(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 112153222 B
(45)授权公告日 2021.10.22

(21)申请号 202011124172.1

(22)申请日 2020.10.20

(65)同一申请的已公布的文献号
申请公布号 CN 112153222 A

(43)申请公布日 2020.12.29

(73)专利权人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 肖征荣 邢建兵 田新雪 马书惠

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
代理人 彭瑞欣 冯建基

(51)Int.Cl.
H04M 3/22(2006.01)

(56)对比文件
CN 101472007 A,2009.07.01
CN 104038648 A,2014.09.10
US 2011211685 A1,2011.09.01
EP 2028911 A2,2009.02.25
CN 105100514 A,2015.11.25
CN 106791231 A,2017.05.31
CN 108924333 A,2018.11.30
CN 104066065 A,2014.09.24

审查员 廖薇

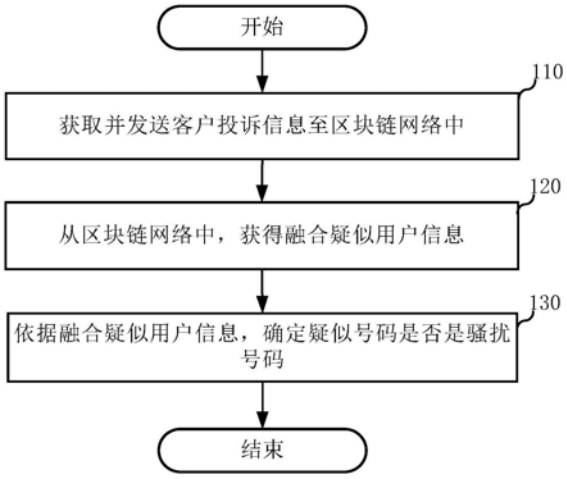
权利要求书3页 说明书11页 附图4页

(54)发明名称

骚扰号码的识别方法及服务器

(57)摘要

本申请公开一种骚扰号码的识别方法及服务器，方法包括：获取并发送客户投诉信息至区块链网络中，以使各个运营商节点获得客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；从区块链网络中，获得融合疑似用户信息，其中，融合疑似用户信息是各个运营商节点依据客户投诉信息反馈的疑似用户的信息的集合，疑似用户是使用疑似号码进行通话的用户；依据融合疑似用户信息，确定疑似号码是否是骚扰号码。依据融合疑似用户信息，确定疑似号码是否是骚扰号码，无需再进行人工审核，在保障正常用户的安全使用的同时，降低了运营成本，有助于推动移动通信业务的发展。



CN 112153222 B

1.一种骚扰号码的识别方法,其特征在于,所述方法包括:

获取并发送客户投诉信息至区块链网络中,以使各个运营商节点获得所述客户投诉信息,其中,所述客户投诉信息包括疑似号码和所述疑似号码对应的通话记录信息;

从所述区块链网络中,获得融合疑似用户信息,其中,所述融合疑似用户信息是各个运营商节点依据所述客户投诉信息反馈的疑似用户的信息的集合,所述疑似用户是使用所述疑似号码进行通话的用户;

依据所述融合疑似用户信息,确定所述疑似号码是否是骚扰号码;

所述依据所述融合疑似用户信息,确定所述疑似号码是否是骚扰号码,包括:

提取所述融合疑似用户信息中的所述疑似用户的身份验证标识、所述疑似号码对应的通话记录信息和所述疑似用户在进行通话时的位置信息,其中,所述身份验证标识是所述运营商节点依据所述疑似用户收到的合法机构的验证信息确定的身份标识;

依据所述身份验证标识确定所述疑似用户是否是合法用户;

在确定所述疑似用户不是所述合法用户时,确定所述疑似号码是所述骚扰号码;

在确定所述疑似用户是所述合法用户时,依据所述疑似号码对应的通话记录信息和所述疑似用户在进行通话时的位置信息,确定所述疑似号码是否是所述骚扰号码。

2.根据权利要求1所述的方法,其特征在于,所述依据所述疑似号码对应的通话记录信息和所述疑似用户在进行通话时的位置信息,确定所述疑似号码是否是所述骚扰号码,包括:

依据所述疑似号码对应的通话记录信息,确定所述疑似用户发起的呼叫对应的被叫号码组和通话时长;

依据所述通话时长和所述疑似用户在进行通话时的位置信息,确定所述疑似用户在同一位置上的同一时间段内的呼叫频率信息;

当确定所述被叫号码组中的被叫号码是预设号码,所述疑似用户发起呼叫的频率超过频率预设阈值,且,所述通话时长是预设时长时,确定所述疑似号码不是所述骚扰号码;

当所述被叫号码组中的被叫号码不是所述预设号码时,依据所述呼叫频率信息和所述频率预设阈值,确定所述疑似号码是否是所述骚扰号码。

3.根据权利要求1所述的方法,其特征在于,所述确定所述疑似号码是所述骚扰号码的步骤之后,还包括:

依据所述骚扰号码,生成并发送屏蔽广播消息至所述区块链网络中,以使各个所述运营商节点获得所述骚扰号码,将所述骚扰号码加入到黑名单中,禁止所述骚扰号码的呼叫业务。

4.一种骚扰号码的识别方法,其特征在于,所述方法包括:

从区块链网络中,获得骚扰号码识别服务器发送的客户投诉信息,其中,所述客户投诉信息包括疑似号码和所述疑似号码对应的通话记录信息;

判断所述疑似号码是否是当前运营商节点的服务用户,若是,则依据所述疑似号码,确定第一疑似用户的信息;

从所述区块链网络中,获得第二运营商节点反馈的第二疑似用户的信息;

依据所述第一疑似用户的信息和第二疑似用户的信息,生成并发送融合疑似用户信息至所述区块链网络中,以使所述骚扰号码识别服务器依据所述融合疑似用户信息确定所述

疑似号码是否是骚扰号码；

所述依据所述疑似号码，确定第一疑似用户的信息，包括：

依据所述疑似号码查询所述当前运营商节点的数据库，获得所述疑似号码对应的通话记录信息和所述第一疑似用户在进行通话时的位置信息；

获取合法机构对所述第一疑似用户的验证信息；

依据所述验证信息，确定所述第一疑似用户的身份验证标识；

依据所述疑似号码对应的通话记录信息、所述第一疑似用户的身份验证标识和所述第一疑似用户在进行通话时的位置信息，确定所述第一疑似用户的信息；

其中，所述融合疑似用户信息是各个运营商节点依据所述客户投诉信息反馈的疑似用户的信息的集合，所述疑似用户是使用所述疑似号码进行通话的用户。

5.根据权利要求4所述的方法，其特征在于，所述依据所述第一疑似用户的信息和第二疑似用户的信息，生成并发送融合疑似用户信息至所述区块链网络中，包括：

提取所述第一疑似用户的信息中的所述疑似用户在进行通话时的第一位置信息和第一通话记录信息；

提取所述第二疑似用户的信息中的所述疑似用户在进行通话时的第二位置信息和第二通话记录信息；

依据第一位置信息、第一通话记录信息、第二位置信息和第二通话记录信息，确定疑似号码集合中的疑似号码的呼叫频率信息，其中，所述疑似号码都是在同一位置上的同一时间段内发起呼叫的号码；

依据所述呼叫频率信息和频率预设阈值，确定所述融合疑似用户信息；

发送所述融合疑似用户信息至所述区块链网络中。

6.根据权利要求5所述的方法，其特征在于，所述融合疑似用户信息包括：运营商节点的标识、所述疑似号码集合、所述疑似号码集合中的疑似号码对应的通话记录信息、所述疑似号码对应的疑似用户的身份验证标识和所述疑似用户在进行通话时的位置信息。

7.一种骚扰号码识别服务器，其特征在于，包括：

客户投诉信息处理模块，用于获取并发送客户投诉信息至区块链网络中，以使各个运营商节点获得所述客户投诉信息，其中，所述客户投诉信息包括疑似号码和所述疑似号码对应的通话记录信息；

第一获取模块，用于从所述区块链网络中，获得融合疑似用户信息，其中，所述融合疑似用户信息是各个运营商节点依据所述客户投诉信息反馈的疑似用户的信息的集合，所述疑似用户是使用所述疑似号码进行通话的用户；

识别模块，用于依据所述融合疑似用户信息，确定所述疑似号码是否是骚扰号码；

所述识别模块，具体用于：提取所述融合疑似用户信息中的所述疑似用户的身份验证标识、所述疑似号码对应的通话记录信息和所述疑似用户在进行通话时的位置信息，其中，所述身份验证标识是所述运营商节点依据所述疑似用户收到的合法机构的验证信息确定的身份标识；依据所述身份验证标识确定所述疑似用户是否是合法用户；在确定所述疑似用户不是所述合法用户时，确定所述疑似号码是所述骚扰号码；在确定所述疑似用户是所述合法用户时，依据所述疑似号码对应的通话记录信息和所述疑似用户在进行通话时的位置信息，确定所述疑似号码是否是所述骚扰号码。

8.一种运营商节点服务器,其特征在于,包括:

第二获取模块,用于从区块链网络中,获得骚扰号码识别服务器发送的客户投诉信息,其中,所述客户投诉信息包括疑似号码和所述疑似号码对应的通话记录信息;

判断模块,用于判断所述疑似号码是否是当前运营商节点的服务用户,若是,则依据所述疑似号码,确定第一疑似用户的信息;

第三获取模块,用于从所述区块链网络中,获得第二运营商节点反馈的第二疑似用户的信息;

融合模块,用于依据所述第一疑似用户的信息和第二疑似用户的信息,生成并发送融合疑似用户信息至所述区块链网络中,以使所述骚扰号码识别服务器依据所述融合疑似用户信息确定所述疑似号码是否是骚扰号码;

所述判断模块中的依据疑似号码,确定第一疑似用户的信息,包括:依据所述疑似号码查询所述当前运营商节点的数据库,获得所述疑似号码对应的通话记录信息和所述第一疑似用户在进行通话时的位置信息;获取合法机构对所述第一疑似用户的验证信息;依据所述验证信息,确定所述第一疑似用户的身份验证标识;依据所述疑似号码对应的通话记录信息、所述第一疑似用户的身份验证标识和所述第一疑似用户在进行通话时的位置信息,确定所述第一疑似用户的信息;

其中,所述融合疑似用户信息是各个运营商节点依据所述客户投诉信息反馈的疑似用户的信息的集合,所述疑似用户是使用所述疑似号码进行通话的用户。

骚扰号码的识别方法及服务器

技术领域

[0001] 本申请涉及通信技术领域，具体涉及一种骚扰号码的识别方法及服务器。

背景技术

[0002] 骚扰电话是指推销产品或者是一些冒充权威部门工作人员进行诈骗以及故意电话骚扰的行为。普通手机用户防范骚扰电话、垃圾短信、诈骗电话的主要方法是保护好个人信息，同时学会使用手机安全软件。此外，有效根治骚扰电话和垃圾短信需要产业链携手共同努力，运营商、网络安全管理的相关职能部门和手机厂商等携手一起做好安全管理，可有效打击各类诈骗行为或骚扰行为等。

[0003] 现有对于骚扰电话的筛选都是基于同一个运营商系统内的筛选，上传信息存在被篡改的可能性，并且，客户上报的疑似号码的总数量高于骚扰号码的确认量，骚扰号码仍需要人工审核，并且骚扰号码的确认比例很低，不仅增加了运营成本，还导致用户体验度差。

发明内容

[0004] 为此，本申请提供一种骚扰号码的识别方法及服务器，以解决如何高效安全地识别骚扰号码的问题。

[0005] 为了实现上述目的，本申请第一方面提供一种骚扰号码的识别方法，方法包括：获取并发送客户投诉信息至区块链网络中，以使各个运营商节点获得客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；从区块链网络中，获得融合疑似用户信息，其中，融合疑似用户信息是各个运营商节点依据客户投诉信息反馈的疑似用户的信息的集合，疑似用户是使用疑似号码进行通话的用户；依据融合疑似用户信息，确定疑似号码是否是骚扰号码。

[0006] 在一些具体实现中，依据融合疑似用户信息，确定疑似号码是否是骚扰号码，包括：提取融合疑似用户信息中的疑似用户的身份验证标识、疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，其中，身份验证标识是运营商节点依据疑似用户收到的合法机构的验证信息确定的身份标识；依据身份验证标识确定疑似用户是否是合法用户；在确定疑似用户不是合法用户时，确定疑似号码是骚扰号码；在确定疑似用户是合法用户时，依据疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，确定疑似号码是否是骚扰号码。

[0007] 在一些具体实现中，依据疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，确定疑似号码是否是骚扰号码，包括：依据疑似号码对应的通话记录信息，确定疑似用户发起的呼叫对应的被叫号码组和通话时长；依据通话时长和疑似用户在进行通话时的位置信息，确定疑似用户在同一位置上的同一时间段内的呼叫频率信息；当确定被叫号码组中的被叫号码是预设号码，疑似用户发起呼叫的频率超过频率预设阈值，且，通话时长是预设时长时，确定疑似号码不是骚扰号码；当被叫号码组中的被叫号码不是预设号码时，依据呼叫频率信息和频率预设阈值，确定疑似号码是否是骚扰号码。

[0008] 在一些具体实现中，确定疑似号码是骚扰号码的步骤之后，还包括：依据骚扰号码，生成并发送屏蔽广播消息至区块链网络中，以使各个运营商节点获得骚扰号码，将骚扰号码加入到黑名单中，禁止骚扰号码的呼叫业务。

[0009] 为了实现上述目的，本申请第二方面提供一种骚扰号码的识别方法，方法包括：从区块链网络中，获得骚扰号码识别服务器发送的客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；判断疑似号码是否是当前运营商节点的服务用户，若是，则依据疑似号码，确定第一疑似用户的信息；从区块链网络中，获得第二运营商节点反馈的第二疑似用户的信息；依据第一疑似用户的信息和第二疑似用户的信息，生成并发送融合疑似用户信息至区块链网络中，以使骚扰号码识别服务器依据融合疑似用户信息确定疑似号码是否是骚扰号码。

[0010] 在一些具体实现中，依据疑似号码，确定第一疑似用户的信息，包括：依据疑似号码查询当前运营商节点的数据库，获得疑似号码对应的通话记录信息和第一疑似用户在进行通话时的位置信息；获取合法机构对第一疑似用户的验证信息；依据验证信息，确定第一疑似用户的身份验证标识；依据疑似号码对应的通话记录信息、第一疑似用户的身份验证标识和第一疑似用户在进行通话时的位置信息，确定第一疑似用户的信息。

[0011] 在一些具体实现中，依据第一疑似用户的信息和第二疑似用户的信息，生成并发送融合疑似用户信息至区块链网络中，包括：提取第一疑似用户的信息中的疑似用户在进行通话时的第一位置信息和第一通话记录信息；提取第二疑似用户的信息中的疑似用户在进行通话时的第二位置信息和第二通话记录信息；依据第一位置信息、第一通话记录信息、第二位置信息和第二通话记录信息，确定疑似号码集合中的疑似号码的呼叫频率信息，其中，疑似号码都是在同一位置上的同一时间段内发起呼叫的号码；依据呼叫频率信息和频率预设阈值，确定融合疑似用户信息；发送融合疑似用户信息至区块链网络中。

[0012] 在一些具体实现中，融合疑似用户信息包括：运营商节点的标识、疑似号码集合、疑似号码集合中的疑似号码对应的通话记录信息、疑似号码对应的疑似用户的身份验证标识和疑似用户在进行通话时的位置信息。

[0013] 为了实现上述目的，本申请第三方面提供一种骚扰号码识别服务器，包括：客户投诉信息处理模块，用于获取并发送客户投诉信息至区块链网络中，以使各个运营商节点获得客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；第一获取模块，用于从区块链网络中，获得融合疑似用户信息，其中，融合疑似用户信息是各个运营商节点依据客户投诉信息反馈的疑似用户的信息的集合，疑似用户是使用疑似号码进行通话的用户；识别模块，用于依据融合疑似用户信息，确定疑似号码是否是骚扰号码。

[0014] 为了实现上述目的，本申请第四方面提供一种运营商节点服务器，包括：第二获取模块，用于从区块链网络中，获得骚扰号码识别服务器发送的客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；判断模块，用于判断疑似号码是否是当前运营商节点的服务用户，若是，则依据疑似号码，确定第一疑似用户的信息；第三获取模块，用于从区块链网络中，获得第二运营商节点反馈的第二疑似用户的信息；融合模块，用于依据第一疑似用户的信息和第二疑似用户的信息，生成并发送融合疑似用户信息至区块链网络中，以使骚扰号码识别服务器依据融合疑似用户信息确定疑似号码是否是骚扰号码。

[0015] 本申请中的骚扰号码的识别方法及服务器，通过获取并发送客户投诉信息至区块链网络中，以使各个运营商节点获得客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；使各个运营商节点能够根据该客户投诉信息对疑似号码进行筛查，加快对骚扰号码的排查。从区块链网络中，获得融合疑似用户信息，其中，融合疑似用户信息是各个运营商节点依据客户投诉信息反馈的疑似用户的信息的集合，疑似用户是使用疑似号码进行通话的用户；通过区块链的通信方式，在多个运营商节点的服务范围内，获得多个运营商节点上报的、经过各个运营商筛查的融合疑似用户信息，扩展了疑似号码的排查范围，提升了疑似号码的排查效率。依据融合疑似用户信息，确定疑似号码是否是骚扰号码，无需再进行人工审核，在保障正常用户的安全使用的同时，降低了运营成本，有助于推动移动通信业务的发展。

附图说明

[0016] 附图用来提供对本申请实施例的进一步理解，并且构成说明书的一部分，与本申请的实施例一起用于解释本申请，并不构成对本申请的限制。通过参考附图对详细示例实施例进行描述，以上和其它特征和优点对本领域技术人员将变得更加显而易见，在附图中：

[0017] 图1示出本申请一实施例中的骚扰号码的识别方法的流程示意图。

[0018] 图2示出本申请又一实施例中的骚扰号码的识别方法的流程示意图。

[0019] 图3示出本申请再一实施例中的骚扰号码的识别方法的流程示意图。

[0020] 图4示出本申请一实施例中的骚扰号码识别服务器的组成方框图。

[0021] 图5示出本申请一实施例中的运营商节点服务器的组成方框图。

[0022] 图6示出本申请一实施例中的骚扰号码的识别系统的组成方框图。

[0023] 图7示出本申请一实施例中的骚扰号码的识别系统的工作方法的流程示意图。

[0024] 在附图中：

[0025] 401:客户投诉信息处理模块 402:第一获取模块

[0026] 403:识别模块 501:第二获取模块

[0027] 502:判断模块 503:第三获取模块

[0028] 504:融合模块 601:第一运营商节点服务器

[0029] 602:第二运营商节点服务器 603:第三运营商节点服务器

[0030] 604:骚扰号码识别服务器

具体实施方式

[0031] 以下结合附图对本申请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申请，并不用于限制本申请。对于本领域技术人员来说，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本申请的示例来提供对本申请更好的理解。

[0032] 骚扰电话是指某些商家为了推销产品，或者，某些人冒充权威部门工作人员进行诈骗而打给普通用户的电话，普通用户还可能会不断接收到通过网络或移动号码发送来的垃圾短信，等多种形式的通信骚扰，以运营商网络为载体进行的各种类型的骚扰号码越来越多，导致客户体验度差。

[0033] 为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

[0034] 图1示出本申请一实施例中的骚扰号码的识别方法的流程示意图。该骚扰号码的识别方法可应用于骚扰号码识别服务器。如图1所示，包括如下步骤。

[0035] 步骤110，获取并发送客户投诉信息至区块链网络中。

[0036] 当各个运营商节点从区块链网络中，获得客户投诉信息时，会对该客户投诉信息进行消息解析，获得客户投诉信息中的疑似号码和疑似号码对应的通话记录信息。各个运营商节点可并行地根据疑似号码查找自己内部的数据库，对疑似号码进行筛查，加快对骚扰号码的排查。

[0037] 步骤120，从区块链网络中，获得融合疑似用户信息。

[0038] 其中，融合疑似用户信息是各个运营商节点依据客户投诉信息反馈的疑似用户的信息的集合，疑似用户是使用疑似号码进行通话的用户。

[0039] 步骤130，依据融合疑似用户信息，确定疑似号码是否是骚扰号码。

[0040] 在一些具体实现中，依据融合疑似用户信息，确定疑似号码是否是骚扰号码，包括：提取融合疑似用户信息中的疑似用户的身份验证标识、疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，其中，身份验证标识是运营商节点依据疑似用户收到的合法机构的验证信息确定的身份标识；依据身份验证标识确定疑似用户是否是合法用户；在确定疑似用户不是合法用户时，确定疑似号码是骚扰号码；在确定疑似用户是合法用户时，进一步依据疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，确定疑似号码是否是骚扰号码。

[0041] 例如，融合疑似用户信息包括的疑似号码是1341xxxxxx4，其中，x为0至9中任意一个。该疑似号码对应的疑似用户是王某某，王某某在使用号码1341xxxxxx4进行呼叫业务时的位置是第一街道，当通过解析融合疑似用户信息时，获得的王某某的身份验证标识表征了王某某不是合法用户(例如，当运营商节点从数据库中能够查询到王某某收到过银行/政府机构发送的验证短消息时，则将王某某的身份验证标识设置为合法用户；否则，将王某某的身份验证标识设置为非法用户)，则确定该疑似号码1341xxxxxx4是骚扰号码。当确定王某某的身份验证标识为合法用户时，还需要通过疑似号码1341xxxxxx4对应的通话记录信息和疑似用户在进行通话时的位置信息(例如，第一街道等)，来判断疑似号码是否是骚扰号码。

[0042] 通过疑似用户的身份验证标识初步判断该疑似用户所述使用的疑似号码是否是骚扰号码，加快对骚扰号码的排查速度；然后再通过疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，进一步判断疑似号码是否是骚扰号码。提升骚扰号码的排查准确性。

[0043] 在一些具体实现中，依据疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，确定疑似号码是否是骚扰号码，包括：依据疑似号码对应的通话记录信息，确定疑似用户发起的呼叫对应的被叫号码组和通话时长；依据通话时长和疑似用户在进行通话时的位置信息，确定疑似用户在同一位置上的同一时间段内的呼叫频率信息；当确定被叫号码组中的被叫号码是预设号码，疑似用户发起呼叫的频率超过频率预设阈值，且，通话时长是预设时长时，确定疑似号码不是骚扰号码；当被叫号码组中的被叫号码不是预设号

码时，依据呼叫频率信息和频率预设阈值，确定疑似号码是否是骚扰号码。

[0044] 例如，设定频率预设阈值为1分钟内呼叫4次，疑似号码1341xxxxxx4会多次呼叫多个被叫号码，当疑似号码1341xxxxxx4所呼叫的被叫号码是运营商的客服号码(例如，10011等)或紧急号码(例如，110，119等)等预设号码时，即使疑似号码1341xxxxxx4发起呼叫的频率是1分钟内呼叫6次，大于频率预设阈值时，该疑似号码1341xxxxxx4也不是骚扰号码，因为该疑似号码1341xxxxxx4没有对其他用户造成不好的影响，没有打扰到其他用户的正常通话。

[0045] 例如，当被叫号码组中的被叫号码不是预设号码时，若呼叫频率信息大于频率预设阈值时，确定疑似号码是骚扰号码；否则，若呼叫频率信息小于或等于频率预设阈值时，确定疑似号码不是骚扰号码。

[0046] 需要说明的是，以上疑似号码可以是一个号码，也可以是多个号码，若疑似用户使用多部移动终端在同一时间段内(例如，下午2点至2点半这段时间内)在同一个位置(例如，都是在第一号楼的606房间内)上，同时向外对多个普通号码进行呼叫，通过多个运营商节点查询其内部数据库，可快速定位到这些疑似号码的相关通信信息，加快对疑似号码的排查和确认，提升骚扰号码的阻截，保证普通用户的正常通信。

[0047] 在本实施例中，通过获取并发送客户投诉信息至区块链网络中，以使各个运营商节点获得客户投诉信息；使各个运营商节点能够根据该客户投诉信息对疑似号码进行筛查，加快对骚扰号码的排查。从区块链网络中，获得融合疑似用户信息；通过区块链的通信方式，在多个运营商节点的服务范围内，获得多个运营商节点上报的、经过各个运营商筛查的融合疑似用户信息，扩展了疑似号码的排查范围，提升了疑似号码的排查效率。依据融合疑似用户信息，确定疑似号码是否是骚扰号码，无需再进行人工审核，在保障正常用户的安全使用的同时，降低了运营成本，有助于推动移动通信业务的发展。

[0048] 图2示出本申请又一实施例中的骚扰号码的识别方法的流程示意图。该骚扰号码的识别方法可应用于骚扰号码识别服务器。如图2所示，包括如下步骤。

[0049] 步骤210，获取并发送客户投诉信息至区块链网络中。

[0050] 步骤220，从区块链网络中，获得融合疑似用户信息。

[0051] 步骤230，依据融合疑似用户信息，确定疑似号码是否是骚扰号码。

[0052] 需要说明的是，本实施例中的步骤210～步骤230与上一实施例中的步骤110～步骤130相同，在此不再赘述。

[0053] 步骤240，在确定疑似号码是骚扰号码时，依据骚扰号码，生成并发送屏蔽广播消息至区块链网络中。

[0054] 当各个运营商节点从区块链网络中，获得屏蔽广播消息中的骚扰号码时，会将该骚扰号码加入到黑名单中，以禁止该骚扰号码的呼叫业务。

[0055] 在本实施例中，通过区块链的通信方式，在多个运营商节点的服务范围内，获得多个运营商节点上报的、经过各个运营商筛查的融合疑似用户信息，扩展了疑似号码的排查范围，提升了疑似号码的排查效率。依据融合疑似用户信息，确定疑似号码是否是骚扰号码，无需再进行人工审核，在保障正常用户的安全使用的同时，降低了运营成本；然后依据骚扰号码，生成并发送屏蔽广播消息至区块链网络中，使各个运营商节点能够及时将该骚扰号码加入到黑名单中，即将该骚扰号码列为不可信号码，使该骚扰号码无法再进行呼叫

业务，以保证其他用户不会被该骚扰号码骚扰，提升用户体验度。

[0056] 图3示出本申请再一实施例中的骚扰号码的识别方法的流程示意图。该骚扰号码的识别方法可应用于运营商节点服务器。如图3所示，包括如下步骤。

[0057] 步骤310，从区块链网络中，获得骚扰号码识别服务器发送的客户投诉信息。

[0058] 其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息。例如，疑似号码是1341xxxxxx4，疑似号码1341xxxxxx4对应的通话记录信息可以包括通话时长、被叫号码、通话的起始时间、进行通话时该疑似号码1341xxxxxx4的使用者所处的地理位置信息(例如，具体的经纬度信息等)。以上对于通话记录信息仅是举例说明，可根据实际情况进行具体设定，其他未说明的通话记录信息也在本申请的保护范围之内，在此不再赘述。

[0059] 步骤320，判断疑似号码是否是当前运营商节点的服务用户。

[0060] 例如，从当前运营商节点的服务范围内，查找是否存在疑似号码1341xxxxxx4，若存在，则确定该疑似号码1341xxxxxx4是当前运营商节点的服务用户；否则，确定该疑似号码1341xxxxxx4不是当前运营商节点的服务用户，当前运营商节点无法对该疑似号码进行查询处理。

[0061] 需要说明的是，若确定疑似号码是当前运营商节点的服务用户，则执行步骤330；否则，结束流程。

[0062] 步骤330，依据疑似号码，确定第一疑似用户的信息。

[0063] 例如，第一疑似用户的信息可以包括：疑似号码1341xxxxxx4、疑似号码1341xxxxxx4对应的第一疑似用户的身份标识(例如，身份证号码等)、第一疑似用户在进行通话时的位置信息、疑似号码对应的通话记录信息等。

[0064] 在一些具体实现中，依据疑似号码，确定第一疑似用户的信息，包括：依据疑似号码查询当前运营商节点的数据库，获得疑似号码对应的通话记录信息和第一疑似用户在进行通话时的位置信息；获取合法机构对第一疑似用户的验证信息；依据验证信息，确定第一疑似用户的身份验证标识；依据疑似号码对应的通话记录信息、第一疑似用户的身份验证标识和第一疑似用户在进行通话时的位置信息，确定第一疑似用户的信息。

[0065] 其中，合法机构对第一疑似用户的验证信息可通过如下方式确定：查找当前运营商节点的数据库，若从数据库中查询到第一疑似用户接收到银行/政府机构发送的验证短消息记录，则表示合法机构对第一疑似用户的验证通过，即合法机构认为该第一疑似用户是合法用户；否则，表示合法机构没有对第一疑似用户的验证通过，即合法机构认为该第一疑似用户是非法用户。

[0066] 步骤340，从区块链网络中，获得第二运营商节点反馈的第二疑似用户的信息。

[0067] 需要说明的是，第二运营商节点反馈的第二疑似用户的信息可以是第二运营商节点根据骚扰号码识别服务器发送的客户投诉信息，查找自己的数据库，获得的信息；也可以是通过获取到的第三运营商节点反馈的第三疑似用户的信息，以及骚扰号码识别服务器发送的客户投诉信息，进行综合判断，获得的第一疑似用户的信息与第三疑似用户的信息相融合的信息，例如，第一疑似用户所处的地理位置信息和第三疑似用户所处的地理位置信息相同，并且，这两个用户都在某个时间段内发起呼叫业务。以扩展疑似号码的搜索范围，提升骚扰号码的排查准确性。

[0068] 步骤350，依据第一疑似用户的信息和第二疑似用户的信息，生成并发送融合疑似

用户信息至区块链网络中。

[0069] 当骚扰号码识别服务器获得融合疑似用户信息时，会依据融合疑似用户信息确定疑似号码是否是骚扰号码。其中，融合疑似用户信息包括：运营商节点的标识、疑似号码集合、疑似号码集合中的疑似号码对应的通话记录信息、疑似号码对应的疑似用户的身份验证标识和疑似用户在进行通话时的位置信息。

[0070] 在一些具体实现中，依据第一疑似用户的信息和第二疑似用户的信息，生成并发送融合疑似用户信息至区块链网络中，包括：提取第一疑似用户的信息中的疑似用户在进行通话时的第一位置信息和第一通话记录信息；提取第二疑似用户的信息中的疑似用户在进行通话时的第二位置信息和第二通话记录信息；依据第一位置信息、第一通话记录信息、第二位置信息和第二通话记录信息，确定疑似号码集合中的疑似号码的呼叫频率信息，其中，疑似号码都是在同一位置上的同一时间段内发起呼叫的号码；依据呼叫频率信息和频率预设阈值，确定融合疑似用户信息；发送融合疑似用户信息至区块链网络中。

[0071] 在本实施例中，通过从区块链网络中，获得骚扰号码识别服务器发送的客户投诉信息，并依据客户投诉信息查询运营商节点的数据库，以确定是否存在疑似号码，并在确定存在疑似号码时，将该疑似号码发送给骚扰号码识别服务器；和/或，获取其他运营商节点服务器发送的疑似号码的相关信息，与自己的数据库所查询到的疑似号码的相关信息进行融合，获得并发送融合疑似号码的相关信息给骚扰号码识别服务器，使骚扰号码识别服务器能够综合判断疑似号码中是否存在骚扰号码，进而对骚扰号码进行处理，减少骚扰号码对用户的骚扰，提升用户体验度。

[0072] 图4示出本申请一实施例中的骚扰号码识别服务器的组成方框图。如图4所示，该骚扰号码识别服务器具体包括：客户投诉信息处理模块401，用于获取并发送客户投诉信息至区块链网络中，以使各个运营商节点获得客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；第一获取模块402，用于从区块链网络中，获得融合疑似用户信息，其中，融合疑似用户信息是各个运营商节点依据客户投诉信息反馈的疑似用户的信息的集合，疑似用户是使用疑似号码进行通话的用户；识别模块403，用于依据融合疑似用户信息，确定疑似号码是否是骚扰号码。

[0073] 在一些具体实现中，识别模块403具体用于：提取融合疑似用户信息中的疑似用户的身份验证标识、疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，其中，身份验证标识是运营商节点依据疑似用户收到的合法机构的验证信息确定的身份标识；依据身份验证标识确定疑似用户是否是合法用户；在确定疑似用户不是合法用户时，确定疑似号码是骚扰号码；在确定疑似用户是合法用户时，依据疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，确定疑似号码是否是骚扰号码。

[0074] 在一些具体实现中，识别模块403中的依据疑似号码对应的通话记录信息和疑似用户在进行通话时的位置信息，确定疑似号码是否是骚扰号码，包括：依据疑似号码对应的通话记录信息，确定疑似用户发起的呼叫对应的被叫号码组和通话时长；依据通话时长和疑似用户在进行通话时的位置信息，确定疑似用户在同一位置上的同一时间段内的呼叫频率信息；当确定被叫号码组中的被叫号码是预设号码，疑似用户发起呼叫的频率超过频率预设阈值，且，通话时长是预设时长时，确定疑似号码不是骚扰号码；当被叫号码组中的被叫号码不是预设号码时，依据呼叫频率信息和频率预设阈值，确定疑似号码是否是骚扰号

码。

[0075] 在一些具体实现中，骚扰号码识别服务器还用于：依据骚扰号码，生成并发送屏蔽广播消息至区块链网络中，以使各个运营商节点获得骚扰号码，将骚扰号码加入到黑名单中，禁止骚扰号码的呼叫业务。

[0076] 在本实施方式中，通过客户投诉信息处理模块获取并发送客户投诉信息至区块链网络中，以使各个运营商节点获得客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；使各个运营商节点能够根据该客户投诉信息对疑似号码进行筛查，加快对骚扰号码的排查。使用第一获取模块从区块链网络中，获得融合疑似用户信息，其中，融合疑似用户信息是各个运营商节点依据客户投诉信息反馈的疑似用户的信息的集合，疑似用户是使用疑似号码进行通话的用户；通过区块链的通信方式，在多个运营商节点的服务范围内，获得多个运营商节点上报的、经过各个运营商筛查的融合疑似用户信息，扩展了疑似号码的排查范围，提升了疑似号码的排查效率。使用识别模块依据融合疑似用户信息，确定疑似号码是否是骚扰号码，无需再进行人工审核，在保障正常用户的安全使用的同时，降低了运营成本，有助于推动移动通信业务的发展。

[0077] 图5示出本申请一实施例中的运营商节点服务器的组成方框图。如图5所示，该运营商节点服务器具体包括：第二获取模块501，用于从区块链网络中，获得骚扰号码识别服务器发送的客户投诉信息，其中，客户投诉信息包括疑似号码和疑似号码对应的通话记录信息；判断模块502，用于判断疑似号码是否是当前运营商节点的服务用户，若是，则依据疑似号码，确定第一疑似用户的信息；第三获取模块503，用于从区块链网络中，获得第二运营商节点反馈的第二疑似用户的信息；融合模块504，用于依据第一疑似用户的信息和第二疑似用户的信息，生成并发送融合疑似用户信息至区块链网络中，以使骚扰号码识别服务器依据融合疑似用户信息确定疑似号码是否是骚扰号码。

[0078] 在一些具体实现中，判断模块502中的依据疑似号码，确定第一疑似用户的信息，包括：依据疑似号码查询当前运营商节点的数据库，获得疑似号码对应的通话记录信息和第一疑似用户在进行通话时的位置信息；获取合法机构对第一疑似用户的验证信息；依据验证信息，确定第一疑似用户的身份验证标识；依据疑似号码对应的通话记录信息、第一疑似用户的身份验证标识和第一疑似用户在进行通话时的位置信息，确定第一疑似用户的信息。

[0079] 在一些具体实现中，融合模块504具体用于：提取第一疑似用户的信息中的疑似用户在进行通话时的第一位置信息和第一通话记录信息；提取第二疑似用户的信息中的疑似用户在进行通话时的第二位置信息和第二通话记录信息；依据第一位置信息、第一通话记录信息、第二位置信息和第二通话记录信息，确定疑似号码集合中的疑似号码的呼叫频率信息，其中，疑似号码都是在同一位置上的同一时间段内发起呼叫的号码；依据呼叫频率信息和频率预设阈值，确定融合疑似用户信息；发送融合疑似用户信息至区块链网络中。

[0080] 在一些具体实现中，融合疑似用户信息包括：运营商节点的标识、疑似号码集合、疑似号码集合中的疑似号码对应的通话记录信息、疑似号码对应的疑似用户的身份验证标识和疑似用户在进行通话时的位置信息。

[0081] 在本实施例中，通过第二获取模块从区块链网络中，获得骚扰号码识别服务器发送的客户投诉信息，并依据客户投诉信息查询运营商节点的数据库，以判断是否存在疑似

号码，并在确定存在疑似号码时，将该疑似号码发送给骚扰号码识别服务器；和/或，使用融合模块将获取到的其他运营商节点服务器发送的疑似号码的相关信息，与自己的数据库所查询到的疑似号码的相关信息进行融合，获得并发送融合疑似号码的相关信息给骚扰号码识别服务器，使骚扰号码识别服务器能够综合判断疑似号码中是否存在骚扰号码，进而对骚扰号码进行处理，减少骚扰号码对用户的骚扰，提升用户体验度。

[0082] 值得一提的是，本实施方式中所涉及到的各模块均为逻辑模块，在实际应用中，一个逻辑单元可以是一个物理单元，也可以是一个物理单元的一部分，还可以以多个物理单元的组合实现。此外，为了突出本申请的创新部分，本实施方式中并没有将与解决本申请所提出的技术问题关系不太密切的单元引入，但这并不表明本实施方式中不存在其它的单元。

[0083] 图6示出本申请一实施例中的骚扰号码的识别系统的组成方框图。如图6所示，包括：通过区块链网络连接的第一运营商节点服务器601、第二运营商节点服务器602、第三运营商节点服务器603和骚扰号码识别服务器604。

[0084] 图7示出本申请一实施例中的骚扰号码的识别系统的工作方法的流程示意图。如图7所示，具体包括如下步骤。

[0085] 步骤701，骚扰号码识别服务器604从区块链网络中，获取到客户投诉信息，并使用自己的私钥对该客户投诉信息进行签名，生成并发送签名后的客户投诉信息至区块链网络中，以使各个运营商节点(例如，第一运营商节点服务器601、第二运营商节点服务器602和第三运营商节点服务器603)获得客户投诉信息。

[0086] 其中，客户投诉信息是客户针对某些电话号码或某个电话号码的投诉信息，客户投诉信息可以包括疑似号码和该疑似号码对应的通话记录信息(例如，疑似号码的呼叫时间等)。

[0087] 步骤702，第一运营商节点服务器601收到签名后的客户投诉信息后，先对其私钥签名进行验证，在验证通过时，获得第一疑似号码和该第一疑似号码的呼叫时间，如果确定该第一疑似号码是由第一运营商节点服务器601提供通信服务的号码，则第一运营商节点服务器601依据第一疑似号码查询自己的数据库，提取该第一疑似号码对应的通话记录信息、该第一疑似号码对应的第一疑似用户的位置信息，并获取合法机构对第一疑似用户的验证信息(例如，若从数据库中查询到第一疑似用户接收到银行/政府机构发送的验证短消息记录，则表示合法机构对第一疑似用户的验证通过，即合法机构认为该第一疑似用户是合法用户；否则，表示合法机构没有对第一疑似用户的验证通过，即合法机构认为该第一疑似用户是非法用户)；然后，根据上述信息(即根据第一疑似号码对应的通话记录信息、第一疑似用户在进行通话时的位置信息、以及合法机构对第一疑似用户的验证信息)确定在同一地理位置上的同一时间段内发起呼叫的初始疑似号码的集合，需要说明的是，初始疑似号码可以是同小区或者邻小区内的发起呼叫频率超过预设阈值的异常号码。

[0088] 步骤703，依据步骤702中查询到的第一疑似号码对应的通话记录信息、第一疑似用户在进行通话时的位置信息、以及合法机构对第一疑似用户的验证信息和初始疑似号码的集合，生成第一广播消息；然后，采用第一运营商节点服务器601的私钥对该第一广播消息进行签名，生成并发送签名后的第一广播消息至区块链网络中，以使第二运营商节点服务器602获取到该第一广播消息。

[0089] 其中，第一广播消息包括如下信息：第一运营商节点服务器601的标识，步骤702中查询到的第一疑似号码、该第一疑似号码对应的通话记录信息、第一疑似用户在进行通话时的位置信息、以及合法机构对第一疑似用户的验证信息和初始疑似号码的集合。

[0090] 步骤704，第二运营商节点服务器602从区块链网络中，获取到第一广播消息后，先对该第一广播消息的私钥签名进行验证，在验证通过时，对第一广播消息进行解析，获得第一疑似用户在进行通话时的位置信息、第一疑似号码对应的通话记录信息和初始疑似号码的集合；然后，依据第一疑似用户在进行通话时的位置信息、第一疑似号码对应的通话记录信息查询第二运营商节点602的数据库，获得第二疑似号码的集合中的第二疑似号码对应的通话记录信息、第二疑似用户在进行通话时的位置信息、以及第二疑似号码的集合中的第二疑似号码的呼叫频率信息，其中，第二疑似号码都是在同一位置上的同一时间段内发起呼叫的号码；依据呼叫频率信息和频率预设阈值(例如，每分钟内发起呼叫的次数为5次等)，确定融合疑似号码集合。

[0091] 需要说明的是，融合疑似号码集合可以是初始疑似号码的集合的子集，也可以是初始疑似号码的集合，需根据第二运营商节点602查询数据库所获得的查询结果来确定具体融合疑似号码集合中的融合疑似号码。

[0092] 步骤705，依据融合疑似号码集合、第二运营商节点602的标识、融合疑似号码集合中的融合疑似号码对应的通话记录信息、获取到的融合疑似号码对应的融合疑似用户的身份验证标识和融合疑似用户在进行通话时的位置信息，生成第二广播消息；然后，采用第二运营商节点服务器602的私钥对第二广播消息进行签名，生成并发送签名后的第二广播消息至区块链网络中，以使骚扰号码识别服务器604获得该第二广播消息。

[0093] 需要说明的是，在第一运营商节点服务器601执行步骤702和步骤703的同时，第三运营商节点服务器603也同时在查询自己的数据库以确定疑似号码的具体信息，第三运营商节点服务器603所执行的步骤706～步骤707，与步骤702～步骤703相同，在此不再赘述，以使骚扰号码识别服务器604能够获得第三运营商节点服务器603发送的第三广播消息。第三广播消息包括：第三疑似号码、该第三疑似号码对应的通话记录信息、第三疑似用户在进行通话时的位置信息、以及合法机构对第三疑似用户的验证信息和初始疑似号码的集合。

[0094] 在一些具体的实现中，第三运营商节点服务器603也可以通过区块链网络，获得第一运营商节点服务器601发送的第一广播消息，或，第二运营商节点服务器602发送的第二广播消息；然后，执行步骤706～步骤707，需要说明的是，步骤706～步骤707，与步骤704～步骤705的操作方法相同，区别在于步骤706～步骤707中查询的数据库是第三运营商节点服务器603的数据库，以更准确的缩小疑似号码的范围，方便骚扰号码识别服务器604的后续处理。

[0095] 步骤708，骚扰号码识别服务器604从区块链网络中，分别获得第二运营商节点服务器602发送的第二广播消息，以及第三运营商节点服务器603发送的第三广播信息。在以上两个广播消息的私钥签名都通过验证时，获得如下信息：融合疑似号码集合，第二运营商节点602的标识，融合疑似号码集合中的融合疑似号码对应的通话记录信息，获取到的融合疑似号码对应的融合疑似用户的身份验证标识和融合疑似用户在进行通话时的位置信息；第三疑似号码，该第三疑似号码对应的通话记录信息，第三疑似用户在进行通话时的位置信息，以及合法机构对第三疑似用户的验证信息和初始疑似号码的集合。

[0096] 然后，当疑似用户不是合法用户时，确定疑似号码是骚扰号码。当疑似用户是合法用户时，依据疑似号码对应的通话记录信息，确定疑似用户发起的呼叫对应的被叫号码组和通话时长；依据通话时长和疑似用户在进行通话时的位置信息，确定疑似用户在同一位置上的同一时间段内的呼叫频率信息；

[0097] 当确定被叫号码组中的被叫号码是预设号码(例如，110、119等紧急呼救号码，或，运营商的客户号码等)，疑似用户发起呼叫的频率超过频率预设阈值(例如，频率预设阈值是每分钟内发起呼叫5次，或10次等)，且，通话时长是预设时长(例如，15秒、60秒或30分钟等)时，确定疑似号码是测试号码，而不是骚扰号码。

[0098] 当被叫号码组中的被叫号码不是预设号码时，若呼叫频率信息大于频率预设阈值，则确定疑似号码是骚扰号码；否则，确定疑似号码不是骚扰号码。

[0099] 步骤709，骚扰号码识别服务器604依据步骤708中确定的骚扰号码，生成并发送屏蔽广播消息至区块链网络中，以使第一运营商节点服务器601、第二运营商节点服务器602和第三运营商节点服务器603获得该骚扰号码，将该骚扰号码加入到黑名单中，禁止骚扰号码的呼叫业务。

[0100] 在本实施例中，通过骚扰号码识别服务器发送客户投诉信息至区块链网络中，使得区块链网络中的各个运营商节点服务器能够通过客户投诉信息查询自己的数据库，以确定是否存在疑似号码，并在确定存在疑似号码时，将该疑似号码发送给骚扰号码识别服务器；和/或，获取其他运营商节点服务器发送的疑似号码的相关信息，与自己的运营商节点服务器内的数据库所查询到的疑似号码的相关信息进行融合，获得并发送融合疑似号码的相关信息给骚扰号码识别服务器，使骚扰号码识别服务器能够综合判断疑似号码中是否存在骚扰号码，进而对骚扰号码进行处理，减少骚扰号码对用户的骚扰，提升用户体验度。

[0101] 可以理解的是，以上实施方式仅仅是为了说明本申请的原理而采用的示例性实施方式，然而本申请并不局限于此。对于本领域内的普通技术人员而言，在不脱离本申请的精神和实质的情况下，可以做出各种变型和改进，这些变型和改进也视为本申请的保护范围。

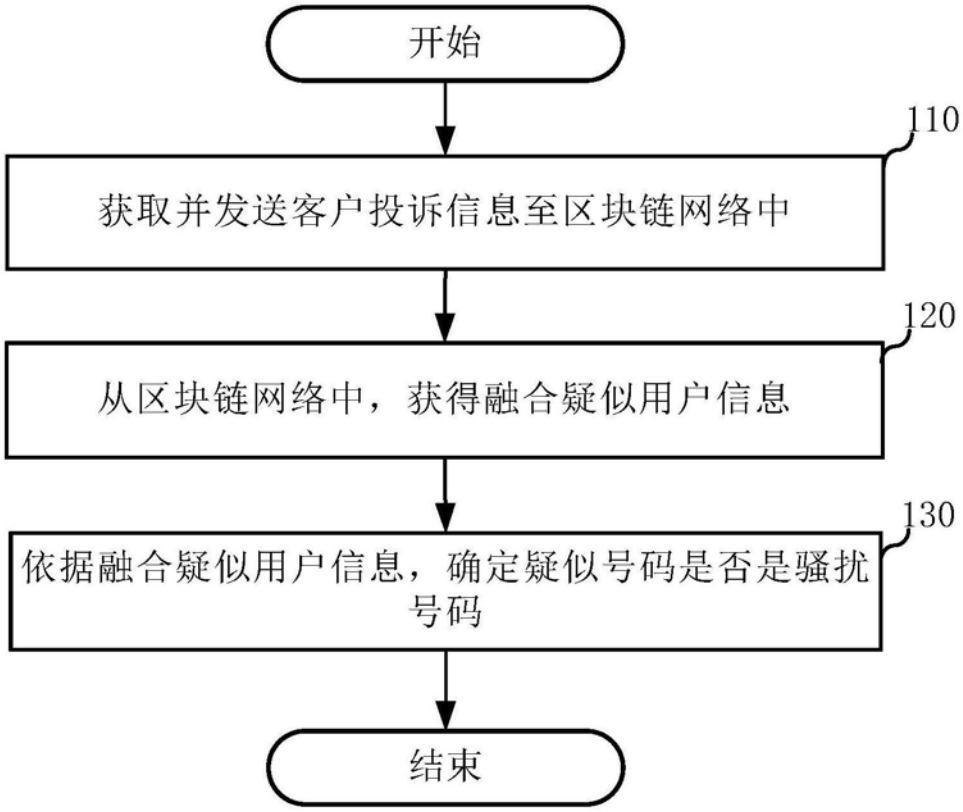

开始
110
获取并发送客户投诉信息至区块链网络中
120
从区块链网络中，获得融合疑似用户信息
130
依据融合疑似用户信息，确定疑似号码是否是骚扰号码
结束

图1

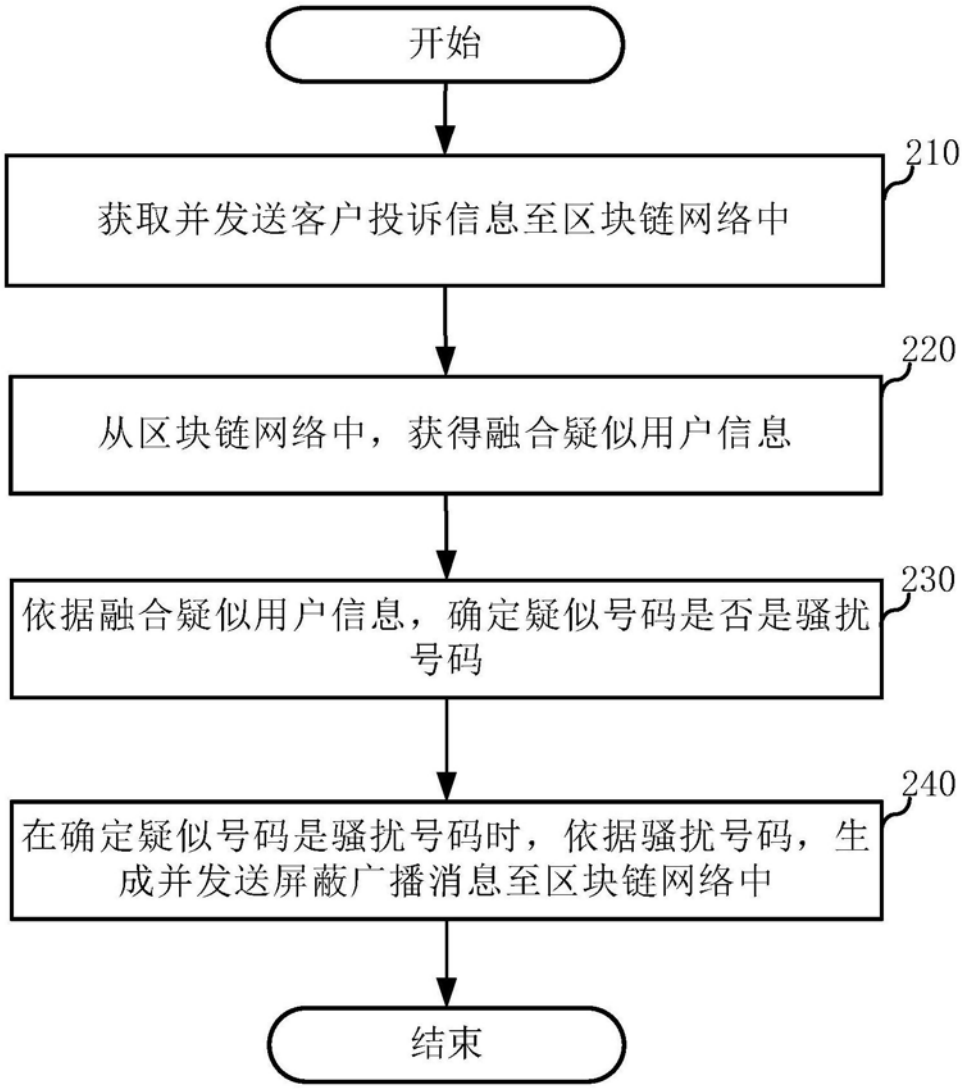

开始
210
获取并发送客户投诉信息至区块链网络中
220
从区块链网络中，获得融合疑似用户信息
230
依据融合疑似用户信息，确定疑似号码是否是骚扰号码
240
在确定疑似号码是骚扰号码时，依据骚扰号码，生成并发送屏蔽广播消息至区块链网络中
结束

图2

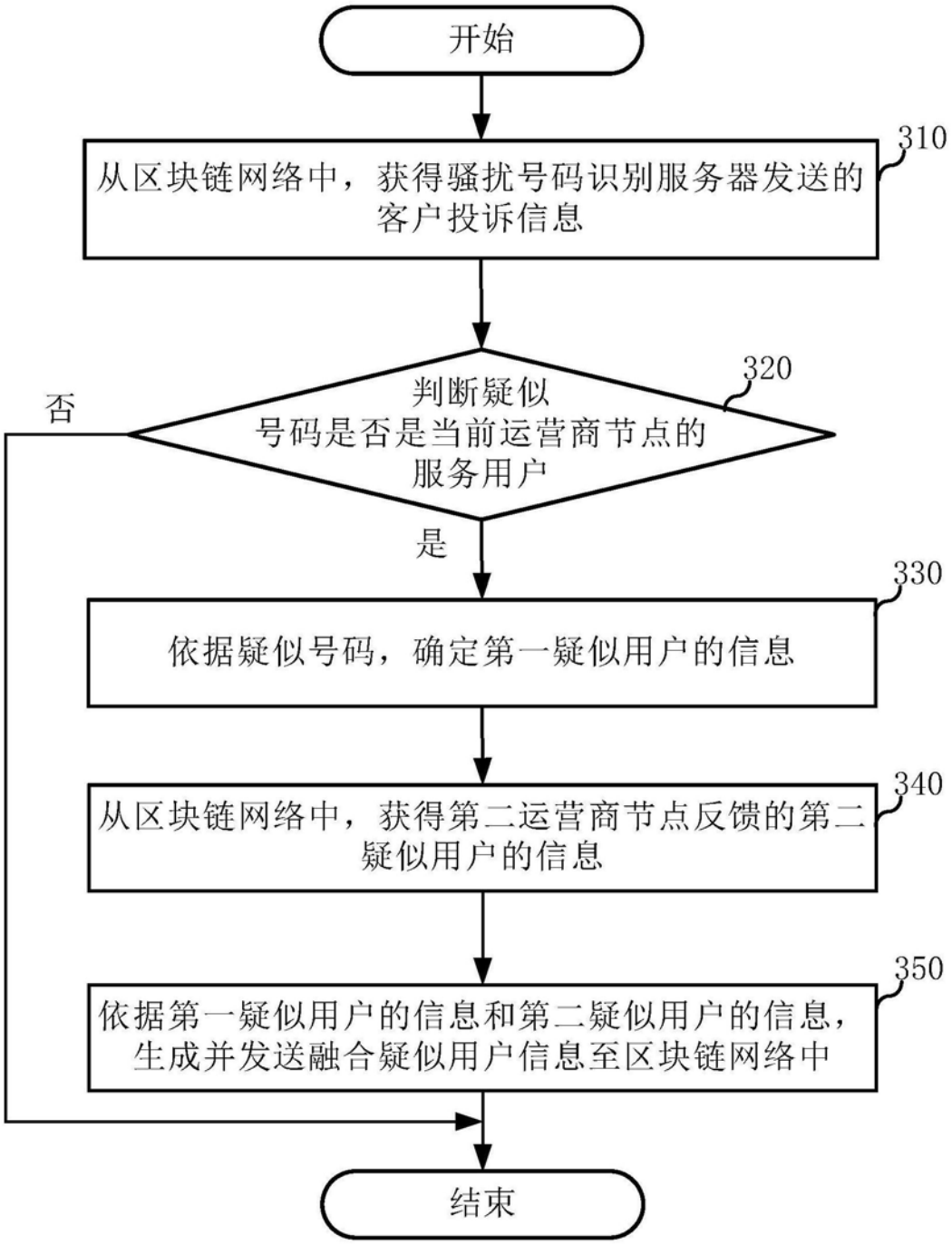

开始
从区块链网络中，获得骚扰号码识别服务器发送的客户投诉信息
310
判断疑似号码是否是当前运营商节点的服务用户
320
否
是
依据疑似号码，确定第一疑似用户的信息
330
从区块链网络中，获得第二运营商节点反馈的第二疑似用户的信息
340
依据第一疑似用户的信息和第二疑似用户的信息，生成并发送融合疑似用户信息至区块链网络中
350
结束

图3

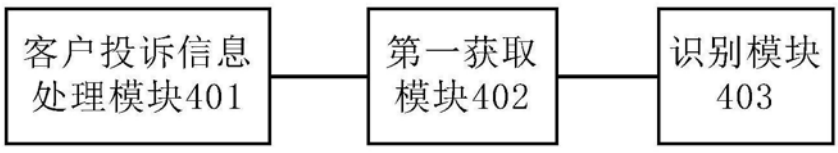

客户投诉信息处理模块401
第一获取模块402
识别模块403

图4

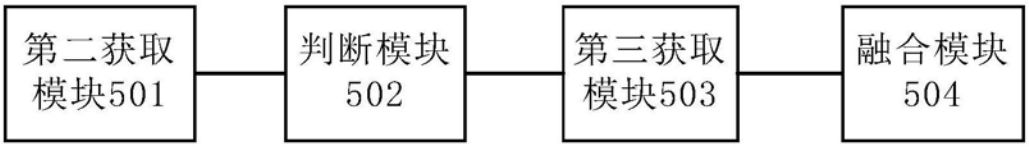

第二获取模块501
判断模块502
第三获取模块503
融合模块504

图5

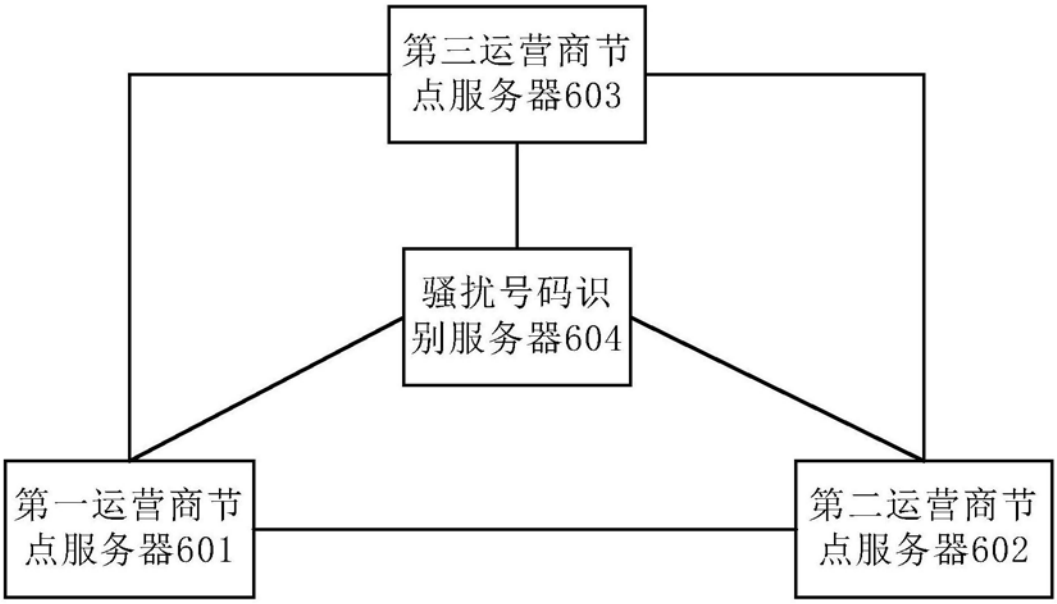

第三运营商节点服务器603
骚扰号码识别服务器604
第一运营商节点服务器601
第二运营商节点服务器602

图6

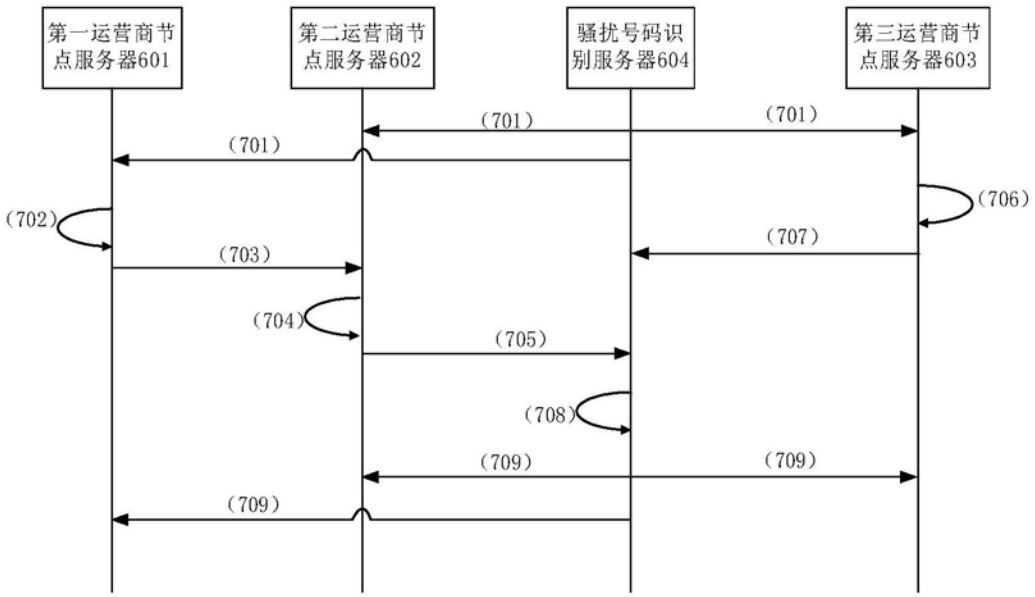

第一运营商节点服务器601
第二运营商节点服务器602
骚扰号码识别服务器604
第三运营商节点服务器603
(701)
(701)
(701)
(702)
(703)
(704)
(705)
(706)
(707)
(708)
(709)
(709)
(709)

图7