(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 112311538 A
(43)申请公布日 2021.02.02

(21)申请号 202011194900.6

(22)申请日 2020.10.30

(71)申请人 北京华弘集成电路设计有限责任公司
地址 100015 北京市朝阳区高家园1号

(72)发明人 尹子栋 孙春桂 何江 王丽红 于佳良

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 刘晓菲

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)
G06F 21/46(2013.01)

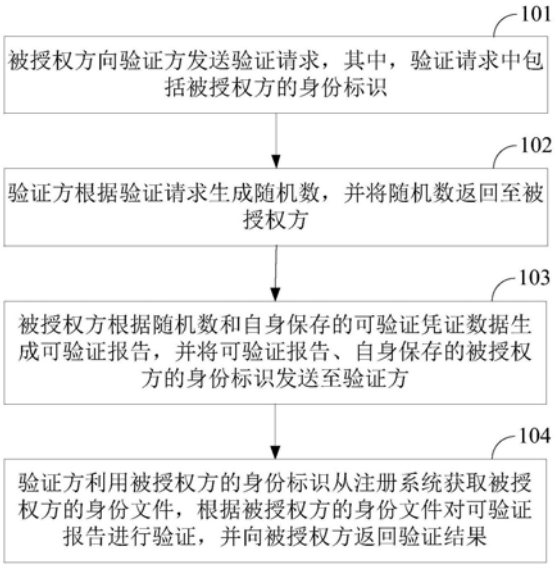
权利要求书3页 说明书33页 附图6页

(54)发明名称

一种身份验证的方法、装置、存储介质及设备

(57)摘要

本申请公开了一种身份验证的方法、装置、存储介质及设备，该方法包括：被授权方向验证方发送包括被授权方的身份标识的验证请求后，验证方可以根据该验证请求生成随机数，并将该随机数返回至被授权方。以便被授权方根据随机数和自身保存的可验证凭证数据生成可验证报告，并将该可验证报告、自身保存的被授权方的身份标识发送至验证方，从而验证方可以利用被授权方的身份标识从注册系统获取被授权方的身份文件，并根据被授权方的身份文件对可验证报告进行验证，并向被授权方返回验证结果。进而基于该注册系统具有的区块链的去中心化优势以及外界无法篡改的优势，可以有效提高被授权方身份验证结果的准确性和可靠性。



CN 112311538 A

1.一种身份验证的方法,其特征在于,应用于包括被授权方、验证方的身份授权区块链系统,所述身份授权区块链系统中部署有注册系统;所述方法包括:

所述被授权方向所述验证方发送验证请求,所述验证请求中包括所述被授权方的身份标识;

所述验证方根据所述验证请求生成随机数,并将所述随机数返回至所述被授权方;

所述被授权方根据所述随机数和自身保存的可验证凭证数据生成可验证报告,并将所述可验证报告、自身保存的被授权方的身份标识发送至所述验证方;

所述验证方利用所述被授权方的身份标识从所述注册系统获取所述被授权方的身份文件,根据所述被授权方的身份文件对所述可验证报告进行验证,并向所述被授权方返回验证结果。

2.根据权利要求1所述的方法,其特征在于,所述被授权方根据所述随机数和自身保存的可验证凭证数据生成可验证报告,具体包括:

所述被授权方使用自身保存的被授权方的私钥对所述随机数进行签名,得到第四签名数据;使用所述被授权方的私钥对所述可验证凭证数据进行签名,得到第五签名数据;

所述被授权方利用所述随机数、所述第四签名数据、所述可验证凭证数据、所述第五签名数据,生成所述可验证报告;

所述验证方根据所述被授权方的身份文件对所述可验证报告进行验证,具体包括:

所述验证方从所述被授权方的身份文件中获取被授权方的公钥,使用所述被授权方的公钥分别对所述第四签名数据和所述第五签名数据进行验签。

3.根据权利要求1或2所述的方法,其特征在于,在所述验证方根据所述被授权方的身份文件对所述可验证报告进行验证通过之后,所述验证方向所述被授权方返回验证结果之前,还包括:

所述验证方从所述可验证报告中获取所述可验证凭证数据,从获取的所述可验证凭证数据中提取授权方的身份标识和可验证凭证数据的标识,向所述注册系统发送所述授权方的身份标识和所述可验证凭证数据的标识;

所述注册系统检查所述被授权方的身份标识和所述可验证凭证数据的标识是否在有效可验证凭证数据列表中,并向所述验证方返回被授权方有效或失效的查询结果;

所述验证方根据所述查询结果向所述被授权方返回所述验证结果。

4.根据权利要求1所述的方法,其特征在于,所述身份授权区块链系统中部署有授权方;所述方法还包括:

所述被授权方从所述注册系统获取所述授权方的声明信息,根据自身保存的被授权方的身份标识请求所述授权方对所述被授权方进行身份验证,当所述授权方对所述被授权方的身份验证结果为通过时,根据所述授权方的声明信息生成身份授权请求,并向所述授权方发送所述身份授权请求;

所述授权方根据所述身份授权请求生成可验证凭证数据,并将所述可验证凭证数据中的可验证凭证数据的标识发送至所述注册系统;

所述注册系统根据所述可验证凭证数据的标识进行更新,并向所述授权方返回更新结果;

所述授权方将所述可验证凭证数据发送至所述被授权方,以便所述被授权方进行保

存。

5.根据权利要求4所述的方法，其特征在于，所述被授权方获取所述授权方的声明信息后，还包括：所述被授权方根据所述授权方的声明信息生成被授权方的声明数据；所述身份授权请求中包括所述被授权方的声明数据；

所述授权方生成可验证凭证数据，具体包括：

所述授权方根据预设规则生成所述可验证凭证数据的标识，并用自身保存的授权方的私钥对所述被授权方的声明数据进行签名，得到被授权方声明数据的签名；

所述授权方根据所述被授权方声明数据、所述被授权方声明数据的签名和所述可验证凭证数据的标识生成所述可验证凭证数据。

6.根据权利要求4所述的方法，其特征在于，所述授权方将所述可验证凭证数据发送至所述被授权方，以便所述被授权方进行保存，包括：

所述授权方将所述可验证凭证数据以及所述授权方的身份标识发送至所述被授权方；

所述被授权方根据所述可验证凭证数据的标识和所述授权方的身份标识向所述注册系统发送查询请求；

所述注册系统根据所述授权方的身份标识检索所述授权方的可验证凭证数据列表中是否存在所述可验证凭证数据的标识，若存在，则表明所述可验证凭证数据的标识有效，并将查询结果及所述授权方的身份标识对应的授权方的身份文件返回至所述被授权方；

所述被授权方根据所述授权方的身份文件对所述可验证凭证数据进行验证，若验证通过，则确认所述可验证凭证数据合法，并将其进行存储。

7.根据权利要求4所述的方法，其特征在于，所述被授权方根据所述授权方的声明信息向所述授权方发送身份授权请求之前，还包括：

所述被授权方生成第二随机数；所述身份授权请求中还包括所述第二随机数；

所述授权方将所述可验证凭证数据发送至所述被授权方，以便所述被授权方进行保存，具体包括：

所述授权方生成第三随机数，根据所述第二随机数、所述第三随机数、所述可验证凭证数据生成身份验证数据和所述可验证凭证数据的加密数据；将所述身份验证数据、所述可验证凭证数据的加密数据、自身保存的授权方身份标识发送给所述被授权方；

所述被授权方根据所述授权方的身份标识从所述注册系统获取授权方的身份文件；根据所述授权方的身份文件对所述身份验证数据进行验证，验证通过则对所述可验证凭证数据的加密数据进行解密得到所述可验证凭证数据，并对解密得到的所述可验证凭证数据进行保存。

8.根据权利要求4所述的方法，其特征在于，所述被授权方向所述授权方发送所述身份授权请求之前，还包括：所述被授权方设置安全标识，将所述安全标识的类型设置为明文回传或密文回传；所述身份授权请求中还包括所述安全标识；

所述授权方将所述可验证凭证数据发送至所述被授权方之前，还包括：所述被授权方判断所述安全标识的类型，当所述安全标识的类型为明文回传时，则将所述可验证凭证数据的明文数据发送给所述被授权方；当所述安全标识的类型为密文回传时，则将所述可验证凭证数据的密文数据发送给所述被授权方。

9.一种身份验证的装置，其特征在于，应用于包括被授权方、验证方的身份授权区块链

系统,所述身份授权区块链系统中部署有注册系统;所述装置包括:

所述被授权方,用于向所述验证方发送验证请求,所述验证请求中包括所述被授权方的身份标识;

所述验证方,用于根据所述验证请求生成随机数,并将所述随机数返回至所述被授权方;

所述被授权方,还用于根据所述随机数和自身保存的可验证凭证数据生成可验证报告,并将所述可验证报告、自身保存的被授权方的身份标识发送至所述验证方;

所述验证方,还用于利用所述被授权方的身份标识从所述注册系统获取所述被授权方的身份文件,根据所述被授权方的身份文件对所述可验证报告进行验证,并向所述被授权方返回验证结果。

10.一种身份验证的设备,其特征在于,所述设备包括处理器以及存储器:

所述存储器用于存储程序代码,并将所述程序代码传输给所述处理器;

所述处理器用于根据所述程序代码中的指令执行权利要求1-8任一项所述的方法。

11.一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用于存储计算机程序,所述计算机程序用于执行权利要求1-8任一项所述的方法。

一种身份验证的方法、装置、存储介质及设备

技术领域

[0001] 本申请涉及数据处理领域，特别是涉及一种身份验证的方法、装置、存储介质及设备。

背景技术

[0002] 目前，授权方与被授权方之间的身份授权方式通常是基于密钥对的方式，以希望提高身份授权的安全性和可靠性。例如：针对媒体平台(授权方)对用户(被授权方)的身份授权，在它们分别经证书机构(Certification Authority，CA)发布对应的数字证书后，可以基于该证书机构对它们之间的身份关系进行身份授权。其中，证书机构是认证机构的国际通称，它是对数字证书的申请者发放、管理、取消数字证书的机构。

[0003] 然而，在实际场景中，证书机构可能被恶意攻击或操控，由此可能将并不存在任何关联关系的两方进行身份授权，导致身份授权关系不可信，进而导致被授权方的身份验证结果不可信，造成后续无法对被授权方实施进一步的数据处理操作。

发明内容

[0004] 有鉴于此，本申请实施例提供一种身份验证的方法、装置、存储介质及设备，以提高被授权方身份验证结果的准确性和可靠性。

[0005] 第一方面，本申请实施例提供了一种身份验证的方法，应用于包括被授权方、验证方的身份授权区块链系统，所述身份授权区块链系统中部署有注册系统；所述方法包括：

[0006] 所述被授权方向所述验证方发送验证请求，所述验证请求中包括所述被授权方的身份标识；

[0007] 所述验证方根据所述验证请求生成随机数，并将所述随机数返回至所述被授权方；

[0008] 所述被授权方根据所述随机数和自身保存的可验证凭证数据生成可验证报告，并将所述可验证报告、自身保存的被授权方的身份标识发送至所述验证方；

[0009] 所述验证方利用所述被授权方的身份标识从所述注册系统获取所述被授权方的身份文件，根据所述被授权方的身份文件对所述可验证报告进行验证，并向所述被授权方返回验证结果。

[0010] 一种可能的实现方式中，所述被授权方根据所述随机数和自身保存的可验证凭证数据生成可验证报告，具体包括：

[0011] 所述被授权方使用自身保存的被授权方的私钥对所述随机数进行签名，得到第四签名数据；使用所述被授权方的私钥对所述可验证凭证数据进行签名，得到第五签名数据；

[0012] 所述被授权方利用所述随机数、所述第四签名数据、所述可验证凭证数据、所述第五签名数据，生成所述可验证报告；

[0013] 所述验证方根据所述被授权方的身份文件对所述可验证报告进行验证，具体包括：

[0014] 所述验证方从所述被授权方的身份文件中获取被授权方的公钥，使用所述被授权方的公钥分别对所述第四签名数据和所述第五签名数据进行验签。

[0015] 一种可能的实现方式中，所述使用所述被授权方的公钥分别对所述第四签名数据和所述第五签名数据进行验签，具体包括：

[0016] 所述验证方从所述可验证报告中获取所述随机数，使用所述被授权方的公钥和所述随机数对所述第四签名数据验签，验签通过，则使用所述被授权方公钥和所述可验证凭证数据对所述第五签名数据验签；

[0017] 或者，

[0018] 所述验证方使用所述被授权方的公钥和所述可验证凭证数据对所述第五签名数据验签，若验签通过，则从所述可验证报告中获取所述随机数，使用所述被授权方的公钥和所述随机数对所述第四签名数据验签。

[0019] 一种可能的实现方式中，在所述验证方根据所述被授权方的身份文件对所述可验证报告进行验证通过之后，所述验证方向所述被授权方返回验证结果之前，还包括：

[0020] 所述验证方从所述可验证报告中获取所述可验证凭证数据，从获取的所述可验证凭证数据中提取授权方的身份标识和可验证凭证数据的标识，向所述注册系统发送所述授权方的身份标识和所述可验证凭证数据的标识；

[0021] 所述注册系统检查所述被授权方的身份标识和所述可验证凭证数据的标识是否在有效可验证凭证数据列表中，并向所述验证方返回被授权方有效或失效的查询结果；

[0022] 所述验证方根据所述查询结果向所述被授权方返回所述验证结果。

[0023] 一种可能的实现方式中，所述身份授权区块链系统中部署有授权方；所述方法包括：

[0024] 所述被授权方从所述注册系统获取所述授权方的声明信息，根据自身保存的被授权方的身份标识请求所述授权方对所述被授权方进行身份验证，当所述授权方对所述被授权方的身份验证结果为通过时，根据所述授权方的声明信息生成身份授权请求，并向所述授权方发送所述身份授权请求；

[0025] 所述授权方根据所述身份授权请求生成可验证凭证数据，并将所述可验证凭证数据中的可验证凭证数据的标识发送至所述注册系统；

[0026] 所述注册系统根据所述可验证凭证数据的标识进行更新，并向所述授权方返回更新结果；

[0027] 所述授权方将所述可验证凭证数据发送至所述被授权方，以便所述被授权方进行保存。

[0028] 一种可能的实现方式中，所述被授权方根据自身保存的被授权方的身份标识请求所述授权方对所述被授权方进行身份验证，具体包括：

[0029] 所述被授权方根据所述被授权方的身份标识生成身份验证请求，并将所述身份验证请求发给所述授权方；

[0030] 所述授权方生成第一随机数，并将所述第一随机数返回给所述被授权方；

[0031] 所述被授权方根据自身保存的被授权方的私钥对所述第一随机数签名得到第一签名结果，将所述第一签名结果、所述第一随机数、所述被授权方的身份标识发给所述授权方；

[0032] 所述授权方根据所述被授权方的身份标识从所述注册系统获取所述被授权方的身份文件，从所述被授权方的身份文件中获取被授权方的公钥，使用获取的所述被授权方的公钥和所述第一随机数对所述第一签名结果进行验签。

[0033] 一种可能的实现方式中，所述被授权方从所述注册系统获取所述授权方的声明信息，具体包括：

[0034] 所述被授权方获取所述授权方的身份标识，向所述注册系统发送所述授权方的身份标识；

[0035] 所述注册系统根据所述授权方的身份标识，检索与所述授权方绑定的声明模板列表，并将其发送给所述被授权方。

[0036] 一种可能的实现方式中，所述被授权方根据所述授权方的声明信息生成身份授权请求，具体为：

[0037] 所述被授权方从所述授权方的声明模板列表中选择所需要的声明模板，根据选择的声明模板生成被授权方的声明数据，根据所述被授权方的声明数据生成所述身份授权请求。

[0038] 一种可能的实现方式中，所述被授权方获取所述授权方的声明信息后，还包括：所述被授权方根据所述授权方的声明信息生成被授权方的声明数据；所述身份授权请求中包括所述被授权方的声明数据；

[0039] 所述授权方生成可验证凭证数据，具体包括：

[0040] 所述授权方根据预设规则生成所述可验证凭证数据的标识，并用自身保存的授权方的私钥对所述被授权方的声明数据进行签名，得到被授权方声明数据的签名；

[0041] 所述授权方根据所述被授权方声明数据、所述被授权方声明数据的签名和所述可验证凭证数据的标识生成所述可验证凭证数据。

[0042] 一种可能的实现方式中，所述授权方将所述可验证凭证数据的标识发送至所述注册系统之前还包括：

[0043] 所述授权方使用所述授权方的私钥对所述可验证凭证数据的标识签名得到可验证凭证数据标识的签名；

[0044] 所述注册系统根据所述可验证凭证数据的标识进行更新之前，还包括：所述授权方将所述可验证凭证数据标识的签名、授权方的身份标识发送至所述注册系统；

[0045] 所述注册系统根据所述授权方的身份标识找到对应授权方的公钥，使用所述授权方的公钥和所述可验证凭证数据的标识对所述可验证凭证数据标识的签名进行验签。

[0046] 一种可能的实现方式中，所述注册系统根据所述可验证凭证数据的标识进行更新，具体为：当验签结果为通过时，所述注册系统将所述可验证凭证数据的标识添加到授权方的可验证凭证数据列表中。

[0047] 一种可能的实现方式中，所述授权方将所述可验证凭证数据发送至所述被授权方，以便所述被授权方进行保存，包括：

[0048] 所述授权方将所述可验证凭证数据以及所述授权方的身份标识发送至所述被授权方；

[0049] 所述被授权方根据所述可验证凭证数据的标识和所述授权方的身份标识向所述注册系统发送查询请求；

[0050] 所述注册系统根据所述授权方的身份标识检索所述授权方的可验证凭证数据列表中是否存在所述可验证凭证数据的标识，若存在，则表明所述可验证凭证数据的标识有效，并将查询结果及所述授权方的身份标识对应的授权方的身份文件返回至所述被授权方；

[0051] 所述被授权方根据所述授权方的身份文件对所述可验证凭证数据进行验证，若验证通过，则确认所述可验证凭证数据合法，并将其进行存储。

[0052] 一种可能的实现方式中，所述被授权方根据所述授权方的身份文件对所述可验证凭证数据进行验证，具体包括：

[0053] 所述被授权方从所述授权方的身份文件中获取授权方的公钥，使用所述授权方的公钥、所述可验证凭证数据中的被授权方声明数据对所述可验证凭证数据中的被授权方声明数据的签名进行验签。

[0054] 一种可能的实现方式中，所述授权方将所述可验证凭证数据发送至所述被授权方，以便所述被授权方进行保存，包括：

[0055] 所述授权方利用私钥对所述可验证凭证数据进行签名，并将签名后的可验证凭证数据发送至所述被授权方；

[0056] 所述被授权方向所述注册系统发送实体身份查询请求；

[0057] 所述注册系统将预先存储的实体的身份文件返回至所述被授权方；

[0058] 所述被授权方利用所述实体的身份文件，对所述签名后的可验证凭证数据进行验签，若验签成功，则确认所述可验证凭证数据合法；

[0059] 所述被授权方将确认所述可验证凭证数据合法的结果发送至所述注册系统进行查询，若所述注册系统查询到所述可验证凭证数据是有效的，则将查询结果返回至所述被授权方，以便所述被授权方存储所述可验证凭证数据。

[0060] 一种可能的实现方式中，所述被授权方根据所述授权方的声明信息向所述授权方发送身份授权请求之前，还包括：

[0061] 所述被授权方生成第二随机数；所述身份授权请求中还包括所述第二随机数；

[0062] 所述授权方将所述可验证凭证数据发送至所述被授权方，以便所述被授权方进行保存，具体包括：

[0063] 所述授权方生成第三随机数，根据所述第二随机数、所述第三随机数、所述可验证凭证数据生成身份验证数据和所述可验证凭证数据的加密数据；将所述身份验证数据、所述可验证凭证数据的加密数据、自身保存的授权方身份标识发送给所述被授权方；

[0064] 所述被授权方根据所述授权方的身份标识从所述注册系统获取授权方的身份文件；根据所述授权方的身份文件对所述身份验证数据进行验证，验证通过则对所述可验证凭证数据的加密数据进行解密得到所述可验证凭证数据，并对解密得到的所述可验证凭证数据进行保存。

[0065] 一种可能的实现方式中，所述授权方根据所述第二随机数和所述第三随机数、所述可验证凭证数据生成身份验证数据和所述可验证凭证数据的加密数据，具体包括：所述授权方使用所述授权方对所述被授权方进行身份验证时获取的所述被授权方的公钥对所述第三随机数加密，得到第三随机数的加密数据；

[0066] 所述授权方使用自身保存的授权方私钥对所述第三随机数签名，得到第三随机数

的签名；

[0067] 所述授权方根据所述第二随机数和所述第三随机数生成第一会话密钥，使用所述第一会话密钥对所述可验证凭证数据进行加密得到所述可验证凭证数据的加密数据。

[0068] 一种可能的实现方式中，所述被授权方根据所述授权方的身份文件对所述身份验证数据进行验证，具体包括：

[0069] 所述被授权方从所述授权方的身份文件中获取授权方的公钥，使用自身保存的被授权方的私钥对所述第三随机数的加密数据进行解密得到第一解密数据；

[0070] 所述被授权方使用所述授权方的公钥和所述第一解密数据对所述第三随机数的签名进行验签。

[0071] 一种可能的实现方式中，所述被授权方对所述可验证凭证数据的加密数据进行解密得到所述可验证凭证数据，并对解密得到的所述可验证凭证数据进行保存，具体包括：

[0072] 若验签成功，所述被授权方根据所述第二随机数和所述第一解密数据生成第二会话密钥；

[0073] 所述被授权方使用所述第二会话密钥对所述可验证凭证数据的加密数据解密，得到所述可验证凭证数据，从所述可验证凭证数据中提取被授权方的声明数据及所述被授权方的声明数据签名，使用所述授权方的公钥和提取的被授权方的声明数据对所述被授权方声明数据的签名进行验签，若验签通过，则对所述可验证凭证数据进行保存。

[0074] 一种可能的实现方式中，所述被授权方对所述可验证凭证数据进行保存之前，还包括：

[0075] 所述被授权方将所述可验证凭证数据中的可验证凭证数据的标识发送给所述注册系统，所述注册系统检查所述可验证凭证数据的标识是否有效；

[0076] 当验证结果为所述可验证凭证数据的标识有效，且所述被授权方对所述身份验证数据验证结果为通过时，所述被授权方对所述可验证凭证数据进行保存。

[0077] 一种可能的实现方式中，所述授权方根据所述身份授权请求生成可验证凭证数据之前，还包括：

[0078] 所述授权方根据所述被授权方发送的身份授权请求进行审核。

[0079] 一种可能的实现方式中，目标方为所述授权方或所述被授权方；所述方法还包括：

[0080] 所述目标方生成对应的身份标识和身份文件，并根据所述身份标识和所述身份文件向所述注册系统进行身份注册；所述身份文件中包括对应的验签公钥；

[0081] 所述注册系统对所述身份标识和所述身份文件进行审核，若通过审核，确定所述目标方完成身份注册，并保存所述目标方对应的身份文件。

[0082] 一种可能的实现方式中，所述目标方生成对应的身份标识和身份文件，包括：

[0083] 所述目标方获取当前时间并设定密钥对类型，并根据所述当前时间和所述密钥对类型，生成公钥和私钥；

[0084] 对所述公钥进行哈希运算，得到其对应的哈希值，并将所述哈希值作为所述目标方的身份标识；

[0085] 根据所述身份标识和所述公钥生成所述目标方的身份文件。

[0086] 一种可能的实现方式中，所述根据所述身份标识和所述身份文件向所述注册系统进行身份注册，包括：所述目标方将所述身份标识和所述身份文件发送至注册系统；

[0087] 所述注册系统对所述身份标识和所述身份文件进行审核，包括：

[0088] 所述注册系统确定所述身份标识是否存在于已保存的身份标识集合中，若否，向所述目标方发送随机标识。

[0089] 一种可能的实现方式中，在所述向所述目标方发送随机标识之后，所述方法还包括：

[0090] 所述目标方接收所述随机标识，并利用所述私钥对所述随机标识进行签名，得到第一签名数据；

[0091] 所述目标方将所述身份文件和所述随机标识以及所述第一签名数据发送至所述注册系统；

[0092] 所述注册系统根据所述身份文件对所述第一签名数据进行验签，若验签通过，确定所述目标方完成身份注册，并保存所述目标方对应的身份文件。

[0093] 一种可能的实现方式中，所述目标方生成所述身份文件后，还包括：所述目标方对所述身份文件进行保存；

[0094] 所述确定所述目标方完成身份注册之后，还包括：

[0095] 所述注册系统将身份标识的查询地址发送给所述目标方；

[0096] 所述目标方根据所述身份标识的查询地址对所述身份文件进行更新。

[0097] 一种可能的实现方式中，当目标方为所述授权方时，所述方法还包括：

[0098] 所述授权方生成授权方身份数据，并利用所述私钥对所述身份数据进行签名，得到第二签名数据；所述授权方身份数据为体现所述授权方具有身份授权权限的数据；

[0099] 所述授权方将所述身份文件和所述身份数据以及所述第二签名数据发送至所述注册系统；

[0100] 所述注册系统根据所述身份文件对所述第二签名数据进行验证，若通过验证，授予所述授权方的身份授权权限资格，并将所述身份授权权限资格保存至自身存储的身份文件中，以及将所述授权方的注册状态和身份查询地址发送至所述授权方；

[0101] 所述授权方将所述身份查询地址更新至自身存储的身份文件中。

[0102] 一种可能的实现方式中，所述方法还包括：

[0103] 所述授权方生成声明信息，并利用所述私钥对所述声明信息中的声明模板查询地址进行签名，得到第三签名数据；所述声明信息包括声明模板和声明模板查询地址；

[0104] 所述授权方将所述身份文件和所述声明信息中的声明模板查询地址以及所述第三签名数据发送至所述注册系统；

[0105] 所述注册系统根据自身保存的所述身份文件对所述第三签名数据进行验证，若通过验证，则将所述声明信息保存在自身存储的身份文件中，并向所述目标方返回所述声明信息的新增结果；

[0106] 所述目标方将所述声明模板查询地址更新至自身存储的身份文件中。

[0107] 一种可能的实现方式中，所述被授权方向所述授权方发送所述身份授权请求之前，还包括：所述被授权方设置安全标识，将所述安全标识的类型设置为明文回传或密文回传；所述身份授权请求中还包括所述安全标识；

[0108] 所述授权方将所述可验证凭证数据发送至所述被授权方之前，还包括：所述被授权方判断所述安全标识的类型，当所述安全标识的类型为明文回传时，则将所述可验证凭

证数据的明文数据发送给所述被授权方；当所述安全标识的类型为密文回传时，则将所述可验证凭证数据的密文数据发送给所述被授权方。

[0109] 第二方面，本申请实施例提供了一种身份验证的装置，应用于包括授权方和被授权方的身份授权区块链系统，所述身份授权区块链系统中部署有注册系统；所述装置包括：

[0110] 所述被授权方，用于向所述验证方发送验证请求，所述验证请求中包括所述被授权方的身份标识；

[0111] 所述验证方，用于根据所述验证请求生成随机数，并将所述随机数返回至所述被授权方；

[0112] 所述被授权方，还用于根据所述随机数和自身保存的可验证凭证数据生成可验证报告，并将所述可验证报告、自身保存的被授权方的身份标识发送至所述验证方；

[0113] 所述验证方，还用于利用所述被授权方的身份标识从所述注册系统获取所述被授权方的身份文件，根据所述被授权方的身份文件对所述可验证报告进行验证，并向所述被授权方返回验证结果。

[0114] 一种可能的实现方式中，所述被授权方具体用于

[0115] 使用自身保存的被授权方的私钥对所述随机数进行签名，得到第四签名数据；使用所述被授权方的私钥对所述可验证凭证数据进行签名，得到第五签名数据；

[0116] 利用所述随机数、所述第四签名数据、所述可验证凭证数据、所述第五签名数据，生成所述可验证报告；

[0117] 所述验证方具体用于：

[0118] 从所述被授权方的身份文件中获取被授权方的公钥，使用所述被授权方的公钥分别对所述第四签名数据和所述第五签名数据进行验签。

[0119] 一种可能的实现方式中，所述验证方具体用于：

[0120] 从所述可验证报告中获取所述随机数，使用所述被授权方的公钥和所述随机数对所述第四签名数据验签，验签通过，则使用所述被授权方公钥和所述可验证凭证数据对所述第五签名数据验签；

[0121] 或者，

[0122] 使用所述被授权方的公钥和所述可验证凭证数据对所述第五签名数据验签，若验签通过，则从所述可验证报告中获取所述随机数，使用所述被授权方的公钥和所述随机数对所述第四签名数据验签。

[0123] 一种可能的实现方式中，所述验证方还用于：

[0124] 从所述可验证报告中获取所述可验证凭证数据，从获取的所述可验证凭证数据中提取授权方的身份标识和可验证凭证数据的标识，向所述注册系统发送所述授权方的身份标识和所述可验证凭证数据的标识；

[0125] 所述注册系统还用于：检查所述被授权方的身份标识和所述可验证凭证数据的标识是否在有效可验证凭证数据列表中，并向所述验证方返回被授权方有效或失效的查询结果；

[0126] 所述验证方还用于：根据所述查询结果向所述被授权方返回所述验证结果。

[0127] 一种可能的实现方式中，所述身份授权区块链系统中部署有授权方；所述装置还包括：

[0128] 被授权方，用于从所述注册系统获取所述授权方的声明信息，根据自身保存的被授权方的身份标识请求所述授权方对所述被授权方进行身份验证，当所述授权方对所述被授权方的身份验证结果为通过时，根据所述授权方的声明信息生成身份授权请求，并向所述授权方发送所述身份授权请求；

[0129] 授权方，用于根据所述身份授权请求生成可验证凭证数据，并将所述可验证凭证数据中的可验证凭证数据的标识发送至所述注册系统；

[0130] 注册系统，用于根据所述可验证凭证数据的标识进行更新，并向所述授权方返回更新结果；

[0131] 所述授权方，还用于将所述可验证凭证数据发送至所述被授权方，以便所述被授权方进行保存。

[0132] 一种可能的实现方式中，所述被授权方具体用于：

[0133] 根据所述被授权方的身份标识生成身份验证请求，并将所述身份验证请求发给所述授权方；

[0134] 所述授权方具体用于：

[0135] 生成第一随机数，并将所述第一随机数返回给所述被授权方；

[0136] 所述被授权方还具体用于：

[0137] 根据自身保存的被授权方的私钥对所述第一随机数签名得到第一签名结果，将所述第一签名结果、所述第一随机数、所述被授权方的身份标识发给所述授权方；

[0138] 所述授权方还具体用于：

[0139] 根据所述被授权方的身份标识从所述注册系统获取所述被授权方的身份文件，从所述被授权方的身份文件中获取被授权方的公钥，使用获取的所述被授权方的公钥和所述第一随机数对所述第一签名结果进行验签。

[0140] 一种可能的实现方式中，所述被授权方具体用于：

[0141] 获取所述授权方的身份标识，向所述注册系统发送所述授权方的身份标识；

[0142] 所述注册系统具体用于：

[0143] 根据所述授权方的身份标识，检索与所述授权方绑定的声明模板列表，并将其发送给所述被授权方。

[0144] 一种可能的实现方式中，所述被授权方具体用于：

[0145] 从所述授权方的声明模板列表中选择所需要的声明模板，根据选择的声明模板生成被授权方的声明数据，根据所述被授权方的声明数据生成所述身份授权请求。

[0146] 一种可能的实现方式中，所述被授权方还用于根据所述授权方的声明信息生成被授权方的声明数据；所述身份授权请求中包括所述被授权方的声明数据；

[0147] 所述授权方具体用于：

[0148] 根据预设规则生成所述可验证凭证数据的标识，并用自身保存的授权方的私钥对所述被授权方的声明数据进行签名，得到被授权方声明数据的签名；

[0149] 根据所述被授权方声明数据、所述被授权方声明数据的签名和所述可验证凭证数据的标识生成所述可验证凭证数据。

[0150] 一种可能的实现方式中，所述授权方还用于：

[0151] 使用所述授权方的私钥对所述可验证凭证数据的标识签名得到可验证凭证数据

标识的签名；

[0152] 将所述可验证凭证数据标识的签名、授权方的身份标识发送至所述注册系统；

[0153] 所述注册系统具体用于：

[0154] 根据所述授权方的身份标识找到对应授权方的公钥，使用所述授权方的公钥和所述可验证凭证数据的标识对所述可验证凭证数据标识的签名进行验签。

[0155] 一种可能的实现方式中，当验签结果为通过时，所述注册系统具体用于将所述可验证凭证数据的标识添加到授权方的可验证凭证数据列表中。

[0156] 一种可能的实现方式中，所述授权方具体用于：

[0157] 将所述可验证凭证数据以及所述授权方的身份标识发送至所述被授权方；

[0158] 根据所述可验证凭证数据的标识和所述授权方的身份标识向所述注册系统发送查询请求；

[0159] 所述注册系统具体用于：

[0160] 根据所述授权方的身份标识检索所述授权方的可验证凭证数据列表中是否存在所述可验证凭证数据的标识，若存在，则表明所述可验证凭证数据的标识有效，并将查询结果及所述授权方的身份标识对应的授权方的身份文件返回至所述被授权方；

[0161] 所述被授权方还具体用于：

[0162] 根据所述授权方的身份文件对所述可验证凭证数据进行验证，若验证通过，则确认所述可验证凭证数据合法，并将其进行存储。

[0163] 一种可能的实现方式中，所述被授权方具体用于：、

[0164] 从所述授权方的身份文件中获取授权方的公钥，使用所述授权方的公钥、所述可验证凭证数据中的被授权方声明数据对所述可验证凭证数据中的被授权方声明数据的签名进行验签。

[0165] 一种可能的实现方式中，所述授权方具体用于：

[0166] 利用私钥对所述可验证凭证数据进行签名，并将签名后的可验证凭证数据发送至所述被授权方；

[0167] 向所述注册系统发送实体身份查询请求；

[0168] 所述注册系统具体用于：

[0169] 将预先存储的实体的身份文件返回至所述被授权方；

[0170] 所述被授权方还具体用于：

[0171] 利用所述实体的身份文件，对所述签名后的可验证凭证数据进行验签，若验签成功，则确认所述可验证凭证数据合法；

[0172] 将确认所述可验证凭证数据合法的结果发送至所述注册系统进行查询，若所述注册系统查询到所述可验证凭证数据是有效的，则将查询结果返回至所述被授权方，以便所述被授权方存储所述可验证凭证数据。

[0173] 一种可能的实现方式中，所述被授权方还用于：

[0174] 生成第二随机数；所述身份授权请求中还包括所述第二随机数；

[0175] 则所述授权方具体用于：

[0176] 生成第三随机数，根据所述第二随机数、所述第三随机数、所述可验证凭证数据生成身份验证数据和所述可验证凭证数据的加密数据；将所述身份验证数据、所述可验证凭

证数据的加密数据、自身保存的授权方身份标识发送给所述被授权方；

[0177] 所述被授权方还用于：根据所述授权方的身份标识从所述注册系统获取授权方的身份文件；根据所述授权方的身份文件对所述身份验证数据进行验证，验证通过则对所述可验证凭证数据的加密数据进行解密得到所述可验证凭证数据，并对解密得到的所述可验证凭证数据进行保存。

[0178] 一种可能的实现方式中，所述授权方具体用于：

[0179] 使用所述授权方对所述被授权方进行身份验证时获取的所述被授权方的公钥对所述第三随机数加密，得到第三随机数的加密数据；

[0180] 使用自身保存的授权方私钥对所述第三随机数签名，得到第三随机数的签名；

[0181] 根据所述第二随机数和所述第三随机数生成第一会话密钥，使用所述第一会话密钥对所述可验证凭证数据进行加密得到所述可验证凭证数据的加密数据。

[0182] 一种可能的实现方式中，所述被授权方具体用于：

[0183] 从所述授权方的身份文件中获取授权方的公钥，使用自身保存的被授权方的私钥对所述第三随机数的加密数据进行解密得到第一解密数据；

[0184] 使用所述授权方的公钥和所述第一解密数据对所述第三随机数的签名进行验签。

[0185] 一种可能的实现方式中，所述被授权方具体用于：

[0186] 若验签成功，则根据所述第二随机数和所述第一解密数据生成第二会话密钥；

[0187] 使用所述第二会话密钥对所述可验证凭证数据的加密数据解密，得到所述可验证凭证数据，从所述可验证凭证数据中提取被授权方的声明数据及所述被授权方的声明数据签名，使用所述授权方的公钥和提取的被授权方的声明数据对所述被授权方声明数据的签名进行验签，若验签通过，则对所述可验证凭证数据进行保存。

[0188] 一种可能的实现方式中，所述被授权方还用于：

[0189] 将所述可验证凭证数据中的可验证凭证数据的标识发送给所述注册系统，所述注册系统检查所述可验证凭证数据的标识是否有效；

[0190] 当验证结果为所述可验证凭证数据的标识有效，且所述被授权方对所述身份验证数据验证结果为通过时，对所述可验证凭证数据进行保存。

[0191] 一种可能的实现方式中，所述授权方还用于：

[0192] 根据所述被授权方发送的身份授权请求进行审核。

[0193] 一种可能的实现方式中，目标方为所述授权方或所述被授权方；所述目标方具体用于：

[0194] 生成对应的身份标识和身份文件，并根据所述身份标识和所述身份文件向所述注册系统进行身份注册；所述身份文件中包括对应的验签公钥；

[0195] 所述注册系统具体用于：对所述身份标识和所述身份文件进行审核，若通过审核，确定所述目标方完成身份注册，并保存所述目标方对应的身份文件。

[0196] 一种可能的实现方式中，所述目标方具体用于：

[0197] 获取当前时间并设定密钥对类型，并根据所述当前时间和所述密钥对类型，生成公钥和私钥；

[0198] 对所述公钥进行哈希运算，得到其对应的哈希值，并将所述哈希值作为所述目标方的身份标识；

[0199] 根据所述身份标识和所述公钥生成所述目标方的身份文件。

[0200] 一种可能的实现方式中，所述目标方具体用于：

[0201] 将所述身份标识和所述身份文件发送至注册系统；

[0202] 所述注册系统具体用于：确定所述身份标识是否存在于已保存的身份标识集合中，若否，向所述目标方发送随机标识。

[0203] 一种可能的实现方式中，所述目标方还用于：

[0204] 接收所述随机标识，并利用所述私钥对所述随机标识进行签名，得到第一签名数据；

[0205] 将所述身份文件和所述随机标识以及所述第一签名数据发送至所述注册系统；

[0206] 所述注册系统还用于：根据所述身份文件对所述第一签名数据进行验签，若验签通过，确定所述目标方完成身份注册，并保存所述目标方对应的身份文件。

[0207] 一种可能的实现方式中，所述目标方还用于：

[0208] 对所述身份文件进行保存；

[0209] 所述注册系统还用于：将身份标识的查询地址发送给所述目标方；

[0210] 所述目标方还用于：根据所述身份标识的查询地址对所述身份文件进行更新。

[0211] 一种可能的实现方式中，当目标方为所述授权方时，所述授权方还用于：

[0212] 生成授权方身份数据，并利用所述私钥对所述身份数据进行签名，得到第二签名数据；所述授权方身份数据为体现所述授权方具有身份授权权限的数据；

[0213] 将所述身份文件和所述身份数据以及所述第二签名数据发送至所述注册系统；

[0214] 所述注册系统还用于：根据所述身份文件对所述第二签名数据进行验证，若通过验证，授予所述授权方的身份授权权限资格，并将所述身份授权权限资格保存至自身存储的身份文件中，以及将所述授权方的注册状态和身份查询地址发送至所述授权方；

[0215] 所述授权方还用于：将所述身份查询地址更新至自身存储的身份文件中。

[0216] 一种可能的实现方式中，所述授权方还用于：

[0217] 生成声明信息，并利用所述私钥对所述声明信息中的声明模板查询地址进行签名，得到第三签名数据；所述声明信息包括声明模板和声明模板查询地址；

[0218] 将所述身份文件和所述声明信息中的声明模板查询地址以及所述第三签名数据发送至所述注册系统；

[0219] 所述注册系统还用于：根据自身保存的所述身份文件对所述第三签名数据进行验证，若通过验证，则将所述声明信息保存在自身存储的身份文件中，并向所述目标方返回所述声明信息的新增结果；

[0220] 所述目标方还用于：将所述声明模板查询地址更新至自身存储的身份文件中。

[0221] 一种可能的实现方式中，所述被授权方还用于：

[0222] 设置安全标识，将所述安全标识的类型设置为明文回传或密文回传；所述身份授权请求中还包括所述安全标识；

[0223] 判断所述安全标识的类型，当所述安全标识的类型为明文回传时，则将所述可验证凭证数据的明文数据发送给所述被授权方；当所述安全标识的类型为密文回传时，则将所述可验证凭证数据的密文数据发送给所述被授权方。

[0224] 由此可见，本申请实施例具有如下有益效果：

[0225] 由上述技术方案可以看出，用于身份验证的身份授权区块链系统包括已注册的被授权方和验证方，该身份授权区块链系统中部署有注册系统；被授权方向验证方发送包括被授权方的身份标识的验证请求后，验证方可以根据该验证请求生成随机数，并将该随机数返回至被授权方。以便被授权方根据随机数和自身保存的可验证凭证数据生成可验证报告，并将该可验证报告、自身保存的被授权方的身份标识发送至验证方，从而验证方可以利用被授权方的身份标识从注册系统获取被授权方的身份文件，并根据被授权方的身份文件对可验证报告进行验证，并向被授权方返回验证结果。进而基于该注册系统具有的区块链的去中心化优势以及外界无法篡改的优势，可以有效提高被授权方身份验证结果的准确性和可靠性。

附图说明

[0226] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0227] 图1为本申请实施例提供的一种身份验证的方法的流程图；

[0228] 图2为本申请实施例提供的身份授权方法的流程图；

[0229] 图3为本申请实施例提供的身份注册阶段的信令交互示例图；

[0230] 图4为本申请实施例提供的授权方身份注册的信令交互示例图；

[0231] 图5为本申请实施例提供的增加声明模板的信令交互示例图；

[0232] 图6为本申请实施例提供的一种身份验证的装置的结构框图。

具体实施方式

[0233] 下面结合附图，对本申请的实施例进行描述。

[0234] 目前，用于进行身份授权的证书机构可能被恶意攻击或操控，由此可能将并不存在任何关联关系的两方进行身份授权，导致身份授权关系不可信，进而导致被授权方的身份验证结果不可信，造成后续无法对被授权方实施进一步的数据处理操作。

[0235] 为此，本申请实施例提供了一种身份验证的系统，该系统基于区块链的去中心化优势以及外界无法篡改的优势，有效提高了被授权方身份验证结果的准确性和可靠性。接下来对本申请实施例提供的身份授权系统进行介绍。

[0236] 参见图1，该图示出了本申请实施例提供的一种身份验证的方法的流程图，如图1所示，该身份授权区块链系统包括已注册的被授权方(Holder)、注册系统和验证方(Verifier)。其中，被授权方可以是任意类型的实体设备(Entity)，可以是人、是设备，亦或是虚拟的网站等。例如，被授权方可以是用户、手机、物联网设备等。验证方(Verifier)指的是用于验证可验证凭证数据(Verifiable Credential，简称VC)的实体，可以是任意类型的实体设备(Entity)，可以是人、是设备，亦或是虚拟的网站等。例如，验证方可以是服务提供商等。利用该验证方和注册系统可以对被授权方的身份进行验证。

[0237] 该注册系统可以是身份授权区块链系统中部署的智能合约或者其他控制系统，需要说明的是，本申请后续实施例将以注册系统为智能合约为例进行介绍，其他控制系统的

实现方式可参见该智能合约的实现过程,其他实现过程不再一一赘述。其中,智能合约是指一种计算机协议,这类协议一旦制定和部署就能实现自我执行(self-executing)和自我验证(self-verifying),而且不再需要人为的干预。智能合约允许在没有第三方的情况下进行可信交易,这些交易可追踪且不可逆转。通过该系统中的智能合约的自动化及外界无法篡改的优势,以提高被授权方身份验证结果的准确性和可靠性。

[0238] 在本申请实施例中,进行身份验证的方法包括:

[0239] S101:被授权方向验证方发送验证请求,其中,验证请求中包括被授权方的身份标识。

[0240] S102:验证方根据验证请求生成随机数(nonce),并将随机数(nonce)返回至被授权方。

[0241] S103:被授权方根据随机数(nonce)和自身保存的可验证凭证数据生成可验证报告(Verifiable Presentation,简称VP),并将可验证报告、自身保存的被授权方的身份标识(此处可将其定义为DID_H)发送至验证方。

[0242] 其中,被授权方自身保存的可验证凭证数据(VC)是通过后续步骤S201-S204得到并保存的,具体获取过程可参见后续步骤S201-S204的详细介绍。

[0243] 具体来讲,在一种可能的实现方式中,本步骤S103中的“被授权方根据随机数(nonce)和自身保存的可验证凭证数据(VC)生成可验证报告(VP)”实现过程包括下述步骤S1031-S1032:

[0244] 步骤S1031:被授权方使用自身保存的被授权方的私钥对随机数(nonce)进行签名,得到签名数据(此处将其定义为第四签名数据)。并使用被授权方的私钥对可验证凭证数据(VC)进行签名,得到签名数据(此处将其定义为第五签名数据)。

[0245] 步骤S1032:被授权方利用随机数(nonce)、第四签名数据、可验证凭证数据(VC)、第五签名数据,生成可验证报告。

[0246] S104:验证方利用被授权方的身份标识(DID_H)从注册系统(即智能合约)获取被授权方的身份文件(DID Document),根据被授权方的身份文件(DID Document)对可验证报告(VP)进行验证,并向被授权方返回验证结果,以实现对被授权方的身份验证。

[0247] 需要说明的是,在一种可能的实现方式中,在通过上述步骤S1031-S1032生成可验证报告(VP)后,本步骤M4中的“验证方根据被授权方的身份文件(DID Document)对可验证报告(VP)进行验证”的具体实现过程为:验证方从被授权方的身份文件(DID Document)中获取被授权方的公钥,并使用该被授权方的公钥分别对得到的第四签名数据和第五签名数据进行验签。具体的验签过程包含以下两种实现方式:

[0248] 一种方式是验证方可以先从可验证报告(VP)中获取随机数(nonce),然后使用被授权方的公钥和随机数(nonce)对第四签名数据验签,并在验签通过时,使用被授权方公钥和可验证凭证数据(VC)对第五签名数据验签。

[0249] 另一种方式是验证方可以先使用被授权方的公钥和可验证凭证数据(VC)对第五签名数据验签,然后在验签通过时,可以从可验证报告(VP)中获取随机数(nonce),并使用被授权方的公钥和该随机数(nonce)对第四签名数据验签。

[0250] 需要说明的是,一种可选的实现方式是,为了提高被授权方身份验证结果的准确性,在执行上述步骤S104中,当验证方根据被授权方的身份文件(DID Document)对可验证

报告(VP)进行验证通过之后,还可以先执行下述步骤(1)-(3),然后向被授权方返回更加准确的验证结果。

[0251] 步骤(1):验证方先从可验证报告(VP)中获取可验证凭证数据(VC),然后从获取的可验证凭证数据(VC)中提取授权方的身份标识(DID_H)和可验证凭证数据的标识(VC_ID),接着,可以向注册系统(即智能合约)发送授权方的身份标识(DID_H)和可验证凭证数据的标识(VC_ID),用以执行后续步骤(2)。

[0252] 步骤(2):注册系统(即智能合约)检查被授权方的身份标识(DID_H)和可验证凭证数据的标识(VC_ID)是否在有效可验证凭证数据列表中,并向验证方返回被授权方有效或失效的查询结果,即,向验证方返回表明被授权方的可验证凭证数据的标识(VC_ID)是有效或失效的查询结果。

[0253] 步骤(3):验证方在接收到注册系统(即智能合约)返回的表明被授权方的可验证凭证数据的标识(VC_ID)是有效或失效的查询结果后,若判断出被授权方的可验证凭证数据的标识(VC_ID)是有效的,则可以向被授权方返回对可验证报告(VP)进行验证的验证结果,即,对被授权身份验证通过,完成VP的验证。但若判断出被授权方的可验证凭证数据的标识(VC_ID)是失效的,则不向被授权方返回对可验证报告(VP)进行验证的验证结果,即被授权身份验证不通过。

[0254] 综上,本实施例提供的一种身份验证的方法,用于身份验证的身份授权区块链系统包括已注册的被授权方和验证方,该身份授权区块链系统中部署有注册系统;被授权方向验证方发送包括被授权方的身份标识的验证请求后,验证方可以根据该验证请求生成随机数,并将该随机数返回至被授权方。以便被授权方根据随机数和自身保存的可验证凭证数据生成可验证报告,并将该可验证报告、自身保存的被授权方的身份标识发送至验证方,从而验证方可以利用被授权方的身份标识从注册系统获取被授权方的身份文件,并根据被授权方的身份文件对可验证报告进行验证,并向被授权方返回验证结果。进而基于该注册系统具有的区块链的去中心化优势以及外界无法篡改的优势,可以有效提高被授权方身份验证结果的准确性和可靠性。

[0255] 接下来,本申请实施例将对被授权方对应的可验证凭证数据(VC)的生成过程进行详细介绍:

[0256] 为了生成被授权方对应的可验证凭证数据(VC),实现被授权方的身份授权。首先在身份授权区块链系统中部署授权方。参见图2,该图示出了本申请实施例提供的身份授权方法的流程图,如图2所示,该身份授权区块链系统包括已注册的授权方(Issuer)、被授权方(Holder)和注册系统。其中,授权方可以向被授权方进行授权,该授权方可以是任意类型的实体设备(Entity),可以是人、是设备,亦或是虚拟的网站等。例如,授权方可以是服务提供商或设备生产商等。从而可以基于区块链的去中心化优势以及外界无法篡改的优势,生成被授权方对应的可验证凭证数据(VC),有效提高了授权方与被授权方间身份授权的安全性及可靠性。

[0257] 在本申请实施例中,进行被授权放的身份授权的方法包括:

[0258] S201:被授权方从注册系统获取授权方的声明信息,根据自身保存的被授权方的身份标识请求授权方对被授权方进行身份验证,当授权方对被授权方的身份验证结果为通过时,根据授权方的声明信息生成身份授权请求,并向授权方发送身份授权请求。

[0259] 其中,授权方的声明信息可以用于标识授权方的身份。

[0260] 例如,对于授权方为被授权方的生产方,该授权方的身份声明(Claim)可以包括授权方生成该被授权方设备的生产说明信息,即该身份声明标识了授权方的身份。

[0261] 在本申请实施例一些可能的实现方式中,本步骤S201中的“被授权方从注册系统获取授权方的声明信息”实现过程包括下述步骤A1-A2:

[0262] 步骤A1:被授权方获取授权方的身份标识,向注册系统发送授权方的身份标识。

[0263] 需要说明的是,授权方通常会通过公开渠道(如官方网站)公示自身对应的身份标识(Decentralized Identifier,简称DID)信息,此处将其定义为DID_I。而被授权方为了获取授权方的声明信息,首先需要通过上述公开渠道获取授权方的身份标识(DID_I),然后可以向注册系统(即智能合约)发送授权方的身份标识(DID_I)。

[0264] 步骤A2:注册系统根据授权方的身份标识,检索与授权方绑定的声明模板列表,并将其发送给被授权方。

[0265] 被授权方通过步骤A1向注册系统(即智能合约)发送授权方的身份标识(DID_I)后,注册系统(即智能合约)根据授权方对应的身份标识(DID_I),检索与该授权方绑定的声明模板列表,并将其发送给被授权方。

[0266] 进而,被授权方在接收到与授权方绑定的声明模板列表后,可以根据自身保存的被授权方的身份标识(DID_H)请求授权方对被授权方进行身份验证,具体验证过程如下步骤B1-B4:

[0267] 步骤B1:被授权方根据被授权方的身份标识生成身份验证请求,并将身份验证请求发给授权方。

[0268] 步骤B2:授权方生成第一随机数,并将该第一随机数返回给被授权方。

[0269] 授权方在接收到被授权方发送的身份验证请求后,首先生成第一随机数(此处可将其定义为r1),然后将该第一随机数(r1)返回给被授权方

[0270] 步骤B3:被授权方根据自身保存的被授权方的私钥对第一随机数(r1)签名得到第一签名结果,并将第一签名结果、第一随机数、被授权方的身份标识(DID_H)发给授权方。

[0271] 步骤B4:授权方根据被授权方的身份标识(DID_H)从注册系统(即智能合约)获取被授权方的身份文件(DID Document),并从被授权方的身份文件(DID Document)中获取被授权方的公钥,进而可以使用获取到的被授权方的公钥和第一随机数(r1)对接收到的第一签名结果进行验签。

[0272] 这样,当授权方对接收到的第一签名结果进行验签,得到的验签结果表明被授权方的身份验证结果为通过时,可以根据授权方的声明信息生成身份授权请求,并向授权方发送该身份授权请求。其中,具体的生成身份授权请求的过程为:被授权从授权方的声明模板列表中选择所需要的声明模板,根据选择的声明模板生成被授权方的声明数据(此处可将其定义为Claim_H),根据被授权方的声明数据生成身份授权请求。并将其发送给授权方,以请求对其进行身份授权。

[0273] S202:授权方根据身份授权请求生成可验证凭证数据,并将可验证凭证数据中的可验证凭证数据的标识发送至注册系统。

[0274] 在本实施例中,授权方在接收到被授权方发送的身份授权请求后,进一步可以根据该身份授权请求生成可验证凭证数据。其中,该可验证凭证数据可以是授权方为被授权

方进行授权时生成的数据,可以用于体现授权方对被授权方的身份授权。在一种可能的实现方式中,该可验证凭证数据包括可验证凭证(Verifiable Credential,VC)或可验证凭证标识。该可验证凭证可以是授权方根据被授权方的声明信息得到的,该可验证凭证标识可以是授权方通过预设的标识生成方式(用于为不同的被授权方生成对应的可验证凭证标识的方式)如一种随机数生成方式生成的。

[0275] 下面对可验证凭证的生成方式进行介绍。

[0276] 具体来讲,在一种可能的实现方式中,在被授权方获取到授权方的声明信息后,被授权方可以根据授权方的声明信息生成被授权方的声明数据;并且,身份授权请求中可以包括该被授权方的声明数据。这样,授权方生成可验证凭证数据的具体实现过程可以包括下述步骤C1-C2:

[0277] 步骤C1:授权方根据预设规则生成可验证凭证数据的标识,并用自身保存的授权方的私钥对被授权方的声明数据进行签名,得到被授权方声明数据的签名。

[0278] 步骤C2:授权方根据被授权方声明数据、被授权方声明数据的签名和可验证凭证数据的标识生成所述可验证凭证数据。

[0279] 具体来讲,授权方可以通过预设规则生成可验证凭证标识即VC_ID,并利用授权方自身保存的私钥对被授权方发送的身份授权请求中包含的自身的声明信息进行签名,得到被授权方声明数据的签名(此处将其定义为sign_claim)。进而可以根据被授权方声明数据、被授权方声明数据的签名(sign_claim)和可验证凭证数据的标识(VC_ID)生成可验证凭证数据。如可以通过将该声明数据的签名和可验证凭证标识组合排列,得到可验证凭证(后续简称VC)。

[0280] 需要说明的是,在实际应用中,通常只会将可验证凭证数据中的可验证凭证标识(即VC_ID)经过授权方的签名后,上传到区块链智能合约,用以执行后续步骤S103。其中,VC_ID是包含在VC数据中的,整个VC数据都会由授权方进行签名再发给被授权方,因此,VC_ID也是具备防篡改特性的,由其可以代替完整VC数据。

[0281] 还需要说明的是,授权方在接收到被授权方发送的身份授权请求后,在根据身份授权请求生成可验证凭证数据之前,还需要先根据被授权方发送的身份授权请求进行审核。比如,需要对被授权方的一些个人实名信息或者其社会属性信息,如姓名、身份证号、营业执照等进行审核,以保证被授权方是合法的,进而才能继续进行后续的身份授权操作步骤,进一步提高了授权方与被授权方间身份授权的安全性及可靠性。

[0282] 在具体实现中,该VC是由授权方如机构或组织颁发给授权方的,是对被授权方提供的声明的认证,授权方可在相关的应用使用该VC,以使除授权方外的服务提供商可通过API对被授权方出示的VC进行验证。

[0283] VC的基本组成可以包括:凭证元数据(Credential Metadata),Claims,证据(Proofs)。Credential Metadata是VC的一些属性,例如Issuer,时间戳等,并由Issuer签名。Claims:由Issuer定义,不同的claim type可能会有不同的字段,一个VC可能包含一个或一组claim。Proos通常是Issuers的数字签名。此外,每个VC也可以有对应的识别码(Identifier)。

[0284] 例如,下面为一个VC示例:

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  //VC 的编号、类型、签发人、签发时间、签发对象。
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "AlumniCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2010-01-01T19:73:24Z",
  "credentialSubject": "did:example:ebfeb1f712ebc6f1c276e12ec21",

//声明的内容
"claim": {
    "type": "alumniOf",
    "name": [{
        "value": "Example University",
        "lang": "en"
      },{
        "value": "Exemple d'Universit é ",
        "lang": "fr"
      }]
  },

//签发证明
  "proof": {
```

[0285]

"type": "RsaSignature2018",
"created": "2017-06-18T21:19:10Z",
"proofPurpose": "assertionMethod",
"verificationMethod": "https://example.edu/issuers/keys/1",
"jws":
"eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5XsI
TJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mg
RxD-WUcX16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb7
8cPN25DGlcTwLtjPAYuNzVBAh4vGHSrQyHUdBBPM"
}
}

[0287] S203:注册系统根据可验证凭证数据的标识进行更新,并向授权方返回更新结果。

[0288] 其中,授权方将可验证凭证数据的标识包含在可验证凭证数据发送至智能合约(即注册系统),以在智能合约进行保存,并更新授权方的有效可验证凭证数据列表,并向授权方返回更新结果。由于该可验证凭证数据的标识不携带有被授权方的身份信息,由此可以防止被授权方的身份数据产生泄露,保证了数据安全性。

[0289] 此外,也可以将可验证凭证作为可验证凭证数据发送至智能合约(即注册系统),以在智能合约进行保存,并更新授权方的有效可验证凭证数据列表,并向授权方返回更新结果。

[0290] 需要说明的是,在一种可能的实现方式中,授权方将可验证凭证数据的标识发送至注册系统之前,授权方还可以使用授权方的私钥对可验证凭证数据的标识签名得到可验证凭证数据标识的签名,由此,在执行本步骤S103中的“注册系统根据可验证凭证数据的标识进行更新”之前,还可以执行下述步骤D1-D2:

[0291] 步骤D1:授权方将可验证凭证数据标识的签名、授权方的身份标识发送至注册系统。

[0292] 步骤D2:注册系统根据授权方的身份标识找到对应授权方的公钥,使用授权方的公钥和可验证凭证数据的标识对可验证凭证数据标识的签名进行验签。

[0293] 进而使得本步骤S103中的“注册系统根据可验证凭证数据的标识进行更新”的具体实现过程为:当验签结果为通过时,注册系统将可验证凭证数据的标识添加到授权方的可验证凭证数据列表中。

[0294] S204:授权方将可验证凭证数据发送至被授权方,以便被授权方进行保存。

[0295] 在本实施例中,授权方在根据身份授权请求生成可验证凭证数据后,可将其发送至被授权方,以便被授权方进行保存,从而能够实现被授权方的身份授权。

[0296] 需要说明的是,被授权方在向授权方发送身份授权请求之前,还可以设置安全标识,并将安全标识的类型设置为明文回传或密文回传。同时,将该安全标识设置在身份授权请求中,即使得身份授权请求中也包括该安全标识。这样,授权方在将可验证凭证数据发送至被授权方之前,可以先判断安全标识的类型,当安全标识的类型为明文回传时,则将可验

证凭证数据的明文数据发送给被授权方;当安全标识的类型为密文回传时,则将可验证凭证数据的密文数据发送给被授权方。以根据实际情况,分别通过这两种实现方式将可验证凭证数据发送至被授权方,以实现对被授权方的身份授权。

[0297] 并且,为了便于理解技术方案,下面以一个具体场景为例进行举例说明,一般而言,DIDs技术的使用流程为:

[0298] 在场景中包括:被授权方(Subject/Holder),授权方(Issuer),验证方(Verifier)和可验证数据凭证注册表(Verifiable Data Registry)。Subject是指产生Claims的Entity,也是VC对应的Entity。Holder即为被授权方,通常和Subject是同一个Entity。Issuer为颁发VC给Holder的Entity(即授权方),需要对Holder提交的针对Subject的Claim进行认证。Verifier是验证VC的Entity,一般是服务提供商。Verifiable Data Registry是所有Entity都能访问到的某种数据库,比如区块链,辅助DID的生成、注册、VC的注册、查询、撤销,Issuer公钥的注册等。

[0299] 在该示例中,Subject、Issuer和Verifier可以分别在身份授权区块链系统中的智能合约(即DIDs智能合约)上注册DID。且Issuer可以注册成为权威(Authority),即授权方。Verifier可以定义自身接受的Claim数据结构。Subject生成Claim,并提交给Issuer认证。Issuer首先通过Subject的DID Document上记录的认证方式对Subject进行身份认证。Issuer再对Claim进行认证,并签名。然后生成VC,将VC的哈希摘要添加到区块链智能合约上的VC列表中。Verifier首先通过DID Document认证Subject身份,再通过区块链上的VC或VC标识确认VC的合法性和有效性。

[0300] 综上,用于身份授权的身份授权区块链系统包括已注册的授权方和被授权方,该身份授权区块链系统中部署有注册系统;被授权方从注册系统获取授权方的声明信息,并根据自身保存的被授权方的身份标识请求授权方对被授权方进行身份验证,当授权方对被授权方的身份验证结果为通过时,根据授权方的声明信息生成身份授权请求,并向授权方发送身份授权请求;授权方根据该身份授权请求生成可验证凭证数据,并将其中的可验证凭证数据的标识发送至注册系统,以便注册系统根据该可验证凭证数据的标识进行更新,并向授权方返回更新结果;授权方还可以将可验证凭证数据发送至被授权方,以便被授权方进行保存。从而基于该注册系统具有的区块链的去中心化优势以及外界无法篡改的优势,可以有效提高授权方与被授权方间身份授权的安全性及可靠性,进而能够保证身份授权关系可信。并解决了传统平台账号认证以及第三方账号认证存在的问题。

[0301] 接下来,本申请实施例将对上述步骤S204中“授权方将可验证凭证数据发送至被授权方,以便被授权方进行保存”的两种实现方式进行介绍:

[0302] (1)授权方将可验证凭证数据以明文数据的形式发送至被授权方,以便被授权方进行保存。具体可以包括下属步骤E1-E4:

[0303] 步骤E1:授权方将可验证凭证数据以及授权方的身份标识发送至被授权方。

[0304] 在本实施例中,若授权方在将可验证凭证数据发送至被授权方之前,先判断出安全标识的类型为明文回传,则可以将可验证凭证数据以及授权方的身份标识(DID_I)的明文数据发送给被授权方。

[0305] 步骤E2:被授权方根据所述可验证凭证数据的标识和授权方的身份标识向注册系统发送查询请求。

[0306] 在本实施例中，被授权方接收到授权方发送的可验证凭证数据以及授权方的身份标识(DID_I)后，进一步，可以根据可验证凭证数据的标识(VC_ID)和授权方的身份标识(DID_I)向注册系统发送查询请求，用以查询可验证凭证数据的标识(VC_ID)和授权方的身份标识(DID_I)的有效性。

[0307] 步骤E3：注册系统根据授权方的身份标识检索授权方的可验证凭证数据列表中是否存在可验证凭证数据的标识，若存在，则表明可验证凭证数据的标识有效，并将查询结果及授权方的身份标识对应的授权方的身份文件返回至被授权方。

[0308] 步骤E4：被授权方根据授权方的身份文件对可验证凭证数据进行验证，若验证通过，则确认可验证凭证数据合法，并将其进行存储。

[0309] 具体来讲，被授权方可以从授权方的身份文件中获取授权方的公钥，保密柜使用该授权方的公钥、可验证凭证数据中的被授权方声明数据对可验证凭证数据中的被授权方声明数据的签名进行验签，并在验签结果表明验证凭证数据验证通过后，确认可验证凭证数据合法，并将其进行存储。

[0310] 举例说明：被授权方的实体程序从授权方的身份文件中获取公钥(pubKey_I)，再通过安全模块(如被授权方的芯片或SIM卡)对可验证凭证数据中的被授权方声明数据(claim_H)的签名(sign_claim_H)进行验签，并将验签结果返回至实体程序，若验签成功，则实体程序可以确定可验证凭证数据的合法性，进一步可以将包含可验证凭证数据的标识(VC_ID)的可验证凭证数据发送至安全模块进行存储，之后安全模块再将存储结果返回至实体程序。

[0311] (2)授权方将可验证凭证数据以密文数据的形式发送至被授权方，以便被授权方进行保存。

[0312] 在第一种实现方式中，授权方将可验证凭证数据以密文数据的形式发送至被授权方，以便被授权方进行保存的具体实现过程可以包括下述步骤F1-F5：

[0313] 步骤F1：授权方利用私钥对可验证凭证数据进行签名，并将签名后的可验证凭证数据发送至被授权方。

[0314] 在本实施例中，若授权方在将可验证凭证数据发送至被授权方之前，先判断出安全标识的类型为密文回传，则可以将可验证凭证数据的密文数据发送给被授权方，具体来讲，授权方首先可以利用私钥对可验证凭证数据进行签名(如数字签名)，然后再将签名后的可验证凭证数据发送至被授权方。

[0315] 步骤F2：被授权方向注册系统发送实体身份查询请求。

[0316] 在本实施例中，被授权方接收到授权方发送的签名后的可验证凭证数据后，进一步，可以向注册系统发送实体身份查询请求。

[0317] 步骤F3：注册系统将预先存储的实体的身份文件返回至被授权方。

[0318] 步骤F4：被授权方利用实体的身份文件，对签名后的可验证凭证数据进行验签，若验签成功，则确认可验证凭证数据合法。

[0319] 步骤F5：被授权方将确认可验证凭证数据合法的结果发送至注册系统进行查询，若注册系统查询到可验证凭证数据是有效的，则将查询结果返回至被授权方，以便被授权方存储可验证凭证数据。

[0320] 在第二种实现方式中，被授权方预先生成了第二随机数，并将该第二随机数设置

在身份授权请求中，即使得身份授权请求中包括了第二随机数。则授权方将可验证凭证数据以密文数据的形式发送至被授权方，以便被授权方进行保存的具体实现过程可以包括下述步骤G1-G2：

[0321] 步骤G1：授权方生成第三随机数，并根据第二随机数、第三随机数、可验证凭证数据生成身份验证数据和可验证凭证数据的加密数据；进而将身份验证数据、可验证凭证数据的加密数据、自身保存的授权方身份标识密文返回给被授权方。

[0322] 步骤G2：被授权方根据授权方的身份标识从注册系统获取授权方的身份文件；根据授权方的身份文件对身份验证数据进行验证，验证通过则对可验证凭证数据的加密数据进行解密得到可验证凭证数据，并对解密得到的可验证凭证数据进行保存。

[0323] 在本申请实施例一些可能的实现方式中，上述步骤G1中的“授权方根据第二随机数和第三随机数、可验证凭证数据生成身份验证数据和可验证凭证数据的加密数据”的具体实现过程包括下述步骤H1-H3：

[0324] 步骤H1：授权方使用授权方对被授权方进行身份验证时获取的被授权方的公钥对第三随机数加密，得到第三随机数的加密数据。

[0325] 步骤H2：授权方使用自身保存的授权方私钥对第三随机数签名，得到第三随机数的签名。

[0326] 步骤H3：授权方根据第二随机数和第三随机数生成第一会话密钥，并使用第一会话密钥对可验证凭证数据进行加密得到可验证凭证数据的加密数据。

[0327] 在此基础上，上述步骤G2中的“根据授权方的身份文件对身份验证数据进行验证”的具体实现过程包括下述步骤I1-I2：

[0328] 步骤I1：被授权方从授权方的身份文件中获取授权方的公钥，并使用自身保存的被授权方的私钥对第三随机数的加密数据进行解密得到第一解密数据。

[0329] 其中，需要说明的是，身份文件中通常会包括多个公钥以及对应的密钥标识，由此，当授权方所属的身份文件中包含多个密钥时，被授权方首先需要通过密钥标识来查找出授权方对应的公钥，然后才能再使用自身保存的被授权方的私钥对第三随机数的加密数据进行解密，以得到第一解密数据。

[0330] 步骤I2：被授权方使用授权方的公钥和第一解密数据对第三随机数的签名进行验签。

[0331] 在此基础上，上述步骤G2中的被授权方对可验证凭证数据的加密数据进行解密得到可验证凭证数据，并对解密得到的可验证凭证数据进行保存的具体实现过程包括下述步骤J1-J2：

[0332] 步骤J1：若验签成功，则被授权方可以根据第二随机数和第一解密数据生成第二会话密钥。

[0333] 步骤J2：被授权方使用第二会话密钥对可验证凭证数据的加密数据解密，得到可验证凭证数据，从可验证凭证数据中提取被授权方的声明数据及被授权方的声明数据签名，使用授权方的公钥和提取的被授权方的声明数据对被授权方声明数据的签名进行验签，若验签通过，则对可验证凭证数据进行保存。

[0334] 此外，一种可选的实现方式是，为了提高授权方与被授权方间身份授权的安全性及可靠性。被授权方对可验证凭证数据进行保存之前，还可以将可验证凭证数据中的可验

证凭证数据的标识(VC_ID)发送给注册系统,以便注册系统检查可验证凭证数据的标识是否有效,如,可以采用检查VC列表是否存在的方式,验证授权方的身份标识(DID_I)的有效性。并且,当验证结果为可验证凭证数据的标识(DID_I)有效,且被授权方对身份验证数据验证结果为通过时,被授权方可以对可验证凭证数据进行保存。

[0335] 接下来,对授权方与被授权方在身份授权区块链系统进行注册的方法进行介绍。在一种可能的实现方式中,以授权方或被授权方作为目标方为例进行说明。

[0336] 在本实现方式中,目标方(具体为授权方或被授权方)可以生成对应的身份标识和身份文件。其中,身份标识可以用于标识该身份授权区块链系统中的该目标方的身份。该目标方还可以生成对应的公私钥对,以用于通过签名和验签的方式来验证目标方的身份。其中,目标方生成的公钥可以作为该目标方对应的验签公钥,目标方生成的身份文件包括对应的验签公钥和验签方式。当目标方通过其私钥进行签名得到对应的签名数据时,可以通过该验签公钥和验签方式对签名数据进行解签。

[0337] 在具体实现中,目标方生成的身份标识可以是去中心化身份(Decentralized Identifiers,DID),即由实体(Entity)自主生成和控制的身份标识信息。

[0338] 该DID包含一些固定字段和一个唯一的随机字符串,用以指向确定的Entity。其语法格式为:"did:"method-name":"method-specific-id",其中method-name为方案名称,method-specific-id是基于场景规则生成的ID号。

[0339] 例如,一个Entity的DID为:

[0340] “DID:bhdc:0d7ef5e3c48123……d10edd982e5b65642af8d2a792964”。

[0341] 另外,为了保证唯一性,DID可以是通过实体持有的公钥的哈希值,并在生成后到区块链上注册并存证,以确保每个DID的唯一性。

[0342] 去中心化身份文档(Decentralized Identifiers Document,DID Document):

[0343] 每一个DID都有对应的DID文档,即身份文档,该DID文档中包含更多的关于目标方身份的信息,例如公钥(Public Key)、验签方式、服务(Service)等。DID Document可以存储在目标方的用户软件中或者设备安全硬件中,也可以在本地加密后存储在用户指定的云平台中,本申请对此不作限定。

[0344] 下面给出一个DID Document的示例:

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey ": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }, {
    "id": "did:example:123456789abcdefghi#keys-2",
    "type": "Secp256k1VerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyHex": "02b97c30de767f … … 35d7116a3263d29f1450936b71"
  }],
  "authentication": [
    "did:example:123456789abcdefghi#keys-1",
    "did:example:123456789abcdefghi#keys-2",
    {
      "id": "did:example:123456789abcdefghi#keys-2",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    }
  ],
  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://www.bhdc.com.cn/vc/"
  }]
}
```


[0345]

[0346]

[0347] 其中,"Public Key"域表明DID实体持有的公钥数据,"authentication"域用来表明可用于DID实体身份认证的公钥(可从"Public Key"域中引用,也可以补充添加新的公钥),"Service"域标识当前DID实体可以对外提供的服务内容,例如作为设备生产商,可以为自己生产的设备签发可验证凭据(Verifiable Credential)。

[0348] 为了便于理解本申请的技术方案,下面对DID、DID Document和VC的关系进行介绍。

[0349] DID Document和DID是一对一关系,每个DID都有对应的DID Document记录其公钥和认证方式。

[0350] DID Document和VC没有直接关系,但是Issuer在颁发VC时可能需要借助Document验证Entity身份。

[0351] DID和VC不是简单的对应关系,DID用来描述Entity,VC则是Entity某些属性的证明,通常来讲,一个DID会拥有多个VC,一个VC至少会对应一个DID,特殊情况下会有对应多个DID的VC,例如结婚证。

[0352] 从而,目标方可以根据身份标识和身份文件向注册系统(即智能合约)进行身份注册。需要说明的是,身份文件中包括对应的验签公钥。

[0353] 然后,注册系统(即智能合约)可以对身份标识和身份文件进行审核,若通过审核,确定目标方完成身份注册,并保存该目标方对应的身份文件。

[0354] 具体来讲,目标方生成对应的身份标识和身份文件的过程可以为:目标方首先可以设定密钥类型(safeType)并获取当前时间(即时间戳(timeStamp)),然后,根据密钥类型(safeType)和当前时间(timeStamp),随机生成一对公钥和私钥(pubKey和privKey)。其中,可以将私钥加密后存储在芯片内部,接着,对公钥进行哈希运算,得到其对应的哈希值,并将该哈希值作为目标方的身份标识(即DID),进而可以根据该身份标识和公钥(pubKey)生成目标方的身份文件(DID Document)。一种可选的实现方式是,目标方生成对应的身份标识和身份文件后,还可以对身份标识和身份文件进行保存。

[0355] 在此基础上,目标方可以将得到的身份标识和身份文件发送至注册系统,以便注册系统对身份标识和身份文件进行审核,即,以便注册系统确定身份标识是否存在于之前已保存的身份标识集合中,若不存在,则可以向目标方发送随机标识。

[0356] 进一步的,目标方在接收到随机标识后,可以利用私钥对随机标识进行签名,得到第一签名数据,并将身份文件和随机标识以及第一签名数据发送至注册系统,以便注册系统根据身份文件对第一签名数据进行验签,若验签通过,则可以确定目标方完成身份注册,并保存目标方对应的身份文件。

[0357] 再进一步的,一种可选的实现方式是,在确定目标方完成身份注册之后后,注册系统可以将身份标识的查询地址发送给目标方,以便目标方根据身份标识的查询地址对身份文件进行更新。

[0358] 举例说明:参见图3,该图示出了本申请实施例提供的一种身份注册阶段的信令交互示例图,如图3所示,包括一个DID实体即上文提及的目标方,可以是授权方或被授权方。该DID实体可以是一个数据处理设备,该数据处理设备可以包括安全模块和设备程序,安全模块和设备程序间通过硬件接口通信。则该被授权方(holder)或授权方(issuer)的注册过程包括:

[0359] S501:实体的设备程序可以获取时间戳(timeStamp)和设定密钥对类型(safeType)。

[0360] 该时间戳即为获取的当前时间。

[0361] S502:设备程序将密钥对类型和时间戳发送至实体的安全模块,向安全模块请求生成身份标识(DID)。

[0362] S503:安全模块根据当前时间(timeStamp)和密钥对类型(safeType)随机生成一对公钥和私钥。

[0363] S504:安全模块将私钥保存,对公钥进行哈希运算,得到其对应的哈希值,并将该哈希值作为目标方(即授权方(holder)或授权方(issuer))的身份标识(DID)。

[0364] 其中,安全模块可以将私钥加密后存储在芯片内部。

[0365] S505:安全模块结合预设模板和传入的当前时间timeStamp生成身份文件(DID Document)。

[0366] S506:安全模块将身份文件(DID Document)返回设备程序。

[0367] S507:设备程序将身份标识(DID)和身份文件(DID Document)发送至注册系统,请求对身份标识和身份文件验证(即审核)。

[0368] 其中,该注册系统是基于区块链智能合约搭建的。

[0369] S508:注册系统检索身份标识(DID)是否已被注册(即注册系统需要确定该身份标识是否存在于保存的身份标识集合中),若否,则说明该身份标识(DID)是可用的,执行S509。

[0370] S509:注册系统向设备程序发送随机标识(Nonce),如随机字符串。

[0371] S510:设备程序向安全模块请求对随机标识(如随机字符串)进行签名。

[0372] S511:安全模块按照利用私钥,预设算法(如ECDSA、RSA、SM2等签名算法)对随机标识(如随机字符串)进行签名,生成签名数据(sign_Nonce),此处将其定义为第一签名数据。

[0373] S512:安全模块将第一签名数据(sign_Nonce)和身份文件(DID Document)发送至设备程序。

[0374] S513:设备程序向注册系统发送身份文件(DID Document)、随机标识(Nonce)和第一签名数据(sign_Nonce),请求身份标识(DID)注册。

[0375] S514:注册系统从身份文件(DID Document)中获取公钥,并对第一签名数据(sgin_Nonce)进行验签。验证通过后,则在注册系统中注册身份标识(DID),即将该身份标识(DID)保存在注册系统中存储的身份标识集合中,也就是保存了该目标方对应的身份文件(DID Document)。

[0376] S515:注册系统向设备程序返回注册结果和身份查询地址(uri_did)。

[0377] S516:设备程序向安全模块返回身份查询地址。

[0378] S517:安全模块将身份查询地址更新至身份文件(DID Document)。

[0379] 接下来,在另一种可能的实现方式中,以授权方作为目标方为例,对授权方的身份注册过程进行说明。具体还可以包括下述步骤K1-K4:

[0380] 步骤K1:授权方生成授权方身份数据,并利用私钥对身份数据进行签名,得到第二签名数据;其中,授权方身份数据指的是体现授权方具有身份授权权限的数据。

[0381] 步骤K2:授权方将身份文件和身份数据以及第二签名数据发送至注册系统。

[0382] 步骤K3:注册系统根据身份文件对第二签名数据进行验证,若通过验证,则授予授权方的身份授权权限资格,并将身份授权权限资格保存至自身存储的身份文件中,以及将授权方的注册状态和身份查询地址发送至授权方。

[0383] 步骤K4:授权方将身份查询地址更新至自身存储的身份文件中。

[0384] 举例说明:参见图4,该图示出了本申请实施例提供的一种授权方身份注册的信令交互示例图,如图4所示,该方法包括:

[0385] S601:设备程序设置发行人身份和生成授权方身份数据(IssuerData)。

[0386] 其中,授权方身份数据为体现授权方具有身份授权权限的数据;

[0387] 具体来讲,可以通过用户在实体对象的设备程序中人工填写发行人身份(即确定该实体对象为授权方)和生成授权方身份数据,或者也可以由设备程序自动设置发行人身份和验证信息,对于一些对外提供服务的DID实体对象,在注册DID身份之后可以注册Issuer身份。

[0388] S602:实体的设备程序向安全模块请求对身份数据签名。

[0389] S603:实体的安全模块利用私钥对身份数据(IssuerData)进行签名,得到签名(sign_IssuerData),此处将其定义为第二签名数据。

[0390] 其中,安全模块可以先解密内部存储的私钥,在利用其对身份数据(IssuerData)按照预设算法生成第二签名数据(sign_IssuerData)。

[0391] S604:安全模块将第二签名数据(sign_IssuerData)返回给设备程序。

[0392] S605:设备程序向注册系统发送身份文件(DID Document)、身份数据IssuerData、第二签名数据(sign_IssuerData),以请求授权方(Issuer)的身份权限注册。

[0393] S606:注册系统根据身份文件(DID Document)中的公钥对第二签名数据(sign_IssuerData)进行验签,若验签成功,注册Issuer身份,即,授予其身份授权权限资格,并将该身份授权权限资格保存至自身存储的身份文件(DID Document)。

[0394] S607:注册系统向设备程序返回注册状态和身份查询地址(uri_issuer)。

[0395] S608:设备程序将身份查询地址(uri_issuer)发送至安全模块。

[0396] S609:安全模块将身份查询地址(uri_issuer)更新到自身存储的身份文件(DID Document)中。

[0397] 接下来,本申请实施例将对授权方和被授权方增加声明模板的过程进行说明。具体可以包括下述步骤L1-L4:

[0398] 步骤L1:授权方生成声明信息,并利用私钥对声明信息中的声明模板查询地址进行签名,得到第三签名数据;其中,声明信息包括声明模板和声明模板查询地址。

[0399] 步骤L2:授权方将身份文件和声明信息中的声明模板查询地址以及第三签名数据发送至注册系统。

[0400] 步骤L3:注册系统根据自身保存的身份文件对第三签名数据进行验证,若通过验证,则将声明信息保存在自身存储的身份文件中,并向目标方返回声明信息的新增结果。

[0401] 步骤L4:目标方将声明模板地址更新至自身存储的身份文件中。

[0402] 举例说明:参见图5,该图示出了本申请实施例提供的增加声明(claim)模板的信令交互示例图,如图5所示,该方法包括:

[0403] S701:实体的设备程序生成声明信息,其中,声明信息包括声明模板和声明模板查

询地址(uri_claim)。

[0404] S702:设备程序向实体的安全模块请求对声明信息中的声明模板查询地址(uri_claim)进行签名。

[0405] S703:安全模块利用内置私钥对声明模板查询地址(uri_claim)签名得到签名数据(sign_uri_claim),此处将其定义为第三签名数据。

[0406] S704:安全模块向设备程序发送第三签名数据(sign_uri_claim)。

[0407] S705:设备程序向注册系统发送身份文件(DID Document)、声明模板查询地址(uri_claim)、第三签名数据(sign_uri_claim),以请求新增该声明(claim)模板。

[0408] S706:注册系统利用身份文件(DID Document)中的公钥对第三签名数据(sign_uri_claim)进行验签,并在验签成功后,将声明模板查询地址所属的声明信息增加至自身存储的身份文件(DID Document)中,若验签失败,则不会添加声明模板查询/获取地址。

[0409] S707:注册系统将声明模板的添加结果发送至设备程序中。

[0410] S708:设备程序将声明模板查询地址(uri_claim)发送至安全模块。

[0411] S709:安全模块将声明模板查询地址(uri_claim)更新到自身存储的身份文件(DID Document)的Service域中,并向设备程序返回新增状态。

[0412] 参见图6所示,本申请还提供了一种身份验证的装置,应用于包括被授权方、验证方的身份授权区块链系统,所述身份授权区块链系统中部署有注册系统,该装置包括:

[0413] 被授权方801,用于向所述验证方发送验证请求,所述验证请求中包括所述被授权方的身份标识;

[0414] 验证方802,用于根据所述验证请求生成随机数,并将所述随机数返回至所述被授权方;

[0415] 被授权方801,还用于根据所述随机数和自身保存的可验证凭证数据生成可验证报告,并将所述可验证报告、自身保存的被授权方的身份标识发送至所述验证方;

[0416] 验证方802,还用于利用所述被授权方的身份标识从所述注册系统803获取所述被授权方的身份文件,根据所述被授权方的身份文件对所述可验证报告进行验证,并向所述被授权方返回验证结果。

[0417] 在一种可能的实现方式中,所述被授权方801具体用于

[0418] 使用自身保存的被授权方的私钥对所述随机数进行签名,得到第四签名数据;使用所述被授权方的私钥对所述可验证凭证数据进行签名,得到第五签名数据;

[0419] 利用所述随机数、所述第四签名数据、所述可验证凭证数据、所述第五签名数据,生成所述可验证报告;

[0420] 所述验证方802具体用于:

[0421] 从所述被授权方的身份文件中获取被授权方的公钥,使用所述被授权方的公钥分别对所述第四签名数据和所述第五签名数据进行验签。

[0422] 在一种可能的实现方式中,所述验证方802具体用于:

[0423] 从所述可验证报告中获取所述随机数,使用所述被授权方的公钥和所述随机数对所述第四签名数据验签,验签通过,则使用所述被授权方公钥和所述可验证凭证数据对所述第五签名数据验签;

[0424] 或者,

[0425] 使用所述被授权方的公钥和所述可验证凭证数据对所述第五签名数据验签，若验签通过，则从所述可验证报告中获取所述随机数，使用所述被授权方的公钥和所述随机数对所述第四签名数据验签。

[0426] 在一种可能的实现方式中，所述验证方802还用于：

[0427] 从所述可验证报告中获取所述可验证凭证数据，从获取的所述可验证凭证数据中提取授权方的身份标识和可验证凭证数据的标识，向所述注册系统发送所述授权方的身份标识和所述可验证凭证数据的标识；

[0428] 所述注册系统803还用于：检查所述被授权方的身份标识和所述可验证凭证数据的标识是否在有效可验证凭证数据列表中，并向所述验证方返回被授权方有效或失效的查询结果；

[0429] 所述验证方802还用于：根据所述查询结果向所述被授权方返回所述验证结果。

[0430] 在一种可能的实现方式中，所述身份授权区块链系统中部署有授权方；所述装置还包括：

[0431] 被授权方801，用于从所述注册系统获取所述授权方的声明信息，根据自身保存的被授权方的身份标识请求所述授权方对所述被授权方进行身份验证，当所述授权方对所述被授权方的身份验证结果为通过时，根据所述授权方的声明信息生成身份授权请求，并向所述授权方发送所述身份授权请求；

[0432] 授权方，用于根据所述身份授权请求生成可验证凭证数据，并将所述可验证凭证数据中的可验证凭证数据的标识发送至所述注册系统；

[0433] 注册系统803，用于根据所述可验证凭证数据的标识进行更新，并向所述授权方返回更新结果；

[0434] 所述授权方，还用于将所述可验证凭证数据发送至所述被授权方，以便所述被授权方进行保存。

[0435] 在一种可能的实现方式中，所述被授权方801具体用于：

[0436] 根据所述被授权方的身份标识生成身份验证请求，并将所述身份验证请求发给所述授权方；

[0437] 所述授权方具体用于：

[0438] 生成第一随机数，并将所述第一随机数返回给所述被授权方；

[0439] 所述被授权方801还具体用于：

[0440] 根据自身保存的被授权方的私钥对所述第一随机数签名得到第一签名结果，将所述第一签名结果、所述第一随机数、所述被授权方的身份标识发给所述授权方；

[0441] 所述授权方还具体用于：

[0442] 根据所述被授权方的身份标识从所述注册系统获取所述被授权方的身份文件，从所述被授权方的身份文件中获取被授权方的公钥，使用获取的所述被授权方的公钥和所述第一随机数对所述第一签名结果进行验签。

[0443] 在一种可能的实现方式中，所述被授权方801具体用于：

[0444] 获取所述授权方的身份标识，向所述注册系统发送所述授权方的身份标识；

[0445] 所述注册系统803具体用于：

[0446] 根据所述授权方的身份标识，检索与所述授权方绑定的声明模板列表，并将其发

送给所述被授权方。

[0447] 在一种可能的实现方式中，所述被授权方801具体用于：

[0448] 从所述授权方的声明模板列表中选择所需要的声明模板，根据选择的声明模板生成被授权方的声明数据，根据所述被授权方的声明数据生成所述身份授权请求。

[0449] 在一种可能的实现方式中，所述被授权方801还用于根据所述授权方的声明信息生成被授权方的声明数据；所述身份授权请求中包括所述被授权方的声明数据；

[0450] 所述授权方具体用于：

[0451] 根据预设规则生成所述可验证凭证数据的标识，并用自身保存的授权方的私钥对所述被授权方的声明数据进行签名，得到被授权方声明数据的签名；

[0452] 根据所述被授权方声明数据、所述被授权方声明数据的签名和所述可验证凭证数据的标识生成所述可验证凭证数据。

[0453] 在一种可能的实现方式中，所述授权方还用于：

[0454] 使用所述授权方的私钥对所述可验证凭证数据的标识签名得到可验证凭证数据标识的签名；

[0455] 将所述可验证凭证数据标识的签名、授权方的身份标识发送至所述注册系统；

[0456] 所述注册系统803具体用于：

[0457] 根据所述授权方的身份标识找到对应授权方的公钥，使用所述授权方的公钥和所述可验证凭证数据的标识对所述可验证凭证数据标识的签名进行验签。

[0458] 在一种可能的实现方式中，当验签结果为通过时，所述注册系统803具体用于将所述可验证凭证数据的标识添加到授权方的可验证凭证数据列表中。

[0459] 在一种可能的实现方式中，所述授权方具体用于：

[0460] 将所述可验证凭证数据以及所述授权方的身份标识发送至所述被授权方；

[0461] 根据所述可验证凭证数据的标识和所述授权方的身份标识向所述注册系统发送查询请求；

[0462] 所述注册系统803具体用于：

[0463] 根据所述授权方的身份标识检索所述授权方的可验证凭证数据列表中是否存在所述可验证凭证数据的标识，若存在，则表明所述可验证凭证数据的标识有效，并将查询结果及所述授权方的身份标识对应的授权方的身份文件返回至所述被授权方；

[0464] 所述被授权方801还具体用于：

[0465] 根据所述授权方的身份文件对所述可验证凭证数据进行验证，若验证通过，则确认所述可验证凭证数据合法，并将其进行存储。

[0466] 在一种可能的实现方式中，所述被授权方801具体用于：、

[0467] 从所述授权方的身份文件中获取授权方的公钥，使用所述授权方的公钥、所述可验证凭证数据中的被授权方声明数据对所述可验证凭证数据中的被授权方声明数据的签名进行验签。

[0468] 在一种可能的实现方式中，所述授权方具体用于：

[0469] 利用私钥对所述可验证凭证数据进行签名，并将签名后的可验证凭证数据发送至所述被授权方；

[0470] 向所述注册系统发送实体身份查询请求；

[0471] 所述注册系统803具体用于：

[0472] 将预先存储的实体的身份文件返回至所述被授权方；

[0473] 所述被授权方801还具体用于：

[0474] 利用所述实体的身份文件，对所述签名后的可验证凭证数据进行验签，若验签成功，则确认所述可验证凭证数据合法；

[0475] 将确认所述可验证凭证数据合法的结果发送至所述注册系统进行查询，若所述注册系统查询到所述可验证凭证数据是有效的，则将查询结果返回至所述被授权方，以便所述被授权方存储所述可验证凭证数据。

[0476] 在一种可能的实现方式中，所述被授权方801还用于：

[0477] 生成第二随机数；所述身份授权请求中还包括所述第二随机数；

[0478] 则所述授权方具体用于：

[0479] 生成第三随机数，根据所述第二随机数、所述第三随机数、所述可验证凭证数据生成身份验证数据和所述可验证凭证数据的加密数据；将所述身份验证数据、所述可验证凭证数据的加密数据、自身保存的授权方身份标识发送给所述被授权方；

[0480] 所述被授权方801还用于：根据所述授权方的身份标识从所述注册系统获取授权方的身份文件；根据所述授权方的身份文件对所述身份验证数据进行验证，验证通过则对所述可验证凭证数据的加密数据进行解密得到所述可验证凭证数据，并对解密得到的所述可验证凭证数据进行保存。

[0481] 在一种可能的实现方式中，所述授权方具体用于：

[0482] 使用所述授权方对所述被授权方进行身份验证时获取的所述被授权方的公钥对所述第三随机数加密，得到第三随机数的加密数据；

[0483] 使用自身保存的授权方私钥对所述第三随机数签名，得到第三随机数的签名；

[0484] 根据所述第二随机数和所述第三随机数生成第一会话密钥，使用所述第一会话密钥对所述可验证凭证数据进行加密得到所述可验证凭证数据的加密数据。

[0485] 在一种可能的实现方式中，所述被授权方801具体用于：

[0486] 从所述授权方的身份文件中获取授权方的公钥，使用自身保存的被授权方的私钥对所述第三随机数的加密数据进行解密得到第一解密数据；

[0487] 使用所述授权方的公钥和所述第一解密数据对所述第三随机数的签名进行验签。

[0488] 在一种可能的实现方式中，所述被授权方801具体用于：

[0489] 若验签成功，则根据所述第二随机数和所述第一解密数据生成第二会话密钥；

[0490] 使用所述第二会话密钥对所述可验证凭证数据的加密数据解密，得到所述可验证凭证数据，从所述可验证凭证数据中提取被授权方的声明数据及所述被授权方的声明数据签名，使用所述授权方的公钥和提取的被授权方的声明数据对所述被授权方声明数据的签名进行验签，若验签通过，则对所述可验证凭证数据进行保存。

[0491] 在一种可能的实现方式中，所述被授权方801还用于：

[0492] 将所述可验证凭证数据中的可验证凭证数据的标识发送给所述注册系统，所述注册系统检查所述可验证凭证数据的标识是否有效；

[0493] 当验证结果为所述可验证凭证数据的标识有效，且所述被授权方对所述身份验证数据验证结果为通过时，对所述可验证凭证数据进行保存。

[0494] 在一种可能的实现方式中，所述授权方还用于：

[0495] 根据所述被授权方发送的身份授权请求进行审核。

[0496] 在一种可能的实现方式中，目标方为所述授权方或所述被授权方801；所述目标方具体用于：

[0497] 生成对应的身份标识和身份文件，并根据所述身份标识和所述身份文件向所述注册系统进行身份注册；所述身份文件中包括对应的验签公钥；

[0498] 所述注册系统803具体用于：对所述身份标识和所述身份文件进行审核，若通过审核，确定所述目标方完成身份注册，并保存所述目标方对应的身份文件。

[0499] 在一种可能的实现方式中，所述目标方具体用于：

[0500] 获取当前时间并设定密钥对类型，并根据所述当前时间和所述密钥对类型，生成公钥和私钥；

[0501] 对所述公钥进行哈希运算，得到其对应的哈希值，并将所述哈希值作为所述目标方的身份标识；

[0502] 根据所述身份标识和所述公钥生成所述目标方的身份文件。

[0503] 在一种可能的实现方式中，所述目标方具体用于：

[0504] 将所述身份标识和所述身份文件发送至注册系统；

[0505] 所述注册系统803具体用于：确定所述身份标识是否存在于已保存的身份标识集合中，若否，向所述目标方发送随机标识。

[0506] 在一种可能的实现方式中，所述目标方还用于：

[0507] 接收所述随机标识，并利用所述私钥对所述随机标识进行签名，得到第一签名数据；

[0508] 将所述身份文件和所述随机标识以及所述第一签名数据发送至所述注册系统；

[0509] 所述注册系统803还用于：根据所述身份文件对所述第一签名数据进行验签，若验签通过，确定所述目标方完成身份注册，并保存所述目标方对应的身份文件。

[0510] 在一种可能的实现方式中，所述目标方还用于：

[0511] 对所述身份文件进行保存；

[0512] 所述注册系统803还用于：将身份标识的查询地址发送给所述目标方；

[0513] 所述目标方还用于：根据所述身份标识的查询地址对所述身份文件进行更新。

[0514] 在一种可能的实现方式中，当目标方为所述授权方时，所述授权方还用于：

[0515] 生成授权方身份数据，并利用所述私钥对所述身份数据进行签名，得到第二签名数据；所述授权方身份数据为体现所述授权方具有身份授权权限的数据；

[0516] 将所述身份文件和所述身份数据以及所述第二签名数据发送至所述注册系统；

[0517] 所述注册系统803还用于：根据所述身份文件对所述第二签名数据进行验证，若通过验证，授予所述授权方的身份授权权限资格，并将所述身份授权权限资格保存至自身存储的身份文件中，以及将所述授权方的注册状态和身份查询地址发送至所述授权方；

[0518] 所述授权方还用于：将所述身份查询地址更新至自身存储的身份文件中。

[0519] 在一种可能的实现方式中，所述授权方还用于：

[0520] 生成声明信息，并利用所述私钥对所述声明信息中的声明模板查询地址进行签名，得到第三签名数据；所述声明信息包括声明模板和声明模板查询地址；

[0521] 将所述身份文件和所述声明信息中的声明模板查询地址以及所述第三签名数据发送至所述注册系统；

[0522] 所述注册系统803还用于：根据自身保存的所述身份文件对所述第三签名数据进行验证，若通过验证，则将所述声明信息保存在自身存储的身份文件中，并向所述目标方返回所述声明信息的新增结果；

[0523] 所述目标方还用于：将所述声明模板查询地址更新至自身存储的身份文件中。

[0524] 在一种可能的实现方式中，所述被授权方801还用于：

[0525] 设置安全标识，将所述安全标识的类型设置为明文回传或密文回传；所述身份授权请求中还包括所述安全标识；

[0526] 判断所述安全标识的类型，当所述安全标识的类型为明文回传时，则将所述可验证凭证数据的明文数据发送给所述被授权方；当所述安全标识的类型为密文回传时，则将所述可验证凭证数据的密文数据发送给所述被授权方。

[0527] 综上，在本实施例提供的一种身份验证的装置中，用于身份验证的身份授权区块链系统包括已注册的被授权方和验证方，该身份授权区块链系统中部署有注册系统；被授权方向验证方发送包括被授权方的身份标识的验证请求后，验证方可以根据该验证请求生成随机数，并将该随机数返回至被授权方。以便被授权方根据随机数和自身保存的可验证凭证数据生成可验证报告，并将该可验证报告、自身保存的被授权方的身份标识发送至验证方，从而验证方可以利用被授权方的身份标识从注册系统获取被授权方的身份文件，并根据被授权方的身份文件对可验证报告进行验证，并向被授权方返回验证结果。进而基于该注册系统具有的区块链的去中心化优势以及外界无法篡改的优势，可以有效提高被授权方身份验证结果的准确性和可靠性。

[0528] 进一步地，本申请实施例还提供了一种身份验证的设备，包括：处理器以及存储器；

[0529] 所述处理器用于存储程序代码，并将所述程序代码传输给所述处理器；

[0530] 所述存储器用于根据所述程序代码中的指令执行上述身份验证的方法的任一种实现方法。

[0531] 进一步地，本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当所述计算机程序在终端设备上运行时，使得所述终端设备执行上述身份验证的方法的任一种实现方法。

[0532] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到上述实施例方法中的全部或部分步骤可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请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，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者诸如媒体网关等网络通信设备，等等)执行本申请各个实施例或者实施例的某些部分所述的方法。

[0533] 需要说明的是，本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的装置而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。

[0534] 还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，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、物品或者设备不仅包括那些要素，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、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0535] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

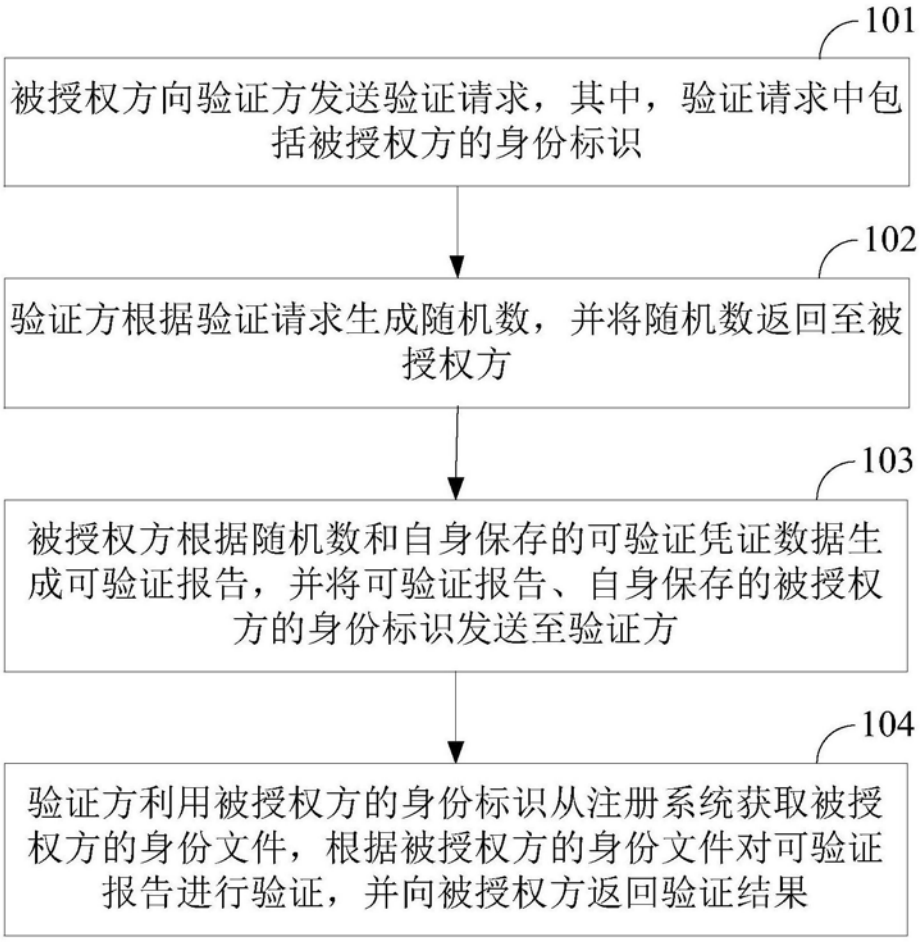

101
被授权方向验证方发送验证请求，其中，验证请求中包括被授权方的身份标识
102
验证方根据验证请求生成随机数，并将随机数返回至被授权方
103
被授权方根据随机数和自身保存的可验证凭证数据生成可验证报告，并将可验证报告、自身保存的被授权方的身份标识发送至验证方
104
验证方利用被授权方的身份标识从注册系统获取被授权方的身份文件，根据被授权方的身份文件对可验证报告进行验证，并向被授权方返回验证结果

图1

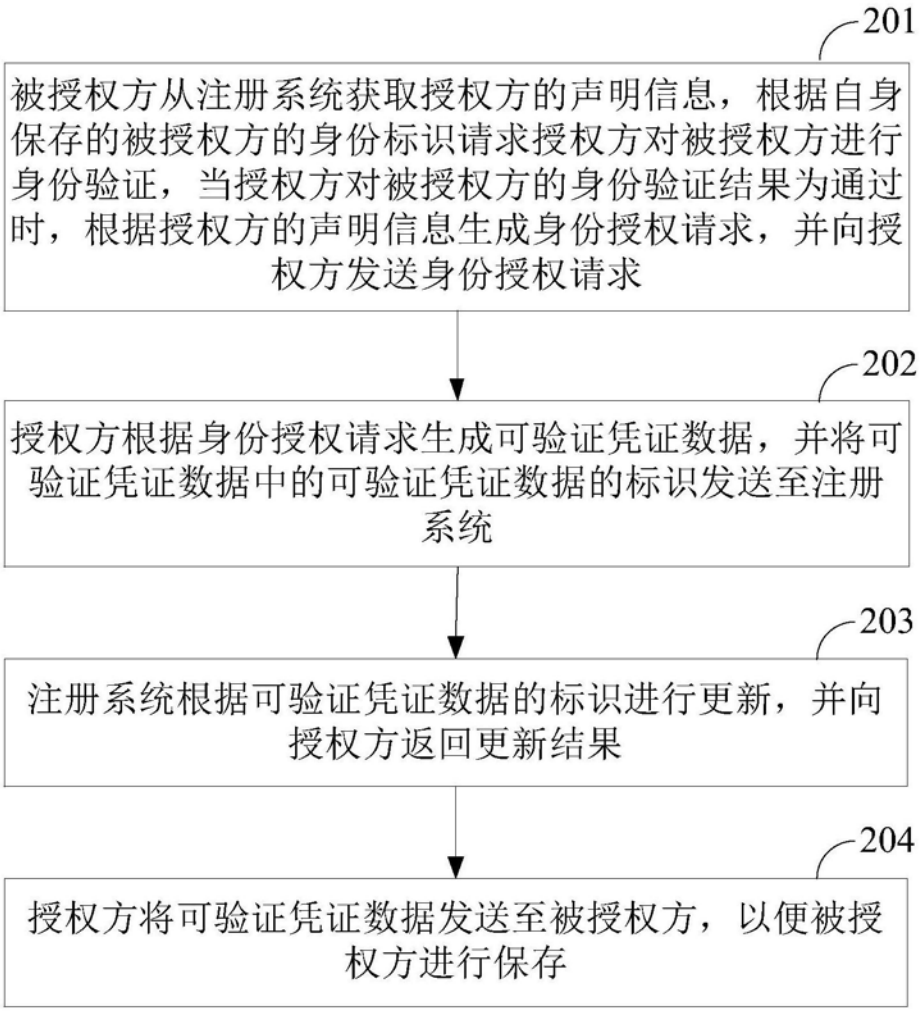

201
被授权方从注册系统获取授权方的声明信息，根据自身保存的被授权方的身份标识请求授权方对被授权方进行身份验证，当授权方对被授权方的身份验证结果为通过时，根据授权方的声明信息生成身份授权请求，并向授权方发送身份授权请求
202
授权方根据身份授权请求生成可验证凭证数据，并将可验证凭证数据中的可验证凭证数据的标识发送至注册系统
203
注册系统根据可验证凭证数据的标识进行更新，并向授权方返回更新结果
204
授权方将可验证凭证数据发送至被授权方，以便被授权方进行保存

图2

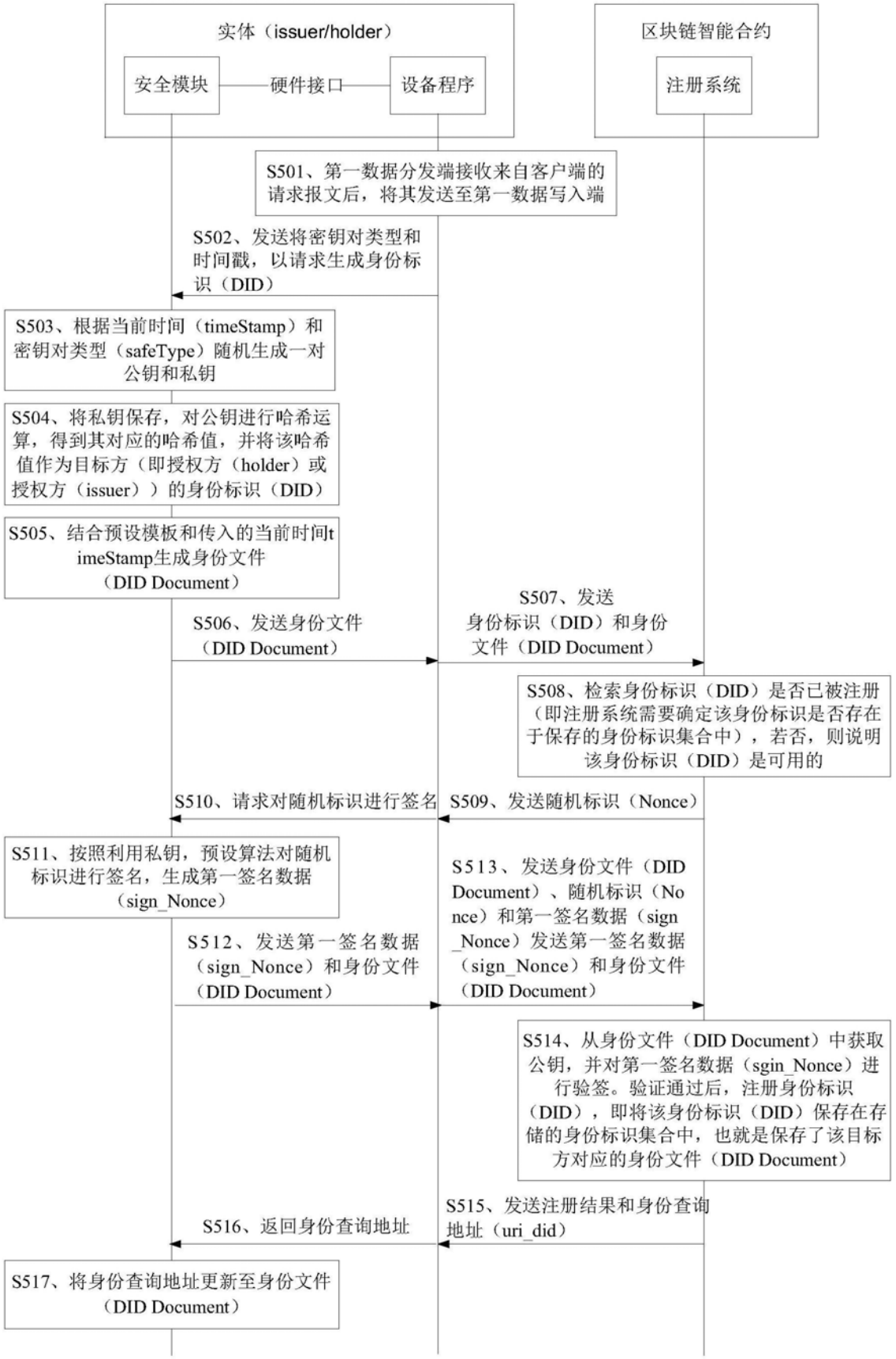

实体（issuer/holder）
安全模块
硬件接口
设备程序
区块链智能合约
注册系统
S501、第一数据分发端接收来自客户端的请求报文后，将其发送至第一数据写入端
S502、发送将密钥对类型和时间戳，以请求生成身份标识（DID）
S503、根据当前时间（timeStamp）和密钥对类型（safeType）随机生成一对公钥和私钥
S504、将私钥保存，对公钥进行哈希运算，得到其对应的哈希值，并将该哈希值作为目标方（即授权方（holder）或授权方（issuer））的身份标识（DID）
S505、结合预设模板和传入的当前时间timeStamp生成身份文件（DID Document）
S506、发送身份文件（DID Document）
S507、发送身份标识（DID）和身份文件（DID Document）
S508、检索身份标识（DID）是否已被注册（即注册系统需要确定该身份标识是否存在于保存的身份标识集合中），若否，则说明该身份标识（DID）是可用的
S509、发送随机标识（Nonce）
S510、请求对随机标识进行签名
S511、按照利用私钥，预设算法对随机标识进行签名，生成第一签名数据（sign_Nonce）
S512、发送第一签名数据（sign_Nonce）和身份文件（DID Document）
S513、发送身份文件（DID Document）、随机标识（Nonce）和第一签名数据（sign_Nonce）发送第一签名数据（sign_Nonce）和身份文件（DID Document）
S514、从身份文件（DID Document）中获取公钥，并对第一签名数据（sgin_Nonce）进行验签。验证通过后，注册身份标识（DID），即将该身份标识（DID）保存在存储的身份标识集合中，也就是保存了该目标方对应的身份文件（DID Document）
S515、发送注册结果和身份查询地址（uri_did）
S516、返回身份查询地址
S517、将身份查询地址更新至身份文件（DID Document）

图3

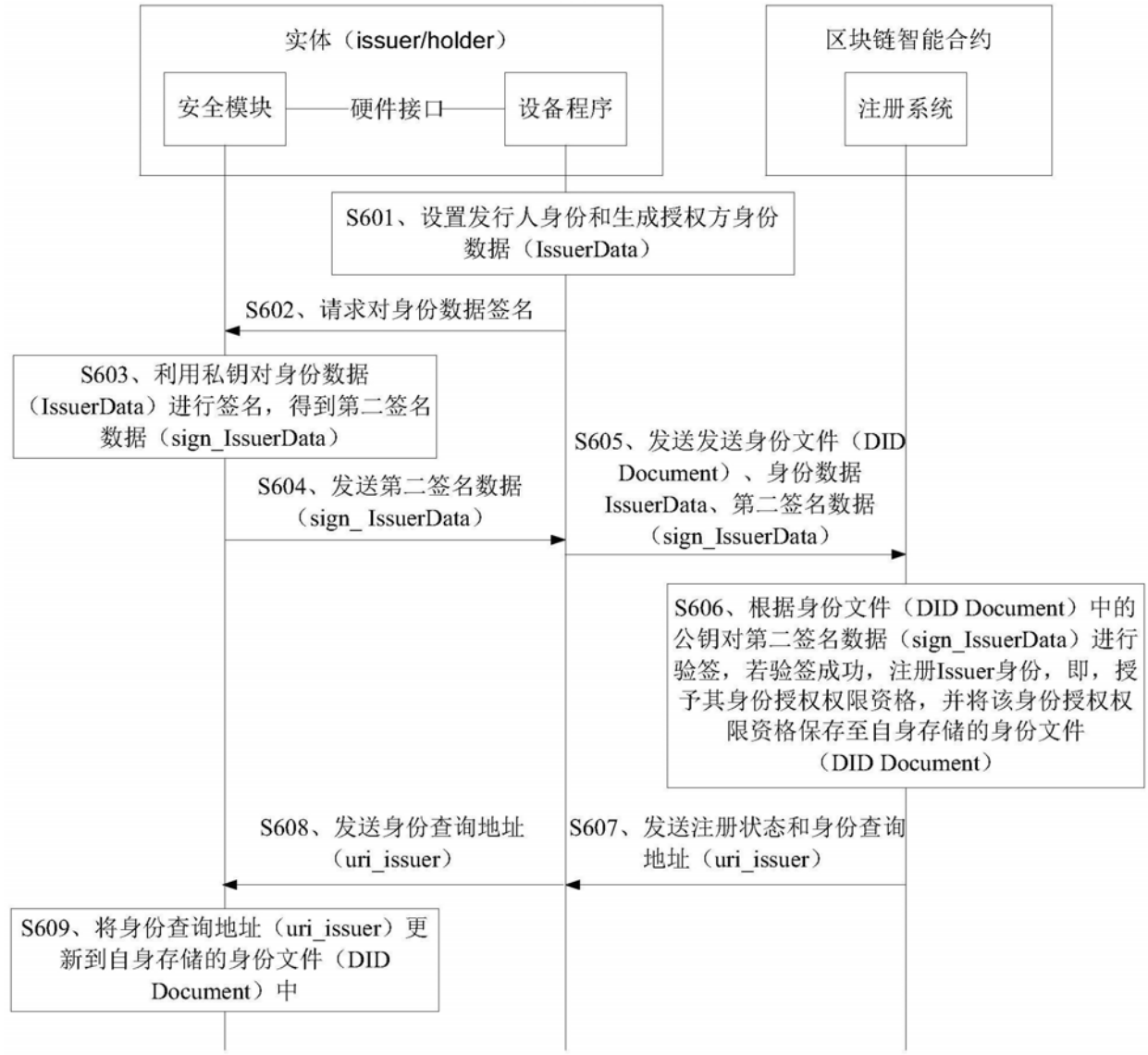

实体（issuer/holder）
安全模块
硬件接口
设备程序
区块链智能合约
注册系统
S601、设置发行人身份和生成授权方身份数据（IssuerData）
S602、请求对身份数据签名
S603、利用私钥对身份数据（IssuerData）进行签名，得到第二签名数据（sign_IssuerData）
S604、发送第二签名数据（sign_ IssuerData）
S605、发送发送身份文件（DID Document）、身份数据IssuerData、第二签名数据（sign_IssuerData）
S606、根据身份文件（DID Document）中的公钥对第二签名数据（sign_IssuerData）进行验签，若验签成功，注册Issuer身份，即，授予其身份授权权限资格，并将该身份授权权限资格保存至自身存储的身份文件（DID Document）
S608、发送身份查询地址（uri_issuer）
S607、发送注册状态和身份查询地址（uri_issuer）
S609、将身份查询地址（uri_issuer）更新到自身存储的身份文件（DID Document）中

图4

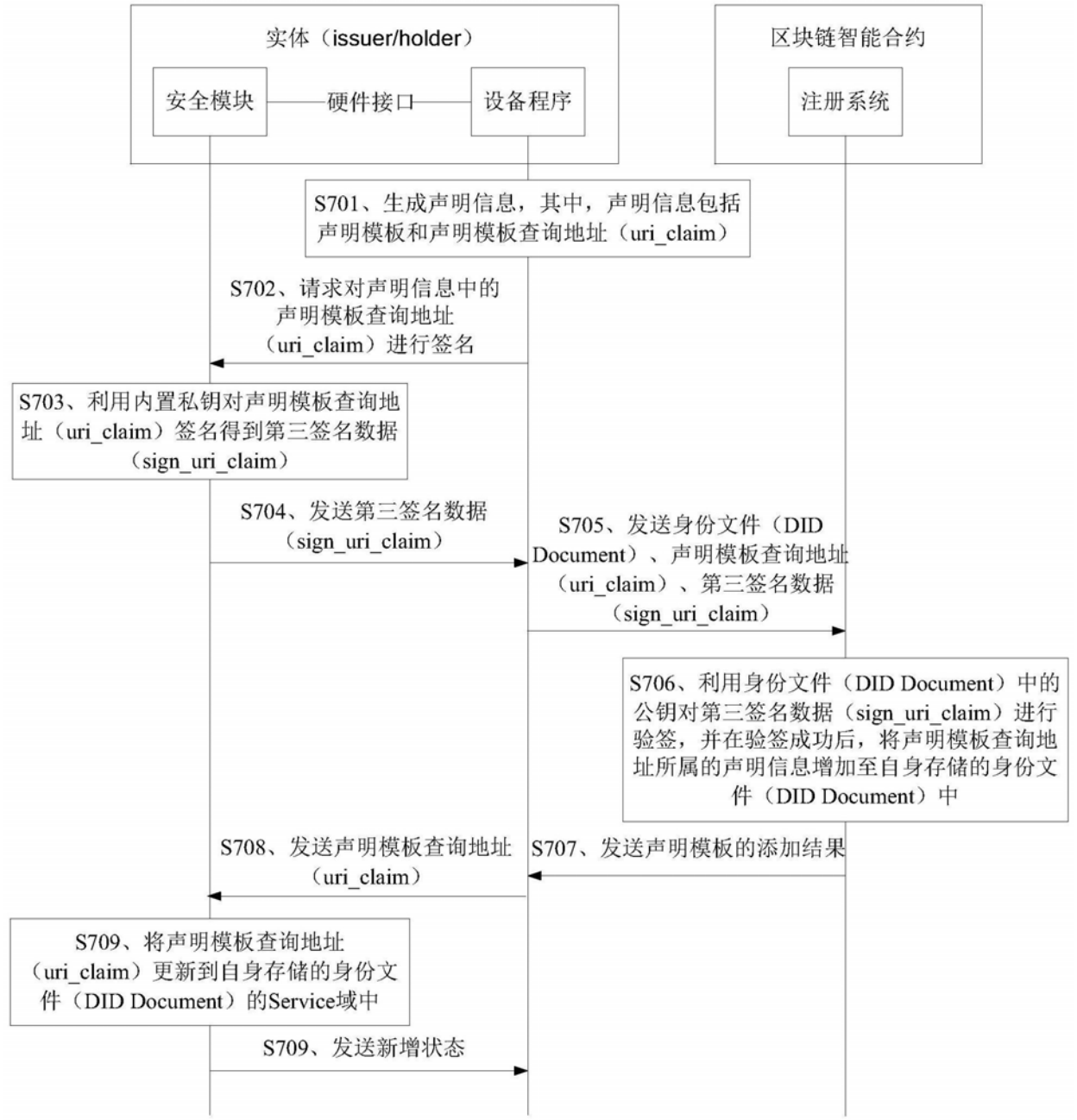

实体（issuer/holder）
安全模块
硬件接口
设备程序
区块链智能合约
注册系统
S701、生成声明信息，其中，声明信息包括声明模板和声明模板查询地址（uri_claim）
S702、请求对声明信息中的声明模板查询地址（uri_claim）进行签名
S703、利用内置私钥对声明模板查询地址（uri_claim）签名得到第三签名数据（sign_uri_claim）
S704、发送第三签名数据（sign_uri_claim）
S705、发送身份文件（DID Document）、声明模板查询地址（uri_claim）、第三签名数据（sign_uri_claim）
S706、利用身份文件（DID Document）中的公钥对第三签名数据（sign_uri_claim）进行验签，并在验签成功后，将声明模板查询地址所属的声明信息增加至自身存储的身份文件（DID Document）中
S708、发送声明模板查询地址（uri_claim）
S707、发送声明模板的添加结果
S709、将声明模板查询地址（uri_claim）更新到自身存储的身份文件（DID Document）的Service域中
S709、发送新增状态

图5

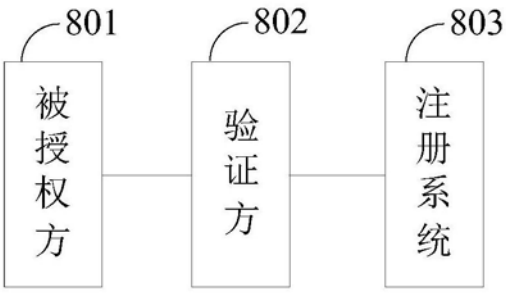


图6