(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 112035806 A
(43)申请公布日 2020.12.04

(21)申请号 202010707944.8

(22)申请日 2020.07.21

(71)申请人 杜晓楠
地址 新加坡大牌233碧山22街门牌05-132，570233

(72)发明人 杜晓楠

(74)专利代理机构 深圳市顺天达专利商标代理有限公司 44217
代理人 邹秋菊

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/64(2013.01)

权利要求书2页 说明书8页 附图4页

(54)发明名称

区块链中基于指纹识别生成分布式身份的方法和计算机可读介质

(57)摘要

本发明涉及一种区块链中基于指纹识别生成分布式身份的方法。扫描身份持有者的指纹以生成指纹码，并基于所述指纹码生成持有者私钥和持有者公钥。所述身份持有者基于所述持有者公钥、签名和可验证证书信息从可验证证书颁发机构获取可验证证书。所述身份持有者采用所述持有者私钥对所述可验证证书进行签名并提交到验证证书机构。所述验证证书机构对所述可验证证书进行验证。本发明还涉及一种计算机可读存储介质。本发明可以录入用户的指纹来生成指纹码，再通过指纹码作为随机种子来生成身份持有者私钥，从而可以使得身份持有者在使用身份信息的时候可以无需输入密码地使用身份信息和使用区块链上的资产，非常便于用户使用。

CN 112035806 A

1.一种区块链中基于指纹识别生成分布式身份的方法,其特征在于,包括:

S1、扫描身份持有者的指纹以生成指纹码,基于所述指纹码生成持有者私钥和持有者公钥;

S2、可验证证书颁发机构基于自身密钥向身份注册机构进行注册;

S3、所述身份持有者基于所述持有者私钥和所述持有者公钥向所述可验证证书颁发机构进行注册;

S4、所述身份持有者基于所述验证证书机构的要求从所述可验证证书颁发机构获取可验证证书;

S5、所述身份持有者采用所述持有者私钥对所述可验证证书进行签名并提交到所述验证证书机构;

S6、所述验证证书机构对所述可验证证书进行验证。

2.根据权利要求1所述的区块链中基于指纹识别生成分布式身份的方法,其特征在于,所述步骤S1进一步包括:

S11、扫描所述身份持有者的指纹以生成指纹码;

S12、对所述指纹码做哈希,使用获得的哈希值作为随机种子生成所述持有者私钥;

S13、基于所述持有者私钥生成所述持有者公钥。

3.根据权利要求2所述的区块链中基于指纹识别生成分布式身份的方法,其特征在于,所述步骤S2进一步包括:

S21、所述可验证证书颁发机构生成机构私钥并基于所述机构私钥生成机构公钥;

S22、所述可验证证书颁发机构生成注册请求,并采用所述机构私钥签名所述注册请求,并将签名注册请求发送到所述身份注册机构;

S23、所述身份注册机构验证所述签名注册请求,并在验证通过后生成所述可验证证书颁发机构的去中心化身份标识符和去中心化身份标识符文档。

4.根据权利要求3所述的区块链中基于指纹识别生成分布式身份的方法,其特征在于,所述步骤S3进一步包括:

S31、所述身份持有者向所述可验证证书颁发机构提交注册请求,并采用所述持有者私钥签名所述注册请求,并将签名注册请求发送到所述可验证证书颁发机构;

S32、所述可验证证书颁发机构验签所述签名注册请求,并在验签通过后验证所述身份持有者的注册信息,并在验证通过之后继续向所述身份注册机构发送验证请求,所述验证请求中包含所述持有者公钥;

S33、所述身份注册机构根据所述持有者公钥生成所述身份持有者的去中心化身份标识符和去中心化身份标识符文档,并将其返回给所述可验证证书颁发机构;

S34、所述可验证证书颁发机构将所述身份持有者的去中心化身份标识符和去中心化身份标识符文档返回给所述身份持有者。

5.根据权利要求4所述的区块链中基于指纹识别生成分布式身份的方法,其特征在于,所述步骤S4进一步包括:

S41、所述身份持有者向所述验证证书机构发送业务开始请求,所述业务开始请求包括所述去中心化身份标识符、所述去中心化身份标识符文档、以及所述身份持有者对业务开始请求的签名;

S42、所述验证证书机构基于所述请求返回可验证证书信息；

S43、所述身份持有者向所述可验证证书颁发机构发送证书颁发请求，所述证书颁发请求包括所述身份持有者的所述去中心化身份标识符、所述可验证证书信息、以及所述身份持有者对证书颁发请求的签名；

S44、所述可验证证书颁发机构基于所述去中心化身份标识符请求所述持有者公钥，并对所述身份持有者对证书颁发请求的签名进行验证，并基于验证结果向所述身份持有者颁发所述可验证证书。

6.根据权利要求5所述的区块链中基于指纹识别生成分布式身份的方法，其特征在于，所述可验证证书包括：所述身份持有者的去中心化身份标识符、颁发所述可验证证书的所述可验证证书颁发机构的去中心化身份标识符、所述身份持有者对所述可验证证书的签名、所述可验证证书颁发机构对所述可验证证书的签名，以及需验证的内容。

7.根据权利要求6所述的区块链中基于指纹识别生成分布式身份的方法，其特征在于，所述步骤S6进一步包括：

S61、所述验证证书机构根据所述可验证证书颁发机构的去中心化身份标识符向所述身份注册机构请求所述机构公钥，并使用所述机构公钥验证所述可验证证书颁发机构对所述可验证证书的签名以获得第一验证结果；

S62、所述验证证书机构根据所述身份持有者的去中心化身份标识符向所述身份注册机构请求所述持有者公钥，并使用所述持有者公钥验证所述身份持有者对所述可验证证书的签名以获得第二验证结果；

S63、基于所述第一验证结果、所述第二验证结果以及所述需验证的内容的验证结果，判定验证是否通过。

8.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现根据权利要求1-7中任意一项权利要求所述的区块链中基于指纹识别生成分布式身份的方法。

区块链中基于指纹识别生成分布式身份的方法和计算机可读介质

技术领域

[0001] 本发明涉及区块链领域，更具体地说，涉及一种区块链中基于指纹识别生成分布式身份的方法和计算机可读介质。

背景技术

[0002] 传统的数字认证是中心化的，比如互联网名称与数字地址分配机构(The Internet Corporation for Assigned Names and Numbers，ICANN)管理的域名与IP地址分配，以及公钥基础设施(Public Key Infrastructure，PKI)系统中的证书授权(Certificate Authority，CA)机构管理的数字证书。中心化身份系统的本质就是，中央集权化的权威机构掌握着身份数据，因为围绕数据进行的认证、授权等也都由中心化的机构来决定。身份不是由用户自己控制的。

[0003] 为了解决这个问题，许多网站自己联合起来推出了联盟身份(这个概念是首先由微软在1999年提出的)。在联盟身份体系下，用户的在线身份有了一定的可移植性。如今的不少网站注册都可以支持第三方登录，比如微信、QQ、新浪微博等。

[0004] 身份系统的去中心化依然成为一个大趋势，著名的国际组织w3c和dif也都推出了其去中心化身份系统标准。然而，w3c和dif制定的标准还是过于宽泛，并没有很详细的具体到实际的行业应用当中来。比如说：规定了可认证证书里面包含的信息要尽量少的透露用户的信息，但是却并没有给出具体的标准和方法来减少用户信息的透露；规定了身份有公钥和私钥但是却没有给出具体使用什么密钥体系和什么方式生成。

发明内容

[0005] 本发明要解决的技术问题在于，针对现有技术的上述缺陷，提供一种区块链中基于指纹识别生成分布式身份的方法和计算机可读介质，其可以无需输入密码可以创建和识别唯一身份，非常便于用户使用。

[0006] 本发明涉及一种区块链中基于指纹识别生成分布式身份的方法，包括：

[0007] S1、扫描身份持有者的指纹以生成指纹码，基于所述指纹码生成持有者私钥和持有者公钥；

[0008] S2、可验证证书颁发机构基于自身密钥向身份注册机构进行注册；

[0009] S3、所述身份持有者基于所述持有者私钥和所述持有者公钥向所述可验证证书颁发机构进行注册；

[0010] S4、所述身份持有者基于所述验证证书机构的要求从所述可验证证书颁发机构获取可验证证书；

[0011] S5、所述身份持有者采用所述持有者私钥对所述可验证证书进行签名并提交到所述验证证书机构；

[0012] S6、所述验证证书机构对所述可验证证书进行验证。

[0013] 在本发明所述的区块链中基于指纹识别生成分布式身份的方法中，所述步骤S1进一步包括：

[0014] S11、扫描所述身份持有者的指纹以生成指纹码；

[0015] S12、对所述指纹码做哈希，使用获得的哈希值作为随机种子生成所述持有者私钥；

[0016] S13、基于所述持有者私钥生成所述持有者公钥。

[0017] 在本发明所述的区块链中基于指纹识别生成分布式身份的方法中，所述步骤S2进一步包括：

[0018] S21、所述可验证证书颁发机构生成机构私钥并基于所述机构私钥生成机构公钥；

[0019] S22、所述可验证证书颁发机构生成注册请求，并采用所述机构私钥签名所述注册请求，并将签名注册请求发送到所述身份注册机构；

[0020] S23、所述身份注册机构验证所述签名注册请求，并在验证通过后生成所述可验证证书颁发机构的去中心化身份标识符和去中心化身份标识符文档。

[0021] 在本发明所述的区块链中基于指纹识别生成分布式身份的方法中，所述步骤S3进一步包括：

[0022] S31、所述身份持有者向所述可验证证书颁发机构提交注册请求，并采用所述持有者私钥签名所述注册请求，并将签名注册请求发送到所述可验证证书颁发机构；

[0023] S32、所述可验证证书颁发机构验签所述签名注册请求，并在验签通过后验证所述身份持有者的注册信息，并在验证通过之后继续向所述身份注册机构发送验证请求，所述验证请求中包含所述持有者公钥；

[0024] S33、所述身份注册机构根据所述持有者公钥生成所述身份持有者的去中心化身份标识符和去中心化身份标识符文档，并将其返回给所述可验证证书颁发机构；

[0025] S34、所述可验证证书颁发机构将所述身份持有者的去中心化身份标识符和去中心化身份标识符文档返回给所述身份持有者。

[0026] 在本发明所述的区块链中基于指纹识别生成分布式身份的方法中，所述步骤S4进一步包括：

[0027] S41、所述身份持有者向所述验证证书机构发送业务开始请求，所述业务开始请求包括所述去中心化身份标识符、所述去中心化身份标识符文档、以及所述身份持有者对业务开始请求的签名；

[0028] S42、所述验证证书机构基于所述请求返回可验证证书信息；

[0029] S43、所述身份持有者向所述可验证证书颁发机构发送证书颁发请求，所述证书颁发请求包括所述身份持有者的所述去中心化身份标识符、所述可验证证书信息、以及所述身份持有者对证书颁发请求的签名；

[0030] S44、所述可验证证书颁发机构基于所述去中心化身份标识符请求所述持有者公钥，并对所述身份持有者对证书颁发请求的签名进行验证，并基于验证结果向所述身份持有者颁发所述可验证证书。

[0031] 在本发明所述的区块链中基于指纹识别生成分布式身份的方法中，所述可验证证书包括：所述身份持有者的去中心化身份标识符、颁发所述可验证证书的所述可验证证书颁发机构的去中心化身份标识符、所述身份持有者对所述可验证证书的签名、所述可验证

证书颁发机构对所述可验证证书的签名,以及需验证的内容。

[0032] 在本发明所述的区块链中基于指纹识别生成分布式身份的方法中,所述步骤S6进一步包括:

[0033] S61、所述验证证书机构根据所述可验证证书颁发机构的去中心化身份标识符向所述身份注册机构请求所述机构公钥,并使用所述机构公钥验证所述可验证证书颁发机构对所述可验证证书的签名以获得第一验证结果;

[0034] S62、所述验证证书机构根据所述身份持有者的去中心化身份标识符向所述身份注册机构请求所述持有者公钥,并使用所述持有者公钥验证所述身份持有者对所述可验证证书的签名以获得第二验证结果;

[0035] S63、基于所述第一验证结果、所述第二验证结果以及所述需验证的内容的验证结果,判定验证是否通过。

[0036] 本发明解决其技术问题采用的另一技术方案是,构造一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被处理器执行时实现所述的区块链中基于指纹识别生成分布式身份的方法。

[0037] 实施本发明的区块链中基于指纹识别生成分布式身份的方法和计算机可读存储介质,可以录入用户的指纹来生成指纹码,再通过指纹码作为随机种子来生成身份持有者私钥,从而可以使得身份持有者在使用身份信息的时候可以无需输入密码地使用身份信息和使用区块链上的资产,非常便于用户使用。进一步地,本发明还明确定义了身份持有者、可验证证书颁发机构的注册过程和验证过程,从而提供了安全有效的构建去中心化区块链身份的方法。

附图说明

[0038] 下面将结合附图及实施例对本发明作进一步说明,附图中:

[0039] 图1是本发明的区块链中基于指纹识别生成分布式身份的方法的第一优选实施例的流程图;

[0040] 图2是本发明的区块链中基于指纹识别生成分布式身份的方法的第二优选实施例的指纹码的生成流程示意图;

[0041] 图3是本发明的区块链中基于指纹识别生成分布式身份的方法的第二优选实施例的可验证证书颁发机构的注册流程示意图;

[0042] 图4是本发明的区块链中基于指纹识别生成分布式身份的方法的第二优选实施例的身份持有者的注册流程示意图;

[0043] 图5是本发明的区块链中基于指纹识别生成分布式身份的方法的第二优选实施例的可验证证书的验证流程示意图。

具体实施方式

[0044] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。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。

[0045] 本发明涉及一种区块链中基于指纹识别生成分布式身份的方法。扫描身份持有者

的指纹以生成指纹码，基于所述指纹码生成持有者私钥和持有者公钥。可验证证书颁发机构基于自身密钥向身份注册机构进行注册。所述身份持有者基于所述持有者私钥和所述持有者公钥向所述可验证证书颁发机构进行注册。所述身份持有者基于所述验证证书机构的要求从所述可验证证书颁发机构获取可验证证书。所述身份持有者采用所述持有者私钥对所述可验证证书进行签名并提交到所述验证证书机构。所述验证证书机构对所述可验证证书进行验证。实施本发明的区块链中基于指纹识别生成分布式身份的方法和计算机可读存储介质，可以录入用户的指纹来生成指纹码，再通过指纹码作为随机种子来生成身份持有者私钥，从而可以使得身份持有者在使用身份信息的时候可以无需输入密码地使用身份信息和使用区块链上的资产，非常便于用户使用。进一步地，本发明还明确定义了身份持有者、可验证证书颁发机构的注册过程和验证过程，从而提供了安全有效的构建去中心化区块链身份的方法。

[0046] 图1是本发明的区块链中基于指纹识别生成分布式身份的方法的第一优选实施例的流程图。如图1所示，在步骤S1中，扫描身份持有者的指纹以生成指纹码，并基于所述指纹码生成持有者私钥和持有者公钥。在本发明的一个优选实施例中，所述步骤S1进一步包括扫描所述身份持有者的指纹以生成指纹码；对所述指纹码做哈希，使用获得的哈希值作为随机种子生成所述持有者私钥；然后基于所述持有者私钥生成所述持有者公钥。本领域技术人员知悉，指纹码可以采用本领域中任何的指纹采集器生成。针对获得的指纹码，可以采用哈希函数，将其进行计算，从而获得具有唯一固定长度的字符串，并将其作为随机种子生成所述持有者私钥。在此，可以采用任何已知方法生成持有者私钥。

[0047] 可以采用任何已知的方法生成所述持有者公钥，例如可以采用椭圆曲线密钥体系获取所述持有者公钥，例如R＝r*G。其中，G表示椭圆曲线算法中的私钥公钥换算因子。因此可以从持有者私钥r推导出持有者公钥R，但是无法从持有者公钥R推导出持有者私钥r，因此是不可逆的。

[0048] 在步骤S2中，可验证证书颁发机构基于自身密钥向身份注册机构进行注册。在本发明的优选实施例中，所述可验证证书颁发机构生成机构私钥并基于所述机构私钥生成机构公钥。所述可验证证书颁发机构生成注册请求，并采用所述机构私钥签名所述注册请求，并将签名注册请求发送到所述身份注册机构。所述身份注册机构验证所述签名注册请求，并在验证通过后生成所述可验证证书颁发机构的去中心化身份标识符和去中心化身份标识符文档。如果验证没有通过，则注册流程结束，显示注册失败。在本发明的优选实施例中，如前所述，所述机构私钥和机构公钥的生成同样可以采用椭圆曲线密钥体系获得。当然，也可以采用本领域中已知的任何密钥生成算法。

[0049] 在步骤S3中，所述身份持有者基于所述持有者私钥和所述持有者公钥向所述可验证证书颁发机构进行注册。在本发明的优选实施例中，所述身份持有者向所述可验证证书颁发机构提交注册请求，并采用所述持有者私钥签名所述注册请求，并将签名注册请求发送到所述可验证证书颁发机构。所述可验证证书颁发机构验签所述签名注册请求，如果验签没有通过，则注册流程结束，显示注册失败。如果验签通过，则在验签通过后验证所述身份持有者的注册信息。同样的，如果验证失败，则注册流程结束，显示注册失败。如果验证通过，在验证通过之后继续向所述身份注册机构发送验证请求，所述验证请求中包含所述持有者公钥。所述身份注册机构根据所述持有者公钥生成所述身份持有者的去中心化身份标

识符和去中心化身份标识符文档，并将其返回给所述可验证证书颁发机构。所述可验证证书颁发机构将所述身份持有者的去中心化身份标识符和去中心化身份标识符文档返回给所述身份持有者。

[0050] 在步骤S4中，所述身份持有者基于所述验证证书机构的要求从所述可验证证书颁发机构获取可验证证书。在本发明的优选实施例中，所述身份持有者向所述验证证书机构发送业务开始请求，所述业务开始请求包括所述去中心化身份标识符、所述去中心化身份标识符文档、以及所述身份持有者对业务开始请求的签名。所述可验证证书信息例如可以是可验证证书的类型信息，其可以根据所述身份持有者的业务开始请求确定，例如可以是所述身份持有者的某个属性，比如年龄、资产金额、身体健康状况等等。所述身份持有者向所述可验证证书颁发机构发送证书颁发请求，所述证书颁发请求包括所述身份持有者的所述去中心化身份标识符、所述可验证证书信息、以及所述身份持有者对证书颁发请求的签名。所述可验证证书颁发机构基于所述去中心化身份标识符请求所述持有者公钥，并对所述身份持有者对证书颁发请求的签名进行验证，并基于验证结果向所述身份持有者颁发所述可验证证书。所述验证证书机构基于所述请求返回可验证证书信息。优选的，所述可验证证书包括：所述身份持有者的去中心化身份标识符、颁发所述可验证证书的所述可验证证书颁发机构的去中心化身份标识符、所述身份持有者对所述可验证证书的签名、所述可验证证书颁发机构对所述可验证证书的签名，以及需验证的内容。在此，所述需验证的内容可以是所述身份持有者的某个属性，比如年龄、资产金额、身体健康状况等等。

[0051] 在步骤S5中，所述身份持有者采用所述持有者私钥对所述可验证证书进行签名并提交到所述验证证书机构。

[0052] 在步骤S6中，所述验证证书机构对所述可验证证书进行验证。在本发明的优选实施例中，整个验证过程可以包括如下步骤。所述验证证书机构根据所述可验证证书颁发机构的去中心化身份标识符向所述身份注册机构请求所述机构公钥，并使用所述机构公钥验证所述可验证证书颁发机构对所述可验证证书的签名以获得第一验证结果。所述验证证书机构根据所述身份持有者的去中心化身份标识符向所述身份注册机构请求所述持有者公钥，并使用所述持有者公钥验证所述身份持有者对所述可验证证书的签名以获得第二验证结果。基于所述第一验证结果、所述第二验证结果以及所述需验证的内容的验证结果，判定验证是否通过。

[0053] 实施本发明的区块链中基于指纹识别生成分布式身份的方法，可以录入用户的指纹来生成指纹码，再通过指纹码作为随机种子来生成身份持有者私钥，从而可以使得身份持有者在使用身份信息的时候可以无需输入密码地使用身份信息和使用区块链上的资产，非常便于用户使用。进一步地，本发明还明确定义了身份持有者、可验证证书颁发机构的注册过程和验证过程，从而提供了安全有效的构建去中心化区块链身份的方法。

[0054] 图2是本发明的区块链中基于指纹识别生成分布式身份的方法的第二优选实施例的指纹码的生成流程示意图。图3是本发明的区块链中基于指纹识别生成分布式身份的方法的第二优选实施例的可验证证书颁发机构的注册流程示意图。图4是本发明的区块链中基于指纹识别生成分布式身份的方法的第二优选实施例的身份持有者的注册流程示意图。图5是本发明的区块链中基于指纹识别生成分布式身份的方法的第二优选实施例的可验证证书的验证流程示意图。

[0055] 下面结合图2-5对本发明的第二优选实施例说明如下。首先对本发明中使用到的进行术语解释如下：

[0056] 去中心化身份标识符(Decentralized Identifier,简称DID)

[0057] 一串作用类似于URL的字符串,其标准可以遵循w3c或者dif等标准组织制定的标准,也可以遵循多个联盟机构制定的标准。DID记录了在多个联盟机构内唯一的身份标识符,以及查找DID所需要的协议。多个联盟机构可以根据DID定位到存储了DID详细信息的实体,并向该实体请求DID的详细信息,包括公钥等。

[0058] 去中心化身份标志符文档(Decentralized Identifier Document,简称DID文档)

[0059] DID文档保存了DID的详细信息,包括:DID的公钥,DID签名类型,DID认证类型,DID支持的服务类型以及支持DID服务的URL等。

[0060] 指纹码(Fingerprint Code,简称FC)

[0061] 通过指纹录入并生成的唯一标识,在计算机存储介质上表现为一个长度固定的字符串

[0062] 指纹采集器(Fingerprint Code Collector,简称FCC)

[0063] 采集指纹并生成指纹码的机器

[0064] 哈希函数(Hash Function,简称HF)

[0065] 对计算机存储介质上内容进行计算后,得到唯一固定长度的函数,在本发明当中用于对指纹码生成唯一固定长度的字符串

[0066] 私钥(Secret Key,简称SK)

[0067] 用于发送消息前,加签本发明各个实体之间交互的消息的密钥,证明实体身份的真实性,该密钥隐私不可见

[0068] 公钥(Public Key,简称PK)

[0069] 用于验证各个实体之间交互的消息的密钥,该密钥公开

[0070] 身份持有者(Identifier Holder,简称IH)

[0071] 持有唯一身份的人,身份持有者需要通过录入指纹来生成自己的SK和PK

[0072] 可验证证书(Verifiable Credentials,简称VC)

[0073] 可以验证的证书,证书中包含颁发证书的机构,以及需要验证的信息,以及颁发机构对该证书的签名等信息

[0074] 可验证证书颁发机构(ISSUER,简称IS)

[0075] 被信任的有资格颁发VC证书的机构,可以是学校,银行,律师事务所,公立医院,连锁饭店,连锁酒店等。

[0076] 验证证书机构(Inspector Verifier,简称IV)

[0077] 需要对IH进行身份验证的机构,例如:用人单位,信贷机构等。IV不仅可以对IH的身份进行验证,并且可以对IH的某个属性进行验证,例如:年龄,资产金额,身体健康状况等。

[0078] 身份注册机构(Identifier Registry,简称IR)

[0079] 用于注册身份的机构,维护本发明当中所有实体的DID的数据库,如某条区块链、分布式账本。

[0080] 在图3所示实施例中,首先IS向IR注册,以获取得到颁发VC的资格,其具体注册步

骤如下：

[0081] ①IS首先生成一个SK，然后通过SK再生成PK；

[0082] ②IS通过SK加签注册请求，并将请求提交到IR；

[0083] ③IR对IS的注册请求进行验证，验证通过之后生成IS的DID，以及DID文档。

[0084] 在图4所示实施例中，IH向IS注册，其具体注册步骤如下：

[0085] ①IH通过录入单个手指的指纹生成唯一的指纹码也就是FC，并通过HF对FC做哈希，生成唯一的哈希值

[0086] ②将唯一哈希值作为生成SK的随机种子，生成SK；

[0087] ③通过SK生成PK；

[0088] ④IH提交注册请求到IS，IS对IH的请求进行验签，并对IH的注册信息进行验证；

[0089] ⑤如果验证通过，则继续向IR提交验证请求，验证请求当中包含IH的公钥；

[0090] ⑥IR根据IS的请求，针对IH的公钥生成DID和DID文档，返回给IS；

[0091] ⑦IS将DID和DID文档返回给IH。

[0092] 在图5所示实施例中IH使用VC向IV进行认证。IH需要进行某项业务，而进行业务的前提条件是IV需要确认IH具有进行该业务的资格，例如：年龄，资产金额等。其具体步骤如下

[0093] ①IH向IV发送业务开始请求，该业务开始请求包括：IH的DID、DID文档，以及IH对业务请求的签名；而IV返回可验证证书信息，该可验证证书信息即为需要IH提交VC的信息，VC的内容包括：IH的DID，颁发VC的IS的DID，IH对VC的签名，IS对VC的签名，需验证的内容(例如年龄、资产金额、身体健康状况等等)。

[0094] ②IH向IS发送VC颁发请求，该VC颁发请求当中携带如下信息：IH的DID、所述可验证证书信息(包含例如年龄、资产金额、身体健康状况等等需要验证的内容)，IH对本次请求的签名。

[0095] ③IS根据IH的DID向IR请求IH的公钥，并对IH的请求签名进行验证，如果验证通过，则颁发VC给IH，否则拒绝颁发VC给IH。

[0096] ④IH提交VC到IV，IV对VC进行认证，具体认证过程如下：

[0097] 根据VC当中IS的DID向IR请求IS的公钥；

[0098] 使用IS的公钥验证VC当中IS的签名；

[0099] 根据VC当中IH的DID向IR请求IH的公钥；

[0100] 使用IH的公钥验证VC当中IH的签名；

[0101] 如果IS和IH的签名都验证通过，则判断所述需要验证的内容是否符合条件，如符合要求则验证通过，否则验证不通过。

[0102] 实施本发明的区块链中基于指纹识别生成分布式身份的方法，可以录入用户的指纹来生成指纹码，再通过指纹码作为随机种子来生成身份持有者私钥，从而可以使得身份持有者在使用身份信息的时候可以无需输入密码地使用身份信息和使用区块链上的资产，非常便于用户使用。进一步地，本发明还明确定义了身份持有者、可验证证书颁发机构的注册过程和验证过程，从而提供了安全有效的构建去中心化区块链身份的方法。

[0103] 本发明解决其技术问题采用的另一技术方案是，构造一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行时实现所述的区块链中基于指纹识别生成

分布式身份的方法。

[0104] 实施本发明的计算机可读存储介质，可以录入用户的指纹来生成指纹码，再通过指纹码作为随机种子来生成身份持有者私钥，从而可以使得身份持有者在使用身份信息的时候可以无需输入密码地使用身份信息和使用区块链上的资产，非常便于用户使用。进一步地，本发明还明确定义了身份持有者、可验证证书颁发机构的注册过程和验证过程，从而提供了安全有效的构建去中心化区块链身份的方法。

[0105] 因此，本发明可以通过硬件、软件或者软、硬件结合来实现。本发明可以在至少一个计算机系统中以集中方式实现，或者由分布在几个互连的计算机系统中的不同部分以分散方式实现。任何可以实现本发明方法的计算机系统或其它设备都是可适用的。常用软硬件的结合可以是安装有计算机程序的通用计算机系统，通过安装和执行程序控制计算机系统，使其按本发明方法运行。

[0106] 本发明还可以通过计算机程序产品进行实施，程序包含能够实现本发明方法的全部特征，当其安装到计算机系统中时，可以实现本发明的方法。本文件中的计算机程序所指的是：可以采用任何程序语言、代码或符号编写的一组指令的任何表达式，该指令组使系统具有信息处理能力，以直接实现特定功能，或在进行下述一个或两个步骤之后实现特定功能：a)转换成其它语言、编码或符号；b)以不同的格式再现。

[0107] 虽然本发明是通过具体实施例进行说明的，本领域技术人员应当明白，在不脱离本发明范围的情况下，还可以对本发明进行各种变换及等同替代。另外，针对特定情形或材料，可以对本发明做各种修改，而不脱离本发明的范围。因此，本发明不局限于所公开的具体实施例，而应当包括落入本发明权利要求范围内的全部实施方式。

[0108] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

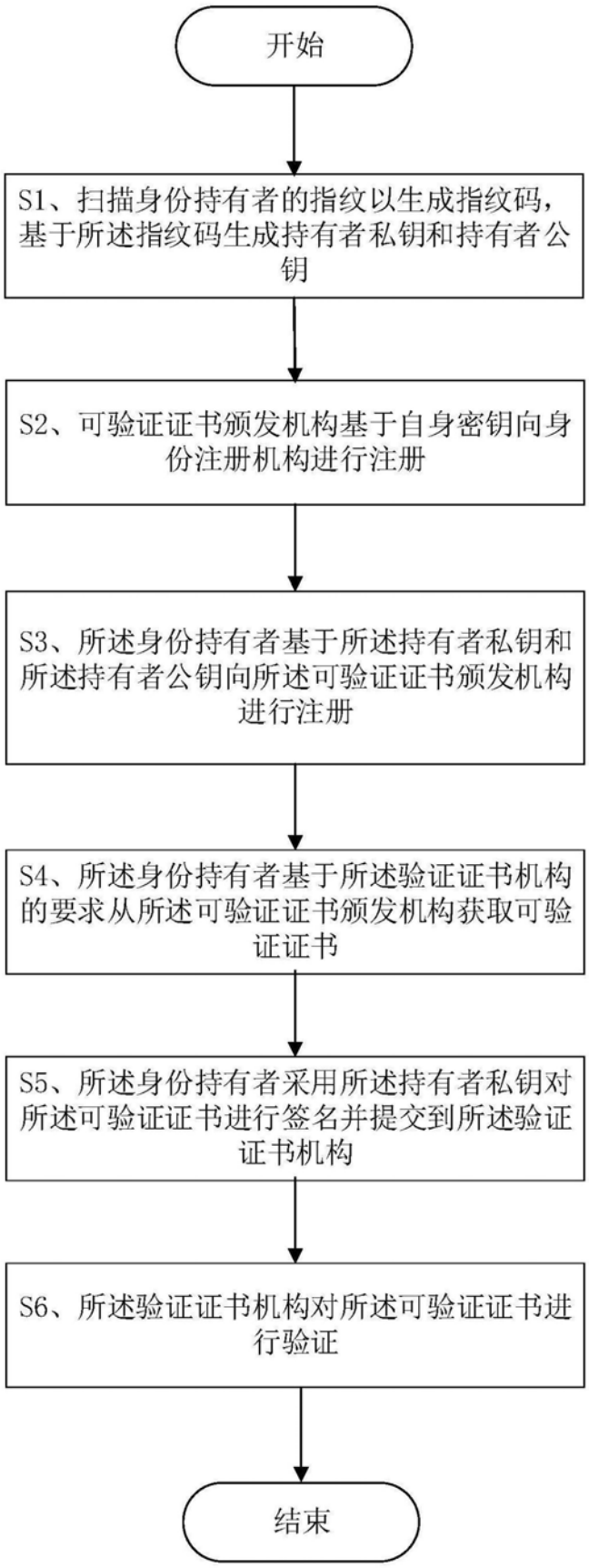
开始
S1、扫描身份持有者的指纹以生成指纹码，基于所述指纹码生成持有者私钥和持有者公钥
S2、可验证证书颁发机构基于自身密钥向身份注册机构进行注册
S3、所述身份持有者基于所述持有者私钥和所述持有者公钥向所述可验证证书颁发机构进行注册
S4、所述身份持有者基于所述验证证书机构的要求从所述可验证证书颁发机构获取可验证证书
S5、所述身份持有者采用所述持有者私钥对所述可验证证书进行签名并提交到所述验证证书机构
S6、所述验证证书机构对所述可验证证书进行验证
结束

图1

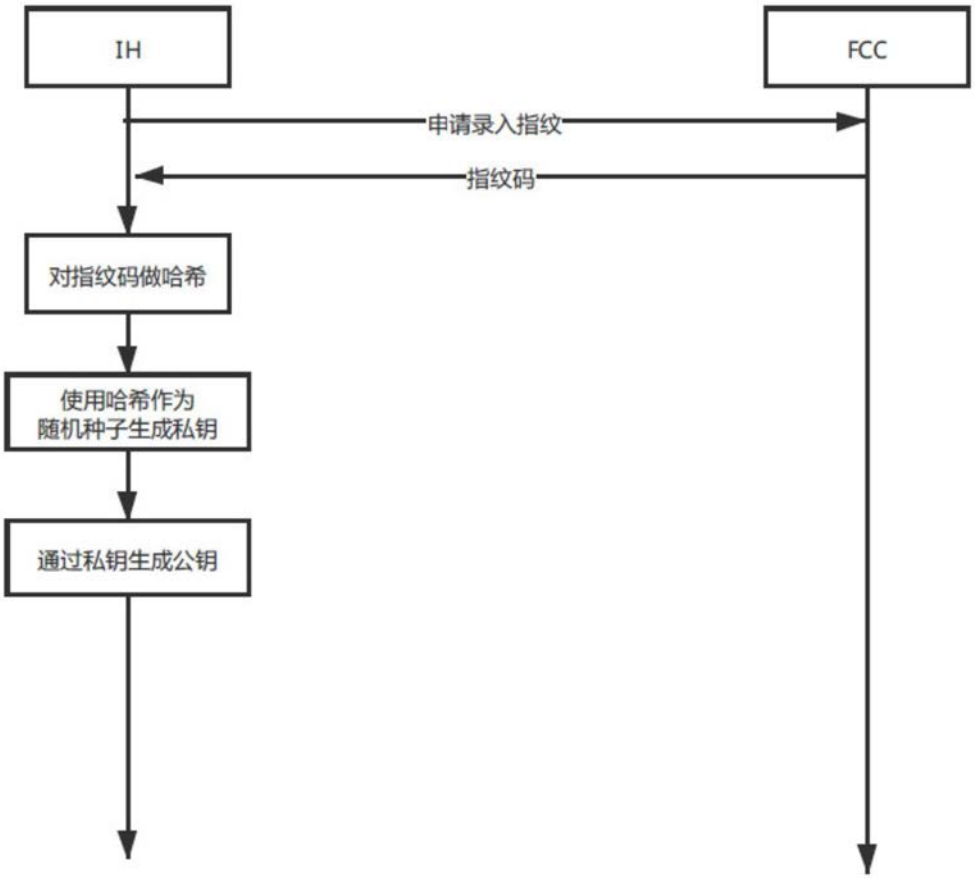

图2

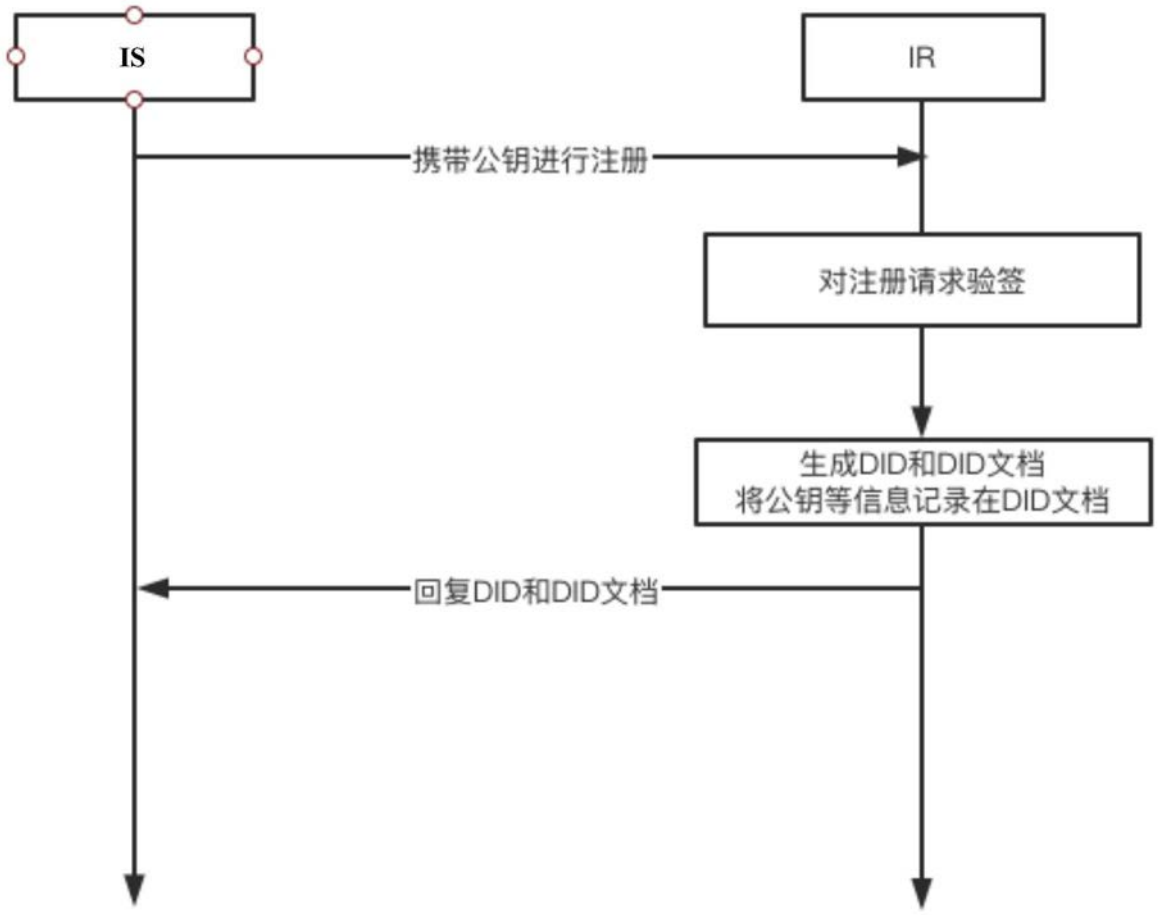
IS
IR
携带公钥进行注册
对注册请求验签
生成DID和DID文档
将公钥等信息记录在DID文档
回复DID和DID文档

图3

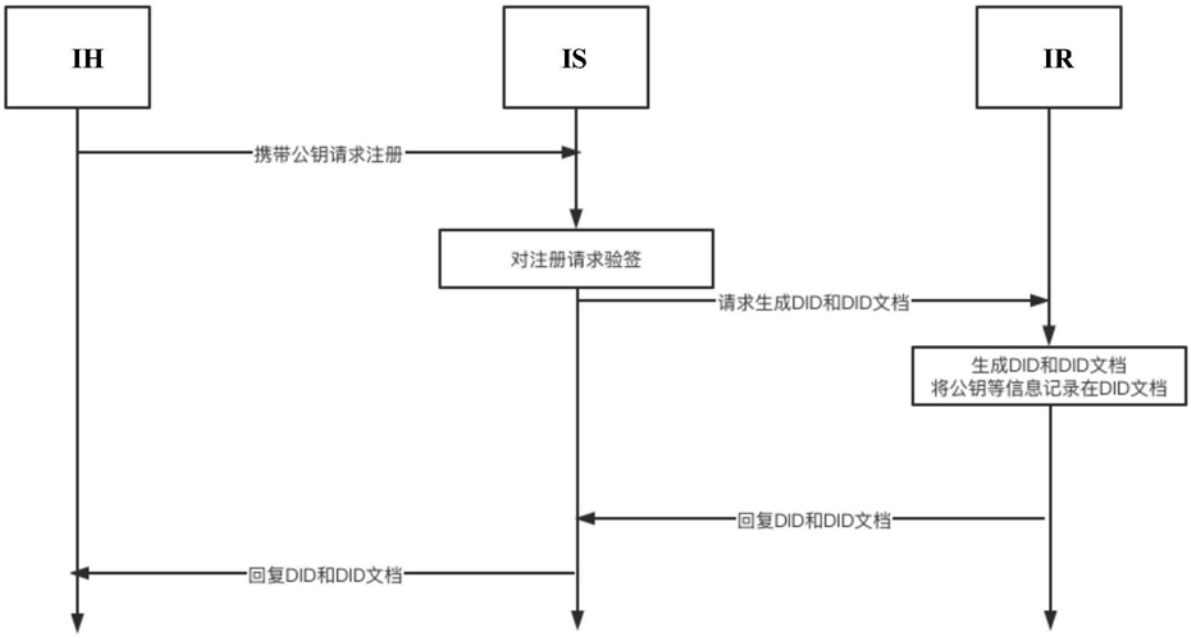
IH
IS
IR
携带公钥请求注册
对注册请求验签
请求生成DID和DID文档
生成DID和DID文档
将公钥等信息记录在DID文档
回复DID和DID文档
回复DID和DID文档

图4

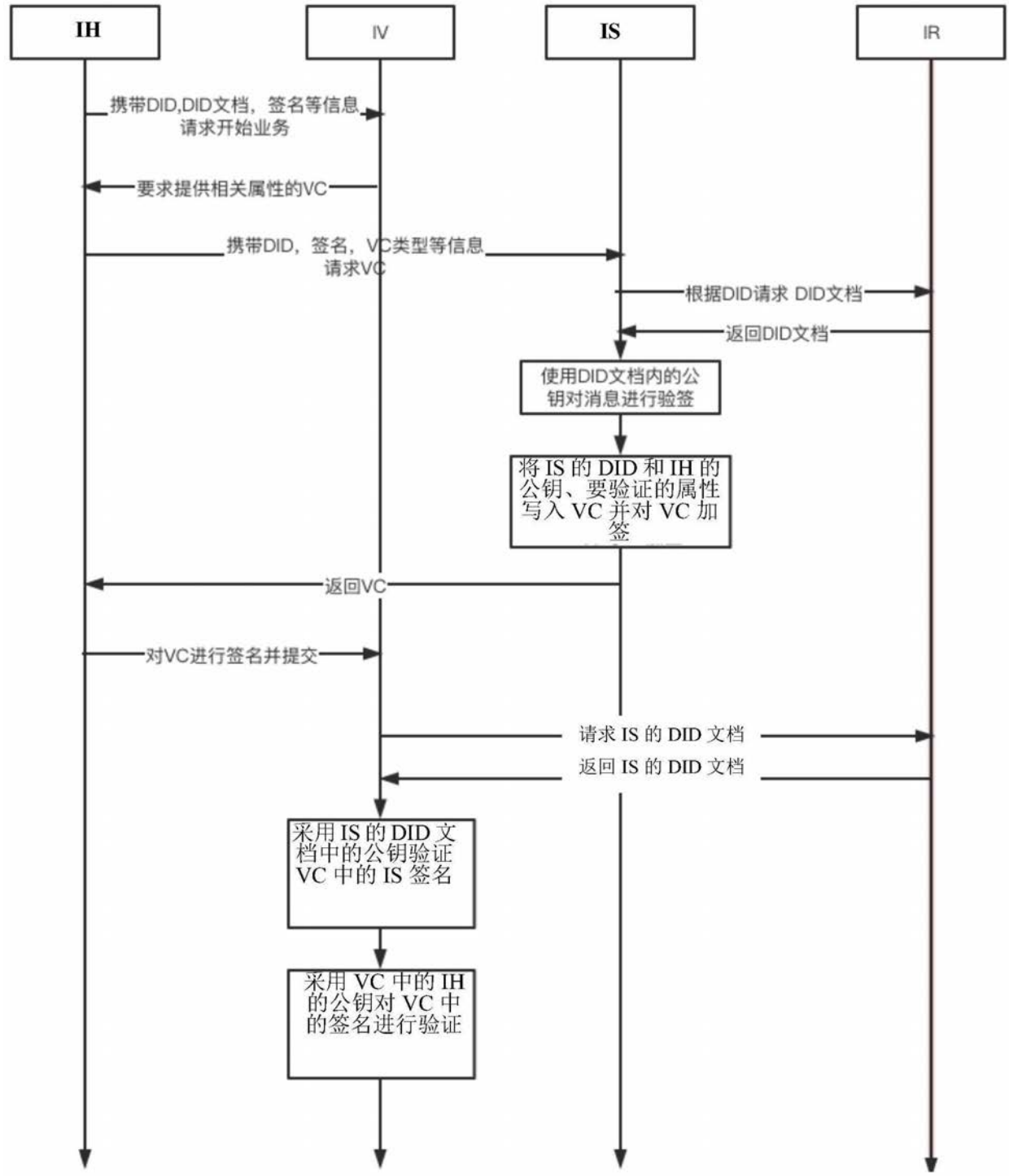
IH
IV
IS
IR
携带DID,DID文档，签名等信息
请求开始业务
要求提供相关属性的VC
携带DID，签名，VC类型等信息
请求VC
根据DID请求 DID文档
返回DID文档
使用DID文档内的公钥对消息进行验签
将 IS 的 DID 和 IH 的公钥、要验证的属性写入 VC 并对 VC 加签
返回VC
对VC进行签名并提交
请求 IS 的 DID 文档
返回 IS 的 DID 文档
采用 IS 的 DID 文档中的公钥验证 VC 中的 IS 签名
采用 VC 中的 IH 的公钥对 VC 中的签名进行验证

图5