(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 107079037 B
(45)授权公告日 2018.10.23

(21)申请号 201680003232.X
(22)申请日 2016.09.18
(65)同一申请的已公布的文献号
申请公布号 CN 107079037 A
(43)申请公布日 2017.08.18
(85)PCT国际申请进入国家阶段日
2017.04.14
(86)PCT国际申请的申请数据
PCT/CN2016/099254 2016.09.18
(87)PCT国际申请的公布数据
WO2018/049656 ZH 2018.03.22

(73)专利权人 深圳前海达闼云端智能科技有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司)
(72)发明人 谢辉 王健
(74)专利代理机构 北京英创嘉友知识产权代理事务所(普通合伙) 11447
代理人 魏嘉熹 南毅宁

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

审查员 陈莹

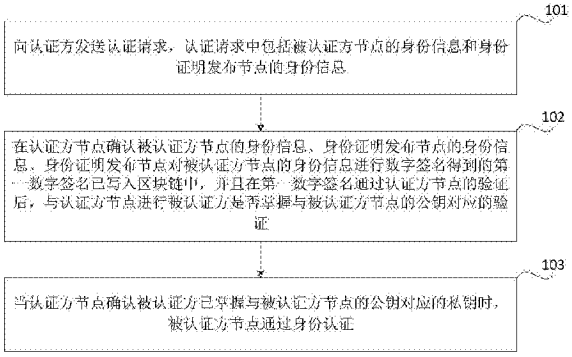
权利要求书7页 说明书20页 附图11页

(54)发明名称

基于区块链的身份认证方法、装置、节点及系统

(57)摘要

本发明公开了一种基于区块链的身份认证方法、装置、节点及系统，涉及安全技术领域。该方法包括：接收被认证方节点发送的认证请求，认证请求包括被认证方节点和身份证明发布节点的身份信息；在确认这些信息，以及身份证明发布节点对被认证方节点的身份信息的数字签名写入区块链中时，根据身份证明发布节点的公钥对该数字签名进行验证；在该一数字签名通过验证后，向验证被认证方是否掌握与被认证方节点的公钥对应的私钥；被认证方节点的公钥是根据被认证方节点的身份信息获取的；当确认被认证方已掌握与被认证方节点的公钥对应的私钥时，确定被认证方节点通过身份认证。



CN 107079037 B

1.一种基于区块链的身份认证方法，其特征在于，应用于认证方节点，所述方法包括：

接收被认证方节点发送的认证请求，所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息；

在确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息，以及所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中时，根据所述身份证明发布节点的公钥对所述第一数字签名进行验证；所述身份证明发布节点的公钥是根据所述身份证明发布节点的身份信息获取的；

在所述第一数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥；所述被认证方节点的公钥是根据所述被认证方节点的身份信息获取的；

当确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时，确定所述被认证方节点通过身份认证。

2.根据权利要求1所述的方法，其特征在于，所述在所述第一数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥，包括：

在所述第一数字签名通过验证后，向所述被认证方节点发送验证信息；

接收所述被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第二数字签名；

根据所述被认证方节点的公钥对所述第二数字签名进行验证；

当所述第二数字签名通过验证时，确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

3.根据权利要求1所述的方法，其特征在于，所述在所述第一数字签名通过验证后，向所述被认证方确认所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥，包括：

接收所述被认证方节点发送的验证信息，以及被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第三数字签名；所述验证信息是所述被认证方节点根据预设的信息生成规则生成的，所述信息生成规则预设置在所述被认证方节点和所述认证方节点；

验证所述验证信息是否是按照所述信息生成规则生成的；

当所述验证信息是按照所述信息生成规则生成的时，根据所述被认证方节点的公钥对所述第三数字签名进行验证；

当所述第三数字签名通过验证时，确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

4.根据权利要求1所述的方法，其特征在于，当所述身份证明发布节点存在上一级身份证明发布节点时，所述根据所述身份证明发布节点的公钥对所述第一数字签名进行验证，包括：

从所述区块链中获取所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名；

根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证；所述上一级身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的；

在所述第四数字签名通过验证后，根据所述身份证明发布节点的公钥对所述第一数字签名进行验证，所述身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储

的。

5.根据权利要求1所述的方法，其特征在于，所述在所述第一数字签名通过验证后，在验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥之前，还包括：

在所述第一数字签名通过验证后，从所述区块链中获取上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名；

根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证；所述上一级身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的；

在所述第四数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥。

6.根据权利要求1-5任一项所述的方法，其特征在于，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的；所述身份证明发布节点的身份信息包括：所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥，所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

7.一种基于区块链的身份认证方法，其特征在于，应用于被认证方节点，所述方法包括：

向认证方发送认证请求，所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息；

在所述认证方节点确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息、所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中，并且在所述第一数字签名通过所述认证方节点的验证后，与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证；

当所述认证方节点确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时，所述被认证方节点通过身份认证。

8.根据权利要求7所述的方法，其特征在于，所述在所述第一数字签名通过所述认证方节点的验证后，与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证，包括：

在所述第一数字签名通过所述认证方节点的验证后，接收所述认证方节点发送的验证信息；

根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第二数字签名；

向所述认证方节点发送所述第二数字签名，当所述第二数字签名通过所述认证方的验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

9.根据权利要求7所述的方法，其特征在于，所述在所述第一数字签名通过所述认证方节点的验证后，与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证，包括：

在所述第一数字签名通过所述认证方节点的验证后，根据预设的信息生成规则生成验证信息；所述信息生成规则预设置在所述被认证方节点和所述认证方节点；

根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第三数字签名；

向所述认证方节点发送所述验证信息以及所述第三数字签名；

当所述认证方节点确认所述验证信息是按照所述信息生成规则生成的，并且所述认证方节点根据所述被认证方节点的公钥对所述第三数字签名进行的验证通过验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

10.根据权利要求7所述的方法，其特征在于，所述身份证明发布节点对所述被认证方节点的身份信息和所述第一数字签名写入所述区块链的方法包括：

向所述区块链写入身份证明请求，所述身份证明请求中包括所述被认证方节点的身份信息，用于所述身份证明发布节点在所述区块链中确认所述被认证方节点的身份信息，并根据所述身份证明发布节点的私钥对所述被认证方节点的身份信息进行数字签名得到所述第一数字签名，并将所述第一数字签名写入所述区块链。

11.根据权利要求7所述的方法，其特征在于，在所述身份证明发布节点向所述区块链写入用于撤销所述第一数字签名的撤销证明后，所述被认证方节点的所述第一数字签名被撤销，所述撤销证明中包括对所述第一数字签名的撤销说明，以及通过所述身份证明发布节点的私钥对所述撤销说明进行数字签名得到第五数字签名。

12.根据权利要求7-11任一项所述的方法，其特征在于，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的；所述身份证明发布节点的身份信息包括：所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥，所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

13.一种基于区块链的身份认证装置，其特征在于，应用于认证方节点，所述装置包括：

接收模块，用于接收被认证方节点发送的认证请求，所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息；

第一验证模块，用于在确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息，以及所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中时，根据所述身份证明发布节点的公钥对所述第一数字签名进行验证；所述身份证明发布节点的公钥是根据所述身份证明发布节点的身份信息获取的；

第二验证模块，用于在所述第一数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥；所述被认证方节点的公钥是根据所述被认证方节点的身份信息获取的；

确定模块，用于当确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时，确定所述被认证方节点通过身份认证。

14.根据权利要求13所述的装置，其特征在于，所述第二验证模块包括：

发送子模块，用于在所述第一数字签名通过验证后，向所述被认证方节点发送验证信息；

接收子模块，用于接收所述被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第二数字签名；

验证子模块，用于根据所述被认证方节点的公钥对所述第二数字签名进行验证；

确认子模块，用于确定当所述第二数字签名通过验证时，确认所述被认证方已掌握与

所述被认证方节点的公钥对应的私钥。

15.根据权利要求13所述的装置，其特征在于，所述第二验证模块包括：

接收子模块，用于接收所述被认证方节点发送的验证信息，以及被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第三数字签名；所述验证信息是所述被认证方节点根据预设的信息生成规则生成的，所述信息生成规则预设置在所述被认证方节点和所述认证方节点；

信息验证子模块，用于验证所述验证信息是否是按照所述信息生成规则生成的；

签名验证子模块，用于当所述验证信息是按照所述信息生成规则生成的时，根据所述被认证方节点的公钥对所述第三数字签名进行验证；

确认子模块，用于当所述第三数字签名通过验证时，确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

16.根据权利要求13所述的装置，其特征在于，当所述身份证明发布节点存在上一级身份证明发布节点时，所述第一验证模块用于：

从所述区块链中获取所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名；

根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证；所述上一级身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的；

在所述第四数字签名通过验证后，根据所述身份证明发布节点的公钥对所述第一数字签名进行验证，所述身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的。

17.根据权利要求13所述的装置，其特征在于，所述第一验证模块用于：

在所述第一数字签名通过验证后，从所述区块链中获取上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名；

根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证；所述上一级身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的；

在所述第四数字签名通过验证后，所述第二验证模块验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥。

18.根据权利要求13-17任一项所述的装置，其特征在于，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的；所述身份证明发布节点的身份信息包括：所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥，所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

19.一种基于区块链的身份认证装置，其特征在于，应用于被认证方节点，所述装置包括：

认证请求模块，用于向认证方发送认证请求，所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息；

验证模块，用于在所述认证方节点确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息、所述身份证明发布节点对所述被认证方节点的身份信息进行数字签

名得到的第一数字签名已写入区块链中，并且在所述第一数字签名通过所述认证方节点的验证后，与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证；当所述认证方节点确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时，所述被认证方节点通过身份认证。

20.根据权利要求19所述的装置，其特征在于，所述验证模块包括：

接收子模块，用于在所述第一数字签名通过所述认证方节点的验证后，接收所述认证方节点发送的验证信息；

签名子模块，用于根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第二数字签名；

发送子模块，用于向所述认证方节点发送所述第二数字签名，当所述第二数字签名通过所述认证方的验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

21.根据权利要求19所述的装置，其特征在于，所述验证模块包括：

信息生成子模块，用于在所述第一数字签名通过所述认证方节点的验证后，根据预设的信息生成规则生成验证信息；所述信息生成规则预设置在所述被认证方节点和所述认证方节点；

签名子模块，用于根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第三数字签名；

发送子模块，用于向所述认证方节点发送所述验证信息以及所述第三数字签名；当所述认证方节点确认所述验证信息是按照所述信息生成规则生成的，并且所述认证方节点根据所述被认证方节点的公钥对所述第三数字签名进行的验证通过验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

22.根据权利要求19所述的装置，其特征在于，所述装置还包括：身份证明请求模块，用于：

向所述区块链写入身份证明请求，所述身份证明请求中包括所述被认证方节点的身份信息，用于所述身份证明发布节点在所述区块链中确认所述被认证方节点的身份信息，并根据所述身份证明发布节点的私钥对所述被认证方节点的身份信息进行数字签名得到所述第一数字签名，并将所述第一数字签名写入所述区块链。

23.根据权利要求19所述的装置，其特征在于，在所述身份证明发布节点向所述区块链写入用于撤销所述第一数字签名的撤销证明后，所述被认证方节点的所述第一数字签名被撤销，所述撤销证明中包括对所述第一数字签名的撤销说明，以及通过所述身份证明发布节点的私钥对所述撤销说明进行数字签名得到第五数字签名。

24.根据权利要求19-23任一项所述的装置，其特征在于，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的；所述身份证明发布节点的身份信息包括：所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥，所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

25.一种非临时性计算机可读存储介质，其特征在于，所述非临时性计算机可读存储介质中包括一个或多个程序，所述一个或多个程序用于执行权利要求1至6中任一项所述的方

法。

26.一种用户节点，其特征在于，所述用户节点包括：

权利要求25中所述的非临时性计算机可读存储介质；以及

一个或者多个处理器，用于执行所述非临时性计算机可读存储介质中的程序。

27.一种非临时性计算机可读存储介质，其特征在于，所述非临时性计算机可读存储介质中包括一个或多个程序，所述一个或多个程序用于执行权利要求7至12中任一项所述的方法。

28.一种用户节点，其特征在于，所述用户节点包括：

权利要求27中所述的非临时性计算机可读存储介质；以及

一个或者多个处理器，用于执行所述非临时性计算机可读存储介质中的程序。

29.一种身份认证系统，其特征在于，所述系统包括：

区块链；

至少一个权利要求26所述的用户节点，作为认证方节点；

至少一个权利要求28所述的用户节点，作为被认证方节点；以及

至少一个身份证明发布节点；

其中，所述区块链，所述至少一个权利要求26所述的用户节点，所述至少一个权利要求28所述的用户节点以及所述至少一个身份证明发布节点属于同一区块链网络。

30.根据权利要求29所述的系统，其特征在于，所述至少一个身份证明发布节点为一个身份证明发布节点，所述身份证明发布节点用于向所述区块链发布第一用户节点的身份证明；所述第一用户节点为任一用户节点；

其中，所述身份证明发布节点向所述区块链发布第一用户节点的身份证明包括：所述身份证明发布节点在所述区块链中确认所述第一用户节点的身份信息，并根据所述身份证明发布节点的私钥对所述第一用户节点的身份信息进行数字签名，并将得到的数字签名写入所述区块链。

31.根据权利要求29所述的系统，其特征在于，所述至少一个身份证明发布节点至少包括一个身份证明发布节点和所述身份证明发布节点的上一级身份证明发布节点，所述身份证明发布节点用于向所述区块链发布第一用户节点的身份证明，所述第一用户节点为任一用户节点，所述上一级身份证明发布节点用于向所述区块链发布所述身份证明发布节点的身份证明；

其中，所述身份证明发布节点向所述区块链发布第一用户节点的身份证明包括：所述身份证明发布节点在所述区块链中确认所述第一用户节点的身份信息，并根据所述身份证明发布节点的私钥对所述第一用户节点的身份信息进行数字签名，并将得到的数字签名写入所述区块链；

所述上一级身份证明发布节点向所述区块链发布所述身份证明发布节点的身份证明包括：所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名，并将得到的数字签名写入所述区块链。

32.根据权利要求29所述的系统，其特征在于，所述系统包括多个身份证明发布子系统，每个身份证明发布子系统中包括至少一个身份证明发布节点和至少一个用户节点；

其中，当第一身份证明发布子系统中包括一个身份证明发布节点时，所述身份证明发

布节点用于向所述区块链发布所述第一身份证明发布子系统的第一用户节点的身份证明，所述第一用户节点为所述第一身份证明发布子系统中的任一用户节点；所述第一身份证明发布子系统为所述多个身份证明发布子系统中的任一身份证明发布子系统；

当第一身份证明发布子系统中至少包括一个身份证明发布节点和所述身份证明发布节点的上一级身份证明发布节点，所述身份证明发布节点用于向所述区块链发布所述第一身份证明发布子系统的所述第一用户节点的身份证明，所述上一级身份证明发布节点用于向所述区块链发布所述身份证明发布节点的身份证明；

其中，所述身份证明发布节点向所述区块链发布所述第一身份证明发布子系统的所述第一用户节点的身份证明包括：所述身份证明发布节点在所述区块链中确认所述第一用户节点的身份信息，并根据所述身份证明发布节点的私钥对所述第一用户节点的身份信息进行数字签名，并将得到的数字签名写入所述区块链；

所述上一级身份证明发布节点向所述区块链发布所述身份证明发布节点的身份证明包括：所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名，并将得到的数字签名写入所述区块链。

基于区块链的身份认证方法、装置、节点及系统

技术领域

[0001] 本公开涉及信息技术领域，尤其涉及一种基于区块链的身份认证方法、装置、节点及系统。

背景技术

[0002] 身份认证是目前计算机及网络系统中确认操作者身份的基本技术手段，是判断被认证对象的身份是否属实和有效的一个过程。网络系统中常用的身份认证技术包括用户名/口令、Kerberos(一种网络认证协议)和PKI(Public Key Infrastructure，公钥基础设施)等。这些认证方法存在一个共同点，即都存在一个认证双方共同信任的第三方机构，通过这个第三方机构为认证双方发布身份信息，并以此身份信息作为认证双方间确认对方身份的基础。

[0003] 但是，这样上述的认证机制容易出现由于单点故障问题和安全问题而影响整个系统的可用性和安全性的问题，这是由于当系统中的某个或某些节点(例如认证双方或者可信第三方机构)的故障容易导致其他节点无法获取身份认证信息，并且可信第三方机构在网络中的地址通常是固定的，极易受到各种攻击，其可信第三方机构自身安全性是整个系统安全的基础，当可信第三方机构的安全出现问题时，整个系统的安全则无法保证。

发明内容

[0004] 本公开的目的是提供一种基于区块链的身份认证方法、装置、节点及系统，用于解决现有认证机制由于单点故障问题和安全问题而影响整个系统的可用性和安全性的问题。

[0005] 为了实现上述目的，根据本公开实施例的第一方面，本公开提供一种基于区块链的身份认证方法，应用于认证方节点，所述方法包括：

[0006] 接收被认证方节点发送的认证请求，所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息；

[0007] 在确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息，以及所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中时，根据所述身份证明发布节点的公钥对所述第一数字签名进行验证；所述身份证明发布节点的公钥是根据所述身份证明发布节点的身份信息获取的；

[0008] 在所述第一数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥；所述被认证方节点的公钥是根据所述被认证方节点的身份信息获取的；

[0009] 当确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时，确定所述被认证方节点通过身份认证。

[0010] 可选的，所述在所述第一数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥，包括：

[0011] 在所述第一数字签名通过验证后，向所述被认证方节点发送验证信息；

[0012] 接收所述被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第二数字签名；

[0013] 根据所述被认证方节点的公钥对所述第二数字签名进行验证；

[0014] 当所述第二数字签名通过验证时，确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

[0015] 可选的，所述在所述第一数字签名通过验证后，向所述被认证方确认所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥，包括：

[0016] 接收所述被认证方节点发送的验证信息，以及被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第三数字签名；所述验证信息是所述被认证方节点根据预设的信息生成规则生成的，所述信息生成规则预设置在所述被认证方节点和所述认证方节点；

[0017] 验证所述验证信息是否是按照所述信息生成规则生成的；

[0018] 当所述验证信息是按照所述信息生成规则生成的时，根据所述被认证方节点的公钥对所述第三数字签名进行验证；

[0019] 当所述第三数字签名通过验证时，确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

[0020] 可选的，当所述身份证明发布节点存在上一级身份证明发布节点时，所述根据所述身份证明发布节点的公钥对所述第一数字签名进行验证，包括：

[0021] 从所述区块链中获取所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名；

[0022] 根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证；所述上一级身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的；

[0023] 在所述第四数字签名通过验证后，根据所述身份证明发布节点的公钥对所述第一数字签名进行验证，所述身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的。

[0024] 可选的，所述在所述第一数字签名通过验证后，在验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥之前，还包括：

[0025] 在所述第一数字签名通过验证后，从所述区块链中获取所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名；

[0026] 根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证；所述上一级身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的；

[0027] 在所述第四数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥。

[0028] 可选的，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的；所述身份证明发布节点的身份信息包括：所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥，所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

[0029] 根据本公开实施例的第二方面，提供一种基于区块链的身份认证方法，应用于被认证方节点，所述方法包括：

[0030] 向认证方发送认证请求，所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息；

[0031] 在所述认证方节点确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息、所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中，并且在所述第一数字签名通过所述认证方节点的验证后，与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证；

[0032] 当所述认证方节点确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时，所述被认证方节点通过身份认证。

[0033] 可选的，所述在所述第一数字签名通过所述认证方节点的验证后，与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证，包括：

[0034] 在所述第一数字签名通过所述认证方节点的验证后，接收所述认证方节点发送的验证信息；

[0035] 根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第二数字签名；

[0036] 向所述认证方节点发送所述第二数字签名，当所述第二数字签名通过所述认证方的验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

[0037] 可选的，所述在所述第一数字签名通过所述认证方节点的验证后，与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证，包括：

[0038] 在所述第一数字签名通过所述认证方节点的验证后，根据预设的信息生成规则生成验证信息；所述信息生成规则预设置在所述被认证方节点和所述认证方节点；

[0039] 根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第三数字签名；

[0040] 向所述认证方节点发送所述验证信息以及所述第三数字签名；

[0041] 当所述认证方节点确认所述验证信息是按照所述信息生成规则生成的，并且所述认证方节点根据所述被认证方节点的公钥对所述第三数字签名进行的验证通过验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

[0042] 可选的，所述身份证明发布节点对所述被认证方节点的身份信息和所述第一数字签名写入所述区块链的方法包括：

[0043] 向所述区块链写入身份证明请求，所述身份证明请求中包括所述被认证方节点的身份信息，用于所述身份证明发布节点在所述区块链中确认所述被认证方节点的身份信息，并根据所述身份证明发布节点的私钥对所述被认证方节点的身份信息进行数字签名得到所述第一数字签名，并将所述第一数字签名写入所述区块链。

[0044] 可选的，在所述身份证明发布节点向所述区块链写入用于撤销所述第一数字签名的撤销证明后，所述被认证方节点的所述第一数字签名被撤销，所述撤销证明中包括对所述第一数字签名的撤销说明，以及通过所述身份证明发布节点的私钥对所述撤销说明进行数字签名得到第五数字签名。

[0045] 可选的，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获

取的;所述身份证明发布节点的身份信息包括:所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥,所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

[0046] 根据本公开实施例的第三方面,提供一种基于区块链的身份认证装置,应用于认证方节点,所述装置包括:

[0047] 接收模块,用于接收被认证方节点发送的认证请求,所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息;

[0048] 第一验证模块,用于在确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息,以及所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中时,根据所述身份证明发布节点的公钥对所述第一数字签名进行验证;所述身份证明发布节点的公钥是根据所述身份证明发布节点的身份信息获取的;

[0049] 第二验证模块,用于在所述第一数字签名通过验证后,验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥;所述被认证方节点的公钥是根据所述被认证方节点的身份信息获取的;

[0050] 确定模块,用于当确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时,确定所述被认证方节点通过身份认证。

[0051] 可选的,所述第二验证模块包括:

[0052] 发送子模块,用于在所述第一数字签名通过验证后,向所述被认证方节点发送验证信息;

[0053] 接收子模块,用于接收所述被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第二数字签名;

[0054] 验证子模块,用于根据所述被认证方节点的公钥对所述第二数字签名进行验证;

[0055] 确认子模块,用于确定当所述第二数字签名通过验证时,确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

[0056] 可选的,所述第二验证模块包括:

[0057] 接收子模块,用于接收所述被认证方节点发送的验证信息,以及被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第三数字签名;所述验证信息是所述被认证方节点根据预设的信息生成规则生成的,所述信息生成规则预设置在所述被认证方节点和所述认证方节点;

[0058] 信息验证子模块,用于验证所述验证信息是否是按照所述信息生成规则生成的;

[0059] 签名验证子模块,用于当所述验证信息是按照所述信息生成规则生成的时,根据所述被认证方节点的公钥对所述第三数字签名进行验证;

[0060] 确认子模块,用于当所述第三数字签名通过验证时,确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

[0061] 可选的,当所述身份证明发布节点存在上一级身份证明发布节点时,所述第一验证模块用于:

[0062] 从所述区块链中获取所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名;所述上一级身份

证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的；

[0063] 根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证；

[0064] 在所述第四数字签名通过验证后，根据所述身份证明发布节点的公钥对所述第一数字签名进行验证，所述身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的。

[0065] 可选的，所述第一验证模块用于：

[0066] 在所述第一数字签名通过验证后，从所述区块链中获取所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名；

[0067] 根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证；所述上一级身份证明发布节点的公钥是从所述区块链中获取的，或者是预先存储的；

[0068] 所述发送模块还用于在所述第四数字签名通过验证后，所述第二验证模块验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥。

[0069] 可选的，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的；所述身份证明发布节点的身份信息包括：所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥，所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

[0070] 根据本公开实施例的第四方面，提供一种基于区块链的身份认证装置，应用于被认证方节点，所述装置包括：

[0071] 认证请求模块，用于向认证方发送认证请求，所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息；

[0072] 验证模块，用于在所述认证方节点确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息、所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中，并且在所述第一数字签名通过所述认证方节点的验证后，与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证；当所述认证方节点确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时，所述被认证方节点通过身份认证。

[0073] 可选的，所述验证模块包括：

[0074] 接收子模块，用于在所述第一数字签名通过所述认证方节点的验证后，接收所述认证方节点发送的验证信息；

[0075] 签名子模块，用于根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第二数字签名；

[0076] 发送子模块，用于向所述认证方节点发送所述第二数字签名，当所述第二数字签名通过所述认证方的验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

[0077] 可选的，所述验证模块包括：

[0078] 信息生成子模块，用于在所述第一数字签名通过所述认证方节点的验证后，根据预设的信息生成规则生成验证信息；所述信息生成规则预设置在所述被认证方节点和所述

认证方节点；

[0079] 签名子模块，用于根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第三数字签名；

[0080] 发送子模块，用于向所述认证方节点发送所述验证信息以及所述第三数字签名；当所述认证方节点确认所述验证信息是按照所述信息生成规则生成的，并且所述认证方节点根据所述被认证方节点的公钥对所述第三数字签名进行的验证通过验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

[0081] 可选的，所述装置还包括：身份证明请求模块，用于：

[0082] 向所述区块链写入身份证明请求，所述身份证明请求中包括所述被认证方节点的身份信息，用于所述身份证明发布节点在所述区块链中确认所述被认证方节点的身份信息，并根据所述身份证明发布节点的私钥对所述被认证方节点的身份信息进行数字签名得到所述第一数字签名，并将所述第一数字签名写入所述区块链。

[0083] 可选的，在所述身份证明发布节点向所述区块链写入用于撤销所述第一数字签名的撤销证明后，所述被认证方节点的所述第一数字签名被撤销，所述撤销证明中包括对所述第一数字签名的撤销说明，以及通过所述身份证明发布节点的私钥对所述撤销说明进行数字签名得到第五数字签名。

[0084] 可选的，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的；所述身份证明发布节点的身份信息包括：所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥，所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

[0085] 根据本公开实施例的第五方面，提供一种非临时性计算机可读存储介质，所述非临时性计算机可读存储介质中包括一个或多个程序，所述一个或多个程序用于第一方面所述的方法。

[0086] 根据本公开实施例的第六方面，提供一种用户节点，所述用户节点包括：

[0087] 第五方面所述的非临时性计算机可读存储介质；以及

[0088] 一个或者多个处理器，用于执行所述非临时性计算机可读存储介质中的程序。

[0089] 根据本公开实施例的第七方面，提供一种非临时性计算机可读存储介质，所述非临时性计算机可读存储介质中包括一个或多个程序，所述一个或多个程序用于第二方面所述的方法。

[0090] 根据本公开实施例的第八方面，提供一种用户节点，所述用户节点包括：

[0091] 第七方面所述的非临时性计算机可读存储介质；以及

[0092] 一个或者多个处理器，用于执行所述非临时性计算机可读存储介质中的程序。

[0093] 根据本公开实施例的第九方面，提供一种身份认证系统，所述系统包括：

[0094] 区块链；

[0095] 至少一个第六方面所述的用户节点，作为认证方节点；

[0096] 至少一个第八方面所述的用户节点，作为被认证方节点；以及

[0097] 至少一个身份证明发布节点；

[0098] 其中，所述区块链，所述至少一个第六方面所述的用户节点，所述至少一个第八方

面所述的用户节点以及所述至少一个身份证明发布节点属于同一区块链网络。

[0099] 可选的，所述至少一个身份证明发布节点为一个身份证明发布节点，所述身份证明发布节点用于向所述区块链发布第一用户节点的身份证明；所述第一用户节点为任一用户节点；

[0100] 其中，所述身份证明发布节点向所述区块链发布第一用户节点的身份证明包括：所述身份证明发布节点在所述区块链中确认所述第一用户节点的身份信息，并根据所述身份证明发布节点的私钥对所述第一用户节点的身份信息进行数字签名，并将得到的数字签名写入所述区块链。

[0101] 可选的，所述至少一个身份证明发布节点至少包括一个身份证明发布节点和所述身份证明发布节点的上一级身份证明发布节点，所述身份证明发布节点用于向所述区块链发布第一用户节点的身份证明，所述第一用户节点为任一用户节点，所述上一级身份证明发布节点用于向所述区块链发布所述身份证明发布节点的身份证明；

[0102] 其中，所述身份证明发布节点向所述区块链发布第一用户节点的身份证明包括：所述身份证明发布节点在所述区块链中确认所述第一用户节点的身份信息，并根据所述身份证明发布节点的私钥对所述第一用户节点的身份信息进行数字签名，并将得到的数字签名写入所述区块链；

[0103] 所述上一级身份证明发布节点向所述区块链发布所述身份证明发布节点的身份证明包括：所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名，并将得到的数字签名写入所述区块链。

[0104] 可选的，所述系统包括多个身份证明发布子系统，每个身份证明发布子系统中包括至少一个身份证明发布节点和至少一个用户节点；

[0105] 其中，当第一身份证明发布子系统中包括一个身份证明发布节点时，所述身份证明发布节点用于向所述区块链发布所述第一身份证明发布子系统的第一用户节点的身份证明，所述第一用户节点为所述第一身份证明发布子系统中的任一用户节点；所述第一身份证明发布子系统为所述多个身份证明发布子系统中的任一身份证明发布子系统；

[0106] 当第一身份证明发布子系统中至少包括一个身份证明发布节点和所述身份证明发布节点的上一级身份证明发布节点，所述身份证明发布节点用于向所述区块链发布所述第一身份证明发布子系统的所述第一用户节点的身份证明，所述上一级身份证明发布节点用于向所述区块链发布所述身份证明发布节点的身份证明；

[0107] 其中，所述身份证明发布节点向所述区块链发布所述第一身份证明发布子系统的所述第一用户节点的身份证明包括：所述身份证明发布节点在所述区块链中确认所述第一用户节点的身份信息，并根据所述身份证明发布节点的私钥对所述第一用户节点的身份信息进行数字签名，并将得到的数字签名写入所述区块链；

[0108] 所述上一级身份证明发布节点向所述区块链发布所述身份证明发布节点的身份证明包括：所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名，并将得到的数字签名写入所述区块链。

[0109] 通过上述技术方案，由于被认证方的身份信息和身份证明发布节点的身份信息均记录在区块链中，不会因为某个或某些节点的故障导致无法获取身份信息，因此能够避免单点故障对整个系统的影响，并且在区块链网络中，由于任何一个节点只要配置了身份证

明发布节点的私钥，其角色就是身份认证发布节点，因此身份证明发布节点不是固定的某一节点，攻击者无法对对身份认证信息发布节点进行定位，从而无法对身份认证节点发起攻击，从而保证了整个系统的安全，因此能够解决由于单点故障问题和安全问题而影响整个系统的可用性和安全性的问题，保证整个系统的可用性和安全性。

[0110] 本公开的其他特征和优点将在随后的具体实施方式部分予以详细说明。

附图说明

[0111] 附图是用来提供对本公开的进一步理解，并且构成说明书的一部分，与下面的具体实施方式一起用于解释本公开，但并不构成对本公开的限制。在附图中：

[0112] 图1是根据一实施例示出的一种基于区块链的身份认证方法的流程图；

[0113] 图2是根据一实施例示出的一种基于区块链的身份认证方法的流程图；

[0114] 图3是根据一实施例示出的另一种基于区块链的身份认证方法的流程图；

[0115] 图4是根据图3所示实施例示出的一种私钥验证方法的流程图；

[0116] 图5是根据图3所示实施例示出的另一种私钥验证方法的流程图；

[0117] 图6是根据一实施例示出的一种基于区块链的身份认证装置框图；

[0118] 图7是根据图6所示实施例示出的一种第二验证模块框图；

[0119] 图8是根据图6所示实施例示出的另一种第二验证模块框图；

[0120] 图9是根据一实施例示出的另一种基于区块链的身份认证装置框图；

[0121] 图10是根据图9所示实施例示出的一种验证模块框图；

[0122] 图11是根据图9所示实施例示出的另一种验证模块框图；

[0123] 图12是根据一实施例示出的又一种基于区块链的身份认证装置框图；

[0124] 图13是根据一实施例示出的一种身份认证系统结构框图；

[0125] 图14a是根据一实施例示出的另一种身份认证系统结构框图；

[0126] 图14b是根据一实施例示出的又一种身份认证系统结构框图；

[0127] 图15是根据一实施例示出的又一种身份认证系统结构框图。

具体实施方式

[0128] 以下结合附图对本公开的具体实施方式进行详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本公开，并不用于限制本公开。

[0129] 在对本公开提供的基于区块链的身份认证方法进行说明之前，先对本公开各个实施例所涉及的应用场景进行介绍。

[0130] 首先，对区块链进行介绍，区块链是由区块链网络中所有节点共同参与维护的去中心化分布式数据库系统，它是由一系列基于密码学方法产生的数据块组成，每个数据块即为区块链中的一个区块。根据产生时间的先后顺序，区块被有序地链接在一起，形成一个数据链条，被形象地称为区块链。下面对区块链网络的一些概念进行介绍。

[0131] 区块链网络中的节点可以称为区块链节点，其中区块链网络基于P2P(Peer to Peer，对等网络)网络，每个参与交易和区块存储、验证、转发的P2P网络节点都是一个区块链网络中的节点。

[0132] 区块链中的用户身份可以使用公钥或者是根据该公钥生成的账户地址表示，并且

公钥和私钥是成对出现的，其中私钥由用户掌握而不发布到上述的区块链网络中，公钥或者上述的账户地址可随意发布在区块链网络中。其中，公钥可以通过特定的哈希和编码后成为上述的账户地址。值得一提的是，用户身份和区块链节点不存在一一对应关系，用户可以在任意一个区块链节点上使用自己的私钥。

[0133] 关于区块链的数据写入，是由区块链节点通过向区块链网络发布交易(Transaction)实现向区块链写入数据。该交易包括：区块链节点按照预设的交易数据格式对生成的交易数据包，以及利用该区块链节点自己的私钥对该交易数据包进行的数字签名，该数字签名用于证明该区块链节点的用户的身份；而后，该交易被区块链网络中的“矿工”(即执行PoW(Proof Of Work，工作证明)共识竞争机制的区块链节点)记录入区块链中产生的新区块，并将该交易发布到区块链网络中，在该交易被其他区块链节点验证通过(其他节点可以从该区块链节点生成的交易中获取该区块链节点的公钥，并根据该区块链节点的公钥对上述的数字签名进行验证，除了验证数字签名之外还可以验证交易数据包是否为规定的数据结构)和接受后，该交易即被写入区块链。其中，区块链中的新区块是由上述的“矿工”通过执行PoW共识竞争机制(该机制可以理解为：各个“矿工”按照区块的预设技术要求，例如按照预设的随机数要求来共同计算随机数，哪一个“矿工”先计算出符合该随机数要求的随机数，该“矿工”产生的区块就作为该新区块)而定期产生的，因此产生新区块的时间间隔通常和上述的预设技术要求相关，通过设置不同的预设技术要求可以改变区块链产生新区块的时间间隔。

[0134] 本发明公开的各个实施例中，向区块链中写入数据的流程均是采用上述流程。本发明公开各个实施例所涉及的应用场景可以是一种身份认证系统，该系统基于区块链，可以至少包括：区块链、两个以上用户节点和一个身份证明发布节点，该区块链、用户节点和身份证明发布节点均属于同一区块链网络。其中，用户节点是身份证明的需求节点，用于实际进行身份认证操作。身份证明发布节点是用于为用户节点发布身份证明的节点，这里的“发布身份证明”，是指对用户节点的身份信息进行确认、数字签名、并将数字签名写入区块链，并且在区块链网络中，身份证明发布节点可以不是固定的某一个节点，任何一个节点只要配置了身份证明发布节点的私钥，其角色就是身份认证发布节点。通常身份证明发布节点的身份信息(的账户地址或公钥)已写入区块链，并得到用户节点的认可。

[0135] 图1是根据一实施例示出的一种基于区块链的身份认证方法的流程图，该方法应用于被认证方节点，该被认证方节点可以是上述身份认证系统中的任一用户节点，参见图1，该方法可以包括以下步骤。

[0136] 步骤101，向认证方发送认证请求，认证请求中包括被认证方节点的身份信息和身份证明发布节点的身份信息。

[0137] 其中，认证方节点也是上述系统中除了该被认证方节点外的任一用户节点，即该身份认证方法是两个用户节点之间进行的，并且每个用户节点既可以作为被认证方节点也可以作为认证方节点。另外被认证方节点的身份信息包括被认证方节点的账户地址或者被认证方节点的公钥，被认证方节点的账户地址是根据被认证方节点的公钥获取的；身份证明发布节点的身份信息包括：身份证明发布节点的账户地址或者身份证明发布节点的公钥，身份证明发布节点的账户地址是根据身份证明发布节点的公钥获取的。其中，上述各个节点的账户地址可以是通过将公钥进行特定的哈希计算以及编码后生成的。

[0138] 步骤102，在认证方节点在确认被认证方节点的身份信息、身份证明发布节点的身份信息、身份证明发布节点对被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中，并且在第一数字签名通过认证方节点的验证后，与认证方节点进行被认证方是否掌握与被认证方节点的公钥对应的私钥的验证。

[0139] 步骤103，当认证方节点确认被认证方已掌握与被认证方节点的公钥对应的私钥时，被认证方节点通过身份认证。

[0140] 图2是根据一实施例示出的一种基于区块链的身份认证方法的流程图，该方法应用于认证方节点，该认证方节点可以是上述身份认证系统中的任一用户节点，参见图2，该方法可以包括以下步骤。

[0141] 步骤201，接收被认证方节点发送的认证请求，认证请求中包括被认证方节点的身份信息和身份证明发布节点的身份信息。

[0142] 其中，被认证方节点也是上述系统中除了该认证方节点外的任一用户节点，即该身份认证方法是两个用户节点之间进行的，并且每个用户节点既可以作为被认证方节点也可以作为认证方节点。另外被认证方节点的身份信息和身份证明发布节点的身份信息所包括的内容可参照步骤101，不再赘述。

[0143] 步骤202，在确认被认证方节点的身份信息、身份证明发布节点的身份信息，以及身份证明发布节点对被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中时，根据身份证明发布节点的公钥对第一数字签名进行验证；身份证明发布节点的公钥是根据身份证明发布节点的身份信息获取的。

[0144] 步骤203，在第一数字签名通过验证后，验证被认证方是否掌握与被认证方节点的公钥对应的私钥；被认证方节点的公钥是根据被认证方节点的身份信息获取的。

[0145] 步骤204，当确认被认证方已掌握与被认证方节点的公钥对应的私钥时，确定被认证方节点通过身份认证。

[0146] 图3是根据一实施例示出的另一种基于区块链的身份认证方法的流程图，该方法应用于上述的身份认证系统，本实施例中的被认证方节点和认证方节点均为该认证系统中的用户节点，参见图3，该方法可以包括以下步骤。

[0147] 步骤301，被认证方节点向认证方发送认证请求，认证请求中包括被认证方节点的身份信息和身份证明发布节点的身份信息。

[0148] 其中，认证方节点和被认证方节点可以是上述身份认证系统中的任意两个用户节点。被认证方节点的身份信息包括被认证方节点的账户地址或者被认证方节点的公钥，被认证方节点的账户地址是根据被认证方节点的公钥获取的；身份证明发布节点的身份信息包括：身份证明发布节点的账户地址或者身份证明发布节点的公钥，身份证明发布节点的账户地址是根据身份证明发布节点的公钥获取的。其中，上述各个节点的账户地址可以是通过将公钥进行特定的哈希计算以及编码后生成的。

[0149] 步骤302，认证方节点接收被认证方节点的认证请求后，确认被认证方节点的身份信息、身份证明发布节点的身份信息，以及身份证明发布节点对被认证方节点的身份信息进行数字签名得到的第一数字签名是否已写入区块链中。

[0150] 其中，由于认证方节点、被认证方节点以及身份证明发布节点属于同一个区块链网络，在被认证方节点的身份信息、身份证明发布节点的身份信息以及第一数字签名已写

入区块链的情况下，认证方节点是能够从区块链中读取到这些信息的。其中，第一数字签名是在身份证明发布节点向区块链中发布被认证方节点的身份证明后产生的。关于身份证明发布节点向区块链中发布被认证方节点的身份证明的方法，可以包括以下步骤：

[0151] 首先，被认证方节点向区块链写入身份证明请求，身份证明请求中包括被认证方节点的身份信息。其中向区块链中写入身份证明请求的过程可以参照前文所述的区块链的数据写入过程。

[0152] 其次，身份证明发布节点在接收到身份证明请求后，在区块链中确认被认证方节点的身份信息(例如确认区块链中已写入被认证方节点的身份信息)，并根据身份证明发布节点的私钥对被认证方节点的身份信息进行数字签名得到该第一数字签名。

[0153] 最后，将该第一数字签名写入区块链中，写入区块链中后，区块链网络中的所有节点均可以读取到该第一数字签名，从而完成了对该被认证方节点的身份证明的发布。

[0154] 另外，值得一提的是，身份证明发布节点向区块链中发布被认证方节点的身份证明的流程应当在被认证方节点向认证方节点发起身份认证之前。并且，向区块链写入身份证明请求不限于上述的被认证方节点，区块链网络中的任一用户节点均可以发起向区块链写入身份证明请求。

[0155] 步骤303，在被认证方节点的身份信息、身份证明发布节点的身份信息以及第一数字签名已写入区块链中时，认证方节点根据身份证明发布节点的公钥对第一数字签名进行验证。

[0156] 由于第一数字签名是根据身份证明发布节点的私钥对被认证方节点的身份信息进行数字签名得到的，因此可以根据身份证明发布节点的公钥对第一数字签名进行验证，以确定该第一数字签名的合法性，其中，身份证明发布节点的公钥可以从区块链中获取，也可以是预先存储在认证方节点上的。其中，由于身份证明发布节点的身份信息已经写入区块链中，因此区块链网络中的任意节点均可以获取该身份信息，因此，如果该身份信息是身份证明发布节点的公钥，则认证方节点可以直接得到身份证明发布节点的公钥，如果该身份信息是身份证明发布节点的账户地址，则认证方节点可以根据该账户地址进行计算得到身份证明发布节点的公钥。

[0157] 步骤304，在第一数字签名通过验证后，认证方节点验证被认证方是否掌握与被认证方节点的公钥对应的私钥。

[0158] 示例的，图4是根据图3所示实施例示出的一种私钥验证方法的流程图，如图4所示，在一种实现方式中，验证被认证方是否掌握与被认证方节点的公钥对应的私钥可以通过以下步骤：

[0159] 步骤3041a，在第一数字签名通过验证后，认证方节点生成验证信息。该验证信息可以是挑战码(challenge)，挑战码也称作挑战口令，是指遵循握手验证协议(英文：Challenge Handshake Authentication Protocol，简称：CHAP)生成的一组加密口令，用于在传输过程中保证用户的真实密码不被泄露。或者验证信息可以是按照预设的信息生成规则生成的信息。

[0160] 步骤3042a，认证方节点向被认证方节点发送验证信息。

[0161] 步骤3043a，被认证方节点根据被认证方节点的私钥对验证信息进行数字签名得到第二数字签名。

[0162] 步骤3044a，认证方节点从被认证方节点获取第二数字签名后，根据被认证方节点的公钥对第二数字签名进行验证。其中，被认证方节点的公钥可以是从区块链中获取的，也可以是预先存储在认证方节点的。

[0163] 步骤3045a，当第二数字签名通过验证时，确认被认证方已掌握与被认证方节点的公钥对应的私钥。

[0164] 图5是根据图3所示实施例示出的另一种私钥验证方法的流程图，如图5所示，在另一种实现方式中，验证被认证方是否掌握与被认证方节点的公钥对应的私钥可以通过以下步骤：

[0165] 步骤3041b，在第一数字签名通过认证方节点的验证后，被认证方节点根据预设的信息生成规则生成验证信息。

[0166] 其中，验证信息可以与步骤3041a中所述的验证信息相同，信息生成规则预设置在被认证方节点和认证方节点。

[0167] 步骤3042b，被认证方节点根据被认证方节点的私钥对验证信息进行数字签名得到第三数字签名。

[0168] 步骤3043b，被认证方节点向认证方节点发送验证信息以及第三数字签名。

[0169] 步骤3044b，认证方节点验证该验证信息是否是按照该信息生成规则生成的。

[0170] 步骤3045b，当认证方节点确认验证信息是按照信息生成规则生成的时，根据被认证方节点的公钥对第三数字签名进行验证。其中，被认证方节点的公钥可以是从区块链中获取的，也可以是预先存储在认证方节点的。

[0171] 步骤3046b，当第三数字签名通过验证时，认证方节点确认被认证方节点已掌握与被认证方节点的公钥对应的私钥。

[0172] 除了上述图4或图5所述的实施方式外，验证被认证方是否掌握与被认证方节点的公钥对应的私钥也可以是其他可能的实施方式，包括但不限于上述的方案。

[0173] 步骤305，当确认被认证方已掌握与被认证方节点的公钥对应的私钥时，认证方节点确定被认证方节点通过身份认证。

[0174] 其中，在上述步骤303和步骤304中有任一个步骤验证失败时，被认证方节点的身份认证均被确认为失败。

[0175] 可选的，当所述身份证明发布节点存在上一级身份证明发布节点时，步骤303所述的根据从区块链中获取的身份证明发布节点的公钥对第一数字签名进行验证的步骤可以包括：

[0176] 首先，从区块链中获取上一级身份证明发布节点的公钥，以及上一级身份证明节点根据上一级身份证明节点的私钥对身份证明发布节点的公钥进行数字签名得到的第四数字签名；

[0177] 其次，根据上一级身份证明发布节点的公钥对第四数字签名进行验证；

[0178] 再次，在第四数字签名通过验证后，根据从区块链中获取的身份证明发布节点的公钥对第一数字签名进行验证。

[0179] 或者，当所述身份证明发布节点存在上一级身份证明发布节点时，在步骤304中所述的在第一数字签名通过验证后，在验证被认证方是否掌握与被认证方节点的公钥对应的私钥之前可以包括：

[0180] 首先，在所述第一数字签名通过验证后，从区块链中获取所述上一级身份证明发布节点的公钥，以及上一级身份证明节点根据上一级身份证明节点的私钥对身份证明发布节点的公钥进行数字签名得到的第四数字签名；

[0181] 其次，根据上一级身份证明发布节点的公钥对第四数字签名进行验证；

[0182] 再次，在第四数字签名通过验证后，向被认证方节点发送挑战码。

[0183] 在实际的应用场景中，上述的上一级身份证明发布节点也可能存在更上一级的身份证明发布节点，这里称为上上一级身份证明发布节点，则在验证了该第四数字签名后，还需要验证上上一级身份证明发布节点利用自身私钥对上一级身份证明发布节点的公钥的数字签名。当然，还可能存在更高一级的身份证明发布节点，其原理与前述方法相同，以此类推，不再一一列举。

[0184] 另外，可选的，身份证明发布节点还可以对已经发布的身份证明进行撤销，示例的，身份证明发布节点可以向所述区块链写入撤销证明，其写入撤销证明的过程可以参照上述的区块链的数据写入过程。该撤销证明中可以包括对之前发布过的某一身份证明，例如上述的第一数字签名进行撤销的，以及利用身份证明发布节点的私钥对撤销说明进行数字签名得到第五数字签名。区块链网络中的其他节点可以通过身份证明发布节点的公钥对第五数字签名进行验证，从而确定撤销说明的合法性。

[0185] 综上所述，本公开提供的基于区块链的身份认证方法中，由于被认证方的身份信息和身份证明发布节点的身份信息均记录在区块链中，不会因为某个或某些节点的故障导致无法获取身份信息，因此能够避免单点故障对整个系统的影响，并且在区块链网络中，由于任何一个节点只要配置了身份证明发布节点的私钥，其角色就是身份认证发布节点，因此身份证明发布节点不是固定的某一节点，攻击者无法对对身份认证信息发布节点进行定位，从而无法对身份认证节点发起攻击，从而保证了整个系统的安全，因此能够解决由于单点故障问题和安全问题而影响整个系统的可用性和安全性的问题，保证整个系统的可用性和安全性。

[0186] 图6是根据一实施例示出的一种基于区块链的身份认证装置框图，该装置600可以应用于认证方节点，用于执行图2或图3至图5任一所示的方法，参见图6，该装置600可以包括：接收模块610、第一验证模块620、第二验证模块630以及确定模块640，其中：

[0187] 接收模块610，用于接收被认证方节点发送的认证请求，认证请求中包括被认证方节点的身份信息和身份证明发布节点的身份信息；

[0188] 第一验证模块620，用于在确认被认证方节点的身份信息、身份证明发布节点的身份信息，以及身份证明发布节点对被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中时，根据身份证明发布节点的公钥对第一数字签名进行验证；身份证明发布节点的公钥是根据身份证明发布节点的身份信息获取的；

[0189] 第二验证模块630，用于在第一数字签名通过验证后，验证被认证方是否掌握与被认证方节点的公钥对应的私钥；被认证方节点的公钥是根据被认证方节点的身份信息获取的；

[0190] 确定模块640，用于当确认被认证方已掌握与被认证方节点的公钥对应的私钥时，确定被认证方节点通过身份认证。

[0191] 可选的，图7是根据图6所示实施例示出的一种第二验证模块框图，如图7所示，第

二验证模块630包括：

[0192] 发送子模块631，用于在第一数字签名通过验证后，向被认证方节点发送验证信息；

[0193] 接收子模块632，用于接收被认证方节点根据被认证方节点的私钥对验证信息进行数字签名得到的第二数字签名；

[0194] 验证子模块633，用于根据被认证方节点的公钥对第二数字签名进行验证；

[0195] 确认子模块634，用于确定当第二数字签名通过验证时，确认被认证方已掌握与被认证方节点的公钥对应的私钥。

[0196] 或者，图8是根据图6所示实施例示出的另一种第二验证模块框图，如图8所示，第二验证模块630包括：

[0197] 接收子模块635，用于接收被认证方节点发送的验证信息，以及被认证方节点根据被认证方节点的私钥对验证信息进行数字签名得到的第三数字签名；验证信息是被认证方节点根据预设的信息生成规则生成的，信息生成规则预设置在被认证方节点和认证方节点；

[0198] 信息验证子模块636，用于验证验证信息是否是按照信息生成规则生成的；

[0199] 签名验证子模块637，用于当验证信息是按照信息生成规则生成的时，根据被认证方节点的公钥对第三数字签名进行验证；

[0200] 确认子模块638，用于当第三数字签名通过验证时，确认被认证方已掌握与被认证方节点的公钥对应的私钥。

[0201] 可选的，当身份证明发布节点存在上一级身份证明发布节点时，第一验证模块620用于：

[0202] 从区块链中获取上一级身份证明发布节点的公钥，以及上一级身份证明节点根据上一级身份证明节点的私钥对身份证明发布节点的公钥进行数字签名得到的第四数字签名；

[0203] 根据上一级身份证明发布节点的公钥对第四数字签名进行验证；

[0204] 在第四数字签名通过验证后，根据从区块链中获取的身份证明发布节点的公钥对第一数字签名进行验证。

[0205] 或者，第一验证模块620用于：

[0206] 在第一数字签名通过验证后，从区块链中获取上一级身份证明发布节点的公钥，以及上一级身份证明节点根据上一级身份证明节点的私钥对身份证明发布节点的公钥进行数字签名得到的第四数字签名；根据上一级身份证明发布节点的公钥对第四数字签名进行验证；

[0207] 发送模块还用于在第四数字签名通过验证后，第二验证模块630验证被认证方是否掌握与被认证方节点的公钥对应的私钥。

[0208] 可选的，被认证方节点的身份信息包括被认证方节点的账户地址或者被认证方节点的公钥，被认证方节点的账户地址是根据被认证方节点的公钥获取的；身份证明发布节点的身份信息包括：身份证明发布节点的账户地址或者身份证明发布节点的公钥，身份证明发布节点的账户地址是根据身份证明发布节点的公钥获取的。

[0209] 图9是根据一实施例示出的另一种基于区块链的身份认证装置框图，该装置900应

用于被认证方节点，用于执行图1或图3至图5任一所示的方法，参见图9，该装置900可以包括：装置包括：认证请求模块910和验证模块920，其中：

[0210] 认证请求模块910，用于向认证方发送认证请求，认证请求中包括被认证方节点的身份信息和身份证明发布节点的身份信息；

[0211] 验证模块920，用于在认证方节点在确认被认证方节点的身份信息、身份证明发布节点的身份信息、身份证明发布节点对被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中，并且在第一数字签名通过认证方节点的验证后，与认证方节点进行被认证方是否掌握与被认证方节点的公钥对应的私钥的验证；当认证方节点确认被认证方已掌握与被认证方节点的公钥对应的私钥时，被认证方节点通过身份认证。

[0212] 可选的，图10是根据图9所示实施例示出的一种验证模块框图，如图10所示，验证模块920包括：

[0213] 接收子模块921，用于在第一数字签名通过认证方节点的验证后，接收认证方节点发送的验证信息；

[0214] 签名子模块922，用于根据被认证方节点的私钥对验证信息进行数字签名得到第二数字签名；

[0215] 发送子模块923，用于向认证方节点发送第二数字签名，当第二数字签名通过认证方的验证时，被认证方节点被确认已掌握与被认证方节点的公钥对应的私钥。

[0216] 可选的，图11是根据图9所示实施例示出的另一种验证模块框图，如图11所示，验证模块920包括：

[0217] 信息生成子模块923，用于在第一数字签名通过认证方节点的验证后，根据预设的信息生成规则生成验证信息；信息生成规则预设置在被认证方节点和认证方节点；

[0218] 签名子模块924，用于根据被认证方节点的私钥对验证信息进行数字签名得到第三数字签名；

[0219] 发送子模块925，用于向认证方节点发送验证信息以及第三数字签名；当认证方节点确认验证信息是按照信息生成规则生成的，并且认证方节点根据被认证方节点的公钥对第三数字签名进行的验证通过验证时，被认证方节点被确认已掌握与被认证方节点的公钥对应的私钥。

[0220] 可选的，图12是根据一实施例示出的又一种基于区块链的身份认证装置框图，装置900还包括：身份证明请求模块930，用于：

[0221] 向区块链写入身份证明请求，身份证明请求中包括被认证方节点的身份信息，用于身份证明发布节点在区块链中确认被认证方节点的身份信息，并根据身份证明发布节点的私钥对被认证方节点的身份信息进行数字签名得到第一数字签名，并将第一数字签名写入区块链。

[0222] 可选的，在身份证明发布节点向区块链写入用于撤销第一数字签名的撤销证明后，被认证方节点的第一数字签名被撤销，撤销证明中包括对第一数字签名的撤销说明，以及通过身份证明发布节点的私钥对撤销说明进行数字签名得到第五数字签名。

[0223] 可选的，被认证方节点的身份信息包括被认证方节点的账户地址或者被认证方节点的公钥，被认证方节点的账户地址是根据被认证方节点的公钥获取的；身份证明发布节点的身份信息包括：身份证明发布节点的账户地址或者身份证明发布节点的公钥，身份证

明发布节点的账户地址是根据身份证明发布节点的公钥获取的。

[0224] 综上所述，由于被认证方的身份信息和身份证明发布节点的身份信息均记录在区块链中，不会因为某个或某些节点的故障导致无法获取身份信息，因此能够避免单点故障对整个系统的影响，并且在区块链网络中，由于任何一个节点只要配置了身份证明发布节点的私钥，其角色就是身份认证发布节点，因此身份证明发布节点不是固定的某一节点，攻击者无法对对身份认证信息发布节点进行定位，从而无法对身份认证节点发起攻击，从而保证了整个系统的安全，因此能够解决由于单点故障问题和安全问题而影响整个系统的可用性和安全性的问题，保证整个系统的可用性和安全性。

[0225] 本公开实施例还提供一种非临时性计算机可读存储介质1，所述非临时性计算机可读存储介质中包括一个或多个程序，所述一个或多个程序用于执行一种基于区块链的身份认证方法，该基于区块链的身份认证方法应用于认证方节点，该基于区块链的身份认证方法包括：接收被认证方节点发送的认证请求，所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息；在确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息，以及所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中时，根据所述身份证明发布节点的公钥对所述第一数字签名进行验证；所述身份证明发布节点的公钥是根据所述身份证明发布节点的身份信息获取的；在所述第一数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥；所述被认证方节点的公钥是根据所述被认证方节点的身份信息获取的；当确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时，确定所述被认证方节点通过身份认证。

[0226] 可选的，所述在所述第一数字签名通过验证后，验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥，包括：在所述第一数字签名通过验证后，向所述被认证方节点发送验证信息；接收所述被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第二数字签名；根据所述被认证方节点的公钥对所述第二数字签名进行验证；当所述第二数字签名通过验证时，确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

[0227] 可选的，所述在所述第一数字签名通过验证后，向所述被认证方确认所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥，包括：接收所述被认证方节点发送的验证信息，以及被认证方节点根据所述被认证方节点的私钥对所述验证信息进行数字签名得到的第三数字签名；所述验证信息是所述被认证方节点根据预设的信息生成规则生成的，所述信息生成规则预设置在所述被认证方节点和所述认证方节点；验证所述验证信息是否是按照所述信息生成规则生成的；当所述验证信息是按照所述信息生成规则生成的时，根据所述被认证方节点的公钥对所述第三数字签名进行验证；当所述第三数字签名通过验证时，确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥。

[0228] 可选的，当所述身份证明发布节点存在上一级身份证明发布节点时，所述根据所述身份证明发布节点的公钥对所述第一数字签名进行验证，包括：

[0229] 从所述区块链中获取所述上一级身份证明发布节点的公钥，以及所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名；根据所述上一级身份证明发布节点的公钥对所述第四数字签名

进行验证;在所述第四数字签名通过验证后,根据从所述区块链中获取的所述身份证明发布节点的公钥对所述第一数字签名进行验证。

[0230] 可选的,所述在所述第一数字签名通过验证后,在验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥之前,还包括:在所述第一数字签名通过验证后,从所述区块链中获取所述上一级身份证明发布节点的公钥,以及所述上一级身份证明节点根据所述上一级身份证明节点的私钥对所述身份证明发布节点的公钥进行数字签名得到的第四数字签名;根据所述上一级身份证明发布节点的公钥对所述第四数字签名进行验证;在所述第四数字签名通过验证后,验证所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥。

[0231] 可选的,所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥,所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的;所述身份证明发布节点的身份信息包括:所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥,所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

[0232] 本公开实施例还提供一种用户节点2,所述用户节点2包括:

[0233] 上述的非临时性计算机可读存储介质1;以及

[0234] 一个或者多个处理器,用于执行上述的非临时性计算机可读存储介质1中的程序。

[0235] 本公开实施例还提供另一种非临时性计算机可读存储介质3,所述非临时性计算机可读存储介质3中包括一个或多个程序,所述一个或多个程序用于执行一种基于区块链的身份认证方法,该基于区块链的身份认证方法应用于被认证方节点,该基于区块链的身份认证方法包括:向认证方发送认证请求,所述认证请求中包括所述被认证方节点的身份信息和身份证明发布节点的身份信息;在所述认证方节点在确认所述被认证方节点的身份信息、所述身份证明发布节点的身份信息、所述身份证明发布节点对所述被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中,并且在所述第一数字签名通过所述认证方节点的验证后,与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证;当所述认证方节点确认所述被认证方已掌握与所述被认证方节点的公钥对应的私钥时,所述被认证方节点通过身份认证。

[0236] 可选的,所述在所述第一数字签名通过所述认证方节点的验证后,与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证,包括:在所述第一数字签名通过所述认证方节点的验证后,接收所述认证方节点发送的验证信息;根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第二数字签名;向所述认证方节点发送所述第二数字签名,当所述第二数字签名通过所述认证方的验证时,所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

[0237] 可选的,所述在所述第一数字签名通过所述认证方节点的验证后,与所述认证方节点进行所述被认证方是否掌握与所述被认证方节点的公钥对应的私钥的验证,包括:在所述第一数字签名通过所述认证方节点的验证后,根据预设的信息生成规则生成验证信息;所述信息生成规则预设置在所述被认证方节点和所述认证方节点;根据所述被认证方节点的私钥对所述验证信息进行数字签名得到第三数字签名;向所述认证方节点发送所述验证信息以及所述第三数字签名;当所述认证方节点确认所述验证信息是按照所述信息生

成规则生成的，并且所述认证方节点根据所述被认证方节点的公钥对所述第三数字签名进行的验证通过验证时，所述被认证方节点被确认已掌握与所述被认证方节点的公钥对应的私钥。

[0238] 可选的，所述身份证明发布节点对所述被认证方节点的身份信息和所述第一数字签名写入所述区块链的方法包括：向所述区块链写入身份证明请求，所述身份证明请求中包括所述被认证方节点的身份信息，用于所述身份证明发布节点在所述区块链中确认所述被认证方节点的身份信息，并根据所述身份证明发布节点的私钥对所述被认证方节点的身份信息进行数字签名得到所述第一数字签名，并将所述第一数字签名写入所述区块链。

[0239] 可选的，在所述身份证明发布节点向所述区块链写入用于撤销所述第一数字签名的撤销证明后，所述被认证方节点的所述第一数字签名被撤销，所述撤销证明中包括对所述第一数字签名的撤销说明，以及通过所述身份证明发布节点的私钥对所述撤销说明进行数字签名得到第五数字签名。

[0240] 可选的，所述被认证方节点的身份信息包括所述被认证方节点的账户地址或者所述被认证方节点的公钥，所述被认证方节点的账户地址是根据所述被认证方节点的公钥获取的；所述身份证明发布节点的身份信息包括：所述身份证明发布节点的账户地址或者所述身份证明发布节点的公钥，所述身份证明发布节点的账户地址是根据所述身份证明发布节点的公钥获取的。

[0241] 本公开实施例还提供另一种用户节点4，所述用户节点4包括：

[0242] 上述的非临时性计算机可读存储介质3；以及

[0243] 一个或者多个处理器，用于执行上述的非临时性计算机可读存储介质3中的程序。

[0244] 本公开实施例还提供一种身份认证系统，所述系统包括：

[0245] 区块链；

[0246] 至少一个上述的用户节点1，作为认证方节点；

[0247] 至少一个上述的用户节点4，作为被认证方节点；以及

[0248] 至少一个身份证明发布节点；

[0249] 其中，所述区块链，所述至少一个上述的用户节点1，所述至少一个上述的用户节点4以及所述至少一个身份证明发布节点属于同一区块链网络。

[0250] 可选的，所述系统中身份证明发布节点和用户节点的关系可以包括以下三种：

[0251] 在第一种实现方式中，如图13所示，图13是根据一实施例示出的一种身份认证系统结构框图，在图13中，所述至少一个身份证明发布节点为一个身份证明发布节点，该身份证明发布节点用于向区块链发布区块链网络中的每个用户节点的身份证明；

[0252] 其中，以第一用户节点为例，该第一用户节点为任一用户节点，身份证明发布节点向区块链发布第一用户节点的身份证明包括：身份证明发布节点在区块链中确认第一用户节点的身份信息，并根据身份证明发布节点的私钥对第一用户节点的身份信息进行数字签名，并将得到的数字签名写入区块链。

[0253] 在第二种实现方式中，如图14a所示，图14a是根据一实施例示出的另一种身份认证系统结构框图，在图14a中，所述至少一个身份证明发布节点至少包括一个身份证明发布节点和该身份证明发布节点的上一级身份证明发布节点，身份证明发布节点用于向区块链发布每个用户节点的身份证明，上一级身份证明发布节点用于向区块链发布身份证明发布

节点的身份证明；另外，如图14b所示，图14b是根据一实施例示出的又一种身份认证系统结构框图，在图14b中，上述的上一级身份证明发布节点也可能存在更上一级的身份证明发布节点，这里称为上上一级身份证明发布节点，上一级身份证明发布节点，用于向区块链发布上一级身份证明发布节点的身份证明，并且，身份证明发布节点可以不用发布每个用户节点的身份证明，而是由身份证明发布节点、上一级身份证明发布节点以及上一级身份证明发布节点各自负责一部分用户节点的身份证明的发布。并且，上上一级身份证明发布节点可以作为另一部分用户节点的身份证明发布节点，当然，还可能存在更高一级的身份证明发布节点，以此类推，不再一一列举。

[0254] 其中，以第一用户节点为例，该第一用户节点为任一用户节点，身份证明发布节点向区块链发布第一用户节点的身份证明包括：身份证明发布节点在区块链中确认第一用户节点的身份信息，并根据身份证明发布节点的私钥对第一用户节点的身份信息进行数字签名，并将得到的数字签名写入区块链；上一级身份证明发布节点向区块链发布身份证明发布节点的身份证明包括：上一级身份证明节点根据上一级身份证明节点的私钥对身份证明发布节点的公钥进行数字签名，并将得到的数字签名写入所述区块链。上上一级身份证明发布节点向区块链发布上一级身份证明发布节点的身份证明包括：上上一级身份证明节点根据上上一级身份证明节点的私钥对上一级身份证明发布节点的公钥进行数字签名，并将得到的数字签名写入所述区块链。

[0255] 另外，上上一级身份证明节点和上上一级身份证明发布节点向区块链发布用户节点的身份证明的方法与上述的身份证明发布节点向区块链发布第一用户节点的身份证明的方法相同，不在赘述。

[0256] 在第三种实现方式中，如图15所示，图15是根据一实施例示出的又一种身份认证系统结构框图，该身份认证系统可以包括多个身份证明发布子系统，每个身份证明发布子系统中可以包括至少一个身份证明发布节点和至少一个用户节点；

[0257] 其中，当第一身份证明发布子系统中包括一个身份证明发布节点时，该身份证明发布节点用于向区块链发布第一身份证明发布子系统的第一用户节点的身份证明，该第一用户节点为第一身份证明发布子系统中的任一用户节点；第一身份证明发布子系统为该多个身份证明发布子系统中的任一身份证明发布子系统；

[0258] 当第一身份证明发布子系统中至少包括一个身份证明发布节点和身份证明发布节点的上一级身份证明发布节点，身份证明发布节点用于向区块链发布第一身份证明发布子系统的第一用户节点的身份证明，上一级身份证明发布节点用于向区块链发布身份证明发布节点的身份证明；

[0259] 其中，身份证明发布节点向区块链发布第一身份证明发布子系统的第一用户节点的身份证明包括：身份证明发布节点在区块链中确认第一用户节点的身份信息，并根据身份证明发布节点的私钥对第一用户节点的身份信息进行数字签名，并将得到的数字签名写入区块链；

[0260] 上一级身份证明发布节点向区块链发布身份证明发布节点的身份证明包括：上一级身份证明节点根据上一级身份证明节点的私钥对身份证明发布节点的公钥进行数字签名，并将得到的数字签名写入区块链。即可以理解为每个身份证明发布子系统可以包括如图13、或图14a或图14b所示的结构。

[0261] 以上结合附图详细描述了本公开的优选实施方式，但是，本公开并不限于上述实施方式中的具体细节，在本公开的技术构思范围内，可以对本公开的技术方案进行多种简单变型，这些简单变型均属于本公开的保护范围。

[0262] 另外需要说明的是，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，可以通过任何合适的方式进行组合，为了避免不必要的重复，本公开对各种可能的组合方式不再另行说明。

[0263] 此外，本公开的各种不同的实施方式之间也可以进行任意组合，只要其不违背本公开的思想，其同样应当视为本公开所公开的内容。

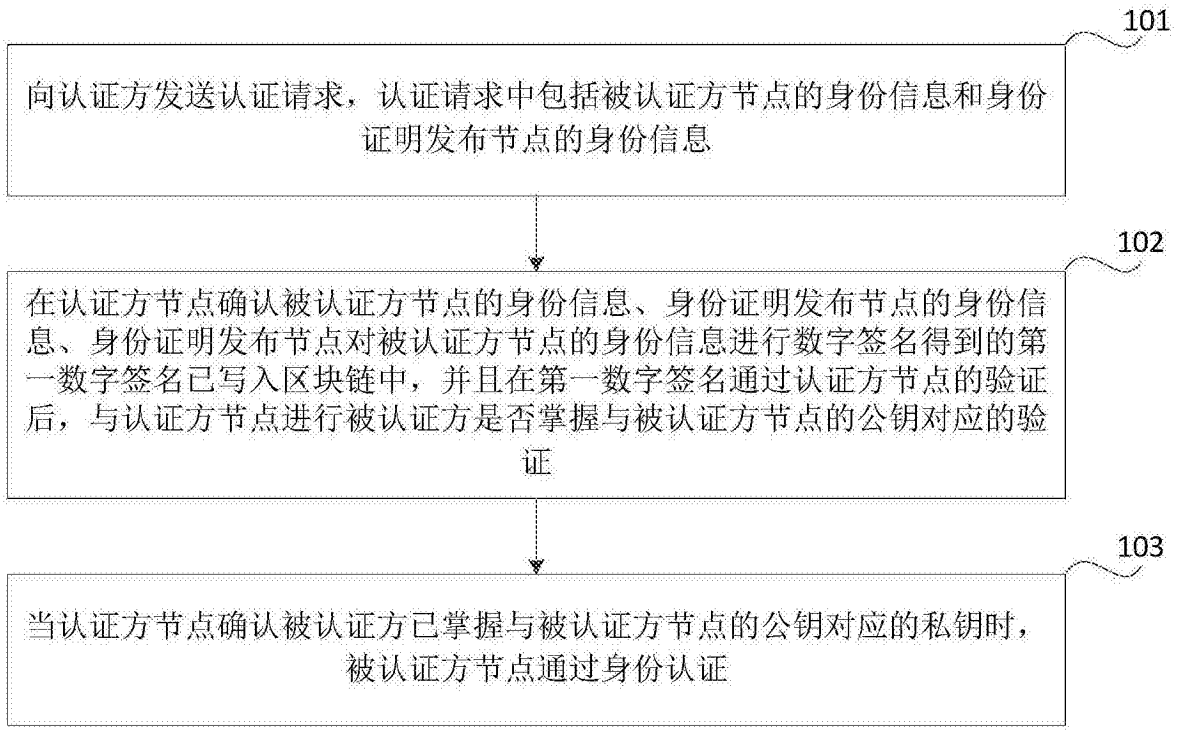

101
向认证方发送认证请求，认证请求中包括被认证方节点的身份信息和身份证明发布节点的身份信息
102
在认证方节点确认被认证方节点的身份信息、身份证明发布节点的身份信息、身份证明发布节点对被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中，并且在第一数字签名通过认证方节点的验证后，与认证方节点进行被认证方是否掌握与被认证方节点的公钥对应的验证
103
当认证方节点确认被认证方已掌握与被认证方节点的公钥对应的私钥时，被认证方节点通过身份认证

图1

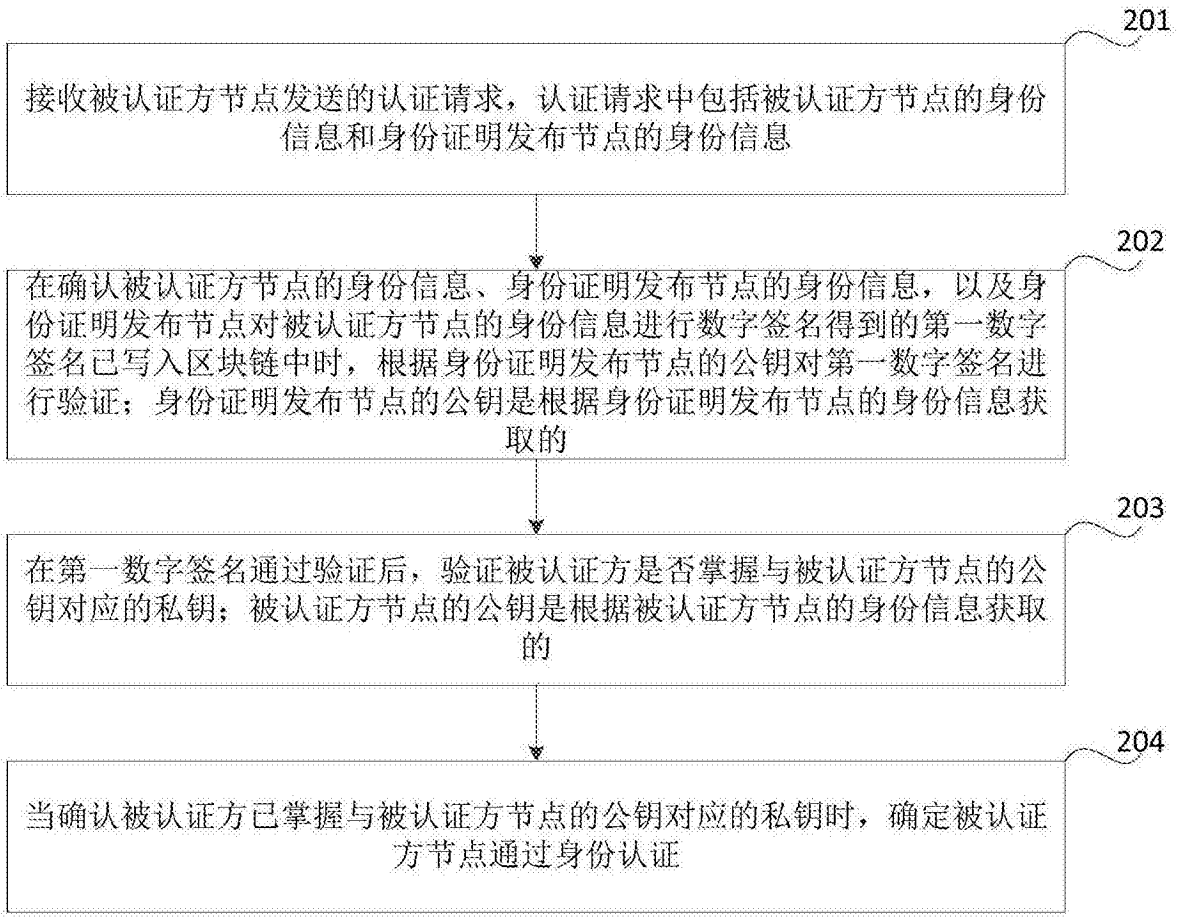

201
接收被认证方节点发送的认证请求，认证请求中包括被认证方节点的身份信息和身份证明发布节点的身份信息
202
在确认被认证方节点的身份信息、身份证明发布节点的身份信息，以及身份证明发布节点对被认证方节点的身份信息进行数字签名得到的第一数字签名已写入区块链中时，根据身份证明发布节点的公钥对第一数字签名进行验证；身份证明发布节点的公钥是根据身份证明发布节点的身份信息获取的
203
在第一数字签名通过验证后，验证被认证方是否掌握与被认证方节点的公钥对应的私钥；被认证方节点的公钥是根据被认证方节点的身份信息获取的
204
当确认被认证方已掌握与被认证方节点的公钥对应的私钥时，确定被认证方节点通过身份认证

图2

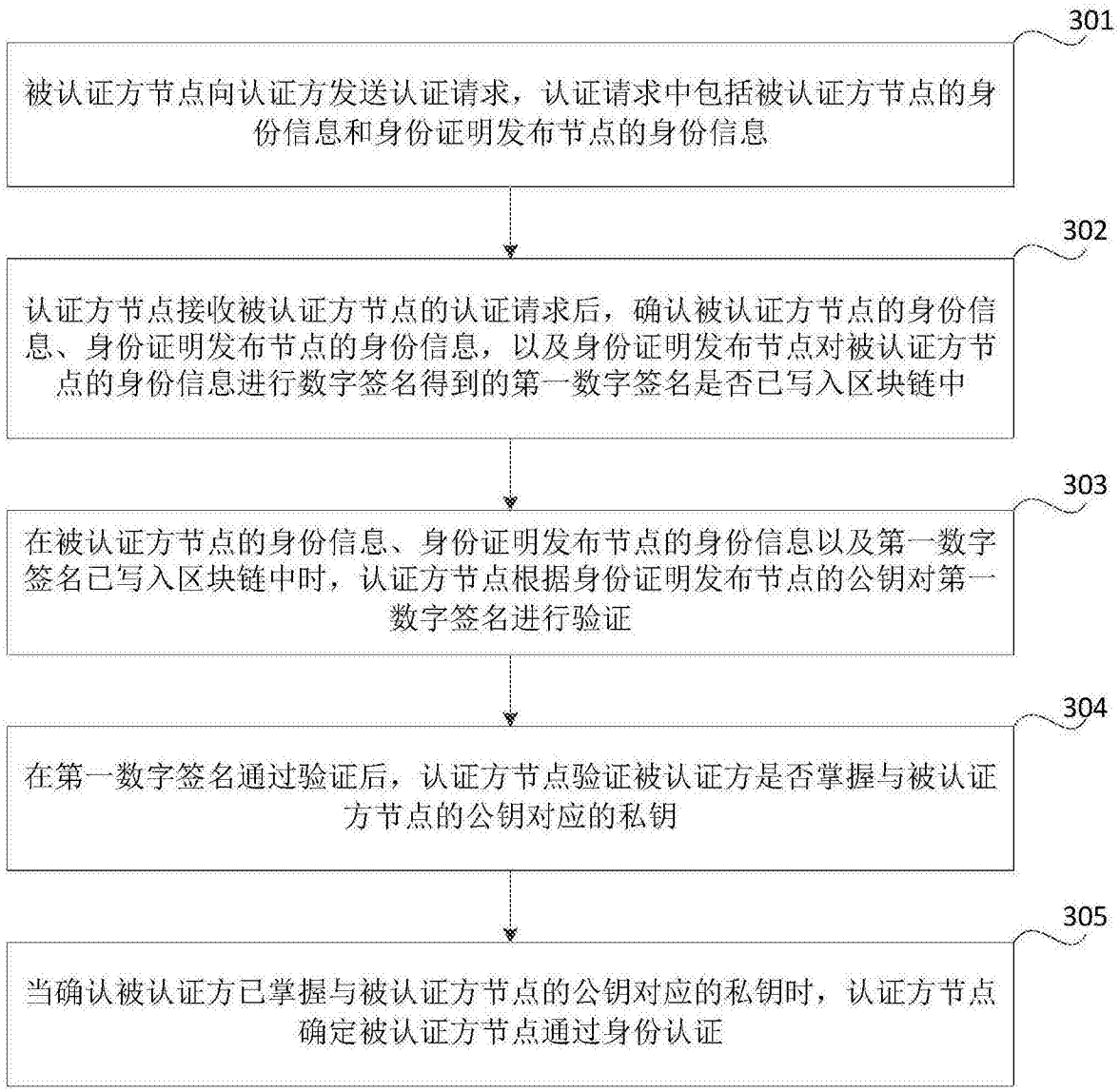

301
被认证方节点向认证方发送认证请求，认证请求中包括被认证方节点的身份信息和身份证明发布节点的身份信息
302
认证方节点接收被认证方节点的认证请求后，确认被认证方节点的身份信息、身份证明发布节点的身份信息，以及身份证明发布节点对被认证方节点的身份信息进行数字签名得到的第一数字签名是否已写入区块链中
303
在被认证方节点的身份信息、身份证明发布节点的身份信息以及第一数字签名已写入区块链中时，认证方节点根据身份证明发布节点的公钥对第一数字签名进行验证
304
在第一数字签名通过验证后，认证方节点验证被认证方是否掌握与被认证方节点的公钥对应的私钥
305
当确认被认证方已掌握与被认证方节点的公钥对应的私钥时，认证方节点确定被认证方节点通过身份认证

图3

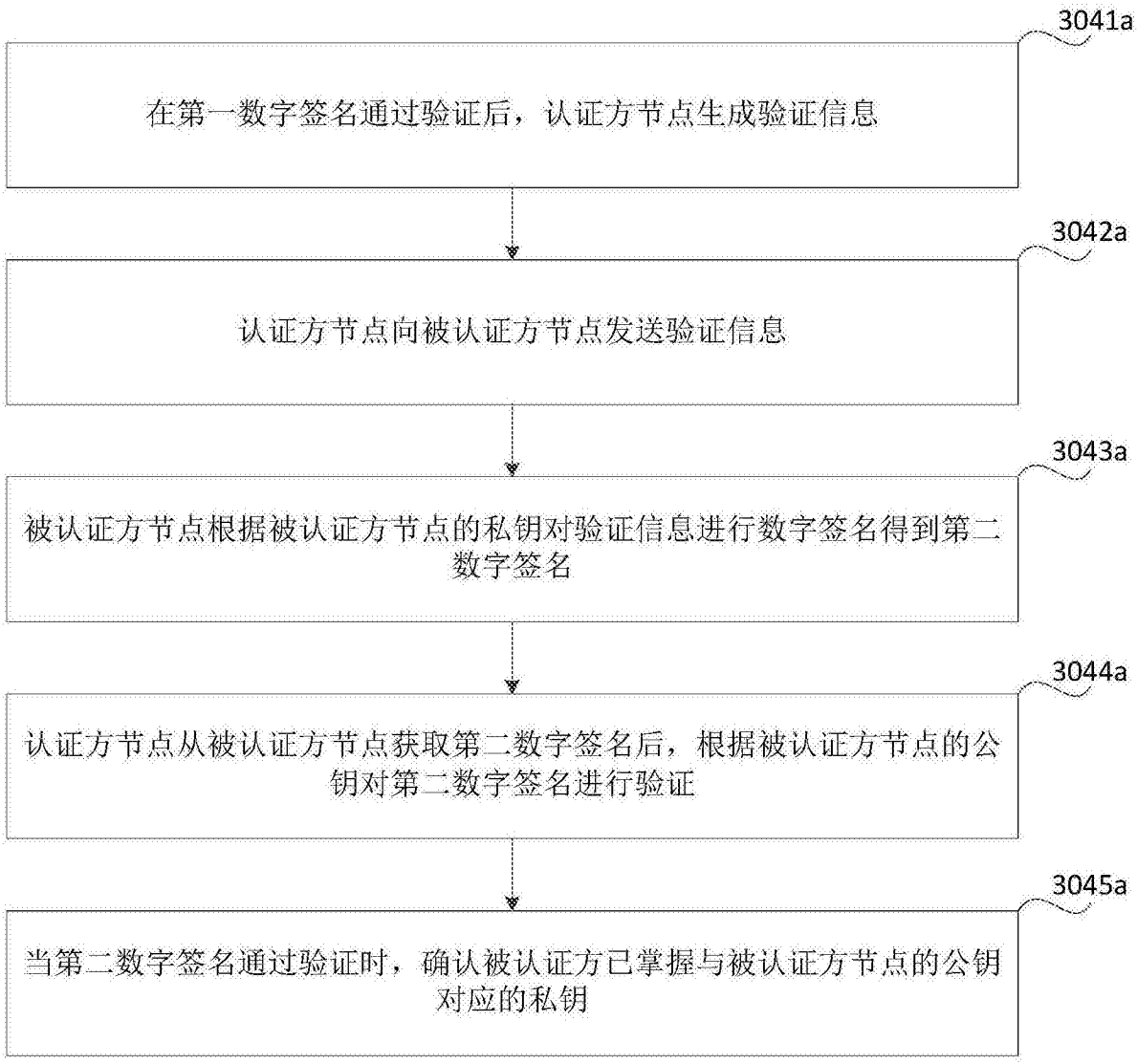

3041a
在第一数字签名通过验证后，认证方节点生成验证信息
3042a
认证方节点向被认证方节点发送验证信息
3043a
被认证方节点根据被认证方节点的私钥对验证信息进行数字签名得到第二数字签名
3044a
认证方节点从被认证方节点获取第二数字签名后，根据被认证方节点的公钥对第二数字签名进行验证
3045a
当第二数字签名通过验证时，确认被认证方已掌握与被认证方节点的公钥对应的私钥

图4

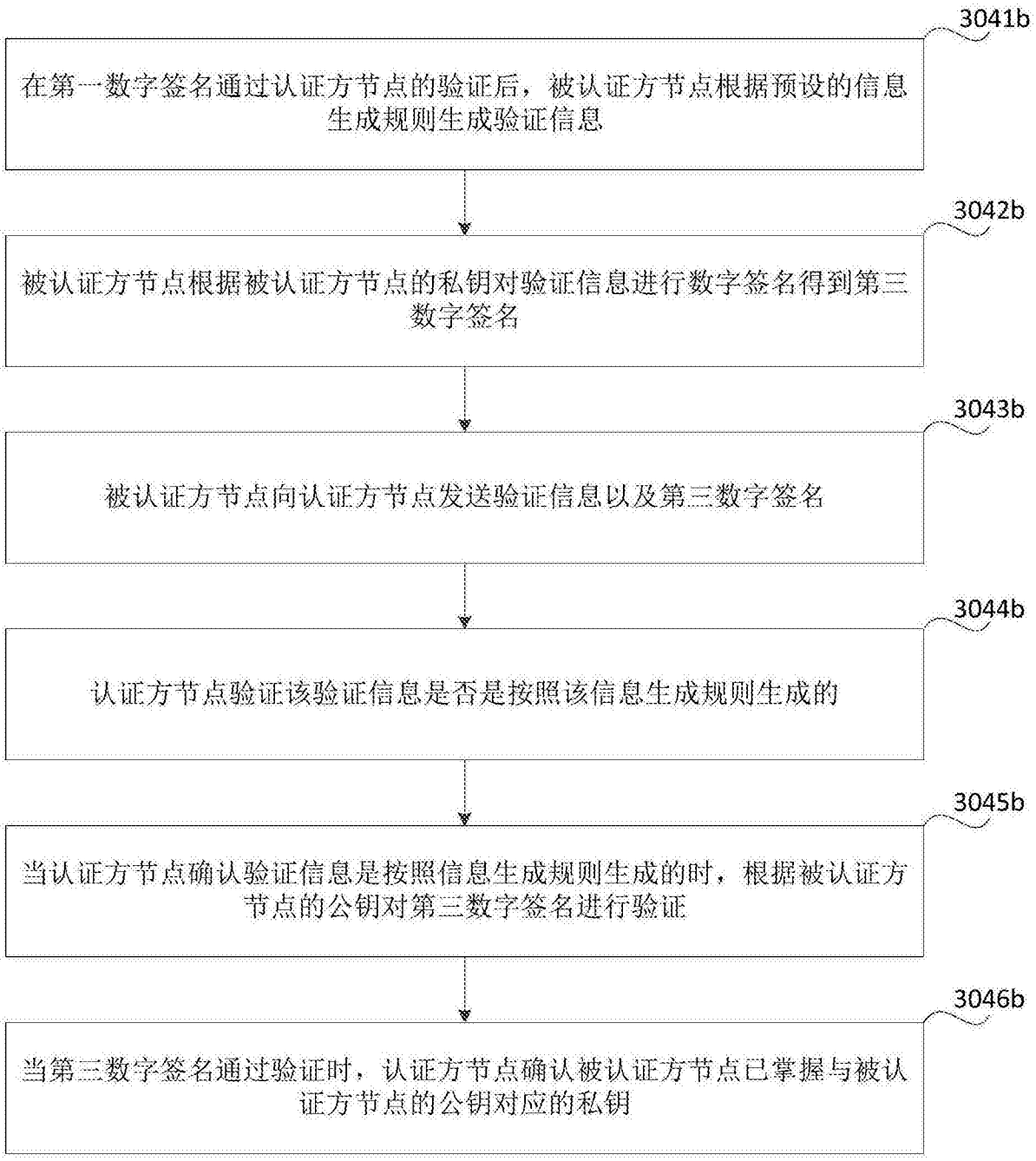

3041b
在第一数字签名通过认证方节点的验证后，被认证方节点根据预设的信息生成规则生成验证信息
3042b
被认证方节点根据被认证方节点的私钥对验证信息进行数字签名得到第三数字签名
3043b
被认证方节点向认证方节点发送验证信息以及第三数字签名
3044b
认证方节点验证该验证信息是否是按照该信息生成规则生成的
3045b
当认证方节点确认验证信息是按照信息生成规则生成的时，根据被认证方节点的公钥对第三数字签名进行验证
3046b
当第三数字签名通过验证时，认证方节点确认被认证方节点已掌握与被认证方节点的公钥对应的私钥

图5

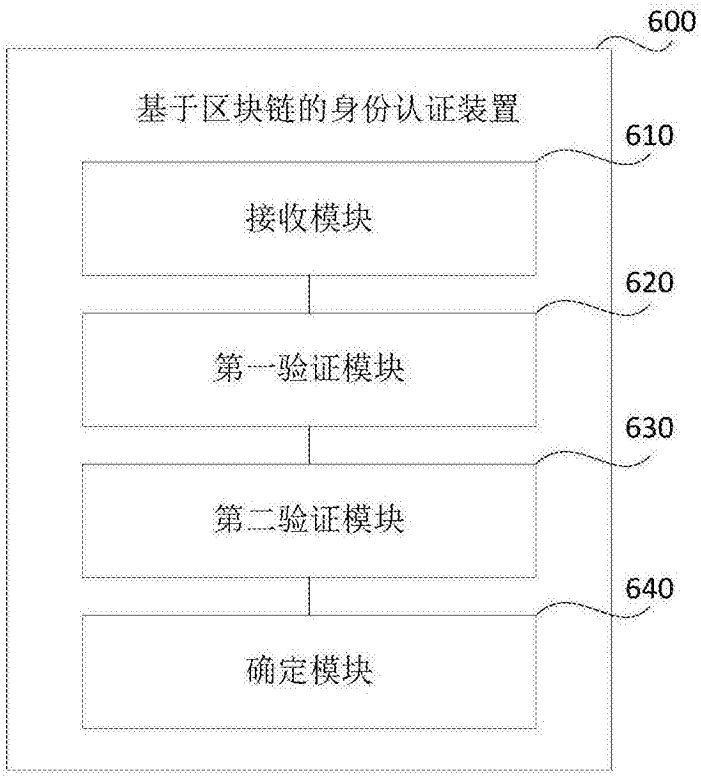

600
基于区块链的身份认证装置
610
接收模块
620
第一验证模块
630
第二验证模块
640
确定模块

图6

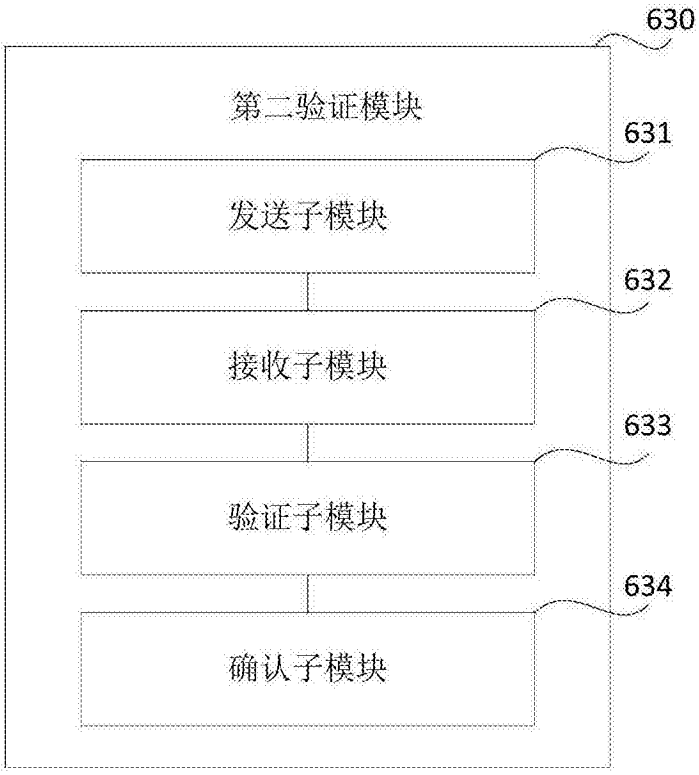

630
第二验证模块
631
发送子模块
632
接收子模块
633
验证子模块
634
确认子模块

图7

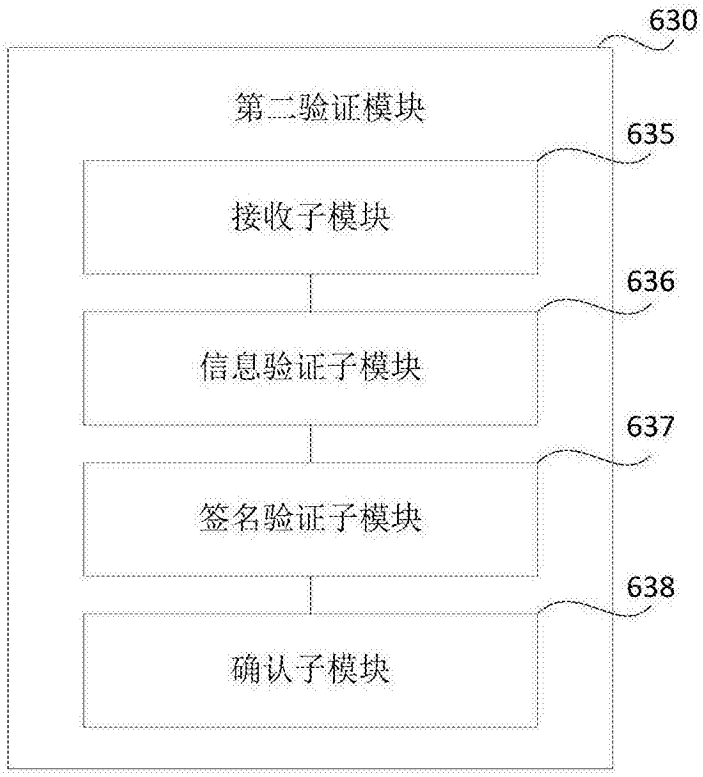

630
第二验证模块
635
接收子模块
636
信息验证子模块
637
签名验证子模块
638
确认子模块

图8

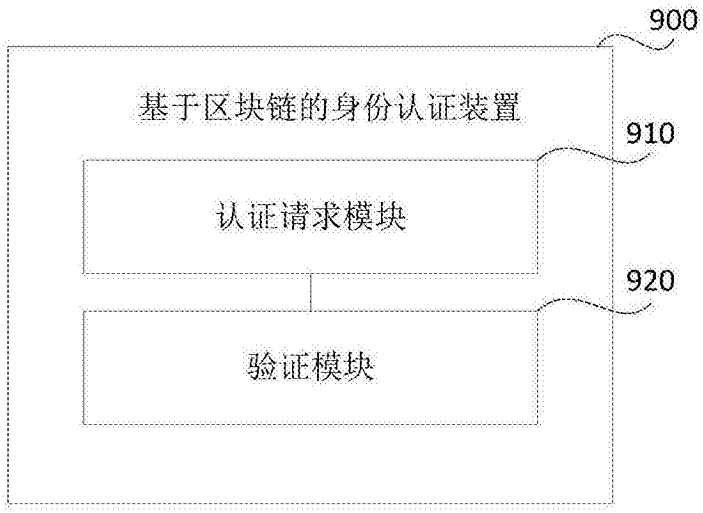

900
基于区块链的身份认证装置
910
认证请求模块
920
验证模块

图9

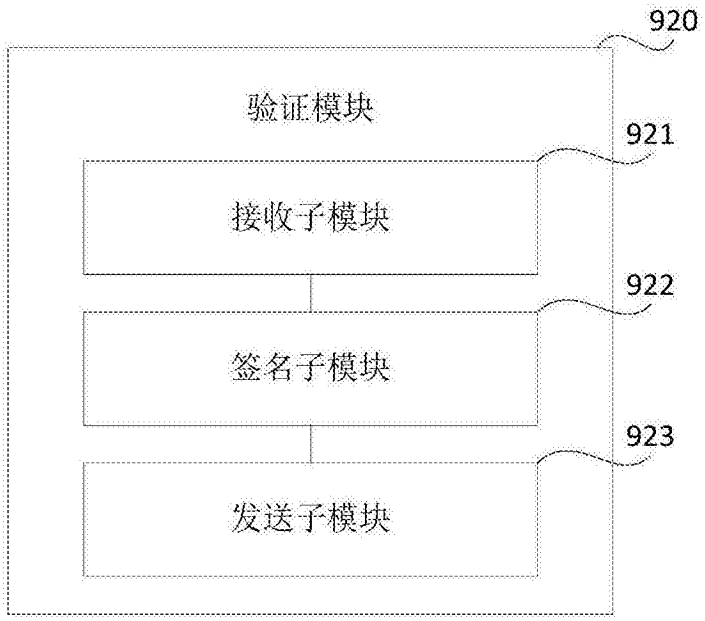

920
验证模块
921
接收子模块
922
签名子模块
923
发送子模块

图10

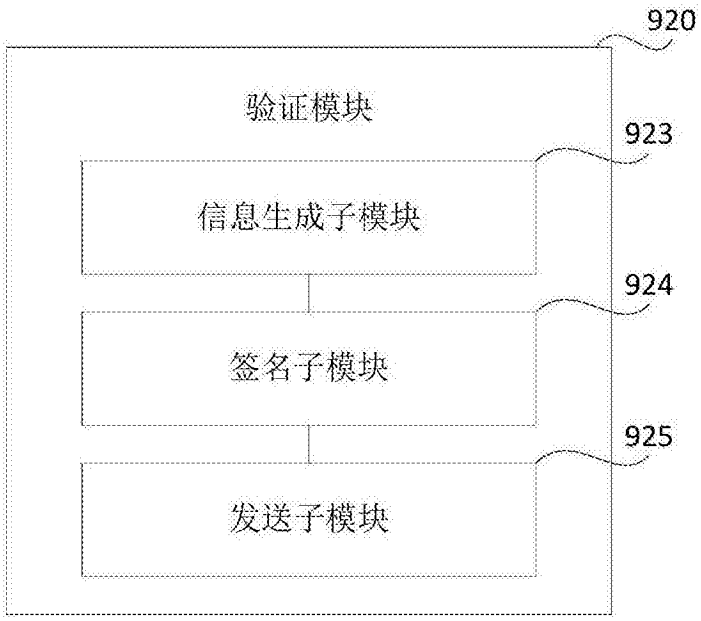

920
验证模块
923
信息生成子模块
924
签名子模块
925
发送子模块

图11

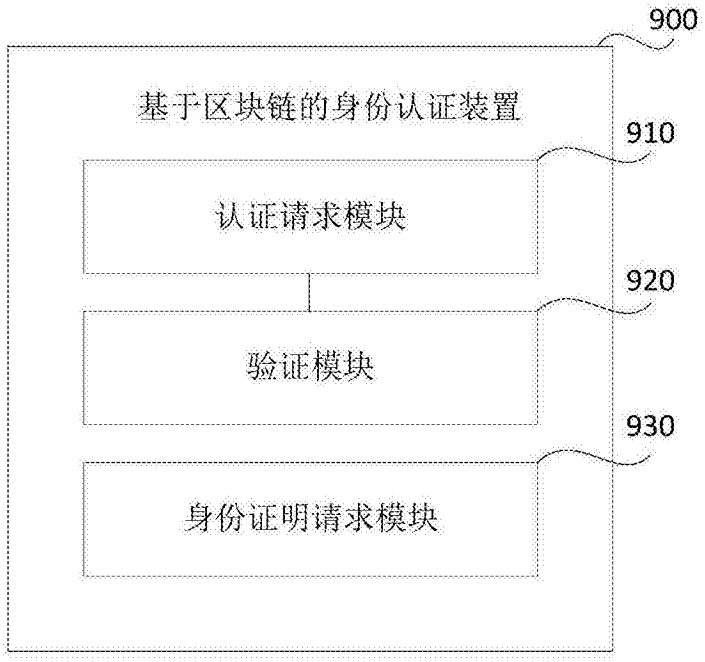

900
基于区块链的身份认证装置
910
认证请求模块
920
验证模块
930
身份证明请求模块

图12

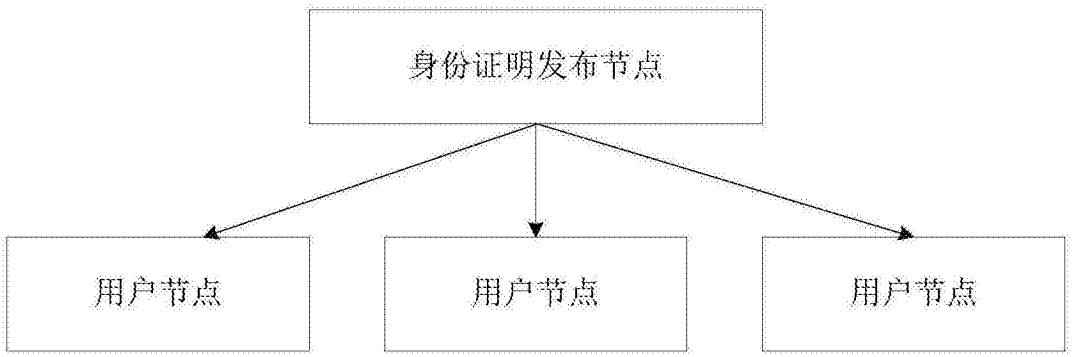

身份证明发布节点
用户节点
用户节点
用户节点

图13

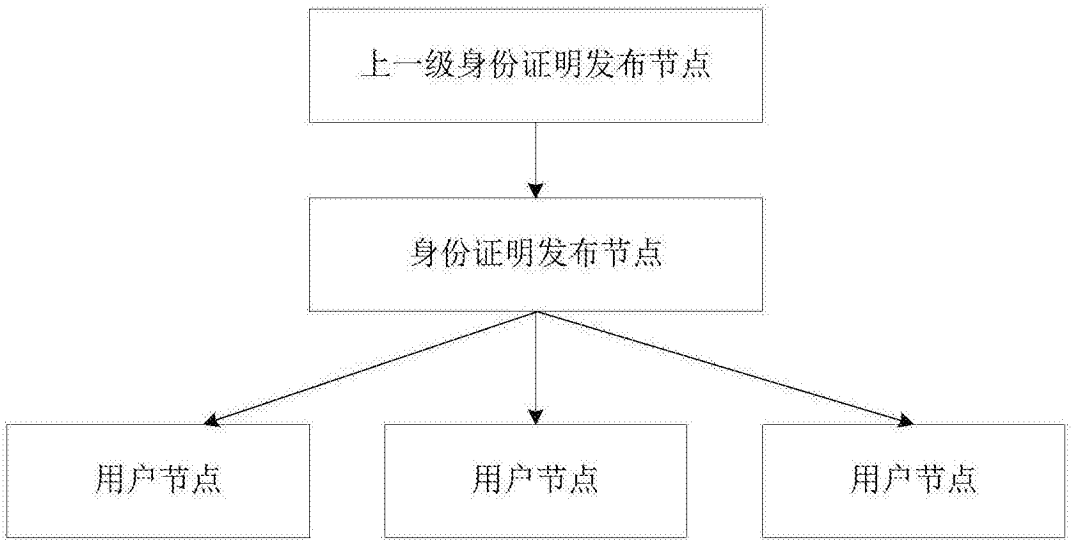

上一级身份证明发布节点
身份证明发布节点
用户节点
用户节点
用户节点

图14a

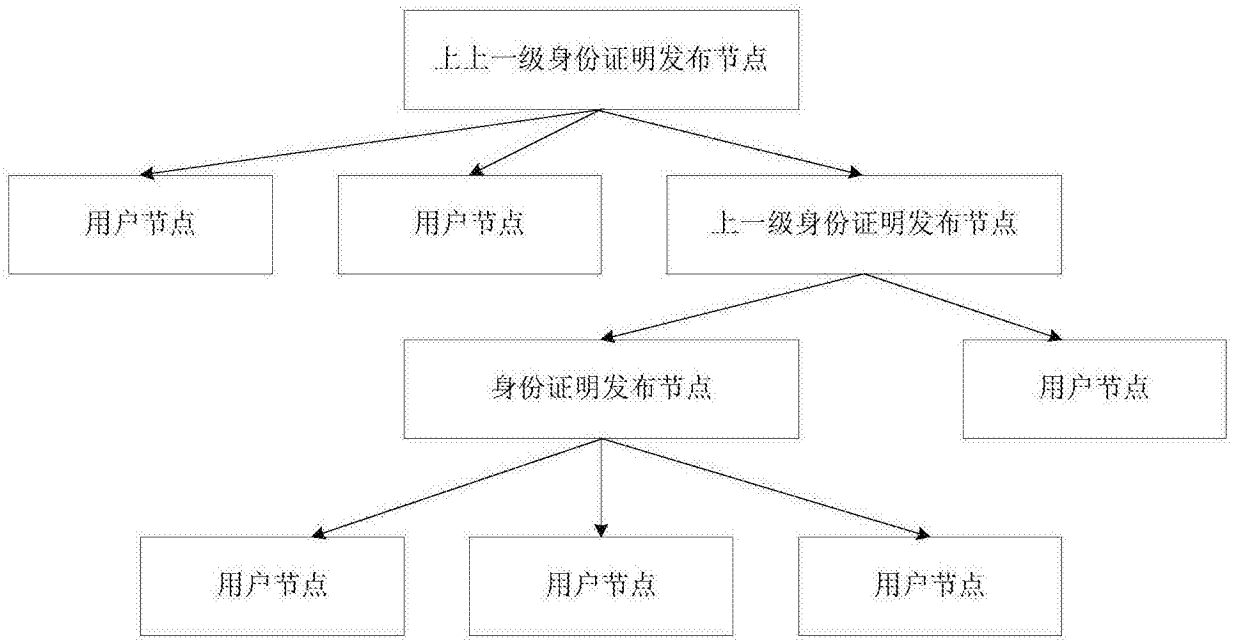

上上一级身份证明发布节点
用户节点
用户节点
上一级身份证明发布节点
身份证明发布节点
用户节点
用户节点
用户节点
用户节点

图14b

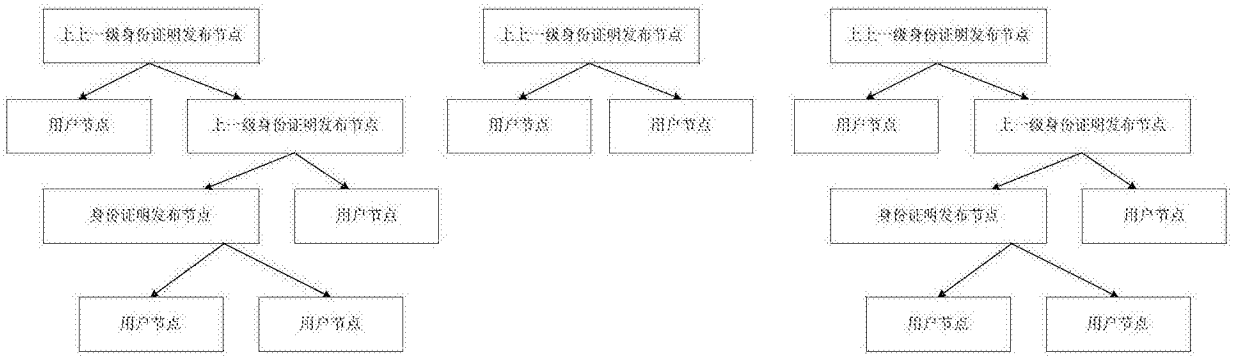

上上一级身份证明发布节点
用户节点
上一级身份证明发布节点
身份证明发布节点
用户节点
用户节点
上上一级身份证明发布节点
用户节点
用户节点
上上一级身份证明发布节点
用户节点
上一级身份证明发布节点
身份证明发布节点
用户节点
用户节点
用户节点

图15