(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 105701372 A
(43)申请公布日 2016.06.22

(21)申请号 201510959207.6

(22)申请日 2015.12.18

(71)申请人 布比(北京)网络技术有限公司
地址 100094 北京市海淀区东北旺村南1号楼7层7590室

(72)发明人 蒋海 王璟 翟海滨 赵正涌 胡楠

(74)专利代理机构 北京工信联合知识产权代理事务所(普通合伙) 11266
代理人 郭一斐

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/33(2013.01)

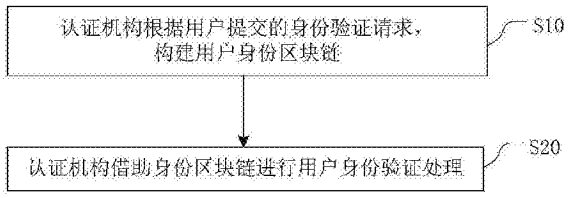
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种区块链身份构建及验证方法

(57)摘要

本发明涉及互联网上的身份构建及验证，提供一种区块链身份构建及验证方法，包括如下步骤：认证机构根据用户提交的身份验证请求，构建用户身份区块链；所述认证机构借助所述身份区块链进行用户身份验证处理。本发明将用户身份信息写入区块链，由多家认证机构通过共识机制共同完成身份信息的确认、存储，此后用户便可以方便地利用区块链进行身份验证。该方法不仅可以提高用户身份验证的效率，同时也不会因个别认证机构的问题影响用户身份信息的准确性，大幅提升身份验证过程的安全性。



CN 105701372 A

1.一种区块链身份构建及验证方法，包括如下步骤：

认证机构根据用户提交的身份验证请求，构建用户身份区块链；

所述认证机构借助所述身份区块链进行用户身份验证处理。

2.根据权利要求1所述的一种区块链身份构建及验证方法，其特征在于，所述构建用户身份区块链的过程包括如下步骤：

所述认证机构根据用户信息生成全网唯一的身份标识，并判断该用户是否为新用户；

如果该用户为新用户，则进行用户身份确认，确认通过后创建新的用户身份证书；如果该用户为老用户，则查询该用户已有的身份证书，并比较已有的用户身份证书信息与用户提交的身份验证请求信息是否一致，如果一致则返回用户证书已经存在的提示，如果不一致则对用户进行身份确认，确认通过则创建新的用户身份证书；

所述认证机构向所有参与身份区块链构建过程的其他所有认证机构广播用户的用户身份证书，并写入身份区块链；

如果接收广播的认证机构与发送广播的所述认证机构为相互信任关系，则接收广播的认证机构将该用户身份证书写入区块链，并向其他认证机构广播；如果接收广播的认证机构与发送广播的所述认证机构没有相互信任关系，则接收广播的认证机构对该用户进行身份确认，确认通过后则将该用户的身份证书写入区块链，并向其他认证机构广播，否则将拒绝将该用户的身份证书写入区块链，并向其他认证机构广播。

3.根据权利要求2所述的一种区块链身份构建及验证方法，其特征在于：

所述生成全网唯一身份标识的方法采用哈希算法，哈希算法的输入为用户信息，输出就是全网唯一身份标识。

4.根据权利要求2所述的一种区块链身份构建及验证方法，其特征在于，所述判断该用户是否为新用户的方法具体为：

所述认证机构保存当前区块链中所有用户的全网唯一身份标识，将所述认证机构根据用户信息生成的全网唯一身份标识与存储的全网唯一身份标识进行对比，未找到存储过的全网唯一身份标识则为新用户，否则为老用户。

5.根据权利要求2所述的一种区块链身份构建及验证方法，其特征在于，所述认证机构对该用户进行身份确认的步骤包括：生成随机数R，利用用户的公钥对随机数R进行加密，并发送给用户。用户需要利用用户的私钥进行解密得到R，进而利用认证机构的公钥对R+1进行加密，发送给认证机构。认证机构收到后，利用认证机构的私钥解密得到R+1，从而确认用户身份正确。

6.根据权利要求2所述的一种区块链身份构建及验证方法，其特征在于，所述认证机构生成用户身份证书的步骤包括：将全网唯一身份标识、用户信息、用户公钥、有效期、认证机构名称、认证机构标识以及扩展项，利用认证机构的密钥进行签名，并生成全网唯一的证书编号，该编号即为用户身份证书。

7.根据权利要求2所述的一种区块链身份构建及验证方法，其特征在于：

所述身份区块链的构建过程中，不同认证机构间的共识达成可以使用PoW、或PoS、或RPCA方式，当共识达成后，新的区块将纳入区块链，用户身份证书信息也纳入了区块链；所述身份区块链由身份区块组成，所述身份区块为周期性生成，所述身份区块包含区块生成时间、当前区块根HASH、前一区块根HASH以及用户身份证书信息。

8.根据权利要求1所述的一种区块链身份构建及验证方法，其特征在于：

所述身份验证请求包括用户信息、用户公钥和申请认证的有效期，所述用户信息包括用户姓名、单位、城市、国家及其他代表用户身份的信息。

9.根据权利要求1所述的一种区块链身份构建及验证方法，其特征在于，所述认证机构借助身份区块链进行用户身份验证包括下述三种情况：

第一种情况，如果所述认证机构参与了身份区块链的构建过程，则直接利用该用户的身份信息生成全网唯一身份标识，并在区块链中进行遍历查询，如果找到该用户的身份证书，则判断证书是否超过有效期，如果未超出有效期，则该用户证书有效，直接将证书发送给该用户即可完成身份验证，否则未找到该用户的身份证书，则身份验证失败；

第二种情况，如果所述认证机构并未参与身份区块链的构建过程，则所述认证机构将向其信任的认证机构列表发送身份证书获取请求，如果所述信任认证机构参与了身份区块链的构建过程，则由所述信任认证机构按照所述第一种情况获取该用户的身份证书，完成身份验证过程；

第三种情况，如果所述认证机构并未参与身份区块链的构建过程，且并未找到所述认证机构信任的认证机构参与了身份区块链的构建过程，则所述认证机构无法借助区块链完成该用户身份验证，需要使用传统方式进行单独的用户身份验证。

10.根据权利要求1所述的一种区块链身份构建及验证方法，其特征在于，所述方法还包括所述认证机构对用户身份区块链进行更新的步骤：

所述认证机构接收到用户的更新请求后，首先根据该用户信息生成全网唯一的身份标识，并通过身份标识查询该用户的已有身份证书，如果未找到，则更新失败；如果找到已有身份证书，则比较已有身份证书中的用户公钥、颁发者信息、有效期信息是否与更新请求中的信息一致，如果一致则更新失败，如果不一致，则首先进行该用户的身份确认，通过确认后为该用户创建新的用户身份证书，并写入身份区块链。

一种区块链身份构建及验证方法

技术领域

[0001] 本发明涉及互联网上的身份构建及验证，特别涉及一种区块链身份验证方法。

背景技术

[0002] 在现实生活中，政府颁发身份证以验证居民的身份。同样的，在互联网上用户也需要进行身份验证，只不过验证是通过认证机构以网络数据的形式颁发的。目前的互联网身份验证对认证机构的依赖性较强，存在如下几个问题：

[0003] (1)由于不同认证机构相对独立，用户往往需要在多个认证机构分别进行注册、登录、验证等操作，身份验证效率低下，用户使用不便；

[0004] (2)如果认证机构被攻击或者存在恶意欺诈，将会造成用户身份信息“失窃”甚至“被篡改”，直接威胁用户财产安全。

发明内容

[0005] 鉴于上述问题，提出了本发明，以便提供一种克服上述问题或至少部分地解决上述问题的一种区块链身份验证方法。

[0006] 作为本发明的一个方面，提供一种区块链身份构建及验证方法，所述方法包括如下步骤：

[0007] 认证机构根据用户提交的身份验证请求，构建用户身份区块链；

[0008] 所述认证机构借助所述身份区块链进行用户身份验证处理。

[0009] 进一步的，所述构建用户身份区块链的过程包括如下步骤：

[0010] 所述认证机构根据用户信息生成全网唯一的身份标识，并判断该用户是否为新用户；

[0011] 如果该用户为新用户，则进行用户身份确认，确认通过后创建新的用户身份证书；如果该用户为老用户，则查询该用户已有的身份证书，并比较已有的用户身份证书信息与用户提交的身份验证请求信息是否一致，如果一致则返回用户证书已经存在的提示，如果不一致则对用户进行身份确认，确认通过则创建新的用户身份证书；

[0012] 所述认证机构向所有参与身份区块链构建过程的其他所有认证机构广播用户的用户身份证书，并写入身份区块链；

[0013] 如果接收广播的认证机构与发送广播的所述认证机构为相互信任关系，则接收广播的认证机构将该用户身份证书写入区块链，并向其他认证机构广播；如果接收广播的认证机构与发送广播的所述认证机构没有相互信任关系，则接收广播的认证机构对该用户进行身份确认，确认通过后则将该用户的身份证书写入区块链，并向其他认证机构广播，否则将拒绝将该用户的身份证书写入区块链，并向其他认证机构广播。

[0014] 进一步的，所述生成全网唯一身份标识的方法采用哈希算法，哈希算法的输入为用户信息，输出就是全网唯一身份标识。

[0015] 进一步的，所述判断该用户是否为新用户的方法具体为：

[0016] 所述认证机构保存当前区块链中所有用户的全网唯一身份标识，将所述认证机构根据用户信息生成的全网唯一身份标识与存储的全网唯一身份标识进行对比，未找到存储过的全网唯一身份标识则为新用户，否则为老用户。

[0017] 进一步的，所述认证机构对该用户进行身份确认的步骤包括：生成随机数R，利用用户的公钥对随机数R进行加密，并发送给用户。用户需要利用用户的私钥进行解密得到R，进而利用认证机构的公钥对R+1进行加密，发送给认证机构。认证机构收到后，利用认证机构的私钥解密得到R+1，从而确认用户身份正确。

[0018] 进一步的，所述认证机构生成用户身份证书的步骤包括：将全网唯一身份标识、用户信息、用户公钥、有效期、认证机构名称、认证机构标识以及扩展项，利用认证机构的密钥进行签名，并生成全网唯一的证书编号，该编号即为用户身份证书。

[0019] 进一步的，所述身份区块链的构建过程中，不同认证机构间的共识达成可以使用PoW、或PoS、或RPCA方式，当共识达成后，新的区块将纳入区块链，用户身份证书信息也纳入了区块链；所述身份区块链由身份区块组成，所述身份区块为周期性生成，所述身份区块包含区块生成时间、当前区块根HASH、前一区块根HASH以及用户身份证书信息。

[0020] 进一步的，所述身份验证请求包括用户信息、用户公钥和申请认证的有效期，所述用户信息包括用户姓名、单位、城市、国家及其他代表用户身份的信息。

[0021] 进一步的，所述认证机构借助身份区块链进行用户身份验证包括下述三种情况：

[0022] 第一种情况，如果所述认证机构参与了身份区块链的构建过程，则直接利用该用户的身份信息生成全网唯一身份标识，并在区块链中进行遍历查询，如果找到该用户的身份证书，则判断证书是否超过有效期，如果未超出有效期，则该用户证书有效，直接将证书发送给该用户即可完成身份验证，否则未找到该用户的身份证书，则身份验证失败；

[0023] 第二种情况，如果所述认证机构并未参与身份区块链的构建过程，则所述认证机构将向其信任的认证机构列表发送身份证书获取请求，如果所述信任认证机构参与了身份区块链的构建过程，则由所述信任认证机构按照所述第一种情况获取该用户的身份证书，完成身份验证过程；

[0024] 第三种情况，如果所述认证机构并未参与身份区块链的构建过程，且并未找到所述认证机构信任的认证机构参与了身份区块链的构建过程，则所述认证机构无法借助区块链完成该用户身份验证，需要使用传统方式进行单独的用户身份验证。

[0025] 进一步的，所述方法还包括所述认证机构对用户身份区块链进行更新的步骤：

[0026] 所述认证机构接收到用户的更新请求后，首先根据该用户信息生成全网唯一的身份标识，并通过身份标识查询该用户的已有身份证书，如果未找到，则更新失败；如果找到已有身份证书，则比较已有身份证书中的用户公钥、颁发者信息、有效期信息是否与更新请求中的信息一致，如果一致则更新失败，如果不一致，则首先进行该用户的身份确认，通过确认后为该用户创建新的用户身份证书，并写入身份区块链。

[0027] 本发明提出的一种区块链身份构建及验证方法，将用户身份信息写入区块链，由多家认证机构通过共识机制共同完成身份信息的确认、存储，此后用户便可以方便地利用区块链进行身份验证。该方法不仅可以提高用户身份验证的效率，同时也不会因个别认证机构的问题影响用户身份信息的准确性，大幅提升身份验证过程的安全性。

附图说明

[0028] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例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发明的一些实施例，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。

[0029] 图1为本发明一个实施例的一种区块链身份构建及验证方法的流程示意图。

[0030] 图2为本发明一个实施例的构建用户身份区块链的过程的流程示意图。

[0031] 图3为本发明一个实施例的用户身份证书的结构示意图。

[0032] 图4为本发明一个实施例的身份区块链结构示意图。

具体实施方式

[0033] 下面将参照附图更详细的描述本发明的示例性实施例。虽然附图中显示了本发明的示例性实施例，然而应当理解，可以以各种形式实现本发明，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更透彻的理解本发明，并且能够将本发明的范围完整的传达给本领域的技术人员。

[0034] 图1示出了根据本发明一个实施例的一种区块链身份构建及验证方法的流程示意图。如图1所示，一种区块链身份构建及验证方法，包括如下步骤：

[0035] 步骤S10，认证机构根据用户提交的身份验证请求，构建用户身份区块链。

[0036] 假设用户i向其信任的认证机构G提交了身份验证请求，身份验证请求包括用户信息(比如用户姓名、单位、城市、国家及其他代表用户身份的信息)、用户公钥、申请认证有效期等，认证机构G接收到用户i的身份验证请求后，构建用户i的身份区块链。

[0037] 具体的，如图2所示，构建用户身份区块链的过程，包括如下步骤：

[0038] 步骤S101，认证机构根据用户信息生成全网唯一的身份标识，并判断该用户是否为新用户。

[0039] 认证机构G接收到用户i的身份验证请求后，首先根据用户信息(比如用户姓名、单位、城市、国家及其他代表用户身份的信息)生成全网唯一的身份标识，根据生成的全网唯一身份标识，判断用户i是否为新用户。生成全网唯一身份标识的方法有多种，比如，可以利用HASH(哈希)算法生成全网唯一身份标识，哈希算法的输入为用户信息，输出就是全网唯一身份标识，这样做的目的可以加快查找速度。原则上，同样的输入会产生同样的HASH输出，而不同的输入产生的输出肯定不同。这类的HASH算法有很多，比如MD5算法、SHA-1算法等。认证机构可以保存当前区块链中所有用户的全网唯一身份标识，可将认证机构根据用户信息生成的全网唯一身份标识与存储过的全网唯一身份标识进行对比，来判断该用户是新用户还是老用户，未找到存储过的全网唯一身份标识则为新用户，否则为老用户。

[0040] 步骤S102，如果该用户为新用户，则进行用户身份确认，确认通过后创建新的用户身份证书；如果该用户为老用户，则查询该用户已有的身份证书，并比较已有的用户身份证书信息与用户提交的身份验证请求信息是否一致，如果一致则返回用户证书已经存在的提示，如果不一致则对用户进行身份确认，确认通过则创建新的用户身份证书。

[0041] 认证机构G对用户进行身份确认的步骤包括：生成随机数R，利用用户的公钥对随

机数R进行加密，并发送给用户。用户需要利用用户的私钥进行解密得到R，进而利用认证机构的公钥对R+1进行加密，发送给认证机构。认证机构收到后，利用认证机构的私钥解密得到R+1，从而确认用户身份正确。

[0042] 认证机构G生成用户身份证书的步骤包括：将全网唯一身份标识、用户信息、用户公钥、有效期、认证机构名称(作为颁发者名称)、认证机构标识(作为颁发者标识)以及扩展项，利用认证机构的密钥进行签名，并生成全网唯一的证书编号，该编号即为用户身份证书。

[0043] 作为本发明用户身份证书的另一实施例，用户身份证书也可以是更为复杂的身份证书，如图3所示，用户身份证书由证书编号、用户标识符、用户身份信息、用户公钥、颁发者名称、颁发者标识符、有效期、颁发者签名和扩展项组成。

[0044] 在比较已有的用户身份证书信息与用户提交的身份验证请求信息是否一致时，可以仅比较用户身份证书信息的某几项即可，比如仅比较用户公钥、颁布者信息和有效期是否与用户提交的身份验证请求信息是否一致即可，以提高处理速度。一般来说，用户可以生成一对公私钥就够了，出于安全考虑，也允许用户生成多对公私钥，这类算法比如有RSA算法、DSA算法等。

[0045] 步骤S103，认证机构向所有参与身份区块链构建过程的其他所有认证机构广播用户的用户身份证书，并写入身份区块链。

[0046] 步骤S104，如果接收广播的认证机构与发送广播的认证机构为相互信任关系，则接收广播的认证机构将该用户身份证书写入区块链，并向其他认证机构广播；如果接收广播的认证机构与发送广播的认证机构没有相互信任关系，则接收广播的认证机构对该用户进行身份确认，确认通过后则将该用户的身份证书写入区块链，并向其他认证机构广播，否则将拒绝将该用户的身份证书写入区块链，并向其他认证机构广播。

[0047] 认证机构G向所有参与身份区块链构建过程的其他所有认证机构广播用户i的身份证书，并要求写入身份区块链。其他认证机构收到了认证机构G的广播信息，设认 证机构H收到了G广播的用户i的身份证书信息，如果认证机构G与H间具有相互信任关系，则H也同意将用户i的身份证书写入区块链，并向其他机构广播；如果认证机构G与H间没有相互信任关系，则认证机构H将对用户i的身份信息进行确认，确认的过程同步骤S102，如果确认通过则认证机构H同意将用户i的身份证书写入区块链，并向其他机构广播，如果确认失败，则认证机构H拒绝将用户i的身份证书写入区块链，并向其他机构广播。

[0048] 区块链的构建过程中，不同认证机构间的共识达成可以使用成熟的PoW(Proof of Work，工作量证明)、PoS(Proof of Stake，权益证明)、RPCA(Ripple Consensus Algorithm，一致性算法)等方式。当共识达成后，新的区块将纳入区块链，用户身份证书信息也纳入了区块链。

[0049] 如图4所示，设参与用户身份区块链构建的认证机构包括认证机构1、认证机构2…认证机构N。身份区块链由身份区块组成，身份区块为周期性生成，不同身份区块的产生时间不同，产生时间越早的区块越靠前。身份区块包含区块生成时间、当前区块根HASH、前一区块根HASH、所包含的用户身份证书等信息。

[0050] 步骤S20，认证机构借助身份区块链进行用户身份验证处理。这里面包括如下几种情况：

[0051] 第一种情况，如果认证机构G参与了身份区块链的构建过程，则直接利用用户i的身份信息生成全网唯一身份标识，并在区块链中进行遍历查询，如果找到用户i的身份证书，则判断证书是否超过有效期，如果未超出有效期，则用户证书有效，直接将证书发送给用户即可完成身份验证，否则未找到用户i的身份证书，则身份验证失败。

[0052] 第二种情况，如果认证机构G并未参与身份区块链的构建过程，则认证机构G将向其信任的认证机构列表发送身份证书获取请求，如果认证机构H为G的信任认证机构且参与了身份区块链的构建过程，则由H按照第一种情况所说的方式获取用户i的身份证书，完成身份验证过程。

[0053] 第三种情况，如果认证机构G并未参与身份区块链的构建过程，且并未找到G信任的认证机构参与了身份区块链的构建过程，则认证机构无法借助区块链完成用户身份验证。需要使用传统方式进行单独的用户身份验证。

[0054] 作为本发明的进一步改进，本发明还包括认证机构对用户身份区块链进行更新的步骤，具体包括：

[0055] 用户i向其信任的认证机构G提交身份证书更新请求，提交的信息包括用户信息(姓名、单位、城市、国家等)、用户公钥、申请认证有效期等；

[0056] 认证机构G接收到用户i的更新请求后，首先根据用户信息生成全网唯一的身份标识，并通过身份标识查询该用户的已有身份证书，如果未找到，则更新失败；如果找到已有身份证书，则比较已有身份证书中的用户公钥、颁发者信息、有效期等信息是否与更新请求中的信息一致，如果一致则更新失败，如果不一致，则首先进行用户i的身份确认，身份确认步骤可参考步骤S102；通过确认后为用户创建新的用户身份证书，并按照步骤S104的方式写入身份区块链。

[0057] 通过上述实施例可知，本发明提出一种区块链身份构建及验证方法，将用户身份信息写入区块链，由多家认证机构通过共识机制共同完成身份信息的确认、存储，此后用户便可以方便地利用区块链进行身份验证。该方法不仅可以提高用户身份验证的效率，同时也不会因个别认证机构的问题影响用户身份信息的准确性，大幅提升身份验证过程的安全性。

[0058] 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本发明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，或者网络设备等)执行本发明各个实施例或者实施例的某些部分所述的方法。

[0059] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置或系统实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的装置及系统实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术

人员在不付出创造性劳动的情况下，即可以理解并实施。

[0060] 需要说明的是：

[0061] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定的编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明内容。

[0062] 本领域那些技术人员可以理解，可以对实施例中各模块进行自适应性的改变并且把它们设置在与该实施例不同的一个或多个设备中。除非另有明确陈述，本说明书中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0063] 本发明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。

[0064] 以上所述仅为本发明之较佳实施例，并非用以限定本发明的权利要求保护范围。同时以上说明，对于相关技术领域的技术人员应可以理解及实施，因此其他基于本发明所揭示内容所完成的等同改变，均应包含在本权利要求书的涵盖范围内。

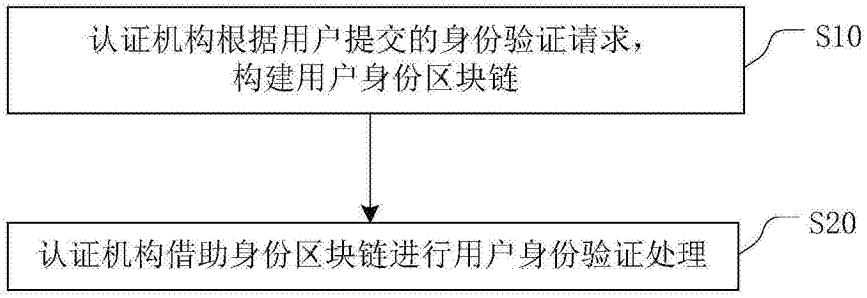

认证机构根据用户提交的身份验证请求，
构建用户身份区块链
S10
认证机构借助身份区块链进行用户身份验证处理
S20

图1

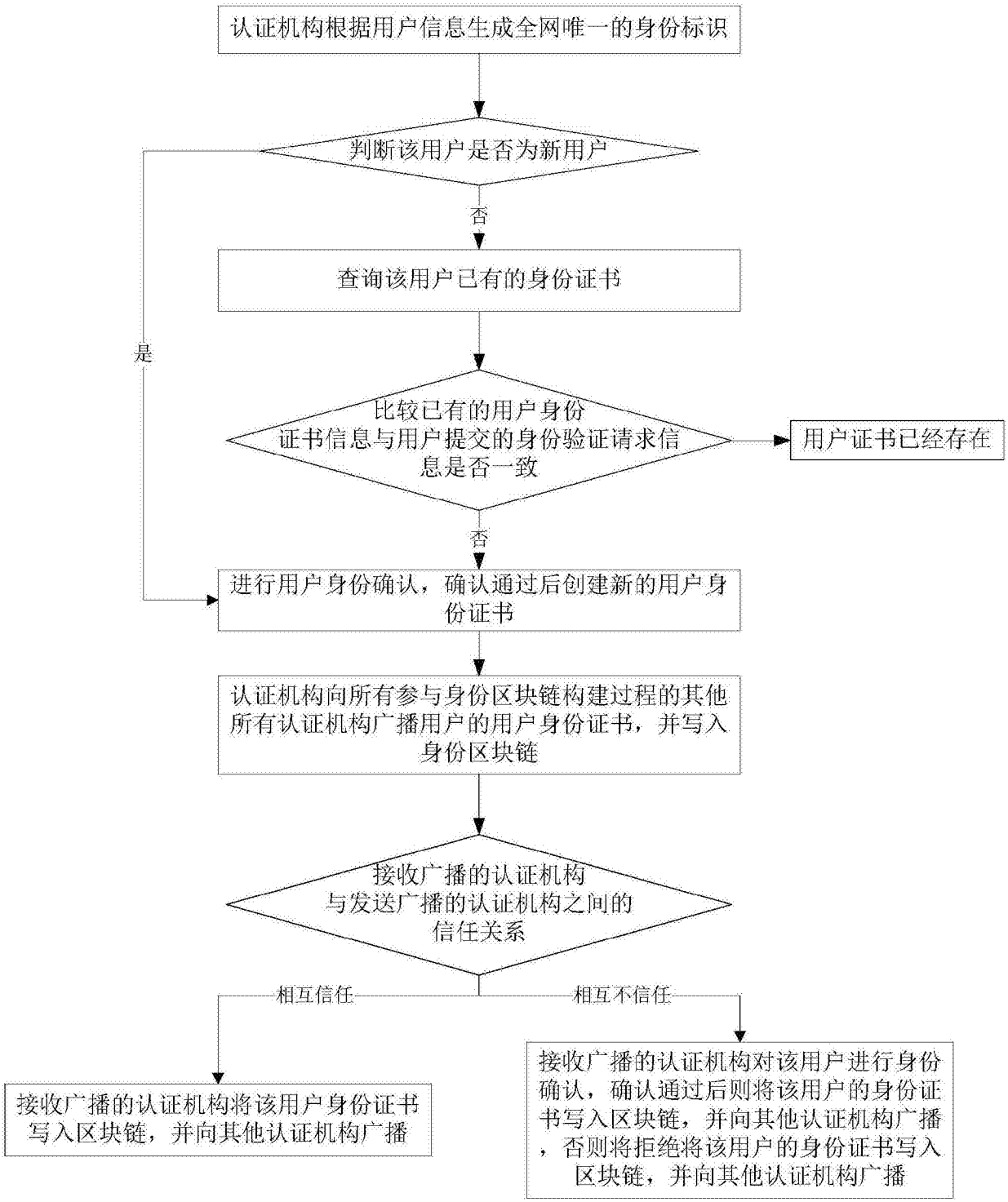

认证机构根据用户信息生成全网唯一的身份标识
判断该用户是否为新用户
否
查询该用户已有的身份证书
是
比较已有的用户身份证书信息与用户提交的身份验证请求信息是否一致
用户证书已经存在
否
进行用户身份确认，确认通过后创建新的用户身份证书
认证机构向所有参与身份区块链构建过程的其他所有认证机构广播用户的用户身份证书，并写入身份区块链
接收广播的认证机构与发送广播的认证机构之间的信任关系
相互信任
相互不信任
接收广播的认证机构将该用户身份证书写入区块链，并向其他认证机构广播
接收广播的认证机构对该用户进行身份确认，确认通过后则将该用户的身份证书写入区块链，并向其他认证机构广播，否则将拒绝将该用户的身份证书写入区块链，并向其他认证机构广播

图2

证书编号
用户标识符
用户身份信息
用户公钥
颁发者名称
颁发者标识符
有效期
颁发者签名
扩展项

图3

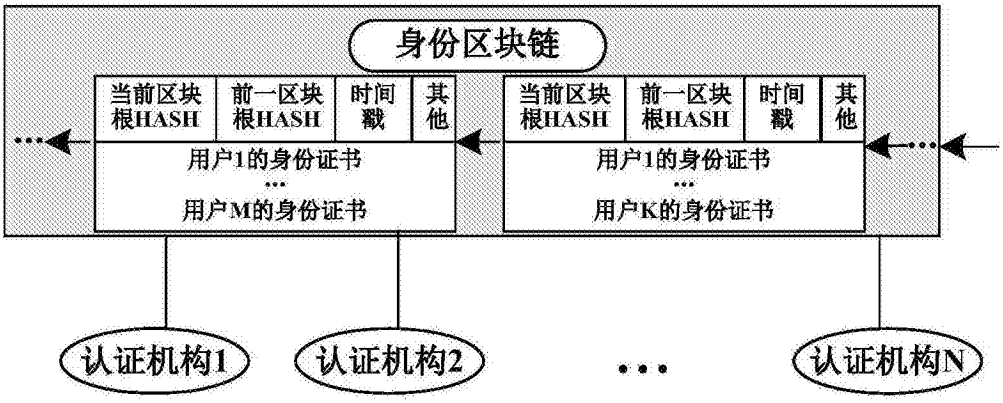


图4