(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 111047763 A
(43)申请公布日 2020.04.21

(21)申请号 201911237873.3

(22)申请日 2019.12.05

(71)申请人 全链通有限公司
地址 100043 北京市石景山区实兴东街11号5层5158室

(72)发明人 路成业 王凌

(51)Int.Cl.
G07C 13/00(2006.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)

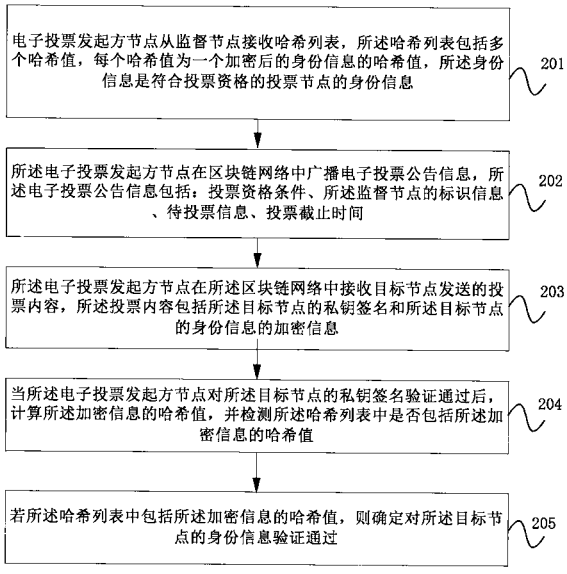
权利要求书2页 说明书9页 附图4页

(54)发明名称

基于区块链的电子投票方法、设备及存储介质

(57)摘要

本发明实施例提供一种基于区块链的电子投票方法、设备及存储介质。本发明实施例区块链网络中公开的是加密后的身份信息的哈希值构成的哈希列表，并不是加密后的身份信息，而投票节点需要在区块链网络中公开的是自己的身份信息的加密信息，由于哈希值的不可逆性，区块链网络中的参与节点只能检测身份信息的加密信息对应的哈希值是否在哈希列表中，而不能根据哈希值确定出加密后的身份信息，保证了投票节点的投票内容不会在线下被篡改，同时投票节点也不会被冒名，使得投票节点既可以匿名投票，同时也实现了电子投票发起方节点对投票节点的身份验证，提高了投票节点的安全性和电子投票的安全性。



CN 111047763 A

1.一种基于区块链的电子投票方法,其特征在于,包括:

电子投票发起方节点从监督节点接收哈希列表,所述哈希列表包括多个哈希值,每个哈希值为一个加密后的身份信息的哈希值,所述身份信息是符合投票资格的投票节点的身份信息;

所述电子投票发起方节点在区块链网络中广播电子投票公告信息,所述电子投票公告信息包括:投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间;

所述电子投票发起方节点在所述区块链网络中接收目标节点发送的投票内容,所述投票内容包括所述目标节点的私钥签名和所述目标节点的身份信息的加密信息;

当所述电子投票发起方节点对所述目标节点的私钥签名验证通过后,计算所述加密信息的哈希值,并检测所述哈希列表中是否包括所述加密信息的哈希值;

若所述哈希列表中包括所述加密信息的哈希值,则确定对所述目标节点的身份信息验证通过。

2.根据权利要求1所述的方法,其特征在于,所述哈希列表中的每个哈希值对应的加密后的身份信息是采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密后得到的。

3.根据权利要求1或2所述的方法,其特征在于,所述电子投票公告信息还包括:用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息。

4.一种基于区块链的电子投票方法,其特征在于,包括:

目标节点接收电子投票发起方节点在区块链网络中广播的电子投票公告信息,所述电子投票公告信息包括:投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间;

所述目标节点确定其是否符合所述投票资格条件;

当所述目标节点确定所述目标节点符合所述投票资格条件时,所述目标节点对所述目标节点的身份信息进行加密,得到所述目标节点的身份信息的加密信息;

所述目标节点在所述区块链网络中广播投票内容,所述投票内容包括所述目标节点的私钥签名和所述加密信息。

5.根据权利要求4所述的方法,其特征在于,所述电子投票公告信息还包括:用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息;

所述目标节点对所述目标节点的身份信息进行加密,包括:

所述目标节点根据所述指示信息指示的所述监督节点的公钥或所述目标节点的公钥对所述目标节点的身份信息进行加密。

6.一种电子投票发起方节点,其特征在于,包括:

存储器;

处理器;

通讯接口;以及

计算机程序;

其中,所述计算机程序存储在所述存储器中,并被配置为由所述处理器执行以下操作:

通过所述通讯接口从监督节点接收哈希列表，所述哈希列表包括多个哈希值，每个哈希值为一个加密后的身份信息的哈希值，所述身份信息是符合投票资格的投票节点的身份信息；

通过所述通讯接口在区块链网络中广播电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间；

通过所述通讯接口在所述区块链网络中接收目标节点发送的投票内容，所述投票内容包括所述目标节点的私钥签名和所述目标节点的身份信息的加密信息；

当所述处理器对所述目标节点的私钥签名验证通过后，计算所述加密信息的哈希值，并检测所述哈希列表中是否包括所述加密信息的哈希值；

若所述哈希列表中包括所述加密信息的哈希值，则确定对所述目标节点的身份信息验证通过。

7.根据权利要求6所述的电子投票发起方节点，其特征在于，所述哈希列表中的每个哈希值对应的加密后的身份信息是采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密后得到的。

8.根据权利要求6或7所述的电子投票发起方节点，其特征在于，所述电子投票公告信息还包括：用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息。

9.一种目标节点，其特征在于，包括：

存储器；

处理器；

通讯接口；以及

计算机程序；

其中，所述计算机程序存储在所述存储器中，并被配置为由所述处理器执行以下操作：

通过所述通讯接口接收电子投票发起方节点在区块链网络中广播的电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间；

确定所述目标节点是否符合所述投票资格条件；

当所述处理器确定所述目标节点符合所述投票资格条件时，对所述目标节点的身份信息进行加密，得到所述目标节点的身份信息的加密信息；

通过所述通讯接口在所述区块链网络中广播投票内容，所述投票内容包括所述目标节点的私钥签名和所述加密信息。

10.根据权利要求9所述的目标节点，其特征在于，所述电子投票公告信息还包括：用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息；

所述处理器对所述目标节点的身份信息进行加密时，具体用于：

根据所述指示信息指示的所述监督节点的公钥或所述目标节点的公钥对所述目标节点的身份信息进行加密。

11.一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任一项所述的方法。

基于区块链的电子投票方法、设备及存储介质

技术领域

[0001] 本发明实施例涉及通信技术领域，尤其涉及一种基于区块链的电子投票方法、设备及存储介质。

背景技术

[0002] 现有技术中，基于区块链网络可实现电子投票，例如，区块链网络中的电子投票发起方节点在该区块链网络中广播待投票内容，区块链网络中参与投票的节点接收到该待投票内容后，在该区块链网络中广播投票内容。

[0003] 但是，现有技术中很难同时兼顾匿名投票和投票资格验证的需求，例如，如果投票节点进行匿名投票，则电子投票发起方节点将无法对投票节点的投票资格进行验证，从而带来一定的安全隐患。如果投票节点进行实名制投票，则电子投票发起方节点可以对投票节点的投票资格进行验证，但是，由于投票内容是在区块链网络中被广播的，因此，该区块链网络中的其他节点都可以确定出投票节点的身份信息，从而无法对投票节点进行有效保护。

发明内容

[0004] 本发明实施例提供一种基于区块链的电子投票方法、设备及存储介质，以使得投票节点既可以匿名投票，同时也实现了电子投票发起方节点对投票节点的身份验证。

[0005] 第一方面，本发明实施例提供一种基于区块链的电子投票方法，包括：

[0006] 电子投票发起方节点从监督节点接收哈希列表，所述哈希列表包括多个哈希值，每个哈希值为一个加密后的身份信息的哈希值，所述身份信息是符合投票资格的投票节点的身份信息；

[0007] 所述电子投票发起方节点在区块链网络中广播电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间；

[0008] 所述电子投票发起方节点在所述区块链网络中接收目标节点发送的投票内容，所述投票内容包括所述目标节点的私钥签名和所述目标节点的身份信息的加密信息；

[0009] 当所述电子投票发起方节点对所述目标节点的私钥签名验证通过后，计算所述加密信息的哈希值，并检测所述哈希列表中是否包括所述加密信息的哈希值；

[0010] 若所述哈希列表中包括所述加密信息的哈希值，则确定对所述目标节点的身份信息验证通过。

[0011] 第二方面，本发明实施例提供一种基于区块链的电子投票方法，包括：

[0012] 目标节点接收电子投票发起方节点在区块链网络中广播的电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间；

[0013] 所述目标节点确定其是否符合所述投票资格条件；

[0014] 当所述目标节点确定所述目标节点符合所述投票资格条件时，所述目标节点对所

述目标节点的身份信息进行加密，得到所述目标节点的身份信息的加密信息；

[0015] 所述目标节点在所述区块链网络中广播投票内容，所述投票内容包括所述目标节点的私钥签名和所述加密信息。

[0016] 第三方面，本发明实施例提供一种电子投票发起方节点，包括：

[0017] 存储器；

[0018] 处理器；

[0019] 通讯接口；以及

[0020] 计算机程序；

[0021] 其中，所述计算机程序存储在所述存储器中，并被配置为由所述处理器执行以下操作：

[0022] 通过所述通讯接口从监督节点接收哈希列表，所述哈希列表包括多个哈希值，每个哈希值为一个加密后的身份信息的哈希值，所述身份信息是符合投票资格的投票节点的身份信息；

[0023] 通过所述通讯接口在区块链网络中广播电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间；

[0024] 通过所述通讯接口在所述区块链网络中接收目标节点发送的投票内容，所述投票内容包括所述目标节点的私钥签名和所述目标节点的身份信息的加密信息；

[0025] 当所述处理器对所述目标节点的私钥签名验证通过后，计算所述加密信息的哈希值，并检测所述哈希列表中是否包括所述加密信息的哈希值；

[0026] 若所述哈希列表中包括所述加密信息的哈希值，则确定对所述目标节点的身份信息验证通过。

[0027] 第四方面，本发明实施例提供一种目标节点，包括：

[0028] 存储器；

[0029] 处理器；

[0030] 通讯接口；以及

[0031] 计算机程序；

[0032] 其中，所述计算机程序存储在所述存储器中，并被配置为由所述处理器执行以下操作：

[0033] 通过所述通讯接口接收电子投票发起方节点在区块链网络中广播的电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间；

[0034] 确定所述目标节点是否符合所述投票资格条件；

[0035] 当所述处理器确定所述目标节点符合所述投票资格条件时，对所述目标节点的身份信息进行加密，得到所述目标节点的身份信息的加密信息；

[0036] 通过所述通讯接口在所述区块链网络中广播投票内容，所述投票内容包括所述目标节点的私钥签名和所述加密信息。

[0037] 第五方面，本发明实施例提供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以实现第一方面或第二方面所述的方法。

[0038] 本发明实施例提供的基于区块链的电子投票方法方法、设备及存储介质，区块链

网络中公开的是加密后的身份信息的哈希值构成的哈希列表，并不是加密后的身份信息，而投票节点需要在区块链网络中公开的是自己的身份信息的加密信息，由于哈希值的不可逆性，区块链网络中的参与节点只能检测身份信息的加密信息对应的哈希值是否在哈希列表中，而不能根据哈希值确定出加密后的身份信息，保证了投票节点的投票内容不会在线下被篡改，同时投票节点也不会被冒名，使得投票节点既可以匿名投票，同时也实现了电子投票发起方节点对投票节点的身份验证，提高了投票节点的安全性，同时电子投票发起方节点还可以通过监督节点对投票节点进行有效监督，提高了电子投票的安全性。

附图说明

[0039] 图1为本发明实施例提供的一种通信系统的示意图；

[0040] 图2为本发明实施例提供的基于区块链的电子投票方法流程图；

[0041] 图3为本发明另一实施例提供的基于区块链的电子投票方法流程图；

[0042] 图4为本发明实施例提供的电子投票发起方节点的结构示意图；

[0043] 图5为本发明实施例提供的目标节点的结构示意图。

[0044] 通过上述附图，已示出本公开明确的实施例，后文中将有更详细的描述。这些附图和文字描述并不是为了通过任何方式限制本公开构思的范围，而是通过参考特定实施例为本领域技术人员说明本公开的概念。

具体实施方式

[0045] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

[0046] 本发明实施例提供的基于区块链的电子投票方法，可以适用于图1所示的通信系统。如图1所示，该通信系统包括：记账节点、电子投票发起方节点、监督节点和投票节点，其中，记账节点、电子投票发起方节点、监督节点、目标节点和投票节点是区块链网络中的参与节点。可以理解，此处只是示意性说明，并不限定该区块链网络中的节点个数和种类。其中，记账节点可以是一个或者是多个云端服务器，云端服务器也就是云服务器，是一个服务器集群，有很多服务器，和通用的计算机架构类似，云端服务器的构成包括处理器、硬盘、内存、系统总线等。电子投票发起方节点或投票节点具体可以是用户终端，例如，智能手机、平板电脑、个人计算机等。另外，在本申请实施例中，区块链网络是一个去中心化的、点对点(peer-to-peer，简称P2P)通信的网络。

[0047] 本发明实施例提供的基于区块链的电子投票方法，旨在解决现有技术的如上技术问题。

[0048] 下面以具体地实施例对本发明的技术方案以及本申请的技术方案如何解决上述技术问题进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例中不再赘述。下面将结合附图，对本发明的实施例进行描述。

[0049] 图2为本发明实施例提供的基于区块链的电子投票方法流程图。本发明实施例针对现有技术的如上技术问题，提供了基于区块链的电子投票方法，该方法具体步骤如下：

[0050] 步骤201、电子投票发起方节点从监督节点接收哈希列表，所述哈希列表包括多个哈希值，每个哈希值为一个加密后的身份信息的哈希值，所述身份信息是符合投票资格的投票节点的身份信息。

[0051] 在本申请实施例中，所述区块链网络包括所述电子投票发起方节点、所述监督节点和所述投票节点。

[0052] 电子投票发起方节点可以是区块链网络中任意的参与节点，也就是说，区块链网络中任意的参与节点可作为一次电子投票的发起方节点，该发起方节点可设定投票节点需要满足的资格条件、以及具体的待投票信息。

[0053] 监督节点具体可以是存储有完备的用户身份信息的数据库，监督节点可根据投票节点的资格条件生成投票节点的身份认证信息。该监督节点具体可以是公证的第三方节点，例如可以是公安部门的数据库。

[0054] 投票节点可以是区块链网络中任意的一个或多个参与节点。

[0055] 可选的，所述哈希列表中的每个哈希值对应的加密后的身份信息是采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密后得到的。

[0056] 具体的，电子投票发起方节点向监督节点发送投票资格条件，监督节点根据投票资格条件，查询获得多个符合投票资格的投票节点的身份信息，例如，身份信息具体可以是投票节点的区块链标识，以下将区块链标识简称为标识。该多个符合投票资格的投票节点的身份信息可构成一个身份信息列表，例如，符合投票资格的投票节点包括投票节点1、投票节点2、投票节点3，其中，投票节点1的标识记为ID1，投票节点2的标识记为ID2，投票节点3的标识记为ID3，该身份信息列表记为{ID1、ID2、ID3}。进一步，监督节点采用该监督节点的公钥或投票节点1的区块链公钥并按照预先约定的加密算法对ID1进行加密得到加密后的身份信息，该加密后的身份信息记为ID1c。监督节点采用该监督节点的公钥或投票节点2的区块链公钥并按照预先约定的加密算法对ID2进行加密得到加密后的身份信息，该加密后的身份信息记为ID2c。监督节点采用该监督节点的公钥或投票节点3的区块链公钥并按照预先约定的加密算法对ID3进行加密得到加密后的身份信息，该加密后的身份信息记为ID3c。从而得到加密后的身份信息列表{ID1c、ID2c、ID3c}。该监督节点将该加密后的身份信息列表{ID1c、ID2c、ID3c}存储在本地。进一步，监督节点采用预设的哈希算法计算该加密后的身份信息列表{ID1c、ID2c、ID3c}中每个加密后的身份信息的哈希值，例如，ID1c的哈希值为IDh1，ID2c的哈希值为IDh2，ID3c的哈希值为IDh3。IDh1、IDh2和IDh3构成哈希列表{IDh1、IDh2、IDh3}。进一步，该监督节点对该哈希列表进行私钥签名，并将私钥签名后的哈希列表广播在该区块链网络中。当该电子投票发起方节点接收到该哈希列表后，将该哈希列表存储在本地。

[0057] 或者，电子投票发起方节点通过区块链链下的方式向监督节点发送身份信息列表，该身份信息列表包括多个投票节点的标识，例如，该多个投票节点的标识依次为ID1、ID2、ID3、ID4、ID5。监督节点根据每个投票节点的标识，确定该投票节点是否符合本次投票资格。例如，投票节点1、投票节点2、投票节点3符合本次投票资格，ID4、ID5对应的投票节点不符合本次投票资格。进一步，监督节点采用该监督节点的公钥或投票节点1的区块链公钥并按照预先约定的加密算法对ID1进行加密得到加密后的身份信息，该加密后的身份信息记为ID1c。监督节点采用该监督节点的公钥或投票节点2的区块链公钥并按照预先约定的

加密算法对ID2进行加密得到加密后的身份信息，该加密后的身份信息记为ID2c。监督节点采用该监督节点的公钥或投票节点3的区块链公钥并按照预先约定的加密算法对ID3进行加密得到加密后的身份信息，该加密后的身份信息记为ID3c。从而得到加密后的身份信息列表{ID1c、ID2c、ID3c}。该监督节点将该加密后的身份信息列表{ID1c、ID2c、ID3c}存储在本地。进一步，监督节点采用预设的哈希算法计算该加密后的身份信息列表{ID1c、ID2c、ID3c}中每个加密后的身份信息的哈希值，例如，ID1c的哈希值为IDh1，ID2c的哈希值为IDh2，ID3c的哈希值为IDh3。IDh1、IDh2和IDh3构成哈希列表{IDh1、IDh2、IDh3}。进一步，该监督节点对该哈希列表进行私钥签名，并将私钥签名后的哈希列表广播在该区块链网络中。当该电子投票发起方节点接收到该哈希列表后，将该哈希列表存储在本地。

[0058] 步骤202、所述电子投票发起方节点在区块链网络中广播电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间。

[0059] 具体的，电子投票发起方节点在区块链网络中以广播消息的方式广播电子投票公告信息，该电子投票公告信息可包括投票资格条件、监督节点的标识信息、待投票信息和投票截止时间。其中，监督节点的标识信息具体可以是监督节点在该区块链网络中的区块链标识、以及监督节点在现实社会中的身份信息。待投票信息具体可包括待投票内容的选项。

[0060] 在一些实施例中，电子投票发起方节点生成电子投票公告信息后，电子投票公告信息可采用自己的私钥对该电子投票公告信息进行签名，进一步，将签名后的该电子投票公告信息广播到该区块链网络中。

[0061] 步骤203、所述电子投票发起方节点在所述区块链网络中接收目标节点发送的投票内容，所述投票内容包括所述目标节点的私钥签名和所述目标节点的身份信息的加密信息。

[0062] 当该区块链网络中的目标节点接收到签名后的该电子投票公告信息时，首先对该电子投票发起方节点的私钥签名进行验证，如果验证通过，则根据该电子投票公告信息中包括的投票资格条件，确定该目标节点是否满足该投票资格条件。如果满足，则该目标节点对该目标节点的身份信息进行加密，得到该目标节点的身份信息的加密信息。可选的，所述电子投票公告信息还包括：用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息。该目标节点根据所述指示信息指示的所述监督节点的公钥或所述目标节点的公钥按照预先约定的加密算法对所述目标节点的身份信息进行加密。

[0063] 例如，该目标节点的身份信息为IDn，该目标节点对IDn进行加密后得到IDnc。由于IDnc是加密后的身份信息，并不是该目标节点的身份信息，从而使得该目标节点可以匿名投票。

[0064] 进一步，该目标节点在该区块链网络中广播自己的投票内容，该投票内容包括该目标节点的私钥签名和IDnc。相应的，该区块链网络中的电子投票发起方节点可接收到该目标节点的投票内容。

[0065] 步骤204、当所述电子投票发起方节点对所述目标节点的私钥签名验证通过后，计算所述加密信息的哈希值，并检测所述哈希列表中是否包括所述加密信息的哈希值。

[0066] 当区块链网络中的电子投票发起方节点接收到该目标节点的投票内容后，首先对

该目标节点的私钥签名进行验证，验证通过后，从该投票内容中提取IDnc，进一步，采用预设的哈希算法计算该IDnc的哈希值，IDnc的哈希值记为IDhn。进一步，检测电子投票发起方节点本地存储的哈希列表中是否包括IDhn。

[0067] 步骤205、若所述哈希列表中包括所述加密信息的哈希值，则确定对所述目标节点的身份信息验证通过。

[0068] 如果电子投票发起方节点本地存储的哈希列表{IDh1、IDh2、IDh3}中包括IDhn，则电子投票发起方节点确定该目标节点符合投票资格，从而确定对目标节点的身份信息验证通过。如果电子投票发起方节点本地存储的哈希列表{IDh1、IDh2、IDh3}中不包括IDhn，则电子投票发起方节点确定该目标节点不符合投票资格。另外，电子投票发起方节点在投票截止时间结束后，可统计多个投票节点的投票内容，并且保证在一次电子投票活动中，同一个投票节点只能投票一次，如果多次投票，可以保留一次投票内容。

[0069] 另外，如果电子投票发起方节点本地存储的哈希列表{IDh1、IDh2、IDh3}中包括IDhn，则该区块链网络中的记账节点可以不将该目标节点的投票内容记录到区块链账本中。如果电子投票发起方节点本地存储的哈希列表{IDh1、IDh2、IDh3}中不包括IDhn，则该区块链网络中的记账节点可以将该目标节点的投票内容记录到区块链账本中，从而记录虚假投票的目标节点。

[0070] 本发明实施例区块链网络中公开的是加密后的身份信息的哈希值构成的哈希列表，并不是加密后的身份信息，而投票节点需要在区块链网络中公开的是自己的身份信息的加密信息，由于哈希值的不可逆性，区块链网络中的参与节点只能检测身份信息的加密信息对应的哈希值是否在哈希列表中，而不能根据哈希值确定出加密后的身份信息，保证了投票节点的投票内容不会在线下被篡改，同时投票节点也不会被冒名，使得投票节点既可以匿名投票，同时也实现了电子投票发起方节点对投票节点的身份验证，提高了投票节点的安全性，同时电子投票发起方节点还可以通过监督节点对投票节点进行有效监督，提高了电子投票的安全性。

[0071] 图3为本发明另一实施例提供的基于区块链的电子投票方法流程图。在上述实施例的基础上，本实施例提供的基于区块链的电子投票方法具体包括如下步骤：

[0072] 步骤301、目标节点接收电子投票发起方节点在区块链网络中广播的电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间。

[0073] 具体的，电子投票发起方节点在区块链网络中以广播消息的方式广播电子投票公告信息，该电子投票公告信息可包括投票资格条件、监督节点的标识信息、待投票信息和投票截止时间。其中，监督节点的标识信息具体可以是监督节点在该区块链网络中的区块链标识、以及监督节点在现实社会中的身份信息。待投票信息具体可包括待投票内容的选项。

[0074] 在一些实施例中，电子投票发起方节点生成电子投票公告信息后，电子投票公告信息可采用自己的私钥对该电子投票公告信息进行签名，进一步，将签名后的该电子投票公告信息广播到该区块链网络中。

[0075] 步骤302、所述目标节点确定其是否符合所述投票资格条件。

[0076] 当该区块链网络中的目标节点接收到签名后的该电子投票公告信息时，首先对该电子投票发起方节点的私钥签名进行验证，如果验证通过，则根据该电子投票公告信息中

包括的投票资格条件，确定该目标节点是否满足该投票资格条件。

[0077] 步骤303、当所述目标节点确定所述目标节点符合所述投票资格条件时，所述目标节点对所述目标节点的身份信息进行加密，得到所述目标节点的身份信息的加密信息。

[0078] 如果该目标节点满足该投票资格条件，则该目标节点对该目标节点的身份信息进行加密，得到该目标节点的身份信息的加密信息。

[0079] 可选的，所述电子投票公告信息还包括：用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息；所述目标节点对所述目标节点的身份信息进行加密，包括：所述目标节点根据所述指示信息指示的所述监督节点的公钥或所述目标节点的公钥对所述目标节点的身份信息进行加密。

[0080] 例如，该电子投票公告信息还包括：用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息。该目标节点根据所述指示信息指示的所述监督节点的公钥或所述目标节点的公钥按照预先约定的加密算法对所述目标节点的身份信息进行加密。

[0081] 例如，该目标节点的身份信息为IDn，该目标节点对IDn进行加密后得到IDnc。由于IDnc是加密后的身份信息，并不是该目标节点的身份信息，从而使得该目标节点可以匿名投票。

[0082] 步骤304、所述目标节点在所述区块链网络中广播投票内容，所述投票内容包括所述目标节点的私钥签名和所述加密信息。

[0083] 进一步，该目标节点在该区块链网络中广播自己的投票内容，该投票内容包括该目标节点的私钥签名和IDnc。相应的，该区块链网络中的电子投票发起方节点可接收到该目标节点的投票内容。当区块链网络中的电子投票发起方节点接收到该目标节点的投票内容后，首先对该目标节点的私钥签名进行验证，验证通过后，从该投票内容中提取IDnc，进一步，采用预设的哈希算法计算该IDnc的哈希值，IDnc的哈希值记为IDhn。进一步，检测电子投票发起方节点本地存储的哈希列表中是否包括IDhn。如果电子投票发起方节点本地存储的哈希列表{IDh1、IDh2、IDh3}中包括IDhn，则电子投票发起方节点确定该目标节点符合投票资格，从而确定对目标节点的身份信息验证通过。如果电子投票发起方节点本地存储的哈希列表{IDh1、IDh2、IDh3}中不包括IDhn，则电子投票发起方节点确定该目标节点不符合投票资格。另外，电子投票发起方节点在投票截止时间结束后，可统计多个投票节点的投票内容，并且保证在一次电子投票活动中，同一个投票节点只能投票一次，如果多次投票，可以保留一次投票内容。

[0084] 本发明实施例区块链网络中公开的是加密后的身份信息的哈希值构成的哈希列表，并不是加密后的身份信息，而投票节点需要在区块链网络中公开的是自己的身份信息的加密信息，由于哈希值的不可逆性，区块链网络中的参与节点只能检测身份信息的加密信息对应的哈希值是否在哈希列表中，而不能根据哈希值确定出加密后的身份信息，保证了投票节点的投票内容不会在线下被篡改，同时投票节点也不会被冒名，使得投票节点既可以匿名投票，同时也实现了电子投票发起方节点对投票节点的身份验证，提高了投票节点的安全性，同时电子投票发起方节点还可以通过监督节点对投票节点进行有效监督，提高了电子投票的安全性。

[0085] 图4为本发明实施例提供的电子投票发起方节点的结构示意图。本发明实施例提

供的电子投票发起方节点可以执行基于区块链的电子投票方法实施例提供的处理流程，如图4所示，电子投票发起方节点40包括：存储器41、处理器42、计算机程序和通讯接口43；其中，计算机程序存储在存储器41中，并被配置为由处理器42执行以下操作：通过所述通讯接口从监督节点接收哈希列表，所述哈希列表包括多个哈希值，每个哈希值为一个加密后的身份信息的哈希值，所述身份信息是符合投票资格的投票节点的身份信息；通过所述通讯接口在区块链网络中广播电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间；通过所述通讯接口在所述区块链网络中接收目标节点发送的投票内容，所述投票内容包括所述目标节点的私钥签名和所述目标节点的身份信息的加密信息；当所述处理器对所述目标节点的私钥签名验证通过后，计算所述加密信息的哈希值，并检测所述哈希列表中是否包括所述加密信息的哈希值；若所述哈希列表中包括所述加密信息的哈希值，则确定对所述目标节点的身份信息验证通过。

[0086] 可选的，所述哈希列表中的每个哈希值对应的加密后的身份信息是采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密后得到的。

[0087] 可选的，所述电子投票公告信息还包括：用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息。

[0088] 图4所示实施例的电子投票发起方节点可用于执行上述方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

[0089] 图5为本发明实施例提供的目标节点的结构示意图。本发明实施例提供的目标节点可以执行基于区块链的电子投票方法实施例提供的处理流程，如图5所示，目标节点50包括：存储器51、处理器52、计算机程序和通讯接口53；其中，计算机程序存储在存储器51中，并被配置为由处理器52执行以下操作：通过所述通讯接口接收电子投票发起方节点在区块链网络中广播的电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间；确定所述目标节点是否符合所述投票资格条件；当所述处理器确定所述目标节点符合所述投票资格条件时，对所述目标节点的身份信息进行加密，得到所述目标节点的身份信息的加密信息；通过所述通讯接口在所述区块链网络中广播投票内容，所述投票内容包括所述目标节点的私钥签名和所述加密信息。

[0090] 可选的，所述电子投票公告信息还包括：用于指示所述投票节点采用所述监督节点的公钥或所述投票节点的公钥对所述投票节点的身份信息进行加密的指示信息；所述处理器对所述目标节点的身份信息进行加密时，具体用于：根据所述指示信息指示的所述监督节点的公钥或所述目标节点的公钥对所述目标节点的身份信息进行加密。

[0091] 图5所示实施例的目标节点可用于执行上述方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

[0092] 另外，本发明实施例还提供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以实现上述实施例所述的基于区块链的电子投票方法。

[0093] 在本发明所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通

信连接,可以是电性,机械或其它的形式。

[0094] 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单元来实现本实施例方案的目的。

[0095] 另外,在本发明各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能单元的形式实现。

[0096] 上述以软件功能单元的形式实现的集成的单元,可以存储在一个计算机可读取存储介质中。上述软件功能单元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)或处理器(processor)执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(Read-Only Memory,ROM)、随机存取存储器(Random Access Memory,RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0097] 本领域技术人员可以清楚地了解到,为描述的方便和简洁,仅以上述各功能模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能模块完成,即将装置的内部结构划分成不同的功能模块,以完成以上描述的全部或者部分功能。上述描述的装置的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0098] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述各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,或者对其中部分或者全部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范围。

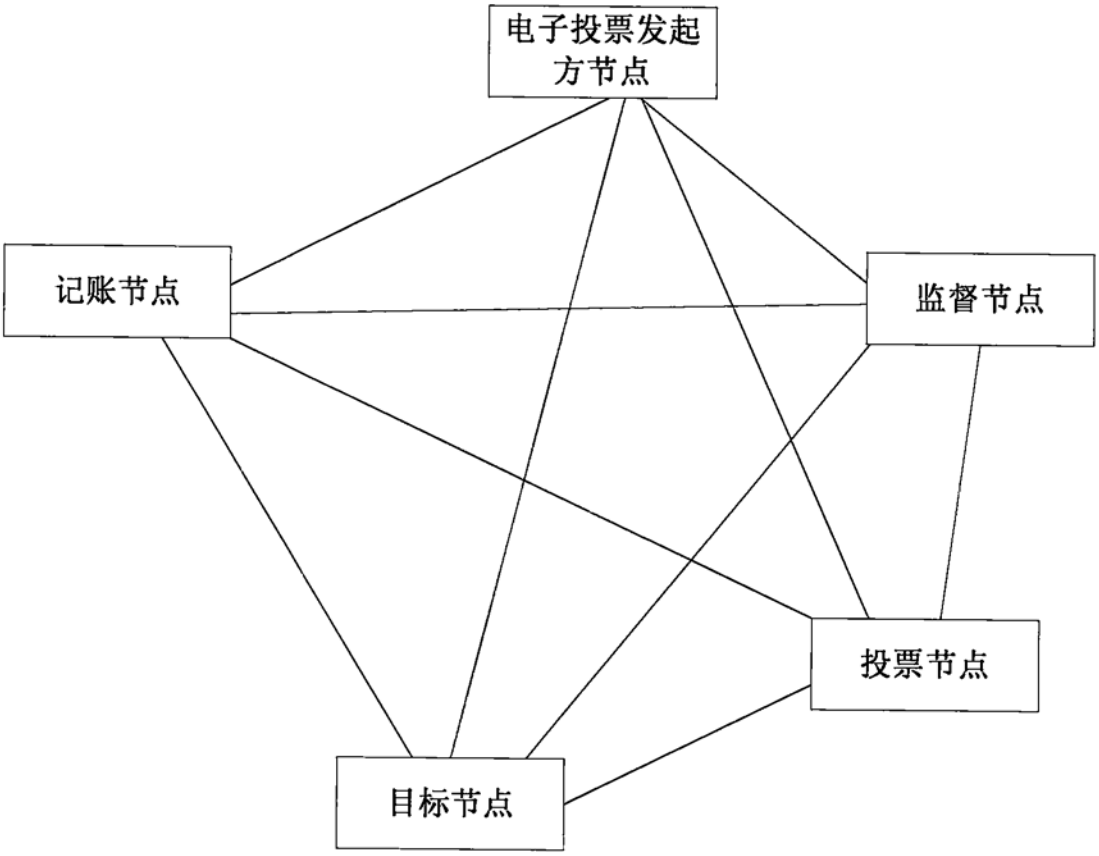


图1

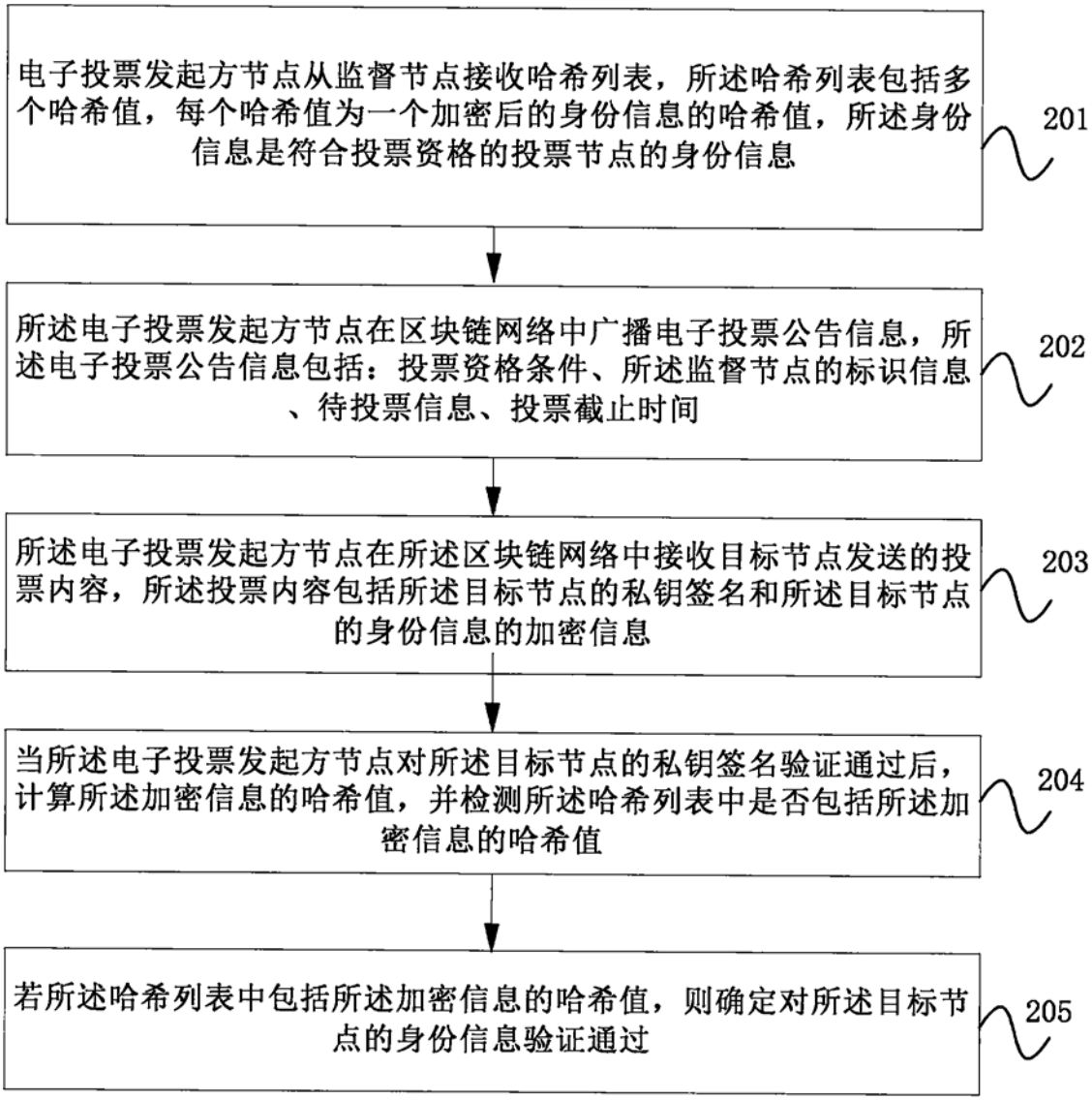

电子投票发起方节点从监督节点接收哈希列表，所述哈希列表包括多个哈希值，每个哈希值为一个加密后的身份信息的哈希值，所述身份信息是符合投票资格的投票节点的身份信息
201
所述电子投票发起方节点在区块链网络中广播电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间
202
所述电子投票发起方节点在所述区块链网络中接收目标节点发送的投票内容，所述投票内容包括所述目标节点的私钥签名和所述目标节点的身份信息的加密信息
203
当所述电子投票发起方节点对所述目标节点的私钥签名验证通过后，计算所述加密信息的哈希值，并检测所述哈希列表中是否包括所述加密信息的哈希值
204
若所述哈希列表中包括所述加密信息的哈希值，则确定对所述目标节点的身份信息验证通过
205

图2

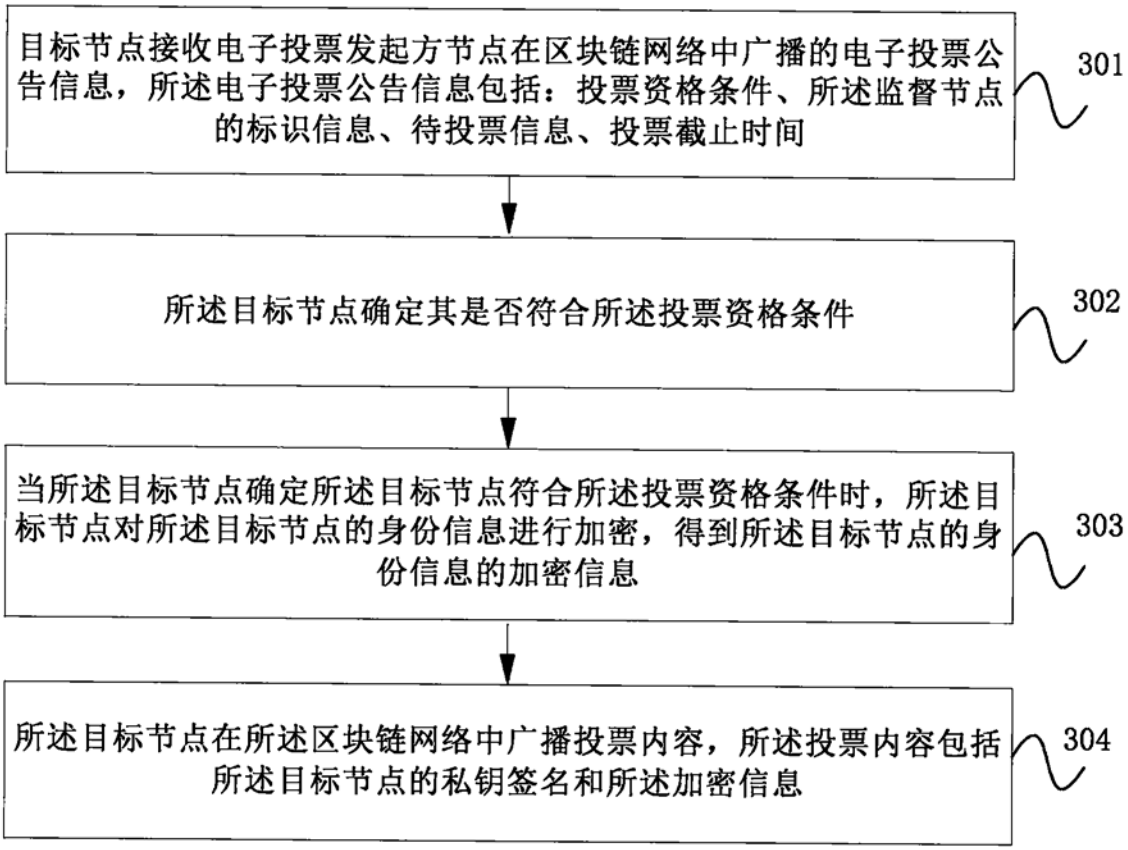

目标节点接收电子投票发起方节点在区块链网络中广播的电子投票公告信息，所述电子投票公告信息包括：投票资格条件、所述监督节点的标识信息、待投票信息、投票截止时间
301
所述目标节点确定其是否符合所述投票资格条件
302
当所述目标节点确定所述目标节点符合所述投票资格条件时，所述目标节点对所述目标节点的身份信息进行加密，得到所述目标节点的身份信息的加密信息
303
所述目标节点在所述区块链网络中广播投票内容，所述投票内容包括所述目标节点的私钥签名和所述加密信息
304

图3

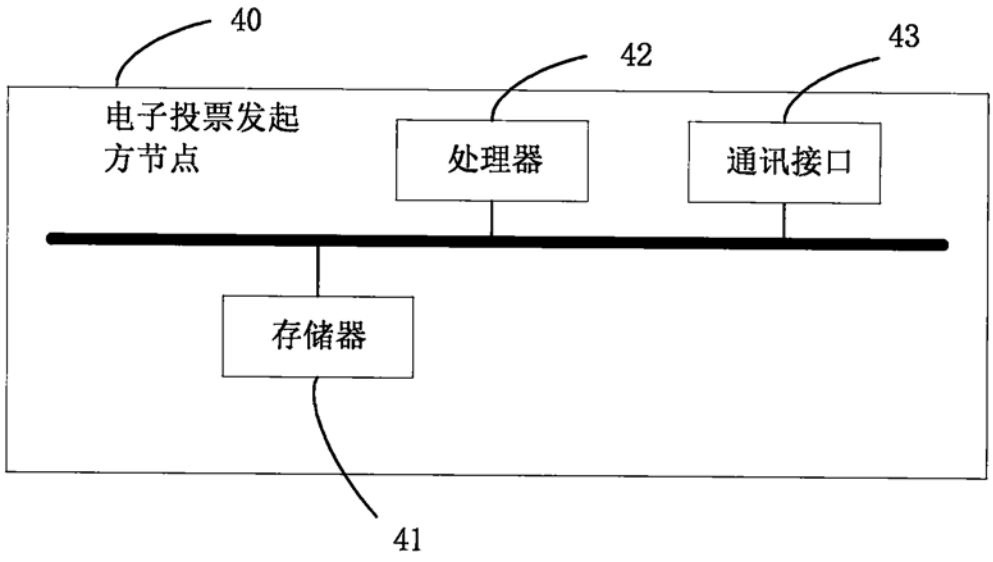

40
电子投票发起方节点
42
处理器
43
通讯接口
存储器
41

图4

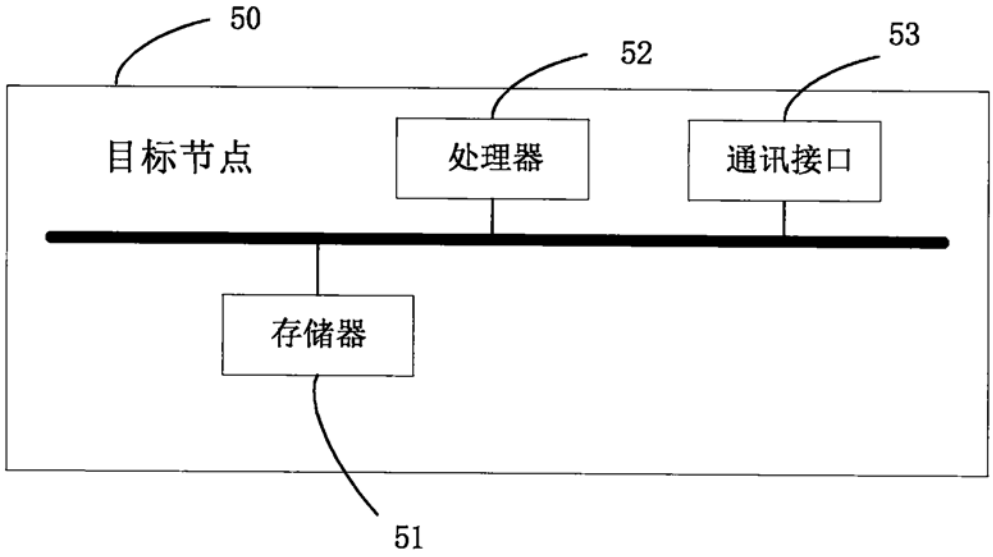


图5