终端以及认证服务器。

[0044] 在步骤S330中，仅接收完成了身份注册的用户终端发送的身份认证请求，由此可以保证发送身份认证请求的用户终端是真实正确的用户终端，而非假冒伪装的用户终端。其中，身份认证请求包括登录类型的身份认证请求以及注销类型的身份认证请求。

[0045] 步骤S340：根据身份认证请求向用户终端返回身份认证信息。

[0046] 具体地，在收到用户终端发送的身份认证请求后，随机生成身份认证信息，将身份认证信息返回给用户终端。其中，所述身份认证信息包括：随机数和/或随机序列。

[0047] 步骤S350：接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证。

[0048] 用户终端将上述身份认证信息发送到区块链中的智能合约中后，智能合约将执行写入数据操作，将上述身份认证信息写入到智能合约中。在智能合约完成写入数据操作后，接收其发送的程序运行结果，对上述程序运行结果进行比对验证，最后将身份验证结果发送给用户终端。由此完成整个身份认证过程。

[0049] 其中，程序运行结果具体包括：智能合约根据身份认证信息执行写入操作后的写

入操作结果，以及智能合约根据身份认证信息以及预存的认证服务器的公钥进行校验后的校验操作结果。对应地，上述根据程序运行结果对用户终端的身份进行验证的步骤具体包括：当程序运行结果与身份认证信息匹配时，确定用户终端的身份验证结果为成功；当程序运行结果与身份认证信息不匹配时，确定用户终端的身份验证结果为失败。

[0050] 综上所述，本申请实施例提供的一种基于区块链的身份认证方法能够将用户身份认证信息写入智能合约中，并利用区块链的智能合约来校验用户信息。由此一来，一方面，将认证信息上传区块链中的智能合约，能够有效利用区块链不易篡改、安全性高的优势；另一方面，由于区块链中的智能合约本身是一段可以自动运行的程序，可以根据输入参数自动验证合约中的信息，利用智能合约验证用户信息使得验证结构更为简单高效。由此可见，本申请实施例中的身份认证方式能够兼顾信息的安全性与高效性。

[0051] 实施例三

[0052] 图4是本申请实施例三提供的一种基于区块链的身份认证方法的流程图，图4所示的方法的执行主体可以为用户终端。如图4所示，该方法包括：

[0053] 步骤S410：向认证服务器发送身份注册信息，接收认证服务器对身份注册信息进行签名后返回的签名后的身份注册信息。

[0054] 在本实施例中，为了避免用户终端的身份认证请求被劫持或者被冒名顶替，在进行认证操作前，需要将用户终端注册到区块链中的智能合约中。因此，用户终端需要向认证服务器发送身份注册信息，并接收经过认证服务器签名后的身份注册信息。通过认证服务器的签名可以保证身份注册信息的准确性和真实性。

[0055] 步骤S420：根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册。

[0056] 具体地，将签名后的身份注册信息、认证服务器的区块链账户地址以及智能合约的区块链账户地址发送给智能合约；则智能合约根据认证服务器的区块链账户地址确定认证服务器的公钥，根据公钥对签名后的身份注册信息进行校验，并将校验结果提供给用户终端以及认证服务器。

[0057] 步骤S430：注册成功后向认证服务器发送身份认证请求，接收认证服务器返回的身份认证信息。

[0058] 在注册成功后，用户终端向认证服务器发送身份认证请求，该请求包括但不限于登录类型的请求和注销类型的请求。接收认证服务器返回的身份认证信息，该信息中包含了认证服务器随机生成的随机数和/或随机序列。

[0059] 步骤S440：将身份认证信息提供给智能合约，以供智能合约根据身份认证信息生成程序运行结果，程序运行结果用于提供给认证服务器进行身份验证。

[0060] 具体地，用户终端将身份认证信息发送给区块链网络中的智能合约，智能合约的程序部分根据该身份认证信息执行写入数据功能，将认证随机信息写入智能合约的数据部分，之后认证服务器将根据智能合约的程序运行结果对认证信息进行验证，最后将验证结果发送给用户终端。

[0061] 综上所述，本申请实施例提供的一种基于区块链的身份认证方法能够将用户身份认证信息写入智能合约中，并利用区块链的智能合约来校验用户信息。由此一来，一方面，将认证信息上传区块链中的智能合约，能够有效利用区块链不易篡改、安全性高的优势；另

一方面，由于区块链中的智能合约本身是一段可以自动运行的程序，可以根据输入参数自动验证合约中的信息，利用智能合约验证用户信息使得验证结构更为简单高效。由此可见，本申请实施例中的身份认证方式能够兼顾信息的安全性与高效性。

[0062] 为了便于理解本发明，下面结合两幅流程交互图进一步详细阐述上述方法的具体实现细节：

[0063] 图8是本申请实施例提供的身份认证方法中身份注册流程的交互序列图，具体流程为：8.1、用户终端向认证服务器发送身份注册请求，该请求包含身份注册信息，该身份注册信息中包括但不限于用户终端的区块链账户地址或用户名；8.2、认证服务器对身份注册信息中的信息进行签名，并将签名后的身份注册信息回复给用户终端；8.3、用户终端将注册所需的信息发送给区块链网络中的智能合约，该信息包括认证服务器的区块链账户地址、签名、所签名的内容和智能合约的区块链账户地址；8.4、智能合约的程序部分执行校验数据功能，将签名、所签名的内容和智能合约中预存的认证服务器公钥进行校验，最后将校验结果发送给用户终端。由此完成整个身份注册流程。

[0064] 图9是本申请实施例提供的身份认证方法中身份认证流程的交互序列图，具体流程为：9.1、用户终端向认证服务器发送身份认证请求，该请求包括但不限于登录和注销等类型，请求内容中包括用户终端的区块链账户地址；9.2、认证服务器收到认证请求后随即生成认证信息，并将随即生成的认证信息回复给用户终端，该认证信息可以是随机数或随即序列；9.3、用户终端将认证信息发送给区块链网络中的智能合约，此时智能合约的程序部分会执行数据写入功能，将认证信息写入智能合约的数据部分，该认证信息包括用户终端的区块链账户地址、随即生成的认证信息和智能合约的区块链账户地址；9.4、一旦智能合约的数据部分发生变化，认证服务器就会接收到由智能合约发送的认证结果(即数据信息和程序执行结果)；9.5、认证服务器根据接收到的数据信息和程序执行结果与认证服务器本地存储的认证信息进行对比验证，最后将认证结果发送给用户终端。由此完成整个身份认证流程。

[0065] 实施例四

[0066] 图5是本申请实施例四提供的一种认证服务器的结构示意图。如图5所示，该认证服务器包括：签名模块510、接收模块520、认证模块530和验证模块540。

[0067] 签名模块510，用于对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给所述用户终端。

[0068] 在本实施例中，为了避免用户终端的身份认证请求被劫持或者被冒名顶替，在进行认证操作前，需要将用户终端注册到区块链中的智能合约中。因此，签名模块510需要对用户终端发送的身份注册信息进行签名，以保证身份注册信息的准确性和真实性，然后将签名后的身份注册信息提供给用户终端，方便其将签名后的身份注册信息发送给区块链中的智能合约。

[0069] 接收模块520，用于接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求。

[0070] 接收模块520仅接收完成了身份注册的用户终端发送的身份认证请求，由此可以保证发送身份认证请求的用户终端是真实正确的用户终端，而非假冒伪装的用户终端。

[0071] 认证模块530，用于根据身份认证请求向用户终端返回身份认证信息。

[0072] 认证模块530在收到用户终端发送的身份认证请求后，根据身份认证请求中的相关信息生成对应的身份认证信息，并将该身份认证信息返回给发送请求的用户终端。

[0073] 验证模块540，用于接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证。

[0074] 用户终端将上述身份认证信息发送到区块链中的智能合约中后，智能合约将执行写入数据操作，将上述身份认证信息写入到智能合约中。在智能合约完成写入数据操作后，验证模块540接收智能合约发送的程序运行结果，对上述程序运行结果进行比对验证，最后将身份验证结果发送给用户终端。由此完成整个身份认证过程。

[0075] 由此可见，本申请实施例提供的一种身份认证服务器，一方面，将认证信息上传区块链中的智能合约，能够有效利用区块链不易篡改、安全性高的优势；另一方面，由于区块链中的智能合约本身是一段可以自动运行的程序，可以根据输入参数自动验证合约中的信息，利用智能合约验证用户信息使得验证结构更为简单高效。由此可见，本申请实施例中的身份认证方式能够兼顾信息的安全性与高效性。

[0076] 实施例五

[0077] 图6是本申请实施例五提供的一种认证服务器的结构示意图。如图6所示，该认证服务器包括：广播模块610、签名模块620、接收模块630、认证模块640和验证模块650。

[0078] 广播模块610，用于将预设的智能合约广播到区块链中。

[0079] 具体地，广播模块610将预设的智能合约以区块链交易的形式广播到区块链网络上，经过多数节点的验证，使该智能合约搭乘区块链网络上的共识，然后该智能合约便可以运行在区块链网络上。其中，上述智能合约的结构分为四个部分，分别是智能合约区块链账户地址、预存的认证服务器公钥、数据部分和程序部分，且该智能合约的程序部分能够实现两个功能，一是向数据部分写入数据，即用于对接收到的数据执行数据写入操作；二是校验已写入数据部分中的数据，即根据预存的认证服务器的公钥与接收到的签名内容和签名来校验签名真伪。

[0080] 签名模块620，用于对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给用户终端。

[0081] 在本实施例中，为了避免用户终端的身份认证请求被劫持或者被冒名顶替，在进行认证操作前，需要将用户终端注册到区块链中的智能合约中。因此，签名模块620需要对用户终端发送的身份注册信息进行签名，以保证身份注册信息的准确性和真实性，然后将签名后的身份注册信息提供给用户终端，方便其将签名后的身份注册信息发送给区块链中的智能合约。其中，上述身份注册信息包括但不限于用户终端的区块链账户或用户名。

[0082] 接收模块630，用于接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求。

[0083] 接收模块630仅接收完成了身份注册的用户终端发送的身份认证请求，由此可以保证发送身份认证请求的用户终端是真实正确的用户终端，而非假冒伪装的用户终端。其中，身份认证请求包括登录类型的身份认证请求以及注销类型的身份认证请求。

[0084] 认证模块640，用于根据身份认证请求向用户终端返回身份认证信息。

[0085] 具体地，认证模块640在收到用户终端发送的身份认证请求后，随机生成身份认证信息，将身份认证信息返回给用户终端。其中，所述身份认证信息包括：随机数和/或随机序

列。

[0086] 验证模块650，用于接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证。

[0087] 用户终端将上述身份认证信息发送到区块链中的智能合约中后，智能合约将执行写入数据操作，将上述身份认证信息写入到智能合约中。在智能合约完成写入数据操作后，验证模块650接收其发送的程序运行结果，对上述程序运行结果进行比对验证，最后将身份验证结果发送给用户终端。由此完成整个身份认证过程。

[0088] 其中，程序运行结果具体包括：智能合约根据身份认证信息执行写入操作后的写入操作结果，以及智能合约根据身份认证信息以及预存的认证服务器的公钥进行校验后的校验操作结果。对应地，验证模块650具体用于当程序运行结果与身份认证信息匹配时，确定用户终端的身份验证结果为成功；当程序运行结果与身份认证信息不匹配时，确定用户终端的身份验证结果为失败。

[0089] 上述各个模块的具体工作原理可参照方法实施例中相应步骤的描述，此处不再赘述。

[0090] 由此可见，本申请实施例提供的一种认证服务器能够将用户身份认证信息写入智能合约中，并利用区块链的智能合约来校验用户信息。由此一来，一方面，将认证信息上传区块链中的智能合约，能够有效利用区块链不易篡改、安全性高的优势；另一方面，由于区块链中的智能合约本身是一段可以自动运行的程序，可以根据输入参数自动验证合约中的信息，利用智能合约验证用户信息使得验证结构更为简单高效。由此可见，本申请实施例中的身份认证方式能够兼顾信息的安全性与高效性。

[0091] 实施例六

[0092] 图7是本申请实施例六提供的一种用户终端的结构示意图。如图7所示，该用户终端包括：签名接收模块710、身份注册模块720、认证请求模块730和认证信息传递模块740。

[0093] 签名接收模块710，用于向认证服务器发送身份注册信息，接收认证服务器对身份注册信息进行签名后返回的签名后的身份注册信息。

[0094] 在本实施例中，为了避免用户终端的身份认证请求被劫持或者被冒名顶替，在进行认证操作前，需要将用户终端注册到区块链中的智能合约中。因此，签名接收模块710需要向认证服务器发送身份注册信息，并接收经过认证服务器签名后的身份注册信息。通过认证服务器的签名可以保证身份注册信息的准确性和真实性。

[0095] 身份注册模块720，用于根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册。

[0096] 具体地，身份注册模块720将签名后的身份注册信息、认证服务器的区块链账户地址以及智能合约的区块链账户地址发送给智能合约；则智能合约根据认证服务器的区块链账户地址确定认证服务器的公钥，根据公钥对签名后的身份注册信息进行校验，并将校验结果提供给用户终端以及认证服务器。

[0097] 认证请求模块730，用于注册成功后向认证服务器发送身份认证请求，接收认证服务器返回的身份认证信息。

[0098] 在注册成功后，认证请求模块730向认证服务器发送身份认证请求，该请求包括但不限于登录类型的请求和注销类型的请求。认证请求模块730接收认证服务器返回的身份

认证信息，该信息中包含了认证服务器随机生成的随机数和/或随机序列。

[0099] 认证信息传递模块740，用于将身份认证信息提供给智能合约，以供智能合约根据身份认证信息生成程序运行结果，程序运行结果用于提供给认证服务器进行身份验证。

[0100] 具体地，认证信息传递模块740将身份认证信息发送给区块链网络中的智能合约，智能合约的程序部分根据该身份认证信息执行写入数据功能，将认证随机信息写入智能合约的数据部分，之后认证服务器将根据智能合约的程序运行结果对认证信息进行验证，最后将验证结果发送给用户终端。

[0101] 上述各个模块的具体工作原理可参照方法实施例中相应步骤的描述，此处不再赘述。

[0102] 综上所述，本申请实施例提供的一种用户终端能够将用户身份认证信息写入智能合约中，并利用区块链的智能合约来校验用户信息。由此一来，一方面，将认证信息上传区块链中的智能合约，能够有效利用区块链不易篡改、安全性高的优势；另一方面，由于区块链中的智能合约本身是一段可以自动运行的程序，可以根据输入参数自动验证合约中的信息，利用智能合约验证用户信息使得验证结构更为简单高效。由此可见，本申请实施例中的身份认证方式能够兼顾信息的安全性与高效性。

[0103] 此外，本领域的技术人员能够理解，尽管在此的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本申请实施例的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0104] 本申请实施例的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本申请实施例的装置中的一些或者全部部件的一些或者全部功能。本申请实施例还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本申请实施例的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0105] 应该注意的是上述实施例对本申请实施例进行说明而不是对本申请实施例进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本申请实施例可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

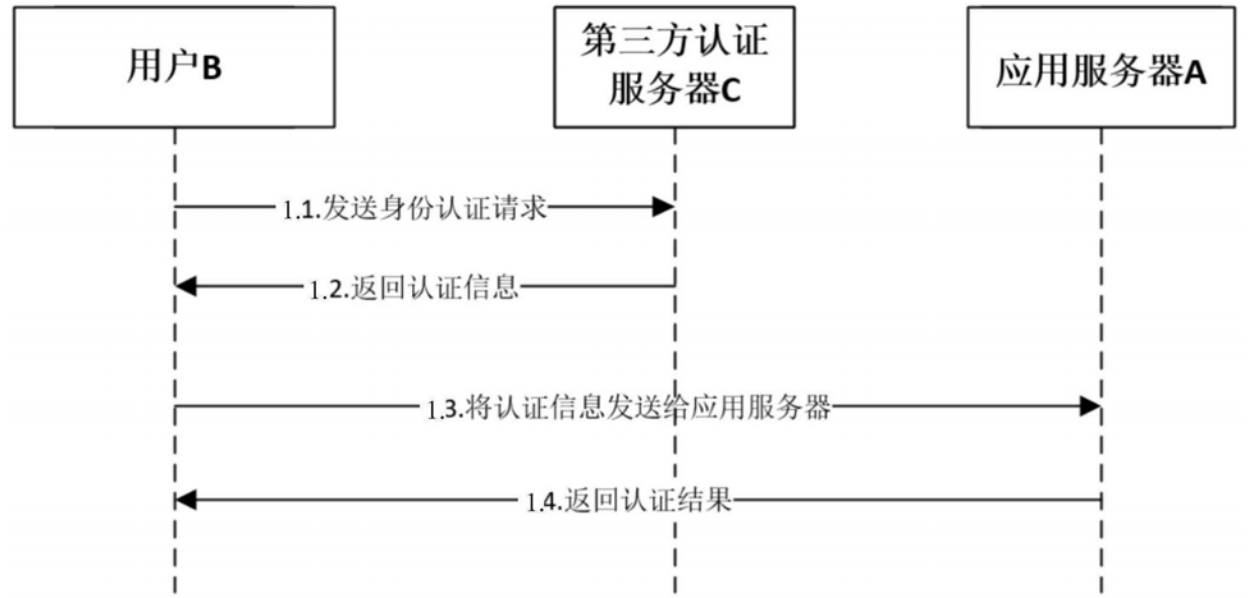

用户B
第三方认证服务器C
应用服务器A
1.1.发送身份认证请求
1.2.返回认证信息
1.3.将认证信息发送给应用服务器
1.4.返回认证结果

图1

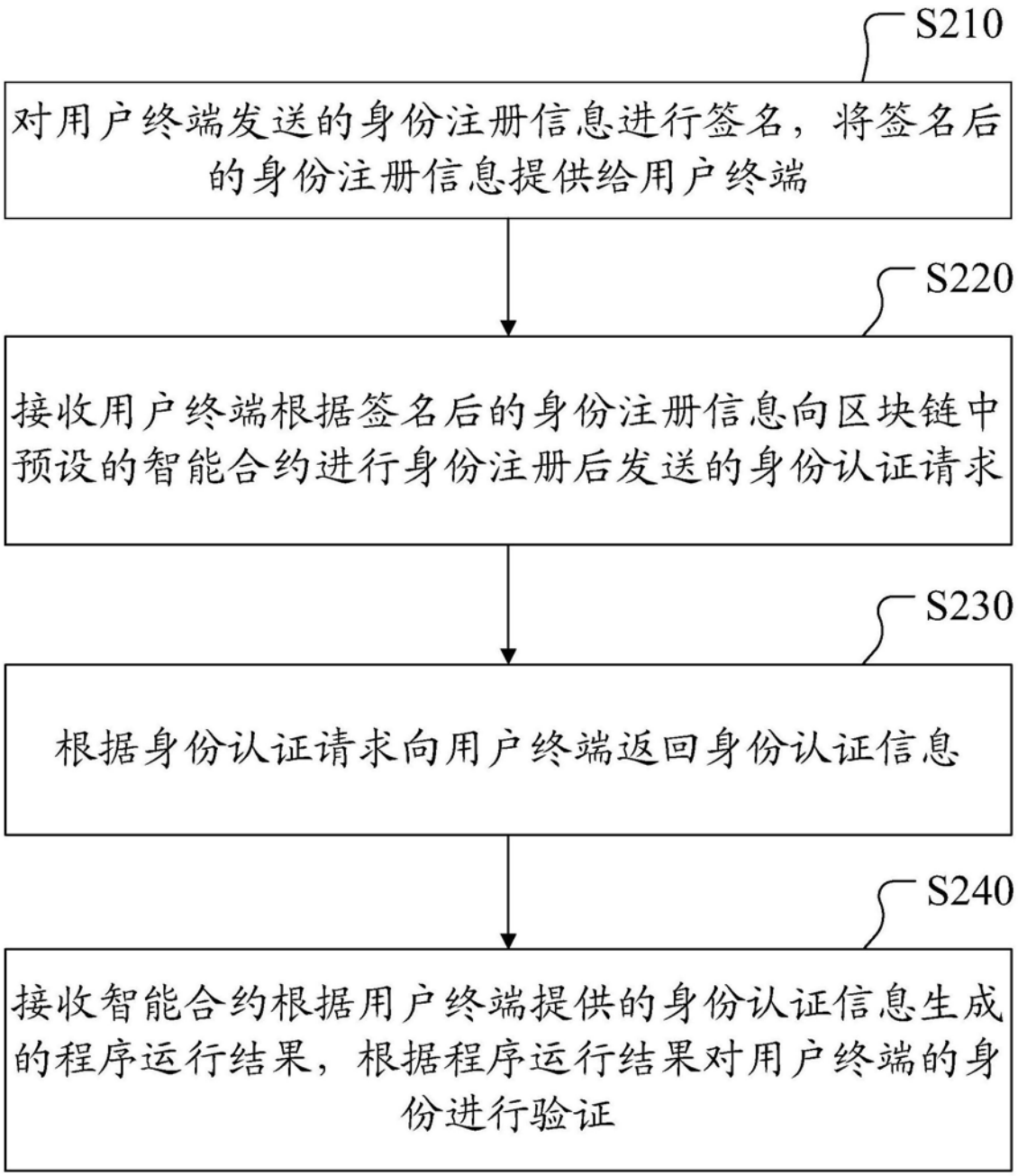

S210
对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给用户终端
S220
接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求
S230
根据身份认证请求向用户终端返回身份认证信息
S240
接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证

图2

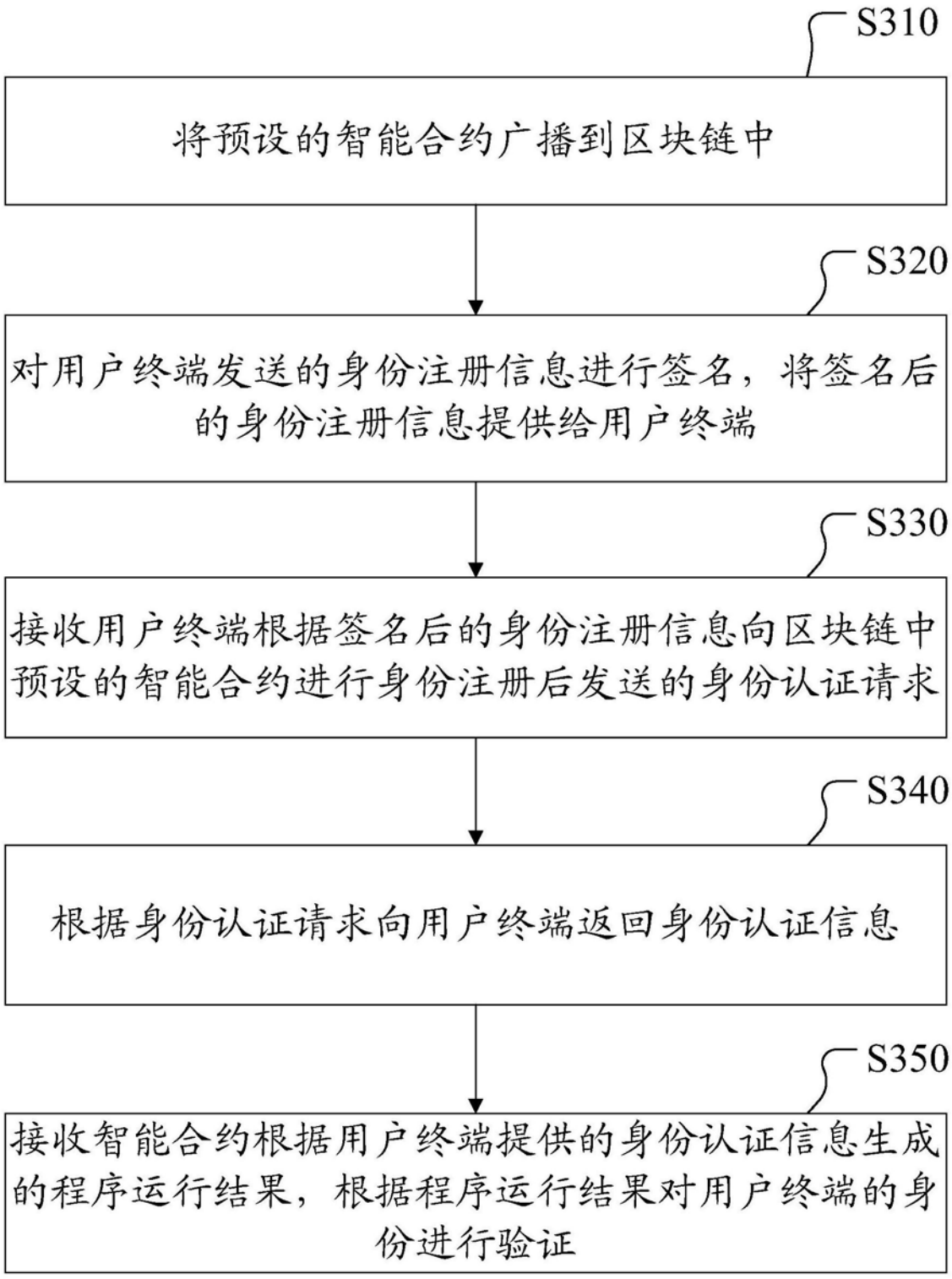

S310
将预设的智能合约广播到区块链中
S320
对用户终端发送的身份注册信息进行签名，将签名后的身份注册信息提供给用户终端
S330
接收用户终端根据签名后的身份注册信息向区块链中预设的智能合约进行身份注册后发送的身份认证请求
S340
根据身份认证请求向用户终端返回身份认证信息
S350
接收智能合约根据用户终端提供的身份认证信息生成的程序运行结果，根据程序运行结果对用户终端的身份进行验证

图3

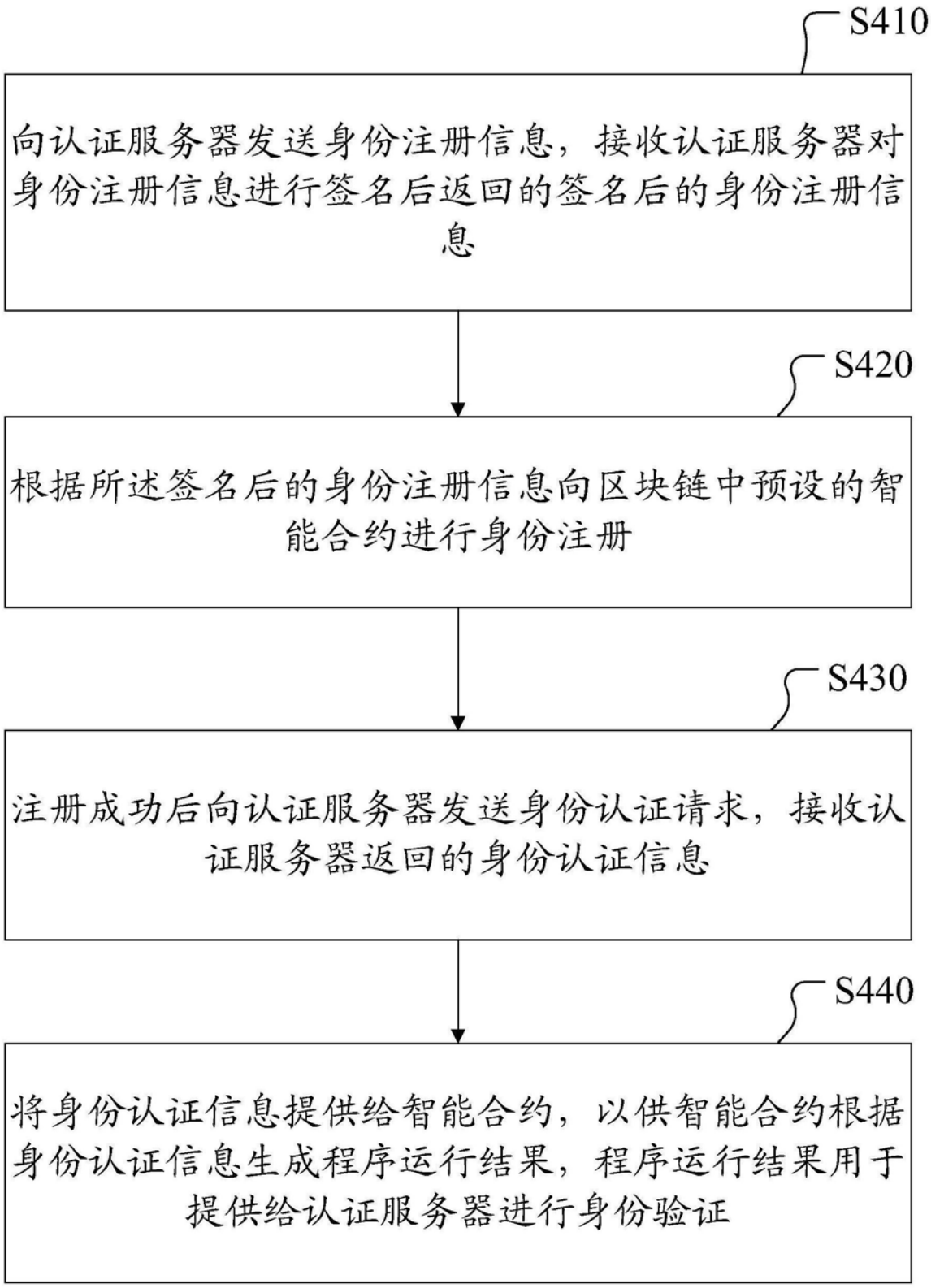

S410
向认证服务器发送身份注册信息，接收认证服务器对身份注册信息进行签名后返回的签名后的身份注册信息
S420
根据所述签名后的身份注册信息向区块链中预设的智能合约进行身份注册
S430
注册成功后向认证服务器发送身份认证请求，接收认证服务器返回的身份认证信息
S440
将身份认证信息提供给智能合约，以供智能合约根据身份认证信息生成程序运行结果，程序运行结果用于提供给认证服务器进行身份验证

图4

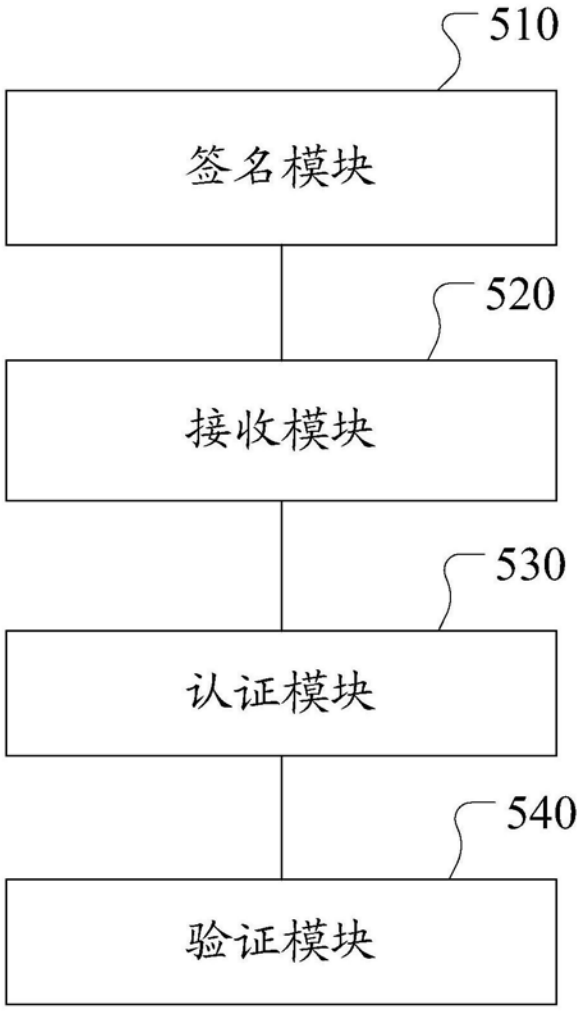


图5

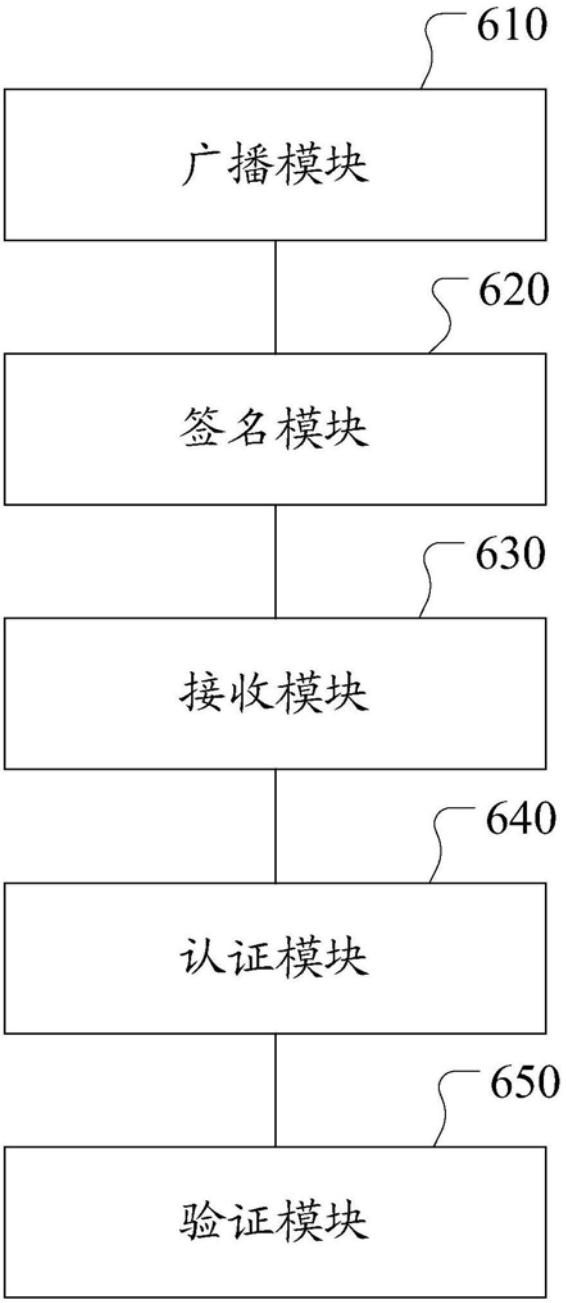


图6

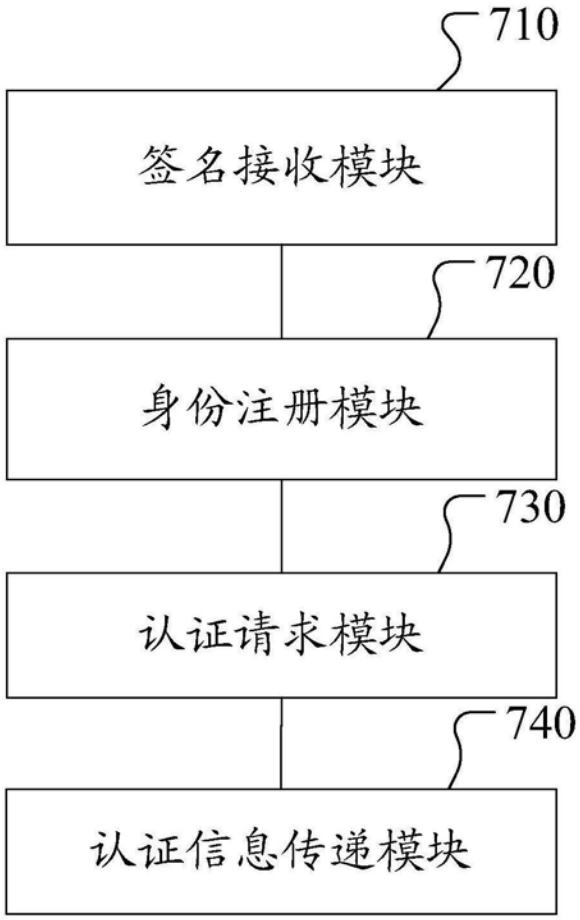

710
签名接收模块
720
身份注册模块
730
认证请求模块
740
认证信息传递模块

图7

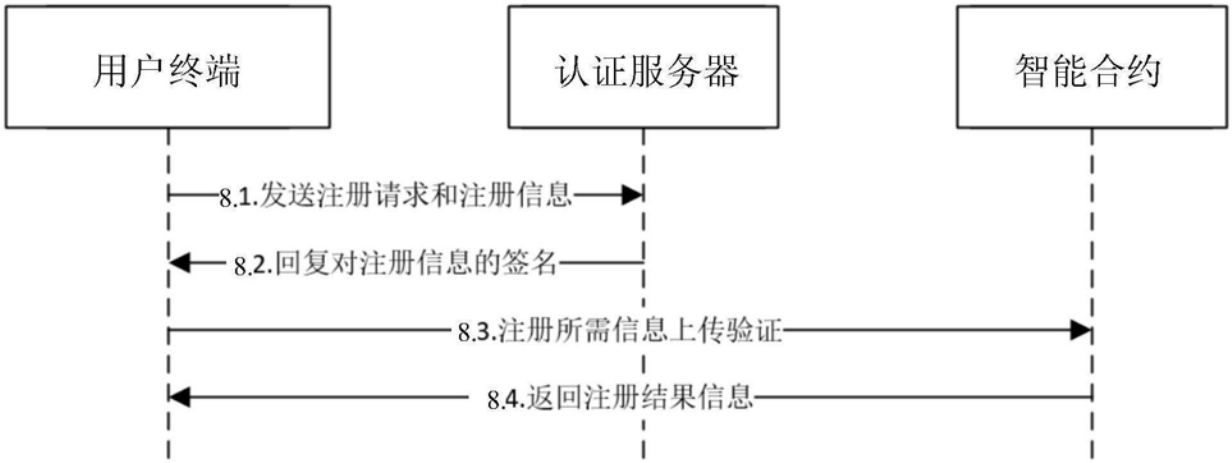

用户终端
认证服务器
智能合约
8.1.发送注册请求和注册信息
8.2.回复对注册信息的签名
8.3.注册所需信息上传验证
8.4.返回注册结果信息

图8

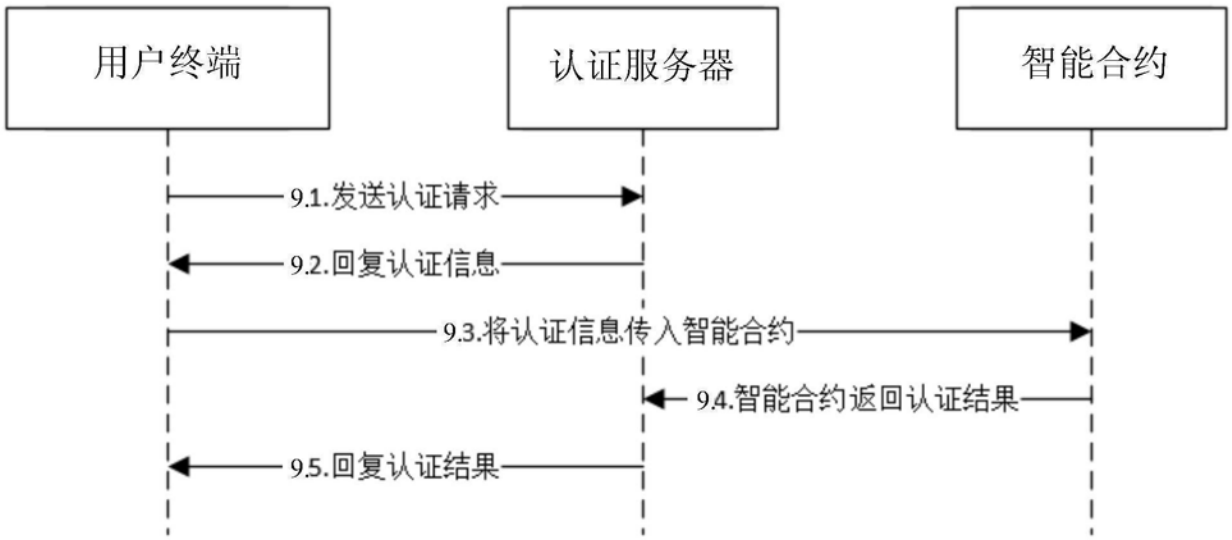

用户终端
认证服务器
智能合约
9.1.发送认证请求
9.2.回复认证信息
9.3.将认证信息传入智能合约
9.4.智能合约返回认证结果
9.5.回复认证结果

图9