(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 113821789 A
(43)申请公布日 2021.12.21

(21)申请号 202111130210.9

(22)申请日 2021.09.26

(71)申请人 北京邮电大学
地址 100876 北京市海淀区西土城路10号北京邮电大学

(72)发明人 关建峰 许长桥 张天鸿 吴一楠

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王宇杨

(51)Int.Cl.
G06F 21/45(2013.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)

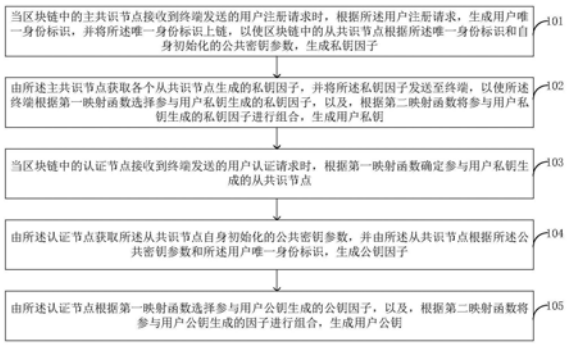
权利要求书2页 说明书10页 附图5页

(54)发明名称

基于区块链的用户密钥生成方法、装置、设备及介质

(57)摘要

本发明公开了一种基于区块链的用户密钥生成方法、装置、设备及介质，方法包括：主共识节点根据用户注册请求，生成用户唯一身份标识，从共识节点根据唯一身份标识和公共密钥参数，生成私钥因子；终端根据第一映射函数选择参与用户私钥生成的私钥因子并根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥；认证节点根据第一映射函数确定参与用户私钥生成的从共识节点并由从共识节点根据公共密钥参数和用户唯一身份标识，生成公钥因子；根据第一映射函数选择参与用户公钥生成的公钥因子，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。本发明解决了单一密钥生成中心所导致的第三方私钥管理问题。



CN 113821789 A

1.一种基于区块链的用户密钥生成方法,其特征在于,包括:

当区块链中的主共识节点接收到终端发送的用户注册请求时,根据所述用户注册请求,生成用户唯一身份标识,并将所述唯一身份标识上链,以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数,生成私钥因子;

由所述主共识节点获取各个从共识节点生成的私钥因子,并将所述私钥因子发送至终端,以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子,以及,根据第二映射函数将参与用户私钥生成的私钥因子进行组合,生成用户私钥;

当区块链中的认证节点接收到终端发送的用户认证请求时,根据第一映射函数确定参与用户私钥生成的从共识节点;

由所述认证节点获取所述从共识节点自身初始化的公共密钥参数,并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识,生成公钥因子;

由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子,以及,根据第二映射函数将参与用户公钥生成的因子进行组合,生成用户公钥。

2.根据权利要求1所述的基于区块链的用户密钥生成方法,其特征在于,所述用户注册请求包括用户的身份注册信息;

相应的,根据所述用户注册请求,生成用户唯一身份标识,包括:

对所述用户的身份注册信息进行建模,生成用户唯一身份标识。

3.根据权利要求1所述的基于区块链的用户密钥生成方法,其特征在于,所述公共密钥参数是由所述从共识节点根据预设密码体系,进行初始化后生成的。

4.根据权利要求1所述的基于区块链的用户密钥生成方法,其特征在于,所述终端根据第一映射函数选择参与用户私钥生成的私钥因子,包括:

所述终端根据用户唯一身份标识和私钥因子,通过第一映射函数生成随机序列,并根据所述随机序列选择参与用户私钥生成的私钥因子;

相应的,所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子,包括:

所述认证节点根据用户唯一身份标识和公钥因子,通过第一映射函数生成随机序列,并根据所述随机序列选择参与用户公钥生成的公钥因子。

5.根据权利要求4所述的基于区块链的用户密钥生成方法,其特征在于,当区块链中的认证节点接收到终端发送的用户认证请求时,根据第一映射函数确定参与用户私钥生成的从共识节点,包括:

根据用户认证请求,确定用户唯一身份标识;

根据所述唯一身份标识在第一映射函数中的映射关系确定参与用户私钥生成从共识节点。

6.一种基于区块链的用户密钥生成装置,其特征在于,包括:

第一处理模块,用于当区块链中的主共识节点接收到终端发送的用户注册请求时,根据所述用户注册请求,生成用户唯一身份标识,并将所述唯一身份标识上链,以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数,生成私钥因子;

第二处理模块,用于由所述主共识节点获取各个从共识节点生成的私钥因子,并将所述私钥因子发送至终端,以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子,以及,根据第二映射函数将参与用户私钥生成的私钥因子进行组合,生成用户私钥;

第三处理模块，用于当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点；

第四处理模块，用于由所述认证节点获取所述从共识节点自身初始化的公共密钥参数，并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识，生成公钥因子；

第五处理模块，用于由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。

7.根据权利要求6所述的基于区块链的用户密钥生成装置，其特征在于，所述公共密钥参数是由所述从共识节点根据预设密码体系，进行初始化后生成的。

8.根据权利要求6所述的基于区块链的用户密钥生成装置，其特征在于，所述第三处理模块，还具体用于：

根据用户认证请求，确定用户唯一身份标识；

根据所述唯一身份标识在第一映射函数中的映射关系确定参与用户私钥生成从共识节点。

9.一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求1-5任一项所述基于区块链的用户密钥生成方法的步骤。

10.一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，所述计算机程序被处理器执行时实现如权利要求1-5任一项所述基于区块链的用户密钥生成方法的步骤。

基于区块链的用户密钥生成方法、装置、设备及介质

技术领域

[0001] 本申请涉及用户认证技术领域，具体涉及一种基于区块链的用户密钥生成方法、装置、设备及介质。

背景技术

[0002] 用户接入认证是无线通信网络的基础，是保证网络内部安全至关重要的一步，其内容包括实现合法用户的入网、拒绝非法用户访问和防止通信数据的泄露。

[0003] 现有的集中式的身份信息管理是最常见的认证模型，用户的密钥信息以及关键参数均是由一个集中的认证节点生成和分发的，当该认证节点受到攻击时，密钥的安全强度无法得到保证，且会影响整个系统的安全性。

发明内容

[0004] 由于现有方法存在上述问题，本申请实施例提供一种基于区块链的用户密钥生成方法、装置、设备及介质。

[0005] 具体的，本申请实施例提供了以下技术方案：

[0006] 第一方面，本申请实施例提供了一种基于区块链的用户密钥生成方法，包括：

[0007] 当区块链中的主共识节点接收到终端发送的用户注册请求时，根据所述用户注册请求，生成用户唯一身份标识，并将所述唯一身份标识上链，以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数，生成私钥因子；

[0008] 由所述主共识节点获取各个从共识节点生成的私钥因子，并将所述私钥因子发送至终端，以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，以及，根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥；

[0009] 当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点；

[0010] 由所述认证节点获取所述从共识节点自身初始化的公共密钥参数，并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识，生成公钥因子；

[0011] 由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。

[0012] 可选的，所述用户注册请求包括用户的身份注册信息；

[0013] 相应的，根据所述用户注册请求，生成用户唯一身份标识，包括：

[0014] 对所述用户的身份注册信息进行建模，生成用户唯一身份标识。

[0015] 可选的，所述公共密钥参数是由所述从共识节点根据预设密码体系，进行初始化后生成的。

[0016] 可选的，所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，包括：

[0017] 所述终端根据用户唯一身份标识和私钥因子，通过第一映射函数生成随机序列，并根据所述随机序列选择参与用户私钥生成的私钥因子；

[0018] 相应的，所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，包括：

[0019] 所述认证节点根据用户唯一身份标识和公钥因子，通过第一映射函数生成随机序列，并根据所述随机序列选择参与用户公钥生成的公钥因子。

[0020] 可选的，当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点，包括：

[0021] 根据用户认证请求，确定用户唯一身份标识；

[0022] 根据所述唯一身份标识在第一映射函数中的映射关系确定参与用户私钥生成从共识节点。

[0023] 第二方面，本申请实施例提供了一种基于区块链的用户密钥生成装置，包括：

[0024] 第一处理模块，用于当区块链中的主共识节点接收到终端发送的用户注册请求时，根据所述用户注册请求，生成用户唯一身份标识，并将所述唯一身份标识上链，以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数，生成私钥因子；

[0025] 第二处理模块，用于由所述主共识节点获取各个从共识节点生成的私钥因子，并将所述私钥因子发送至终端，以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，以及，根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥；

[0026] 第三处理模块，用于当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点；

[0027] 第四处理模块，用于由所述认证节点获取所述从共识节点自身初始化的公共密钥参数，并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识，生成公钥因子；

[0028] 第五处理模块，用于由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。

[0029] 可选的，所述公共密钥参数是由所述从共识节点根据预设密码体系，进行初始化后生成的。

[0030] 可选的，所述第三处理模块，还具体用于：

[0031] 根据用户认证请求，确定用户唯一身份标识；

[0032] 根据所述唯一身份标识在第一映射函数中的映射关系确定参与用户私钥生成从共识节点。

[0033] 由上面技术方案可知，本申请实施例当区块链中的主共识节点接收到终端发送的用户注册请求时，首先根据用户注册请求，生成用户唯一身份标识，并将所述唯一身份标识上链，以使区块链中的从共识节点根据唯一身份标识和自身初始化的公共密钥参数，生成私钥因子。然后由主共识节点获取各个从共识节点生成的私钥因子，并将私钥因子发送至终端，以使终端根据第一映射函数选择参与用户私钥生成的私钥因子，以及，根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥。在用户认证阶段，当区块链中的认证节点接收到终端发送的用户认证请求时，首先根据第一映射函数确定参与用户私钥生成的从共识节点，然后由认证节点获取从共识节点自身初始化的公共密钥参数，并由

从共识节点根据公共密钥参数和用户唯一身份标识，生成公钥因子。最终由认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。由此可见，本申请实施例引入了区块链技术，很好的解决了传统用户认证方案中由于单一节点而导致的第三方密钥管理问题。网络内各个通信实体的私钥不再由集中式的密钥管理中心统一生成，而是从不同共识节点中产生的私钥因子组合而成，大大降低了单一节点情况下私钥泄露的风险。同时，当需要对方公钥进行验签时，不需要从其他的可信节点或者数据库进行查询，而是由事先在本地配置的公共参数和对方的身份标识ID即可快速计算获得其公钥，节约了查询请求以及结果传输过程中的时延和消耗。

附图说明

[0034] 为了更清楚地说明本发明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的前提下，还可以根据这些图获得其他的附图。

[0035] 图1是本申请实施例提供的基于区块链的用户密钥生成方法的步骤流程图之一；

[0036] 图2是本申请实施例提供的基于区块链的用户密钥生成方法的步骤流程图之二；

[0037] 图3是本申请实施例提供的基于区块链的用户密钥生成网络模型示意图；

[0038] 图4是本申请实施例提供的基于区块链的用户密钥生成系统模块示意图；

[0039] 图5是本申请实施例提供的基于区块链的用户密钥生成系统的流程示意图；

[0040] 图6是本申请实施例提供的基于区块链的用户密钥生成装置的结构示意图；

[0041] 图7是本申请实施例的电子设备的结构示意图。

具体实施方式

[0042] 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的前提下，还可以根据这些图获得其他的附图。

[0043] 如图1所示，本申请实施例提供的一种基于区块链的用户密钥生成方法，包括：

[0044] 步骤101：当区块链中的主共识节点接收到终端发送的用户注册请求时，根据所述用户注册请求，生成用户唯一身份标识，并将所述唯一身份标识上链，以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数，生成私钥因子；

[0045] 在本步骤中，需要说明的是，用户终端先在本地选择一对公私钥TPK_{MN}和TSK_{MN}用于和区块链间通信时的信息加密。当有用户终端向系统内的某一个共识节点提交注册请求时，当前的共识节点可以视为系统中的主共识节点。用户向主共识节点提交注册时需要的身份信息和公钥TPK_{MN}，主共识节点对用户的各项属性信息进行建模生成能在整个系统中唯一标识该用户身份的唯一标识ID_{MN}，并将该ID_{MN}加密后上链共识。其余的共识节点根据该ID_{MN}，结合之前各自生成的公共密钥参数，分别生成私钥因子。

[0046] 步骤102：由所述主共识节点获取各个从共识节点生成的私钥因子，并将所述私钥

因子发送至终端，以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，以及，根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥；

[0047] 在本步骤中，主共识节点在确保所有的共识节点均生成完私钥因子后，收集齐所有的私钥因子并使用TPK_{MN}加密，将他们打包后通过安全的信道返回给用户。用户在收到主共识节点返回的消息以后，先进行解密获取里面的私钥因子PPK_i和身份标识ID_{MN}，之后调用用户自主私钥组合算法对获得的PPK_i进行随机组合生成最终的私钥SK_{MN}。该算法的思路是根据ID_{MN}，通过Hash函数1的映射生成随机01序列，该序列决定了选取系统中哪些共识节点生成的私钥因子参与私钥的计算。再通过另一个Hash函数2生成加权序列，将参与私钥生成的私钥因子进行序列内系数的加权组合最终生成用户的私钥。该算法详细内容如下：

[0048] 输入：1.由各个共识节点生成的私钥因子PPKi，{i＝1,2,3,.....n}；

[0049] 2.用户唯一身份标识ID_{MN}。

[0050] 输出：用户私钥：SK_{MN}；

[0051] 算法步骤：

[0052] 1、从用户的ID_{MN}中获得用户的等级UL_{MN}；

[0053] 2、基于ID_{MN}和UL_{MN}，通过哈希函数(HashFunc1)生成随机序列$x=\{x_1,x_2,...,x_k\}$，$1\leqslant k\leqslant n$。HashFunc1：$\{AID_{MN},UL_{MN}\}\rightarrow\{0,1\}^*$

[0054] 3、基于ID_{MN}和UL_{MN}，通过哈希函数(HashFunc2)生成随机序列$\Delta=\{\delta_1,\delta_2,...,\delta_k\}$，$1\leqslant k\leqslant n$。HashFunc2：$\{AID_{MN},UL_{MN}\}\rightarrow\{Z^*q\}^*$；

[0055]
```
1. for each i ∈ [1, k] do
        if  xi == 1  then.
            S K = S K + δiPPKxi ;
        end if
    end for
    return SKMN;
```

[0056] 需要说明的是，本申请实施例基于区块链技术从不同单一私钥生成中心PKG(Private Key Generators)-共识节点中的私钥因子组合生成最终的用户私钥，不再由集中式的PKG统一生成，而是从不同共识节点中产生的私钥因子组合而成，大大降低了单一PKG情况下私钥泄露的风险和单点故障的问题。在密钥安全保障方面具有着良好的可扩展性。同时本申请实施例也可以应用于天地一体化网络的认证系统，在提高私钥安全性的同时，引入区块链作为空间节点的用户吊销列表同步信息的来源，能快速检测用户的吊销，完善系统中各种各样的安全性需求。此外，本申请实施例通过用户自主私钥组合算法生成用户私钥，相比于传统的通过公共算法生成密钥，安全强度能够得到保障。

[0057] 步骤103：当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点；

[0058] 在本步骤中，当用户需要登录认证时，将包含用户的私钥签名和唯一身份标识的认证请求发送给系统中的认证节点。当认证节点接收用户认证请求后，首先获取用户的唯一身份标识，根据唯一身份标识在哈希函数中的映射关系定位参与用户私钥生成的共识节

点。

[0059] 步骤104:由所述认证节点获取所述从共识节点自身初始化的公共密钥参数,并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识,生成公钥因子;

[0060] 在本步骤中,由于区块链上的每一个共识节点对应的公共密钥参数在系统初始化阶段进行了公开上链,因此,认证节点可以调用所有已定位的共识节点的公共密钥参数,并由这些共识节点根据公共密钥参数和用户唯一身份标识生成公钥因子。

[0061] 步骤105:由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子,以及,根据第二映射函数将参与用户公钥生成的因子进行组合,生成用户公钥。

[0062] 在本步骤中,基于用户自主私钥组合对称算法对用户公钥进行组合计算,进而用组合完成后的公钥对用户的签名信息进行验签来认证用户的合法性。其中,用户自主私钥组合对称算法详细内容如下:

[0063] 输入:1.由各个共识节点依据公开的公共密钥参数生成的公钥因子PKi,{i=1,2,3,.....n};

[0064] 2.用户唯一身份标识ID_{MN}。

[0065] 输出:用户公钥:PK_{MN};

[0066] 算法步骤:

[0067] 1、从用户的ID_{MN}中获得用户的等级UL_{MN};

[0068] 2、基于ID_{MN}和UL_{MN},通过哈希函数(HashFunc1)生成随机序列$x=\{x_1,x_2,...,x_k\}$,$1\leqslant k\leqslant n$。HashFunc1:$\{AID_{MN},UL_{MN}\}\rightarrow\{0,1\}^*$

[0069] 3、基于ID_{MN}和UL_{MN},通过哈希函数(HashFunc2)生成随机序列$\Delta=\{\delta_1,\delta_2,...,\delta_k\}$,$1\leqslant k\leqslant n$。HashFunc2:$\{AID_{MN},UL_{MN}\}\rightarrow\{Z^*q\}^*$;

for each $i \in [1,k]$ **do**

if $x_i == 1$ **then.**

[0070] $PK = PK + \delta_i PK x_i$;

end if

end for

[0071] **return** PK_{MN};

[0072] 由此可见,用户生成私钥和认证节点生成所述用户公钥都是基于用户自主私钥组合算法通过传入不同的密钥参数实现的,认证节点只需要知道所述用户的唯一身份标识即可通过所述用户自主密钥组合算法和所述公共密钥参数即可计算出所述用户的公钥,对所述用户签名进行认证。

[0073] 由上面技术方案可知,本申请实施例当区块链中的主共识节点接收到终端发送的用户注册请求时,首先根据用户注册请求,生成用户唯一身份标识,并将所述唯一身份标识上链,以使区块链中的从共识节点根据唯一身份标识和自身初始化的公共密钥参数,生成私钥因子。然后由主共识节点获取各个从共识节点生成的私钥因子,并将私钥因子发送至终端,以使终端根据第一映射函数选择参与用户私钥生成的私钥因子,以及,根据第二映射函数将参与用户私钥生成的私钥因子进行组合,生成用户私钥。在用户认证阶段,当区块链

中的认证节点接收到终端发送的用户认证请求时，首先根据第一映射函数确定参与用户私钥生成的从共识节点，然后由认证节点获取从共识节点自身初始化的公共密钥参数，并由从共识节点根据公共密钥参数和用户唯一身份标识，生成公钥因子。最终由认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。由此可见，本申请实施例引入了区块链技术，很好的解决了传统用户认证方案中由于单一节点而导致的第三方密钥管理问题。网络内各个通信实体的私钥不再由集中式的密钥管理中心统一生成，而是从不同共识节点中产生的私钥因子组合而成，大大降低了单一节点情况下私钥泄露的风险。同时，当需要对方公钥进行验签时，不需要从其他的可信节点或者数据库进行查询，而是由事先在本地配置的公共参数和对方的身份标识ID即可快速计算获得其公钥，节约了查询请求以及结果传输过程中的时延和消耗。

[0074] 基于上述实施例的内容，在本实施例中，所述用户注册请求包括用户的身份注册信息；

[0075] 相应的，根据所述用户注册请求，生成用户唯一身份标识，包括：

[0076] 对所述用户的身份注册信息进行建模，生成用户唯一身份标识。

[0077] 基于上述实施例的内容，在本实施例中，所述公共密钥参数是由所述从共识节点根据预设密码体系，进行初始化后生成的。

[0078] 在本实施例中，可选的，系统中的每个共识节点根据身份标识密码体系IBC(Identity-Based Cryptograph)初始化自身的椭圆曲线ECC(Elliptic curve cryptography)公共密钥参数，并将各自的公共密钥参数公开给系统内所有的实体。系统内的所有实体都可以知道所有共识节点的公共密钥参数并在后续需要时进行调用。

[0079] 基于上述实施例的内容，在本实施例中，所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，包括：

[0080] 所述终端根据用户唯一身份标识和私钥因子，通过第一映射函数生成随机序列，并根据所述随机序列选择参与用户私钥生成的私钥因子；

[0081] 相应的，所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，包括：

[0082] 所述认证节点根据用户唯一身份标识和公钥因子，通过第一映射函数生成随机序列，并根据所述随机序列选择参与用户公钥生成的公钥因子。

[0083] 在本实施例中，需要说明的是，在用户私钥的生成过程中，首先根据唯一身份标识获得用户的等级，进而基于唯一用户标识和用户等级，通过哈希函数生成01随机序列，由该序列决定系统中哪些共识节点参与私钥的计算。因此，可以根据唯一身份标识在哈希函数中的映射关系定位参与用户私钥生成的多个对等且分布式的共识节点。

[0084] 基于上述实施例的内容，在本实施例中，当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点，包括：

[0085] 根据用户认证请求，确定用户唯一身份标识；

[0086] 根据所述唯一身份标识在第一映射函数中的映射关系确定参与用户私钥生成从共识节点。

[0087] 下面通过具体实施例进行说明：

[0088] 第一实施例：

[0089] 如图3所示，本申请实施例提供的基于区块链的用户密钥生成网络模型示意图，里面包含的实体包括作为非共识节点NVP_i和代理认证中心PAC的低轨卫星LEO，用户节点MN，区块链节点RA_i。其中包含的网络又分为用户端的接入网，由区块链节点组成的区块链网络和卫星节点间通信的核心网。

[0090] 如图2所示，本申请实施例提供的基于区块链的用户密钥生成方法的步骤流程图之二。主要包括如下五个阶段：1.初始化阶段2.用户注册阶段3.广播认证阶段4.单播认证阶段5.多播认证阶段。下面将针对各个阶段的工作流程以及在方案运行时的具体效果展开具体的描述和分析。

[0091] 1.初始化阶段：本阶段开始时，每个共识节点RA作为区块链的节点，选择主键S_i并初始化各自的ECC公共密钥参数，并将其公布到SGIN上。网络内的通信实体都可以根据这些参数来计算出其他实体的公钥。同时，用户MN与PAC选择各自用于链上通信所使用的密钥对。

[0092] 2.用户注册阶段：用户MN在获得密钥对以后，将个人的属性信息(ID_{mn},UL)和其公钥TPK_{MN}发送给其接入的RA节点。PAC节点也执行和MN相似的操作，将ID_{PAC},UL,TPK_{PAC}发送给相应的RA节点。主RA节点对节点的属性信息进行建模，根据各自信息生成其相应的接入标识AID。之后各个RA基于AID计算出私钥因子PPK_i，RA将生成的私钥因子和密钥有效期信息打包上链共识，共识操作所带来的时延也将在后面展开分析。由主RA统一收集PPK_i并加密后同AID一起通过安全的信道返回给相应MN和PAC节点。之后主RA会将AID_{MN}和密钥有效期信息上链共识。在用户和PAC收到注册响应后，解密出私钥因子PPK_i并基于用户自主私钥组合算法在本地计算出各自的私钥SK_{MN}和SK_{PAC}。

[0093] 在本实例中，可以选择FISCO-BCOS共识链作为实验平台，不同数量的区块链节点部署在64G内存的DELL R740服务器上。每个节点都在同一局域网下作为主机并配置为桥接模式通过物理网络直接进行互联。分别选取4,8,16,32,64和128个节点数量作为实例的变量，并在每个节点数上都进行500次的实验，取它们的平均值作为实验结果。

[0094] 由此可见，本申请实施例由于生成用户私钥的私钥因子是由分布式的区块链节点共同生成并加密传输的，并且最终的私钥是用户自己根据需要在其终端组合而成的，因此确保了秘钥在传输过程中的安全，同时也避免了单一密钥管理节点所带来的瓶颈和问题。

[0095] 3.广播认证阶段：由于低轨卫星LEO与地面通信延迟低，容易部署低资源消耗的广播服务等特性，因此选择LEO作为PAC(代理认证中心)来进行周期性地广播私钥签名过的认证请求消息。PAC将认证消息广播给所有MN，MN收到PAC的认证消息后，基于用户自主私钥组合的对称算法来计算出PAC的公钥，进而检验PAC的签名来保证其入网的安全性。

[0096] 4.单播认证阶段：MN以单播的形式向PAC发送认证请求消息，PAC收到消息后首先与本地经过区块链共识的吊销列表进行核对验证MN的有效性；之后根据公共参数和请求消息中包含的AID_{MN}来计算出MN的公钥以验证其签名。验证成功后，会为期分配GID_{MN}和会话密钥SK并返回响应消息。MN收到响应消息后验证PAC的有效期并根据GID生成相应的组播地址。至此双向认证过程结束，MN可以合法的接入SGIN。

[0097] 5.组播认证阶段：由于LEO卫星的高速移动，其信号覆盖范围会随之发生相应改变。因此MN需要持续地切换接入的卫星节点。切换发生时需由当前的接入PAC对MN进行重新

认证。为解决切换动作频繁和用户数量庞大所带来的问题，因此选择组播的方式来减少接入认证消息的数量。当一个组里的MN检测到链路发生切换后，立刻以组播的方式发送一个重新认证消息。一旦同一个组内的其他成员接受到了此消息，他们会扣留他们自身的重新认证消息并等待来自PAC的认证回复消息。PAC以组播的方式返回认证响应消息，当验证结果为成功时，所有的组成员都视为通过了验证，GID_{MN}变为激活状态并使用PAC生成的新会话密钥SK来进行之后的通信。

[0098] 第二实施例：

[0099] 在本实施例中，如图4和图5所示，本申请实施例提供的基于区块链的用户密钥生成系统包括：用户节点、认证节点和共识节点；

[0100] 其中，用户节点用于向共识节点提交注册请求和各项属性信息，共识节点响应用户节点请求，并返回用户节点对应的唯一身份标识和公私钥因子；用户节点还用于向认证节点发送认证消息，认证消息中包括私钥签名和唯一身份标识，认证节点响应用户节点认证消息，并根据唯一身份标识，定位该用户私钥生成的共识节点的公共密钥参数计算用户公钥，对用户进行认证。

[0101] 下文描述的基于区块链的用户密钥生成装置与上文描述的基于区块链的用户密钥生成方法可相互对应参照。

[0102] 基于相同的发明构思，本发明另一实施例提供了一种基于区块链的用户密钥生成装置，如图6所示，本申请实施例提供的基于区块链的用户密钥生成装置，包括：

[0103] 第一处理模块，用于当区块链中的主共识节点接收到终端发送的用户注册请求时，根据所述用户注册请求，生成用户唯一身份标识，并将所述唯一身份标识上链，以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数，生成私钥因子；

[0104] 第二处理模块，用于由所述主共识节点获取各个从共识节点生成的私钥因子，并将所述私钥因子发送至终端，以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，以及，根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥；

[0105] 第三处理模块，用于当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点；

[0106] 第四处理模块，用于由所述认证节点获取所述从共识节点自身初始化的公共密钥参数，并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识，生成公钥因子；

[0107] 第五处理模块，用于由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。

[0108] 基于上述实施例的内容，在本实施例中，所述公共密钥参数是由所述从共识节点根据预设密码体系，进行初始化后生成的。

[0109] 基于上述实施例的内容，在本实施例中，所述第三处理模块，还具体用于：

[0110] 根据用户认证请求，确定用户唯一身份标识；

[0111] 根据所述唯一身份标识在第一映射函数中的映射关系确定参与用户私钥生成从共识节点。

[0112] 基于相同的发明构思，本发明又一实施例提供了一种电子设备，参见图7所述电子设备的结构示意图，具体包括如下内容：处理器701、存储器702、通信接口703和通信总线704；

[0113] 其中，所述处理器701、存储器702、通信接口703通过所述通信总线704完成相互间的通信；所述通信接口703用于实现各设备之间的信息传输；

[0114] 所述处理器701用于调用所述存储器702中的计算机程序，所述处理器执行所述计算机程序时实现上述一种基于区块链的用户密钥生成方法的全部步骤，例如，当区块链中的主共识节点接收到终端发送的用户注册请求时，根据所述用户注册请求，生成用户唯一身份标识，并将所述唯一身份标识上链，以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数，生成私钥因子；由所述主共识节点获取各个从共识节点生成的私钥因子，并将所述私钥因子发送至终端，以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，以及，根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥；当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点；由所述认证节点获取所述从共识节点自身初始化的公共密钥参数，并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识，生成公钥因子；由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。

[0115] 基于相同的发明构思，本发明又一实施例提供了一种非暂态计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现上述一种基于区块链的用户密钥生成方法的全部步骤，例如，当区块链中的主共识节点接收到终端发送的用户注册请求时，根据所述用户注册请求，生成用户唯一身份标识，并将所述唯一身份标识上链，以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数，生成私钥因子；由所述主共识节点获取各个从共识节点生成的私钥因子，并将所述私钥因子发送至终端，以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，以及，根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥；当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点；由所述认证节点获取所述从共识节点自身初始化的公共密钥参数，并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识，生成公钥因子；由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥。此外，上述的存储器中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。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或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0116] 以上所描述的装置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发明实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下,即可以理解并实施。

[0117] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件。基于这样的理解,上述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计算机可读存储介质中,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)执行各个实施例或者实施例的某些部分所述的基于区块链的用户密钥生成方法。

[0118] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

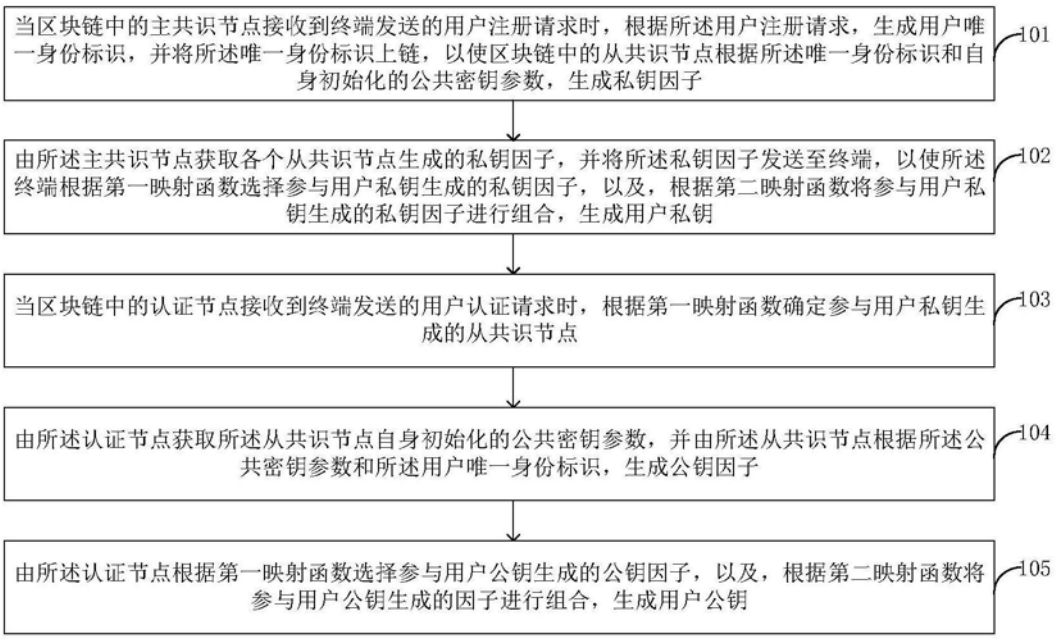

当区块链中的主共识节点接收到终端发送的用户注册请求时，根据所述用户注册请求，生成用户唯一身份标识，并将所述唯一身份标识上链，以使区块链中的从共识节点根据所述唯一身份标识和自身初始化的公共密钥参数，生成私钥因子
101
由所述主共识节点获取各个从共识节点生成的私钥因子，并将所述私钥因子发送至终端，以使所述终端根据第一映射函数选择参与用户私钥生成的私钥因子，以及，根据第二映射函数将参与用户私钥生成的私钥因子进行组合，生成用户私钥
102
当区块链中的认证节点接收到终端发送的用户认证请求时，根据第一映射函数确定参与用户私钥生成的从共识节点
103
由所述认证节点获取所述从共识节点自身初始化的公共密钥参数，并由所述从共识节点根据所述公共密钥参数和所述用户唯一身份标识，生成公钥因子
104
由所述认证节点根据第一映射函数选择参与用户公钥生成的公钥因子，以及，根据第二映射函数将参与用户公钥生成的因子进行组合，生成用户公钥
105

图1

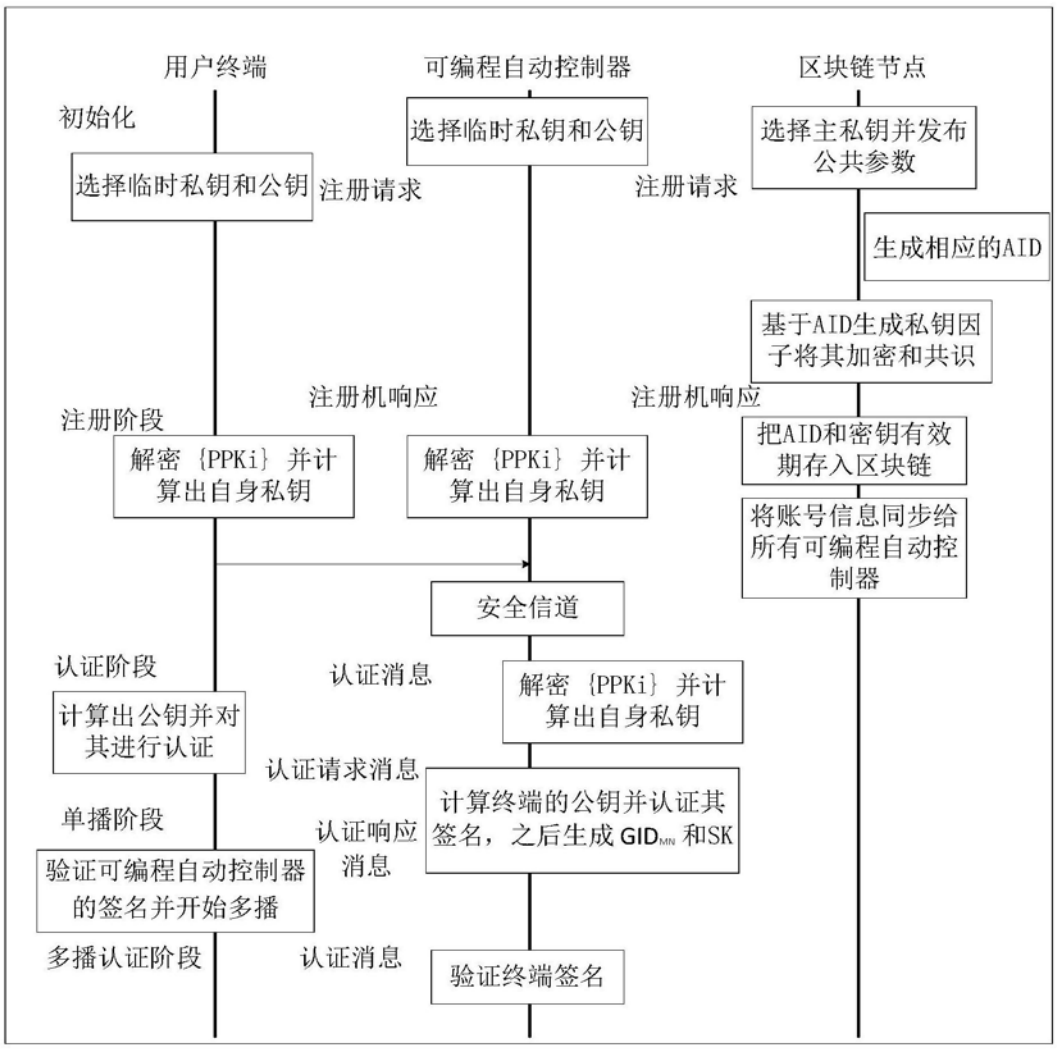

用户终端
可编程自动控制器
区块链节点
初始化
选择临时私钥和公钥
选择临时私钥和公钥
注册请求
注册请求
选择主私钥并发布公共参数
生成相应的AID
基于AID生成私钥因子将其加密和共识
注册机响应
注册机响应
注册阶段
解密｛PPKi｝并计算出自身私钥
解密｛PPKi｝并计算出自身私钥
把AID和密钥有效期存入区块链
将账号信息同步给所有可编程自动控制器
安全信道
认证阶段
认证消息
解密｛PPKi｝并计算出自身私钥
计算出公钥并对其进行认证
认证请求消息
计算终端的公钥并认证其签名，之后生成 GIDMN 和SK
单播阶段
认证响应消息
验证可编程自动控制器的签名并开始多播
多播认证阶段
认证消息
验证终端签名

图2

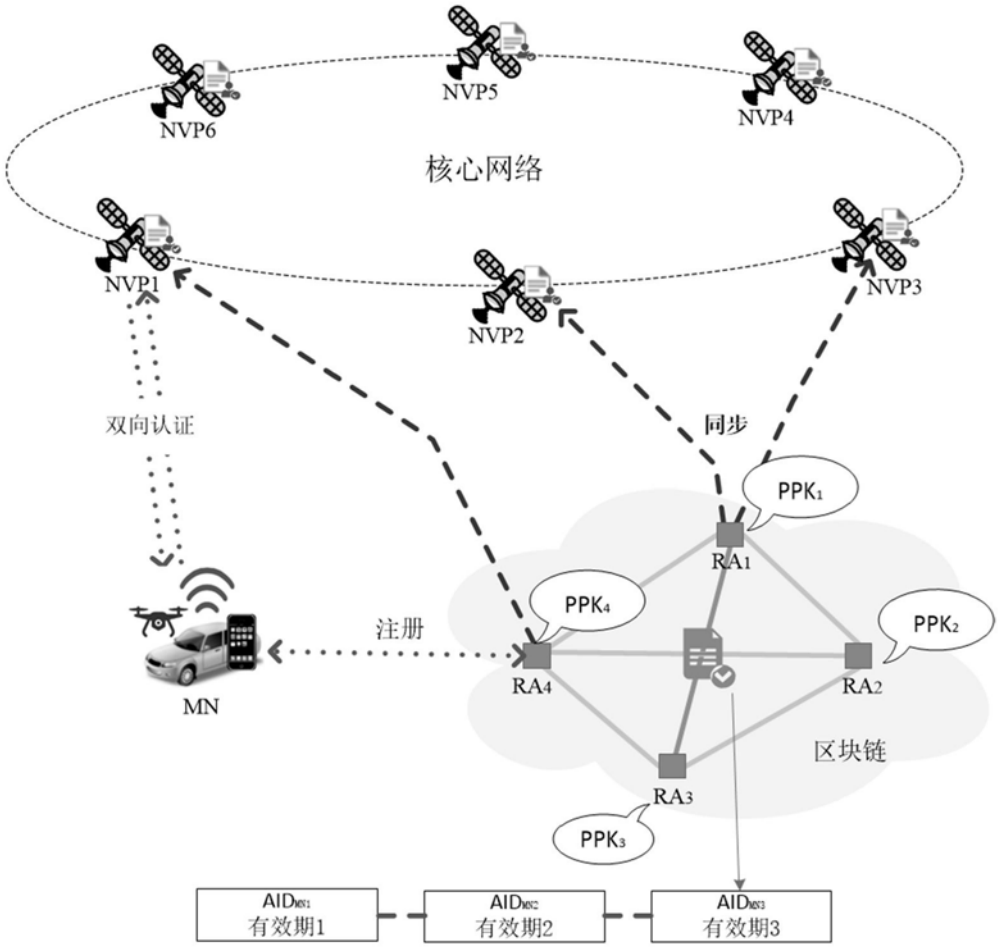

NVP6
NVP5
NVP4
核心网络
NVP1
NVP2
NVP3
双向认证
同步
PPK1
RA1
PPK4
PPK2
注册
RA4
RA2
MN
区块链
RA3
PPK3
AIDMN1
有效期1
AIDMN2
有效期2
AIDMN3
有效期3

图3

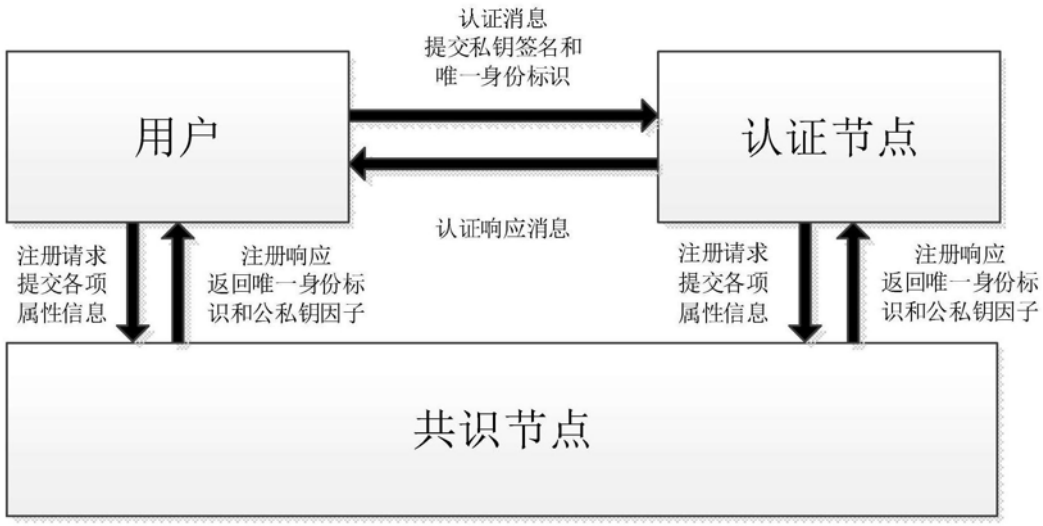

认证消息
提交私钥签名和
唯一身份标识
用户
认证节点
认证响应消息
注册请求
提交各项
属性信息
注册响应
返回唯一身份标
识和公私钥因子
注册请求
提交各项
属性信息
注册响应
返回唯一身份标
识和公私钥因子
共识节点

图4

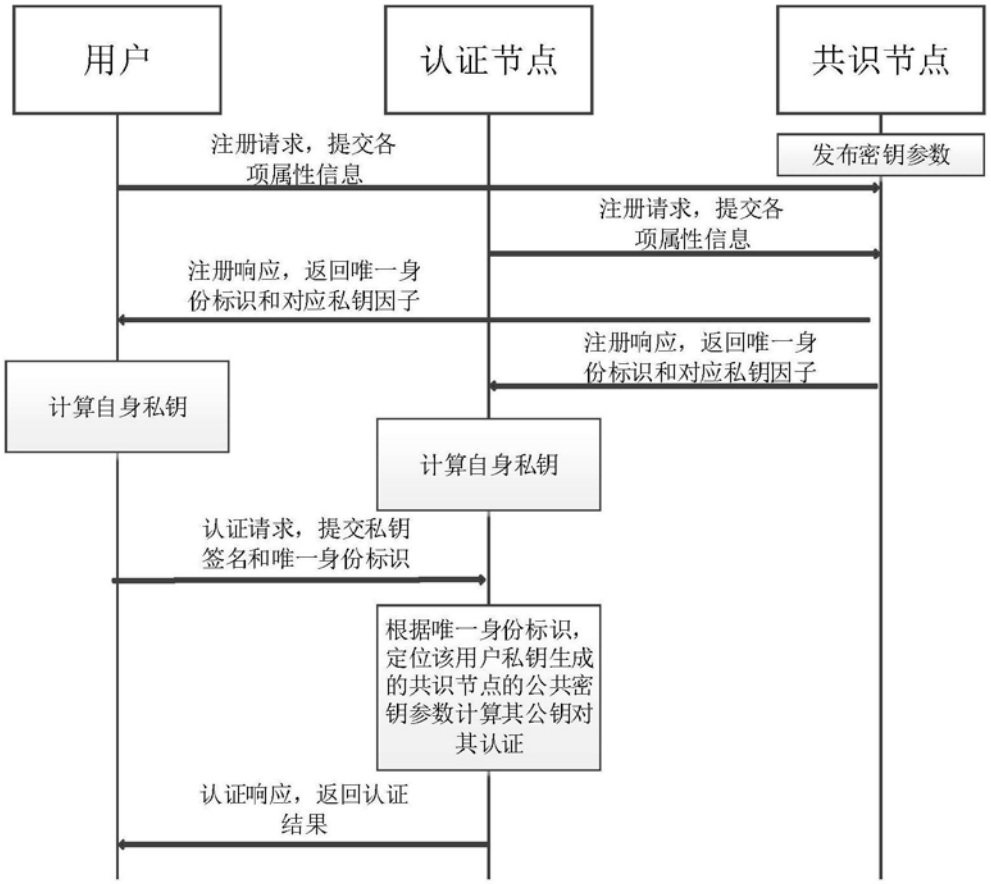

用户
认证节点
共识节点
发布密钥参数
注册请求，提交各项属性信息
注册请求，提交各项属性信息
注册响应，返回唯一身份标识和对应私钥因子
注册响应，返回唯一身份标识和对应私钥因子
计算自身私钥
计算自身私钥
认证请求，提交私钥签名和唯一身份标识
根据唯一身份标识，定位该用户私钥生成的共识节点的公共密钥参数计算其公钥对其认证
认证响应，返回认证结果

图5

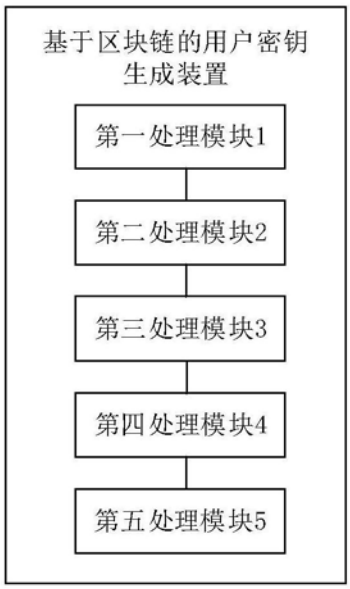

基于区块链的用户密钥生成装置
第一处理模块1
第二处理模块2
第三处理模块3
第四处理模块4
第五处理模块5

图6

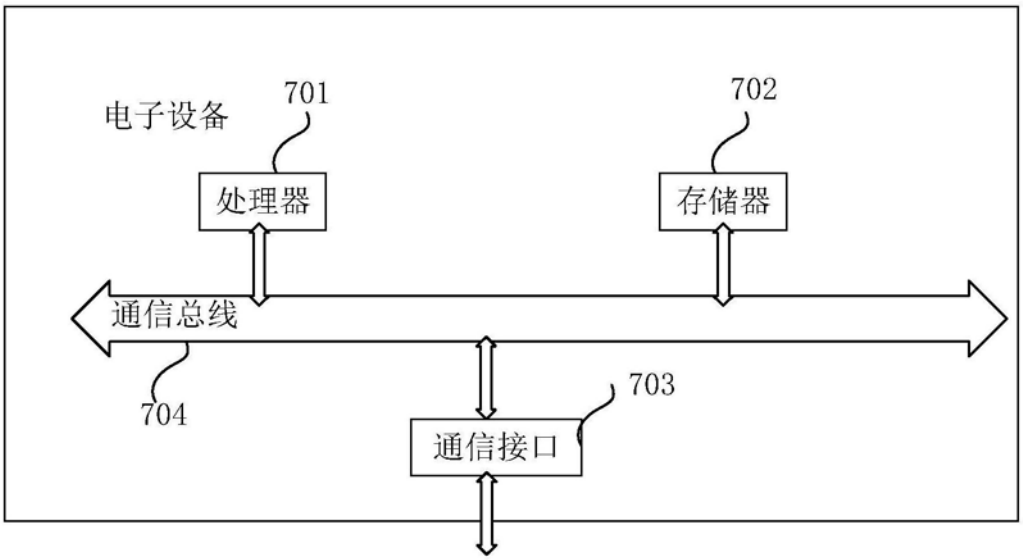


图7