(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 110033602 A
(43)申请公布日 2019.07.19

(21)申请号 201811482684.8

(22)申请日 2018.12.05

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 栗志果

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 周嗣勇

(51)Int.Cl.
G08B 25/01(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)
H04M 1/725(2006.01)

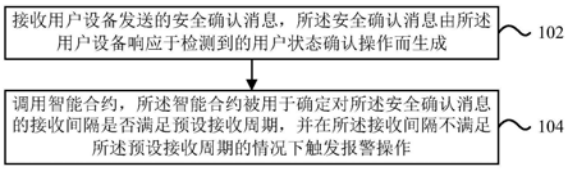
权利要求书2页 说明书8页 附图3页

(54)发明名称

基于区块链的智能报警方法及装置、电子设备

(57)摘要

本说明书一个或多个实施例提供一种基于区块链的智能报警方法及装置、电子设备，应用于区块链节点，所述方法包括：接收用户设备发送的安全确认消息，所述安全确认消息由所述用户设备响应于检测到的用户状态确认操作而生成；调用智能合约，所述智能合约被用于确定对所述安全确认消息的接收间隔是否满足预设接收周期，并在所述接收间隔不满足所述预设接收周期的情况下触发报警操作。



CN 110033602 A

1.一种基于区块链的智能报警方法,应用于区块链节点,所述方法包括:

接收用户设备发送的安全确认消息,所述安全确认消息由所述用户设备响应于检测到的用户状态确认操作而生成;

调用智能合约,所述智能合约被用于确定对所述安全确认消息的接收间隔是否满足预设接收周期,并在所述接收间隔不满足所述预设接收周期的情况下触发报警操作。

2.根据权利要求1所述的方法,所述安全确认消息由所述用户设备的使用者通过对应的数字身份进行签名。

3.根据权利要求1所述的方法,所述安全确认消息中包含所述用户设备所处环境的环境描述信息。

4.根据权利要求3所述的方法,所述环境描述信息包括以下至少之一:所述用户设备拍摄的照片或视频、所述用户设备采集的音频、所述用户设备采集的定位信息、所述用户设备生成的轨迹信息。

5.根据权利要求1所述的方法,所述智能合约还用于在触发报警操作时,向报警对象提供已收到的来自所述用户设备的安全确认消息。

6.根据权利要求1所述的方法,还包括:

分析所述安全确认消息包含的内容;

向所述智能合约传递分析结果,使所述智能合约在根据所述分析结果确认存在异常内容时,触发所述报警操作。

7.根据权利要求1所述的方法,还包括:

将所述安全确认消息和/或所述安全确认消息的数字摘要信息发布至区块链。

8.一种基于区块链的智能报警装置,应用于区块链节点,所述装置包括:

接收单元,接收用户设备发送的安全确认消息,所述安全确认消息由所述用户设备响应于检测到的用户状态确认操作而生成;

调用单元,调用智能合约,所述智能合约被用于确定对所述安全确认消息的接收间隔是否满足预设接收周期,并在所述接收间隔不满足所述预设接收周期的情况下触发报警操作。

9.根据权利要求8所述的装置,所述安全确认消息由所述用户设备的使用者通过对应的数字身份进行签名。

10.根据权利要求8所述的装置,所述安全确认消息中包含所述用户设备所处环境的环境描述信息。

11.根据权利要求10所述的装置,所述环境描述信息包括以下至少之一:所述用户设备拍摄的照片或视频、所述用户设备采集的音频、所述用户设备采集的定位信息、所述用户设备生成的轨迹信息。

12.根据权利要求8所述的装置,所述智能合约还用于在触发报警操作时,向报警对象提供已收到的来自所述用户设备的安全确认消息。

13.根据权利要求8所述的装置,还包括:

分析单元,分析所述安全确认消息包含的内容;

传递单元,向所述智能合约传递分析结果,使所述智能合约在根据所述分析结果确认存在异常内容时,触发所述报警操作。

14.根据权利要求8所述的装置,还包括:

发布单元,将所述安全确认消息和/或所述安全确认消息的数字摘要信息发布至区块链。

15.一种电子设备,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器通过运行所述可执行指令以实现如权利要求1-7中任一项所述的方法。

基于区块链的智能报警方法及装置、电子设备

技术领域

[0001] 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于区块链的智能报警方法及装置、电子设备。

背景技术

[0002] 在相关技术中，用户在面临紧急状况时，可以通过手机拨打报警电话(或其他紧急电话)的方式进行报警。但是，成功报警的前提是：用户能够及时发现紧急状况、成功拿出手机，并顺利拨号或按压手机上的组合按键。

发明内容

[0003] 有鉴于此，本说明书一个或多个实施例提供一种基于区块链的智能报警方法及装置、电子设备。

[0004] 为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[0005] 根据本说明书一个或多个实施例的第一方面，提出了一种基于区块链的智能报警方法，应用于区块链节点，所述方法包括：

[0006] 接收用户设备发送的安全确认消息，所述安全确认消息由所述用户设备响应于检测到的用户状态确认操作而生成；

[0007] 调用智能合约，所述智能合约被用于确定对所述安全确认消息的接收间隔是否满足预设接收周期，并在所述接收间隔不满足所述预设接收周期的情况下触发报警操作。

[0008] 根据本说明书一个或多个实施例的第二方面，提出了一种基于区块链的智能报警装置，应用于区块链节点，所述装置包括：

[0009] 接收单元，接收用户设备发送的安全确认消息，所述安全确认消息由所述用户设备响应于检测到的用户状态确认操作而生成；

[0010] 调用单元，调用智能合约，所述智能合约被用于确定对所述安全确认消息的接收间隔是否满足预设接收周期，并在所述接收间隔不满足所述预设接收周期的情况下触发报警操作。

[0011] 根据本说明书一个或多个实施例的第三方面，提出了一种电子设备，包括：

[0012] 处理器；

[0013] 用于存储处理器可执行指令的存储器；

[0014] 其中，所述处理器通过运行所述可执行指令以实现如上述实施例中所述的方法。

附图说明

[0015] 图1是一示例性实施例提供的一种基于区块链的智能报警方法的流程图。

[0016] 图2是一示例性实施例提供的一种智能报警的整体架构示意图。

[0017] 图3是一示例性实施例提供的一种用于实现智能报警的交互示意图。

[0018] 图4是一示例性实施例提供的一种设备的结构示意图。

[0019] 图5是一示例性实施例提供的一种基于区块链的智能报警装置的框图。

具体实施方式

[0020] 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说明书一个或多个实施例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、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[0021] 需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[0022] 图1是一示例性实施例提供的一种基于区块链的智能报警方法的流程图。如图1所示，该方法应用于区块链节点，可以包括以下步骤：

[0023] 步骤102，接收用户设备发送的安全确认消息，所述安全确认消息由所述用户设备响应于检测到的用户状态确认操作而生成。

[0024] 在一实施例中，用户设备可以为用户使用的手机、平板电脑、智能手表等任意类型的电子设备，本说明书并不对此进行限制。通过在电子设备上登录用户的已注册账号、使用该用户实名登记的电话卡或预先将电子设备的MAC地址等标识与用户进行绑定，可以建立该电子设备与用户之间的唯一映射关系，使得该电子设备可以被认定为该用户对应的用户设备。

[0025] 在一实施例中，区别于用户在紧急状况下实施报警等触发动作，用户可以在尚未面临紧急状况之前、处于安全状态的情况下，针对用户设备实施用户状态确认操作，以表明该用户尚处于安全状态下。用户可以在用户设备上进行设定，以确定是否需要开启智能报警功能，该智能报警功能用于实现本说明书的智能报警方案；换言之，当该智能报警功能被开启时，即可基于本说明书的技术方案实现智能报警。其中，用户可以手动开关智能报警功能，也可以设定一定的判断规则，以使得用户设备可以基于该判断规则自动开关智能报警功能；例如，判断规则可以包括时间范围，譬如该时间范围可以为每天晚上的9点-12点，使得当处于时间范围时用户设备可以自动开启智能报警功能，否则自动关闭智能报警功能；再例如，判断规则可以包括地理位置范围，譬如该地理位置范围可以为犯罪率较高的地区，使得当用户设备处于该地理位置范围时可以自动开启智能报警功能，否则自动关闭智能报警功能；又例如，判断规则可以包括时间范围和地理位置范围，使得当处于时间范围且用户设备处于该地理位置范围时，用户设备可以自动开启智能报警功能，否则自动关闭智能报警功能。

[0026] 在一实施例中，用户状态确认操作可以包括：解锁用户设备、开启用户设备的摄像头、通过用户设备的摄像头进行拍摄等至少之一，本说明书并不对此进行限制。

[0027] 在一实施例中，用户设备的使用者预先获得对应的数字身份，并向用户设备进行授权，使得用户设备可以基于该数字身份对所发送的安全确认消息进行签名，而区块链节

点可以据此对安全确认消息的发送方进行身份验证，以识别出非法用户冒用身份的行为。同时，当发现存在非法用户冒用身份的行为时，可以判定用户设备的使用者存在较高的面临紧急状态的风险，从而向该用户设备的使用者进行风险提醒；或者，用户设备的使用者甚至可能已经面临紧急状况，可以通过触发报警操作，向警方及时汇报相关信息，以便确认使用者的真实处境，从而解除安全风险。

[0028] 在一实施例中，当用户设备基于使用者的数字身份对所发送的安全确认消息进行签名时，使得使用者即便并未登录已注册账号、用户设备并未使用该用户实名登记的电话卡、用户设备的MAC地址等标识并未预先与该使用者进行绑定的情况下，也可以通过该签名来表明使用者的身份。

[0029] 步骤104，调用智能合约，所述智能合约被用于确定对所述安全确认消息的接收间隔是否满足预设接收周期，并在所述接收间隔不满足所述预设接收周期的情况下触发报警操作。

[0030] 在一实施例中，当用户已经面临紧急状况时，比如抢劫、绑架等，一方面用户可能受到犯罪分子的威胁而无法顺利拿出用户设备进行操作，或者用户设备可能已经被犯罪分子抢夺或损毁，另一方面用户可能已经丧失了对用户设备进行操作的能力(如受伤或晕厥等)，因而本说明书中通过在用户处于安全状态时实施用户状态确认操作、并由区块链节点接收和统计用户设备相应发送的安全确认消息，可以在安全确认消息的接收状况异常(如接收间隔不满足预设接收周期)时，推测出用户可能已经面临紧急状况，而无需用户在面临紧急状况时实施任何操作，既可以降低用户的操作难度、提升对用户状态的判断准确度，又能够避免用户在紧急状况下对用户设备的操作引起犯罪分子的疑虑或激怒犯罪分子，有助于保障用户的人身安全。

[0031] 在一实施例中，通过调用智能合约对安全确认消息的接收状况进行识别确认，可以确保该识别确认的操作能够自动、可靠地实施，不易受到影响，从而准确触发报警操作，以维护用户的人身安全。

[0032] 在一实施例中，当安全确认消息的接收间隔过大，比如超出预设接收周期且差值大于预设数值时，用户很可能已经面临紧急状况而无法实施用户状态确认操作，可以判定为不满足该预设接收周期，从而触发报警操作；或者，当安全确认消息的接收间隔过小，比如同一预设接收周期内收到多条安全确认消息时，用户很可能已经面临紧急状况但不便于实施报警等容易引起犯罪分子的疑虑或激怒犯罪分子的操作，因而可以连续实施用户状态确认操作而造成安全确认消息的异常发送，此时可以判定为不满足该预设接收周期，从而触发报警操作。

[0033] 在一实施例中，当智能报警功能被开启时，用户设备可以基于上述的预设接收周期向用户发出提示，以使得用户在处于安全状态的情况下，按时完成用户状态确认操作，避免由于忘记操作等原因而造成安全确认消息的发送状况出现异常，防止由此造成的误报警。

[0034] 在一实施例中，所述智能合约还用于在触发报警操作时，向报警对象提供已收到的来自所述用户设备的安全确认消息，以供报警对象(如警方)进行参考，比如报警对象可以对安全确认消息的数量、发送方、接收间隔等进行确认，从而分析出相关用户是否已面临紧急状况等。

[0035] 在一实施例中，所述安全确认消息中包含所述用户设备所处环境的环境描述信息。例如，所述环境描述信息可以包括以下至少之一：所述用户设备拍摄的照片或视频、所述用户设备采集的音频、所述用户设备采集的定位信息、所述用户设备生成的轨迹信息等，本说明书并不对此进行限制。那么，通过将安全确认消息提供至报警对象，尤其是当安全确认消息包含上述的环境描述信息时，有助于报警对象据此确认相关用户的所处位置、周边建筑，甚至从照片、音频或视频中分辨出疑似犯罪分子或者分析出可能面临何种紧急状况等，使得报警对象更好地协助相关用户脱离紧急状况。

[0036] 在一实施例中，区块链节点可以将安全确认消息和/或所述安全确认消息的数字摘要信息(如哈希值)发布至区块链，可以对安全确认消息进行存证，以便于后续查阅、管理或追责。

[0037] 在一实施例中，区块链节点可以分析所述安全确认消息包含的内容，并向所述智能合约传递分析结果，使所述智能合约在根据所述分析结果确认存在异常内容时，触发所述报警操作。用户在实施用户状态确认操作时，可能尚未意识到已经面临紧急状况或者存在面临紧急状况的风险，或者犯罪分子在实施犯罪后可能模拟用户行为而实施用户状态确认操作，使得区块链节点对安全确认消息的接收间隔并无异常，此时可以通过对安全确认消息包含的内容进行分析，比如照片或视频中包含的人、地点、行为(如打斗、求救手势等)等信息，视频或音频中出现的哭叫、求救等声音，非正常的定位信息或轨迹信息等，以分析出可能存在的安全问题，从而及时触发报警操作。

[0038] 图2是一示例性实施例提供的一种智能报警的整体架构示意图。如图2所示，假定用户A使用手机21的过程中，可以针对该手机21实施用户状态确认操作，而手机21可以据此生成相应的安全确认消息，并将该安全确认消息发送至服务器22。进一步地，服务器22可以通过调用智能合约，对安全确认消息的接收情况予以确认，从而在达到预设条件时，自动触发报警操作。

[0039] 为了便于理解，下面针对手机21、服务器22分别在智能报警过程中实现的操作和功能，结合图3对本说明书的智能报警方案进行详细说明。图3是一示例性实施例提供的一种用于实现智能报警的交互示意图。如图3所示，该交互过程可以包括以下步骤：

[0040] 步骤301，在手机21与服务器22之间实现对绑定关系的建立。

[0041] 在一实施例中，所需建立的绑定关系为用户A的身份信息与手机21的设备信息之间的绑定关系。基于该绑定关系，使得服务器22在接收到手机21后续发送的安全确认消息时，可以确认该安全确认消息对应于该用户A。

[0042] 例如，用户A可以预先在服务器22处进行账号注册，得到与用户A唯一对应的已注册账号。然后，用户A可以通过在手机21上登录该已注册账号，而服务器22基于该已注册账号在手机21上的登录信息，确定该已注册账号(对应于用户A)与手机21之间建立了绑定关系。类似地，用户A可以在手机21上使用已实名登记的手机号码，同样可以使得服务器22确定该手机号码(对应于用户A)与手机21之间建立了绑定关系。

[0043] 步骤302，手机21启用智能报警功能。

[0044] 在一实施例中，手机21可以默认关闭智能报警功能，而用户A可以在需要时临时开启该智能报警功能；比如，当用户A在某一天加班到较晚时，可以通过开启该智能报警功能，以保障回家途中的安全性。

[0045] 在一实施例中，手机21可以通过对预设条件的判断，以自动开启和关闭智能报警功能。例如，用户A可以设定该预设条件包括：a.时间条件为晚上10点至次日凌晨4点、b.地理位置条件为处于某摄像头未覆盖区域；那么，通过对时间信息和地理位置信息的综合判断，比如当手机21在晚上11点处于上述的摄像头未覆盖区域时，可以判定为满足上述的预设条件，因而可以自动开启智能报警功能；而当未处于上述时间段或离开相关摄像头未覆盖区域时，手机21可以自动关闭智能报警功能。

[0046] 步骤303，手机21可以在提醒时刻实施操作提醒。

[0047] 在一实施例中，基于本说明书的技术方案，当智能报警功能开启时，用户A需要定期实施预定义的用户状态确认操作，以表明自身尚处于安全状态。而为了避免用户A由于忘记实施该用户状态确认操作而导致误判，手机21可以按照预设周期确定相应的提醒时刻，从而在提醒时刻针对用户A实施操作提醒，使得用户A可以按时实施用户状态确认操作。

[0048] 针对用户状态确认操作的提醒可以为用户A预定义的特殊提醒方式，且提醒内容避免透露与智能报警功能相关的信息，比如当用户状态确认操作为拍摄操作时，可以输出“请拍摄照片”或类似的提醒内容，而避免输出“请拍摄至少一张照片，以确认自身处于安全状态，否则将触发报警”或类似的提醒内容，从而在用户A已面临紧急状况的情况下，防止向犯罪分子发出提示，避免犯罪分子模拟或胁迫用户A实施相关操作。甚至，可以避免在提醒内容中包含与操作类型相关的信息，比如可以输出“请执行预设操作”或类似的提醒内容，而避免输出“请拍摄照片”或类似的提醒内容。

[0049] 步骤304，手机21检测到拍摄操作。

[0050] 在一实施例中，当预定义的用户状态确认操作为拍摄操作时，如果用户A尚处于安全状态，可以主动或在上述操作提醒的提示作用下，开启手机21的摄像头以实施拍摄操作，比如拍摄至少一张照片。

[0051] 当然，用户状态确认操作可以包括其他类型，比如对手机21进行解锁、在手机21上输入特定字符串等，本说明书并不对此进行限制。

[0052] 步骤305，手机21收集环境描述信息。

[0053] 在一实施例中，在用户A实施预定义的用户状态确认操作之前、过程中或之后，手机21可以对所处环境进行信息采集，得到相应的环境描述信息，以用于从更多维度、更为详细地描述手机21或用户A所处的环境。比如，该环境描述信息可以包括：手机21在步骤304中拍摄的照片、手机21在摄像头开启后采集的视频、手机21采集的音频、手机21采集的定位信息、手机21生成的轨迹信息等，本说明书并不对此进行限制。

[0054] 步骤306，手机21向服务器22发送安全确认消息。

[0055] 在一实施例中，安全确认消息可以包含上述的环境描述信息。此外，用户A可以预先注册得到唯一对应的数字身份，该数字身份由一组公私钥对进行表征；相应地，手机21可以通过对应于用户A的数字身份的私钥对安全确认消息进行签名。

[0056] 步骤307，服务器22可以对收到的安全确认消息进行签名验证。

[0057] 在一实施例中，服务器22收到手机21上传的安全确认消息后，可以通过用户A对应的公钥进行验签，以确定该安全确认消息已由用户A进行授权，且并非由不法分子冒充用户A的身份进行发送。

[0058] 在一实施例中，当验签未通过时，由于手机21预先绑定至用户A，表明可能存在不

法分子冒充用户A的身份，而用户A存在处于紧急状况的风险，服务器22可以触发报警操作。

[0059] 步骤308，服务器22调用智能合约，以验证接收间隔是否合规。

[0060] 在一实施例中，服务器22上运行有区块链的客户端，使得该服务器22被配置为一区块链节点，而服务器22可以据此调用智能合约，并将对安全确认消息的接收时刻输入智能合约，以由智能合约验证来自手机21的安全确认消息的接收间隔是否符合预设接收周期。

[0061] 例如，假定预设接收周期为5分钟、预警时长为3分钟，那么假定最近一次为22:20接收到手机21发送的安全确认消息，那么正常情况下应当在22:25左右收到手机21再次发送的安全确认消息；而考虑到用户A的操作无法十分准时，上述3分钟的预警时长可以作为容错时间段，那么如果在22:28仍未收到手机21再次发送的安全确认消息，智能合约可以判定为用户A并未按时实施用户状态确认操作，用户A具有较大概率面临了紧急状况，因而智能合约可以自动触发报警操作。

[0062] 再例如，假定预设接收周期为5分钟，那么假定最近一次为22:20接收到手机21发送的安全确认消息，那么正常情况下应当在22:25左右收到手机21再次发送的安全确认消息；而智能合约如果在22:22就再次收到手机21再次发送的安全确认消息，甚至连续收到多条安全确认消息，那么智能合约可以判定为用户A可能已经面临了紧急状况，并希望通过上述的异常操作发出警告，因而智能合约可以自动触发报警操作。

[0063] 步骤309，服务器22通过调用智能合约，验证环境描述信息。

[0064] 在一实施例中，当安全确认消息包含环境描述信息时，服务器22可以提取该环境描述信息或其进一步包含的信息内容，并将该环境描述信息或信息内容输入智能合约，以由智能合约进行检验。

[0065] 在一实施例中，智能合约对安全确认消息的接收间隔可能验证通过，但通过对上述环境描述信息或信息内容进行分析，比如拍摄的照片中是否包含可疑人员(比如通过人脸识别确定照片中的人具有犯罪前科等)、拍摄的视频中是否包含正在发生的犯罪行为、拍摄的视频或采集的音频中是否包含打斗声或呼救声等，可以进一步确定已收到的安全确认消息是否为用户A在安全状态下发送，是否存在犯罪分子模拟用户A或胁迫用户A实施用户状态确认操作的情况等。如果发现存在犯罪分子模拟用户A或胁迫用户A的情况或风险，智能合约可以触发报警操作。

[0066] 在一实施例中，当智能合约已经验证为安全确认消息的接收间隔不正常时，可以通过对环境描述信息或信息内容进行分析，以获取用户A的周边环境(如街道状态、周边建筑等)、周围人员、地理位置信息、行走轨迹信息以及用户A的面部表情、发出的声音和行为动作等，并在实施报警操作时将相关信息提供至报警对象，以便于报警对象实施更为准确的分析和更有效的处理措施。

[0067] 需要指出的是，当手机21的智能报警功能处于开启状态时，将持续循环实施上述的步骤303～309，从而对用户A实现持续保护，直至用户A到达安全区域并关闭该智能报警功能。

[0068] 图4是一示例性实施例提供的一种设备的示意结构图。请参考图4，在硬件层面，该设备包括处理器402、内部总线404、网络接口406、内存408以及非易失性存储器410，当然还可能包括其他业务所需要的硬件。处理器402从非易失性存储器410中读取对应的计算机程

序到内存408中然后运行，在逻辑层面上形成基于区块链的智能报警装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[0069] 请参考图5，在软件实施方式中，该基于区块链的智能报警装置应用于区块链节点，可以包括：

[0070] 接收单元51，接收用户设备发送的安全确认消息，所述安全确认消息由所述用户设备响应于检测到的用户状态确认操作而生成；

[0071] 调用单元52，调用智能合约，所述智能合约被用于确定对所述安全确认消息的接收间隔是否满足预设接收周期，并在所述接收间隔不满足所述预设接收周期的情况下触发报警操作。

[0072] 可选的，所述安全确认消息由所述用户设备的使用者通过对应的数字身份进行签名。

[0073] 可选的，所述安全确认消息中包含所述用户设备所处环境的环境描述信息。

[0074] 可选的，所述环境描述信息包括以下至少之一：所述用户设备拍摄的照片或视频、所述用户设备采集的音频、所述用户设备采集的定位信息、所述用户设备生成的轨迹信息。

[0075] 可选的，所述智能合约还用于在触发报警操作时，向报警对象提供已收到的来自所述用户设备的安全确认消息。

[0076] 可选的，还包括：

[0077] 分析单元53，分析所述安全确认消息包含的内容；

[0078] 传递单元54，向所述智能合约传递分析结果，使所述智能合约在根据所述分析结果确认存在异常内容时，触发所述报警操作。

[0079] 可选的，还包括：

[0080] 发布单元55，将所述安全确认消息和/或所述安全确认消息的数字摘要信息发布至区块链。

[0081] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0082] 本说明书提出了一种计算机可读介质，其上存储有计算机指令，该指令被处理器执行时实现本说明书的技术方案，比如上述任一实施例的基于区块链的智能报警方法，此处不再一一赘述。

[0083] 在一个典型的配置中，计算机包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0084] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0085] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法

或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0086] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0087] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[0088] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0089] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0090] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

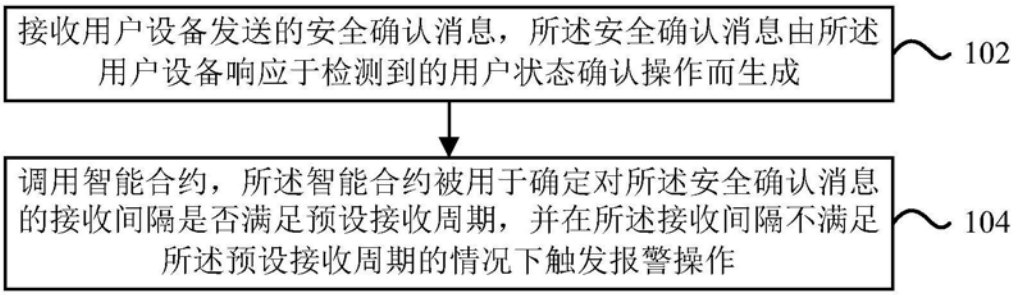

接收用户设备发送的安全确认消息，所述安全确认消息由所述用户设备响应于检测到的用户状态确认操作而生成
102
调用智能合约，所述智能合约被用于确定对所述安全确认消息的接收间隔是否满足预设接收周期，并在所述接收间隔不满足所述预设接收周期的情况下触发报警操作
104

图1

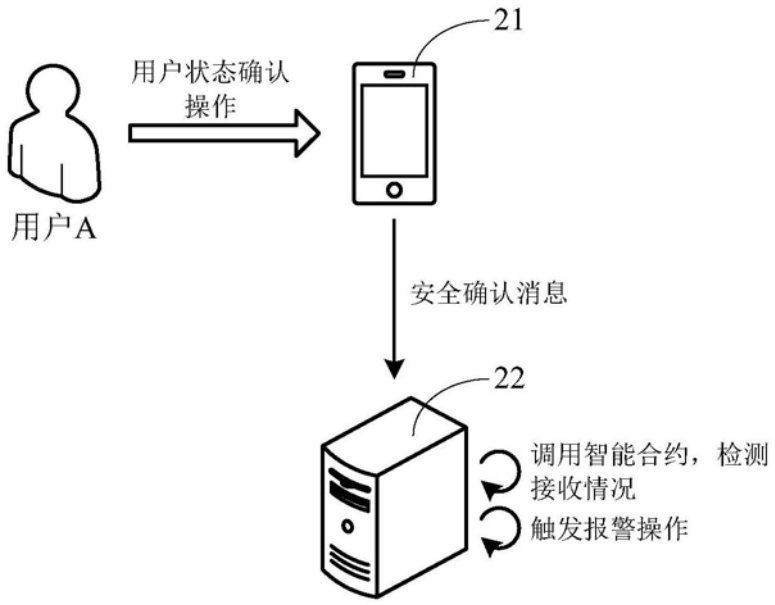

21
用户状态确认操作
用户A
安全确认消息
22
调用智能合约，检测接收情况
触发报警操作

图2

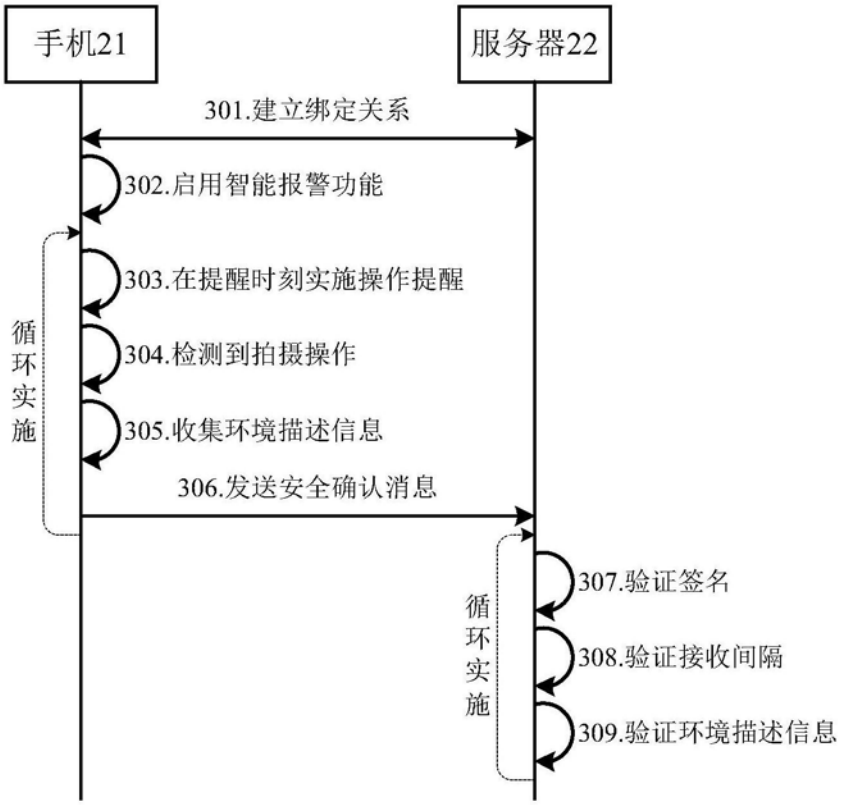

手机21
服务器22
301.建立绑定关系
302.启用智能报警功能
303.在提醒时刻实施操作提醒
304.检测到拍摄操作
305.收集环境描述信息
循环实施
306.发送安全确认消息
307.验证签名
308.验证接收间隔
309.验证环境描述信息
循环实施

图3

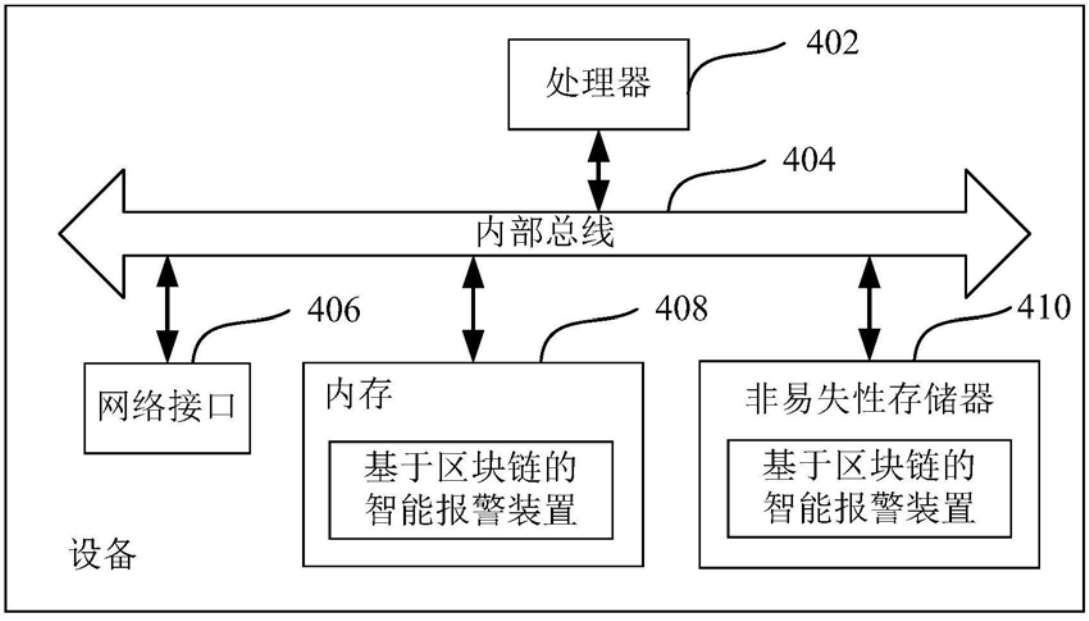

处理器
402
404
内部总线
406
408
410
网络接口
内存
基于区块链的智能报警装置
非易失性存储器
基于区块链的智能报警装置
设备

图4

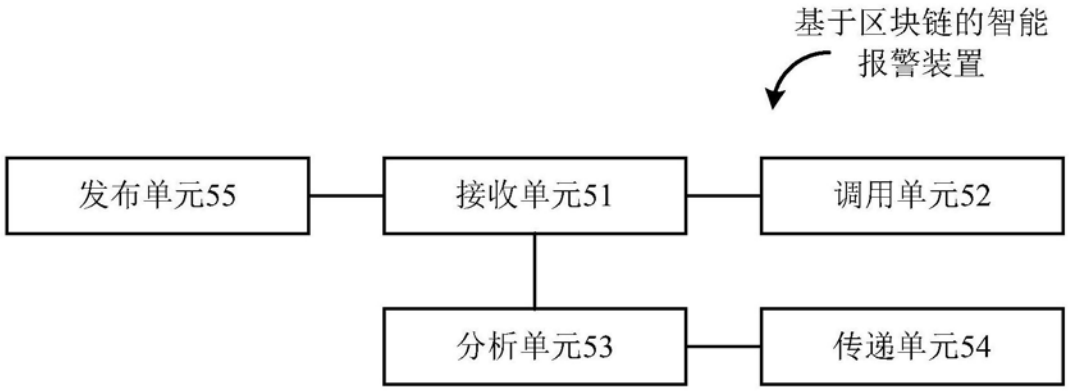


图5