(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 12 月 24 日 (24.12.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/253230 A1

(51) 国际专利分类号:
H04W 12/00 (2009.01) *H04W 12/10* (2009.01)
G07C 1/20 (2006.01)

(21) 国际申请号: PCT/CN2020/071563

(22) 国际申请日: 2020 年 1 月 11 日 (11.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910521227.3 2019年6月17日 (17.06.2019) CN

(71) 申请人: 创新先进技术有限公司 (**ADVANCED NEW TECHNOLOGIES CO., LTD.**) [—/CN]; 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心, Grand Cayman KY1-9008 (KY)。

(72) 发明人: **蔡鸿博(CAI, Hongbo)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **黄凯明(HUANG, Kaiming)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **韩喆(HAN, Zhe)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **姜世琦(JIANG, Shiqi)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **杨磊(YANG, Lei)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街9号嘉华大厦B座409, Beijing 100085 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,

(54) **Title:** BLOCK CHAIN-BASED PATROL INSPECTION AND DEPOSIT METHOD AND APPARATUS, AND ELECTRONIC DEVICE

(54) **发明名称**: 基于区块链的巡检存证方法、装置和电子设备

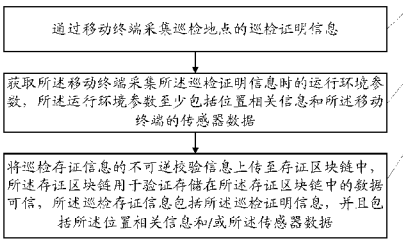


图 2

S21 Collect patrol inspection certification information of a patrol inspection place by means of a mobile terminal

S23 Acquire operating environment parameters of the mobile terminal when the mobile terminal collects the patrol inspection certification information, the operating environment parameters at least including position related information and sensor data of the mobile terminal

S25 Upload irreversible check information of patrol inspection and deposit information to a deposit block chain, the deposit block chain being used to verify that data stored in the deposit block chain is trusted, and the patrol inspection and deposit information including the patrol inspection certification information, and including the position related information and/or the sensor data

(57) **Abstract:** The embodiments of the present application disclose a block chain-based patrol inspection and deposit method, and an electronic device. Said method comprises: collecting patrol inspection certification information of a patrol inspection place by means of a mobile terminal, and acquiring operating environment parameters of the mobile terminal when the mobile terminal collects the patrol inspection certification information, the operating environment parameters at least including position related information and sensor data of the mobile terminal, and then uploading irreversible check information of the patrol inspection certification information, the position related information and the sensor data to a deposit block chain, the deposit block chain being used to verify that data stored in the deposit block chain is trusted.

(57) **摘要**: 本申请实施例公开了一种基于区块链的巡检存证方法、装置和电子设备，该方法包括：通过移动终端采集巡检地点的巡检证明信息，同时，获取移动终端采集巡检证明信息时的运行环境参数，运行环境参数至少包括位置相关信息和移动终端的传感器数据，再将巡检证明信息、位置相关信息和传感器数据的不可逆校验信息上传至存证区块链中，其中，存证区块链用于验证存储在存证区块链中的数据可信。

WO 2020/253230 A1

[见续页]

AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

基于区块链的巡检存证方法、装置和电子设备

技术领域

[01]本申请涉及计算机技术领域，尤其涉及一种基于区块链的巡检存证方法、装置和电子设备。

背景技术

[02]大量线下场所中，如商场，写字楼，学校，工厂，酒店，住宅等，都需要定期持续的进行消防、安全等巡逻检查任务。目前，主要巡检方法为人工方式，具体为值班人员在指点时间或按照指定频次到达指定巡检地点，对场所的安全状况进行巡检确认。由于绝大部分巡检由人工完成且无监督机制，无数据记录，导致事后原因确认和责任追溯成本高或难实现。

发明内容

[03]本申请实施例的目的是提供一种基于区块链的巡检存证方法、装置和电子设备，能够较方便地实现信息记录的可追溯以及不可篡改。

[04]为解决上述技术问题，本申请实施例是这样实现的：

[05]本申请实施例提供一种基于区块链的巡检存证方法，包括：

[06]通过移动终端采集巡检地点的巡检证明信息；

[07]获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据；

[08]将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

[09]本申请实施例还提供一种基于区块链的巡检存证方法，包括：

[10]通过移动终端采集巡检地点的巡检证明信息；

[11]获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据；

[12]基于所述位置相关信息和所述传感器数据对所述巡检地点进行可信验证;

[13]当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息至少包括所述巡检证明信息。

[14]本申请实施例还提供一种巡检验证方法，包括:

[15]接收检验人员输入的筛选条件，所述筛选条件用于筛选指定巡检人员在指定巡检地点的巡检存证信息;

[16]根据所述筛选条件，查询所述指定巡检人员和所述指定巡检地点对应的巡检存证信息;

[17]基于存证区块链中存储的所述指定巡检人员和所述指定巡检地点对应的不可逆校验信息，对所述巡检存证信息进行可信验证。

[18]本申请实施例还提供一种基于区块链的巡检存证装置，包括:

[19]证明信息采集模块，采集巡检地点的巡检证明信息;

[20]环境参数采集模块，获取采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据;

[21]信息存储模块，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

[22]本申请实施例还提供一种基于区块链的巡检存证装置，包括:

[23]证明信息采集模块，采集巡检地点的巡检证明信息;

[24]环境参数采集模块，获取采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据;

[25]可信验证模块，基于所述位置相关信息和所述传感器数据对所述巡检地点进行可信验证;

[26]证明信息存储模块，当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息至少包括所述巡检证明信息。

[27]本申请实施例还提供一种巡检验证装置，包括:

[28]条件接收模块，接收检验人员输入的筛选条件，所述筛选条件用于筛选指定巡检人员在指定巡检地点的巡检存证信息;

[29]文件查询模块，根据所述筛选条件，查询所述指定巡检人员和所述指定巡检地点对应的巡检存证信息;

[30]文件验证模块，基于存证区块链中存储的所述指定巡检人员和所述指定巡检地点对应的的不可逆校验信息，对所述巡检存证信息进行可信验证。

[31]本申请实施例还提供一种计算机设备，包括：存储器、处理器和存储在所述存储器上并可在所述处理器上运行的计算机可执行指令，所述计算机可执行指令被所述处理器执行时实现以下操作:

[32]通过移动终端采集巡检地点的巡检证明信息;

[33]获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据;

[34]将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

[35]本申请实施例还提供一种计算机可读存储介质，其特征在于，包括：所述计算机可读存储介质用于存储计算机可执行指令，所述计算机可执行指令被处理器执行时实现以下操作:

[36]通过移动终端采集巡检地点的巡检证明信息;

[37]获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据;

[38]将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

[39]由以上本申请实施例提供的技术方案可见，本申请实施例方案能够达到以下有益效果:

[40]通过采用区块链技术对巡检证明信息和运行环境参数进行存储，能够较方便地实现

巡检信息记录的可追溯以及不可篡改，一旦需要追溯信息记录，便可以通过区块链存储的巡检信息记录实现事件原因的确认，并保证追溯的信息记录可信，以此可提高巡检人员巡检信息记录的置信度和可追溯性，进而提高场所安全性，降低安全问题发生的概率。

附图说明

[41]此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[42]图 1 为本申请的一个实施例提供的一种巡检点位标定方法的流程图。

[43]图 2 为本申请的一个实施例提供的一种基于区块链的巡检存证方法的流程图。

[44]图 3 为本申请的另一个实施例提供的一种基于区块链的巡检存证方法的流程图。

[45]图 4 为本申请的一个实施例提供的一种巡检验证方法的流程图。

[46]图 5 为本申请的一个实施例提供的一种基于区块链的巡检存证装置的结构示意图。

[47]图 6 为本申请的另一个实施例提供的一种基于区块链的巡检存证装置的结构示意图。

[48]图 7 为本申请的一个实施例提供的一种巡检验证装置的结构示意图。

[49]图 8 为本申请的一个实施例提供的一种电子设备的结构示意图。

[50]图 9 为本申请的一个实施例提供的另一种电子设备的结构示意图。

具体实施方式

[51]为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[52]以下结合附图，详细说明本申请各实施例提供的技术方案。

[53]本申请实施例的主要流程为：巡检管理人员通过移动终端在待标定地点完成点位标定，巡检人员利用移动终端到标定点位进行巡检打卡，检验人员对巡检人员的打卡记录进行验证。

[54]在巡检人员进行巡检打卡之前，巡检管理人员需要通过移动终端在待标定地点进行

点位标定，如图 1 所示，为本申请的一个实施例提供的一种巡检点位标定方法的流程图，具体过程为：

[55] 步骤 S11：通过移动终端获取待标定点位的标定标识信息；

[56] 步骤 S13：获取所述移动终端在所述待标定点位的标定运行环境参数；

[57] 步骤 S15：根据所述标定运行环境参数，计算所述待标定点位的点位质量；

[58] 步骤 S17：根据所述点位质量，判断所述待标定点位是否可作为标定点位；若否，则放弃所述待标定点位；若是，则存储所述标定标识信息和标定运行环境参数，并将所述标定标识信息和标定运行环境参数的不可逆校验信息存储至区块链，完成该点位标定。

[59] 其中，标定标识信息为巡检管理人员在标定点位设定的标识信息。标定标识信息可以包括：参考标志物照片、参考标志物视频、二维码信息、NFC 信息等中的一种或多种。

[60] 此外，巡检管理人员使用的移动终端可以是手机或其它能满足传感参数需求的设备。下面以手机为例进行说明。

[61] 手机上安装有点位标定的应用（APP）或小程序，巡检管理人员通过管理账号登录 APP 或小程序，进入巡检点位标定页面进行点位标定。

[62] 在本申请实施例中，标定点位设置的标识可以是某一标志物，例如，特定建筑、草木等；可以是包含特定信息的二维码；可以是包含特定信息的 NFC 设备等。

[63] 当标识为标志物时，巡检管理人员移步至待标定点位，选取一处标志物，利用手机进入标定页面，从标定页面启动第一摄像头对标志物进行拍照，获得参考标志物照片，将该照片作为该待标定点位的标定表示信息。在拍照同时采集手机在当前待标定点位的标定运行环境参数。标定运行环境参数是指在标定点位时移动终端的运行环境参数，该运行环境参数包括：位置相关信息、移动终端的传感器数据、摄像头焦距等的一种或多种的组合。

[64] 其中，位置相关信息至少包括如下的一种或多种的组合：

[65] 移动终端的全球定位系统（Global Positioning System，GPS）定位信息；

[66] 移动终端的第一预定距离内的基站信息；

[67] 移动终端的第二预定距离内的无线保真 Wifi 信息；

[68] 移动终端的第三预定距离内的蓝牙信息；

[69]移动终端的第四预定距离内的热点信息。

[70]其中，基站信息可以包括基站标识信息、基站信号强度等中的一种或多种组合。基站标识信息可以包括基站名称、基站地址等。

[71]无线保真 WiFi 信息可以包括：WiFi 标识信息、信号强度等中的一种或多种。类似地，WiFi 标识信息可以包括 WiFi 名称、WiFi 的 Mac 地址等。

[72]热点信息可以包括：热点标识信息、热点信号强度等中的一种或多种组合。类似地，热点标识信息可以包括热点名称、热点地址等。

[73]此外，传感器数据可以包括如下一种：

[74]温度信息、

[75]湿度信息、

[76]气压信息、

[77]多轴传感器中至少一轴的传感器数据。

[78]其中，温度信息可以通过温度传感器或温湿度传感器采集；湿度信息可以通过湿度传感器或温湿度传感器采集；气压信息可以通过其它传感器采集。多轴传感器可以包括 3 轴传感器、6 轴传感器、9 轴传感器等。

[79]此外，第一摄像头可以为手机的后置摄像头。

[80]当标识为二维码时，巡检管理人员移步至待标定点位，在该待标定点位黏贴二维码，并利用手机进入标定页面，从标定页面启动第一摄像头扫描该二维码，获取二维码信息；在利用手机扫描该二维码的同时，采集手机在当前待标定点位的标定运行环境参数，该标定运行环境参数同上。其中，第一摄像头可以为手机的后置摄像头。

[81]当标识为 NFC 设备时，巡检管理人员移步至待标定点位，在该待标定点位设置 NFC 设备，并利用手机进入标定页面，从标定页面启动手机的 NFC 模块，使手机与 NFC 设备连接，获取 NFC 信息；在利用手机连接 NFC 设备的同时，采集手机在当前待标定点位的标定运行环境参数。

[82]在本申请实施例中，标识还可以设置为其它形式，并且标识可以设置为标志物、二维码、NFC 设备等中的一种或多种。其中，标识为标志物的方案成本较低，无需额外消耗资源，且不易发生变动。而二维码的方案需要在各个巡检地点张贴二维码，而且二维码容易被损毁，致使巡检人员无法打卡；NFC 设备的方案成本较高，且容易被损坏，致

使巡检人员无法打卡。

[83] 步骤 S15：根据所述标定运行环境参数，计算所述待标定点位的点位质量。

[84] 该点位质量分越高，表明后续的巡检打卡验证的位置定位会越准确。例如周围 Wi-Fi 数量越多，信号强度越强，则后续的巡检打卡验证的位置定位会越准确，该点位的标定质量分就越高，其它参数同理。

[85] 步骤 S17：根据所述点位质量，判断所述待标定点位是否可作为标定点位；若否，则放弃所述待标定点位；若是，则存储所述标定标识信息和标定运行环境参数，并将所述标定标识信息和标定运行环境参数的不可逆校验信息存储至区块链，完成该点位标定。

[86] 根据计算的待标定点位的点位质量，与预设质量阈值进行对比，若小于预设阈值，则表明该待标定点位不可作为标定点位，放弃该待标定点位；若不小于预设阈值，则表明该待标定点位可作为标定点位，将采集的该待标定点位的标定标识信息和标定运行环境参数以文件形式存储至云端，并计算该文件的哈希值，将该哈希值存储至区块链，完成该点位标定。

[87] 完成该点位标定后，巡检管理人员还可以在手机的管理页面进行查询和管理。

[88] 标定完巡检点位后，巡检人员就可以在该点位进行打卡。如图 2 所示，本申请实施例提供的一种基于区块链的巡检存证方法，包括：

[89] 步骤 S21：通过移动终端采集巡检地点的巡检证明信息。

[90] 其中，巡检证明信息是指巡检人员在巡检地点获取的标识信息。例如，带有标志物的可视化文件、条形码信息、NFC 信号等中的一种或多种。

[91] 获取巡检证明信息可以以下三种方式中的一种或多种：

[92] 第一种，通过移动终端拍摄巡检地点的标志物以得到标志物的可视化文件，将所述可视化文件作为巡检证明信息。其中，可视化文件可以是拍摄的视频或图片。

[93] 第二种，通过移动终端扫描巡检地点的条形码以获取条形码中携带的巡检证明信息。其中，条形码可以包括一维码或者二维码。条形码中携带有码信息，可作为巡检证明信息。

[94] 第三种，通过移动终端的 NFC 模块接收巡检地点的 NFC 设备发出的信号，以获取所述信号中携带的巡检证明信息。

[95] 在通过移动终端采集巡检地点的巡检证明信息时，可以携带有时间戳，该时间戳是

指获取巡检证明信息时移动终端系统的时间。

[96]步骤 S23：获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据。

[97]在获取巡检证明信息的同时，需要获取移动终端的运行环境参数。在获取运行环境参数时，也可以获取当前的时间戳，该时间戳为获取运行环境参数时移动终端系统的时间。

[98]通过对比运行环境参数的时间戳和巡检证明信息的时间戳，能够判断两者是否是同时获取的信息，若不是同时获取，则表明本次打卡为非正常打卡。

[99]本申请实施例中的运行环境参数、位置相关信息、传感器数据可参考图 2 所示实施例中的位置相关信息、传感器数据，不再赘述。

[100] 在将所述巡检证明信息、所述位置相关信息和所述传感器数据的不可逆校验信息上传至存证区块链之前，还可以包括：

[101] 对所述巡检地点和/或巡检人员进行可信验证；

[102] 其中，将所述巡检证明信息、所述位置相关信息和所述传感器数据的不可逆校验信息上传至存证区块链中，包括：当所述可信验证通过时，将所述巡检证明信息、所述位置相关信息和所述传感器数据的不可逆校验信息上传至存证区块链中。

[103] 在获取到巡检证明信息和运行环境参数后，可以根据巡检证明信息和运行环境参数，对当前的巡检地点进行可信验证。这样，能够验证移动终端采集的巡检证明信息是否是在巡检地点真实采集的，以排出伪造巡检证明信息的场景。

[104] 在通过移动终端采集巡检地点的巡检证明信息时，所述方法还可以包括：采集所述巡检人员的生物识别信息；

[105] 其中，对所述巡检人员进行可信验证，包括：根据所述生物识别信息，对所述巡检人员进行可信验证。

[106] 当需要对巡检人员进行验证时，需要在获取巡检证明信息的同时，获取巡检人员的生物识别信息，进而根据生物识别信息，对巡检人员进行可信验证。通过对巡检人员的可信验证，能够确定巡检人员的真实身份，以验证巡检人员是对应巡检地点在巡检时间对应的巡检人员。当对巡检的人物没要求，只对巡检地点有要求时，可以关闭人物验证功能，只需要获取巡检证明信息和运行环境参数，对巡检地点进行可信验证。其中，

生物识别信息可以包括：包含有人物头像的可视化文件、人物面部特征、人物指纹特征等中的一种或多种。该可视化文件可以是视频或图片。

[107] 巡检人员使用的移动终端可以是手机或其它能满足传感参数采集需求的设备，下面以手机为例进行说明。

[108] 巡检人员到达某巡检点位，通过手机 APP 或小程序进入打卡页面，选取打卡地点，进行打卡操作。在步骤 S21 中描述了三种获取巡检证明信息的方式，具体获取运行环境参数和生物识别信息的方式包括以下几种情况：

[109] 第一种情况，当标识为标识物：

[110] 当需要采集生物识别信息时，包括以下三种方式：

[111] 1）当移动终端接收到巡检人员发出的打卡指令时，移动终端同时启动设备的第一摄像头和第二摄像头，巡检人员将第一摄像头对准标志物拍照，同时，将第二摄像头对准自身人脸进行同步拍摄，获得包含有标志物的可视化文件和包含有人物头像的可视化文件。

[112] 2）当移动终端接收到巡检人员发出的打卡指令时，移动终端同时启动第一摄像头和第二摄像头，巡检人员将第一摄像头对准标志物拍照，同时，将第二摄像头对准自身人脸进行面部识别，获得包含有标志物的可视化文件和人物面部特征。

[113] 3）当移动终端接收到巡检人员发出的打卡指令时，移动终端启动第一摄像头，同时启动屏幕上的指纹识别模块，巡检人员将第一摄像头对准标志物拍照，同时在屏幕上验证指纹，获得包含有标志物的可视化文件和人物指纹特征。

[114] 当不需要采集生物识别信息时，则当移动终端接收到巡检人员发出的打卡指令时，移动终端只启动第一摄像头，巡检人员将第一摄像头对准标志物拍照，获得包含有标志物的可视化文件。

[115] 无论是否采集生物识别信息，在利用第一摄像头对准标志物拍照的同时，采集移动终端的运行环境参数。

[116] 第二种情况，当标识为二维码：

[117] 同样，当需要采集生物识别信息时，包括三种方式：

[118] 1）当移动终端接收到巡检人员发出的打卡指令时，移动终端同时启动设备的第一摄像头和第二摄像头，巡检人员将第一摄像头对准二维码进行扫描，同时，将第二摄

像头对准自身人脸进行同步拍摄，获得二维码信息和包含有人物头像的可视化文件。

[119] 2）当移动终端接收到巡检人员发出的打卡指令时，移动终端同时启动第一摄像头和第二摄像头，巡检人员将第一摄像头对准二维码进行扫描，同时，将第二摄像头对准自身人脸进行面部识别，获得二维码信息和人物面部特征。

[120] 3）当移动终端接收到巡检人员发出的打卡指令时，移动终端启动第一摄像头，同时启动屏幕上的指纹识别模块，巡检人员将第一摄像头对准二维码进行扫描，同时在屏幕上验证指纹，获得二维码信息和人物指纹特征。

[121] 当不需要采集生物识别信息时，则当移动终端接收到巡检人员发出的打卡指令时，移动终端只启动第一摄像头，巡检人员将第一摄像头对准二维码进行扫描，获得二维码信息。

[122] 无论是否采集生物识别信息，在利用第一摄像头对准二维码扫描的同时，采集移动终端的运行环境参数。

[123] 第三种情况，当标识为 NFC 设备:

[124] 同样，当需要采集生物识别信息时，包括三种方式:

[125] 1）当移动终端接收到巡检人员发出的打卡指令时，移动终端同时启动设备的 NFC 模块和第二摄像头，巡检人员利用移动终端的 NFC 模块获取 NFC 设备发出的信号，同时，将第二摄像头对准自身人脸进行同步拍摄，获得 NFC 信息和包含有人物头像的可视化文件。

[126] 2）当移动终端接收到巡检人员发出的打卡指令时，移动终端同时启动设备的 NFC 模块和第二摄像头，巡检人员利用移动终端的 NFC 模块获取 NFC 设备发出的信号，同时，将第二摄像头对准自身人脸进行面部识别，获得 NFC 信息和人物面部特征。

[127] 3）当移动终端接收到巡检人员发出的打卡指令时，移动终端启动 NFC 模块，同时启动屏幕上的指纹识别模块，巡检人员利用移动终端的 NFC 模块获取 NFC 设备发出的信号，同时在屏幕上验证指纹，获得 NFC 信息和人物指纹特征。

[128] 当不需要采集生物识别信息时，则当移动终端接收到巡检人员发出的打卡指令时，移动终端只启动 NFC 模块，巡检人员利用移动终端的 NFC 模块获取 NFC 设备发出的信号，获得 NFC 信息。

[129] 无论是否采集生物识别信息，在利用移动终端的 NFC 模块获取 NFC 设备发出

信号的同时，采集移动终端的运行环境参数。

[130] 在上述三种情况中，第一摄像头可以为后置摄像头，第二摄像头可以为前置摄像头。生物识别信息采集的三种方式分别为指纹验证、人物拍照和人物面部识别，三种方式之间可独立存在，其中，指纹验证和人物拍照可同时存在，指纹验证和人物面部识别也可以同时存在，可以与巡检证明信息的采集方式可以进行多种组合，这都在本申请的保护范围内。

[131] 在本申请实施例中，在采集巡检证明信息、运行环境参数和生物识别信息时，记录有时间戳，可以根据三者的时间戳判断三者是否是同时采集，还可以根据采集的巡检证明信息、运行环境参数和生物识别信息综合判断三者是否是同时采集，例如，可以根据照片中标志物的位置变化、拍照时的抖动方向、拍照移动距离、摄像头焦距等特征来判断，这样，能够避免恶意打卡事件的发生。

[132] 步骤 S25：将所述巡检证明信息、所述位置相关信息和所述传感器数据的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信。

[133] 在本申请实施例中，还可以包括获取巡检事件信息，并将所述巡检事件信息与所述巡检证明信息、所述位置相关信息和所述传感器数据的不可逆校验信息上传至存证区块链中。其中，巡检事件信息是指巡检人员巡检某个巡检地点的巡检结果信息。

[134] 其中，不可逆校验信息为巡检人员对摘要进行私钥签名后的签名信息，或者，所述不可逆校验信息包括摘要和巡检人员对所述摘要进行私钥签名的签名信息。摘要是指所述巡检证明信息、所述位置相关信息和所述传感器数据等。不可逆校验信息，可以是所有信息按预定顺序排列后整体的不可逆校验信息，也可以是分成多个之后各自的不可逆校验信息，还可以是对所有文件按照一个或多个不可逆加密算法经过多次不可逆加密得到的不可逆校验信息。

[135] 通过采用区块链技术进行存储，能够保证信息记录的可追溯以及不可篡改，一旦发生问题，事件原因的确认以及追责过程可信，以此可提高巡检人员完成任务的质量，进而提高场所安全性，降低火灾等安全问题发生的概率。

[136] 在获取所述巡检证明信息、所述位置相关信息和所述传感器数据之后，还可以根据巡检证明信息、所述位置相关信息和所述传感器数据，对巡检地点进行可信验证；在获取生物识别信息之后，还可以根据生物识别信息对人物进行可信验证。

[137] 对巡检地点进行可信验证时，可以采用预先建立算法模型，结合预先存储的标定标识信息、标定运行环境参数和历史打卡信息，对巡检地点进行可信验证。其中，算法模型是根据标定标识信息、标定运行环境参数和历史打卡信息，采用神经网络算法，计算模拟出的算法模型。通过对地点进行可信验证，能够验证巡检人员是否在指定地点打卡，进而实现对巡检人员的监督。

[138] 根据生物识别信息和运行环境参数，对巡检人物进行可信验证，当生物识别信息为包含有人物头像的可视化文件时，采用人脸识别，环境图片比对识别，基于 Wi-Fi 的局部定位，前后摄像头画面同步验证，基于 9 轴传感器的行为动作识别，基于双摄像头及焦距的拍照立体性识别等方法，对人物进行可信验证。

[139] 当生物识别信息为人物面部特征时，根据预先存储的人物面部特征集合，对人物进行可信验证。当生物识别信息为人物指纹特征时，根据预先存储的人物指纹集合，对人物进行可信验证。

[140] 当不需要对人物进行验证时，则不需要对巡检人物进行可信验证。

[141] 应理解，本申请实施例中提到的对巡检地点和巡检人物进行可信验证的过程，可以由巡检人员使用的移动终端完成，也可以由后台服务器完成。

[142] 在对所述巡检地点和/或巡检人员进行可信验证之后，所述方法还可以包括：当所述可信验证通过时，记录所述巡检人员在所述巡检地点成功打卡的信息。

[143] 在得出可信环境的计算结果后，可以根据可信环境的计算结果判断打卡是否成功。当没有对人物进行可信验证时，根据巡检地点的可信验证结果，判断打卡是否成功；当对巡检地点和人物都进行了可信验证时，根据巡检地点的可信验证结果和巡检人物的可信验证结果，判断打卡是否成功。

[144] 判断完成后，可以将本次打卡的相关信息存储上链。为了节约区块链的存储空间，若打卡成功，则记录本次打卡的成功信息，并将打卡成功的相关信息存储上链，向用户返回打卡成功信息，完成本次点位打卡；若打卡失败，则不存储本次打卡的相关信息，并向用户返回打卡失败信息，提示用户重新打卡。这样，可以节省存储空间，优化打卡过程。

[145] 其中，打卡相关信息包括：巡检证明信息、位置相关信息、传感器数据和可信环境计算结果等。

[146] 在本申请实施例中，在步骤 S21 通过移动终端采集巡检地点的巡检证明信息之

前，还可以包括：对移动终端的系统环境的可靠性进行检测。

[147] 通过对移动终端的系统环境的可靠性进行检测，能够避免系统异常所导致的异常打卡。

[148] 本申请实施例通过获取巡检证明信息、运行环境参数和生物识别信息，并根据上述三种信息对巡检的可信环境进行计算，能够对指定巡检人员是否在指定时间到达指定巡检地点进行确认，并且，利用区块链技术存储巡检证明信息、运行环境参数和生物识别信息，能够较方便地实现巡检信息记录的可追溯以及不可篡改，一旦需要追溯信息记录，便可以通过区块链存储的巡检信息记录实现事件原因的确认，并保证追溯的信息记录可信，以此可提高巡检人员巡检信息记录的置信度和可追溯性，进而提高场所安全性，降低安全问题发生的概率。

[149] 在本申请的另一个实施例中，还提供了一种基于区块链的巡检存证方法，如图 3 所示，该方法首先通过移动终端采集巡检地点的巡检证明信息，并获取移动终端的运行环境参数，再根据运行环境参数对巡检地点进行可信计算，当地点可信验证通过后，将巡检证明信息存储至存证区块链。这样，既可以确保地点的置信度，又可以使检验人员只对巡检证明信息进行验证，节省检验时间，并且节省存储空间。

[150] 本申请实施例提供的一种区块链的巡检存证方法，如图 3 所示，具体包括：

[151] 步骤 S31：通过移动终端采集巡检地点的巡检证明信息。

[152] 步骤 S33：获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据。

[153] 步骤 S35：基于所述位置相关信息和所述传感器数据对所述巡检地点进行可信验证。

[154] 步骤 S37：当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息至少包括所述巡检证明信息。

[155] 其中，步骤 S31 的具体描述与步骤 S21 类似，相关之处参见步骤 S21 的相关内容。步骤 S33 的具体过程与步骤 S23 类似，相关之处参见步骤 S23，这里不再赘述。

[156] 对于步骤 S35，当获取到移动终端采集巡检证明信时的运行环境参数后，根据运行环境参数，对巡检地点进行可信验证。其中的运行环境参数、位置相关信息、传感

器数据可参考图 2 所示实施例提到的运行环境参数、位置相关信息，不再赘述。

[157] 通过位置相关信息和传感器数据可以定位出巡检地点的位置，再结合预先存储的标定的巡检地点的位置信息，对定位出的巡检地点的位置进行可信验证，这样，能够验证处该位置是否为巡检地点。

[158] 另外，还可以根据巡检证明信息和运行环境参数，对巡检地点进行可信验证，通过运行环境参数能够确定是巡检位置是否为标定的巡检地点，结合巡检证明信息能够验证该巡检地点是否为指定的巡检地点，若是，则表明地点可信验证通过，若否，则即使验证巡检位置为标定的巡检地点但并非指定巡检地点，也表明该地点可信验证不通过。只有当两者验证都通过时，才表明可信验证通过。相关之处参见步骤 S25 的部分内容。

[159] 当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，该巡检存证信息至少包括巡检证明信息，不可逆校验信息是指巡检证明信息的摘要和巡检人员对所述摘要进行私钥签名的签名信息，或者，不可逆校验信息是指巡检人员对所述摘要进行私钥签名的签名信息。

[160] 在采集运行环境参数时，还可以采集巡检人员的生物识别信息，具体采集过程参见步骤 S23 的部分内容。在对巡检地点验证通过后，还可以对巡检人员进行人物验证，具体参见步骤 S25 的部分内容。若巡检计划要求指定巡检人在指定巡检地点进行巡检，则必须对巡检人员进行验证，当验证通过后，将巡检存证信息的不可逆校验信息上传至存证区块链中，其中，巡检存证信息至少包括巡检证明信息和巡检人员的生物识别信息。这样，可以实现对人物和地点的双重可信验证。

[161] 在本申请提供的一个具体实施例中，在对所述巡检地点和/或巡检人员进行可信验证之后，所述方法还包括：当所述可信验证通过时，记录所述巡检人员在所述巡检地点成功打卡的信息。

[162] 在本申请提供的一个具体实施例中，所述传感器数据包括如下的一种或多种的组合：温度信息、湿度信息、气压信息和多轴传感器中至少一轴的传感器数据。

[163] 在本申请提供的一个具体实施例中，所述运行环境参数，还包括：摄像头焦距。

[164] 在本申请提供的一个具体实施例中，所述通过移动终端采集巡检地点的巡检证明信息，包括：

[165] 通过移动终端拍摄巡检地点的标志物以得到标志物的可视化文件，将所述可视化文件作为巡检证明信息。

[166] 在本申请提供的一个具体实施例中，所述通过移动终端采集巡检地点的巡检证明信息，包括:

[167] 通过移动终端扫描巡检地点的条形码以获取条形码中携带的巡检证明信息。

[168] 在本申请提供的一个具体实施例中，所述通过移动终端采集巡检地点的巡检证明信息，包括:

[169] 通过移动终端的 NFC 模块接收巡检地点的 NFC 设备发出的信号，以获取所述信号中携带的巡检证明信息。

[170] 在本申请提供的一个具体实施例中，所述巡检证明信息携带有时间戳。

[171] 在本申请提供的一个具体实施例中，所述运行环境参数还包括时间戳。

[172] 在本申请提供的一个具体实施例中，在所述通过移动终端采集巡检地点的巡检证明信息的步骤之前，还包括：对移动终端的系统环境的可靠性进行检测；所述通过移动终端采集巡检地点的巡检证明信息，包括：检测通过后，通过移动终端采集巡检地点的巡检证明信息。

[173] 本实施例提供的一种基于区块链的巡检存证方法，与步骤 S21-步骤 S25 提供的一种基于区块链的巡检存证方法具有相同的发明构思，相关之处请参加步骤 S21-步骤 S25 的部分内容，这里不再赘述。

[174] 相应地，本申请实施例还提供一种巡检验证方法，如图 4 所示，为本实施例提供的一种巡检验证方法的流程图。本申请提供了一种巡检验证方法，包括:

[175] 步骤 S41：接收检验人员输入的筛选条件，所述筛选条件用于筛选指定巡检人员在指定巡检地点的巡检存证信息;

[176] 步骤 S43：根据所述筛选条件，查询所述指定巡检人员和所述指定巡检地点对应的巡检存证信息。

[177] 当对巡检信息进行检验时，检验人员使用检验终端，进入巡检验证页面，对巡检信息进行验证。检验终端可以是手机或其它能登录巡检验证页面的设备。

[178] 检验人员登录 APP 或小程序后，进入验证页面，输入筛选条件，例如时间、巡检人员编号等。检验终端接收到巡检申请后，将巡检申请发送至服务端，查询对应的巡检存证信息。

[179] 步骤 S45：基于存证区块链中存储的所述指定巡检人员和所述指定巡检地点对

应的不可逆校验信息，对所述巡检存证信息进行可信验证。

[180] 其中，巡检存证信息是指打卡相关信息，包括巡检证明信息、位置相关信息、传感器数据和可信环境计算结果等。

[181] 在对巡检存证信息进行验证之前，需要保证巡检存证信息的可靠性，若是巡检存证信息已被篡改，则对其进行验证也没有任何意义。

[182] 查询到巡检存证信息后，计算该巡检存证信息的不可逆校验信息，将该不可逆校验信息与区块链上存储的相应的不可逆校验信息进行对比，若两者一致，则表明巡检存证信息没有被篡改，是可信的，若不一致，则表明巡检存证信息可能被篡改，是不可信的。通过对巡检存证信息哈希值的验证，能够判断巡检存证信息是否可信。

[183] 在对巡检存证信息的可信性验证完成后，还可以向检验人员输出验证结果。通过该验证结果，检验人员可以选择性地对巡检存证信息进行验证，进而提高检验效率。

[184] 需要说明的是，实施例所提供方法的各步骤的执行主体均可以是同一设备，或者，该方法也由不同设备作为执行主体。比如，步骤 11 和步骤 12 的执行主体可以为设备 1，步骤 13 的执行主体可以为设备 2；又比如，步骤 11 的执行主体可以为设备 1，步骤 12 和步骤 13 的执行主体可以为设备 2；等等。

[185] 上述对本申请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。

[186] 图 5 是本申请的一个实施例巡检存证装置的结构示意图。请参考图 5，在一种软件实施方式中，巡检存证装置 500 可以包括:

[187] 证明信息采集模块 502，通过移动终端采集巡检地点的巡检证明信息;

[188] 环境参数采集模块 504，获取采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据;

[189] 信息存储模块 506，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

[190] 可选地，所述巡检存证装置 500，还包括:

[191] 可信验证模块 508，对所述巡检地点和/或巡检人员进行可信验证;

[192] 其中，所述信息存储模块 506，具体用于：当所述可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链。

[193] 可选地，所述巡检存证装置 500，还包括:

[194] 生物信息采集模块 510，采集巡检人员的生物识别信息;

[195] 其中，可信验证模块 508 可用于：根据所述生物识别信息，对所述巡检人员进行可信验证。

[196] 可选地，可信验证模块 508 还可用于：根据所述巡检证明信息和所述运行环境参数，对所述巡检地点进行可信验证。

[197] 可选地，所述巡检存证装置 500，还包括:

[198] 成功打卡记录模块，当所述可信验证通过时，记录所述巡检人员在所述巡检地点成功打卡的信息。

[199] 具体地，所述位置相关信息至少包括如下的一种或多种的组合:

[200] 所述移动终端的全球定位系统 GPS 定位信息;

[201] 所述移动终端的第一预定距离内的基站信息;

[202] 所述移动终端的第二预定距离内的无线保真 Wifi 信息;

[203] 所述移动终端的第三预定距离内的蓝牙信息;

[204] 所述移动终端的第四预定距离内的热点信息。

[205] 具体地，所述传感器数据包括如下的一种或多种的组合：温度信息、湿度信息、气压信息和多轴传感器中至少一轴的传感器数据。

[206] 可选地，所述运行环境参数，还包括：摄像头焦距。

[207] 可选地，所述证明信息采集模块 502，具体用于:

[208] 通过移动终端拍摄巡检地点的标志物以得到标志物的可视化文件，将所述可视化文件作为巡检证明信息。

[209] 可选地，所述证明信息采集模块 502，具体用于:

[210] 通过移动终端扫描巡检地点的条形码以获取条形码中携带的巡检证明信息。

[211] 可选地，所述证明信息采集模块 502，具体用于：

[212] 通过移动终端的 NFC 模块接收巡检地点的 NFC 设备发出的信号，以获取所述信号中携带的巡检证明信息。

[213] 可选地，所述不可逆校验信息可包括：所述巡检存证信息的摘要和/或巡检人员对所述摘要进行私钥签名后的签名信息。

[214] 可选地，所述巡检证明信息携带有时间戳。

[215] 可选地，所述运行环境参数还包括时间戳。

[216] 可选地，所述巡检存证装置 500，还包括：

[217] 系统检测模块 512，对移动终端的系统环境的可靠性进行检测；

[218] 所述证明信息采集模块 502，具体用于：

[219] 检测通过后，通过移动终端采集巡检地点的巡检证明信息。

[220] 需要说明的是，本实施例中提供的装置可以采用计算机硬件的方式实现，也可以采用软件方式实现，这里不做限定。基于区块链的巡检存证装置 500 可以实现图 2 所示的方法实施例的方法，具体参考图 2 所示的基于区块链的巡检存证方法，此处不再赘述。

[221] 图 6 是本申请的另一个实施例一种基于区块链的巡检存证装置的结构示意图，请参考图 6，在一种软件实施例方式中，一种基于区块链的巡检存证装置 600，包括：

[222] 证明信息采集模块 602，采集巡检地点的巡检证明信息；

[223] 环境参数采集模块 604，获取采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据；

[224] 可信验证模块 606，基于所述位置相关信息和所述传感器数据对所述巡检地点进行可信验证；

[225] 证明信息存储模块 608，当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息至少包括所述巡检证明信息。

[226] 在本申请提供的一个具体实施例中，所述巡检存证装置 600，还包括：打卡记录

模块 610，当所述可信验证通过时，记录所述巡检人员在所述巡检地点成功打卡的信息。

[227] 在本申请提供的一个具体实施例中，所述位置相关信息至少包括如下的一种或多种的组合：

[228] 所述移动终端的全球定位系统 GPS 定位信息；

[229] 所述移动终端的第一预定距离内的基站信息；

[230] 所述移动终端的第二预定距离内的无线保真 Wifi 信息；

[231] 所述移动终端的第三预定距离内的蓝牙信息；

[232] 所述移动终端的第四预定距离内的热点信息。

[233] 在本申请提供的一个具体实施例中，所述传感器数据包括如下的一种或多种的组合：温度信息、湿度信息、气压信息和多轴传感器中至少一轴的传感器数据。

[234] 在本申请提供的一个具体实施例中，所述运行环境参数，还包括：摄像头焦距。

[235] 在本申请提供的一个具体实施例中，所述证明信息采集模块 602，具体用于：

[236] 通过移动终端拍摄巡检地点的标志物以得到标志物的可视化文件，将所述可视化文件作为巡检证明信息。

[237] 在本申请提供的一个具体实施例中，所述证明信息采集模块 602，具体用于：

[238] 通过移动终端扫描巡检地点的条形码以获取条形码中携带的巡检证明信息。

[239] 在本申请提供的一个具体实施例中，所述证明信息采集模块 602，具体用于：

[240] 通过移动终端的 NFC 模块接收巡检地点的 NFC 设备发出的信号，以获取所述信号中携带的巡检证明信息。

[241] 在本申请提供的一个具体实施例中，所述巡检证明信息携带有时间戳。

[242] 在本申请提供的一个具体实施例中，所述运行环境参数还包括时间戳。

[243] 在本申请提供的一个具体实施例中，所述巡检存证装置 600，还包括：系统检测模块 612，对移动终端的系统环境的可靠性进行检测；所述证明信息采集模块 602，具体用于：检测通过后，通过移动终端采集巡检地点的巡检证明信息。

[244] 需要说明的是，本实施例中提供的装置可以采用计算机硬件的方式实现，也可以采用软件方式实现，这里不做限定。基于区块链的巡检存证装置 600 可以实现图 3 所

示的方法实施例的方法，具体参考图 3 所示的基于区块链的巡检存证方法，此处不再赘述。

[245] 图 7 是本申请的一个实施例巡检验证装置的结构示意图。请参考图 7，在一种软件实施方式中，巡检验证装置 700 可包括:

[246] 条件接收模块 701，接收检验人员输入的筛选条件;

[247] 文件查询模块 702，根据所述筛选条件，查询对应的巡检存证信息;

[248] 文件验证模块 703，基于存证区块链中存储的不可逆校验信息，对所述巡检存证信息进行可信验证。

[249] 具体地，所述筛选条件，包括：时间、巡检人员编号等。

[250] 需要说明的是，本实施例中提供的装置可以采用计算机硬件的方式实现，也可以采用软件方式实现，这里不做限定。巡检验证装置 700 可以实现图 4 所示的方法实施例的方法，具体参考图 4 所示的巡检验证方法，此处不再赘述。

[251] 图 8 是本申请的一个实施例电子设备的结构示意图。请参考图 8，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器（non-volatile memory），例如至少 1 个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[252] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是 ISA（Industry Standard Architecture，工业标准体系结构）总线、PCI（Peripheral Component Interconnect，外设部件互连标准)总线或 EISA（Extended Industry Standard Architecture，扩展工业标准结构）总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 8 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[253] 存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

[254] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成基于区块链的巡检存证装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作:

[255] 采集巡检地点的巡检证明信息;

[256] 获取采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据；

[257] 将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

[258] 或者，处理器执行存储器所存放的程序，并具体用于执行以下操作：

[259] 通过移动终端采集巡检地点的巡检证明信息；获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据；

[260] 基于所述位置相关信息和所述传感器数据对所述巡检地点进行可信验证；

[261] 当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息至少包括所述巡检证明信息。

[262] 上述如本申请图 2 或图 3 所示实施例揭示的巡检存证装置执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器（Central Processing Unit，CPU）、网络处理器（Network Processor，NP）等；还可以是数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field－Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[263] 该电子设备还可执行图 2 或图 3 的方法，并实现巡检存证装置在图 2 或图 3 所示实施例的功能，本申请实施例在此不再赘述。

[264] 图 9 是本申请的一个实施例电子设备的结构示意图。请参考图 9，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器（non-volatile memory），例如至少 1 个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[265] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是 ISA（Industry Standard Architecture，工业标准体系结构）总线、PCI（Peripheral Component Interconnect，外设部件互连标准)总线或 EISA（Extended Industry Standard Architecture，扩展工业标准结构）总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 9 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[266] 存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

[267] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成基于区块链的巡检验证装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作:

[268] 接收检验人员输入的筛选条件，所述筛选条件用于筛选指定巡检人员在指定巡检地点的巡检存证信息;

[269] 根据所述筛选条件，查询所述指定巡检人员和所述指定巡检地点对应的巡检存证信息;

[270] 基于存证区块链中存储的所述指定巡检人员和所述指定巡检地点对应的不可逆校验信息，对所述巡检存证信息进行可信验证。

[271] 上述如本申请图 4 所示实施例揭示的巡检验证装置执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器(Central Processing Unit，CPU)、网络处理器(Network Processor，NP)等；还可以是数字信号处理器(Digital Signal Processor，DSP)、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field－Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开

的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[272] 该电子设备还可执行图 4 的方法，并实现巡检验证装置在图 4 所示实施例的功能，本申请实施例在此不再赘述。

[273] 当然，除了软件实现方式之外，本申请的电子设备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。

[274] 上述对本申请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。

[275] 总之，以上所述仅为本申请的较佳实施例而已，并非用于限定本申请的保护范围。凡在本申请一个或多个实施例的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请一个或多个实施例的保护范围之内。

[276] 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。具体的，计算机例如可以为个人计算机、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何设备的组合。

[277] 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，磁带磁磁盘存储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。

[278] 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。

[279] 本申请中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

权利要求书

1、一种基于区块链的巡检存证方法，包括:

通过移动终端采集巡检地点的巡检证明信息;

获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据;

将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

2、如权利要求 1 所述的方法，在将巡检存证信息的不可逆校验信息上传至存证区块链之前，还包括:

对所述巡检地点和/或巡检人员进行可信验证;

其中，将巡检存证信息的不可逆校验信息上传至存证区块链，包括: 当所述可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链。

3、如权利要求 2 所述的方法，在通过移动终端采集巡检地点的巡检证明信息时，所述方法还包括:

采集巡检人员的生物识别信息;

其中，对巡检人员进行可信验证，包括: 根据所述生物识别信息，对所述巡检人员进行可信验证。

4、如权利要求 2 所述的方法，

对所述巡检地点进行可信验证，包括: 根据所述巡检证明信息和所述运行环境参数，对所述巡检地点进行可信验证。

5、如权利要求 2-4 任意一项所述的方法，在对所述巡检地点和/或巡检人员进行可信验证之后，所述方法还包括:

当所述可信验证通过时，记录所述巡检人员在所述巡检地点成功打卡的信息。

6、如权利要求 1 所述的方法，所述位置相关信息至少包括如下的一种或多种的组合:

所述移动终端的全球定位系统 GPS 定位信息;

所述移动终端的第一预定距离内的基站信息;

所述移动终端的第二预定距离内的无线保真 Wifi 信息;

所述移动终端的第三预定距离内的蓝牙信息;

所述移动终端的第四预定距离内的热点信息。

7、如权利要求 1 所述的方法，所述传感器数据包括如下的一种或多种的组合：温度信息、湿度信息、气压信息和多轴传感器中至少一轴的传感器数据。

8、如权利要求 1 所述的方法，所述运行环境参数，还包括：摄像头焦距。

9、如权利要求 1 所述的方法，所述通过移动终端采集巡检地点的巡检证明信息，包括：

通过移动终端拍摄巡检地点的标志物以得到标志物的可视化文件，将所述可视化文件作为巡检证明信息。

10、如权利要求 1 所述的方法，所述通过移动终端采集巡检地点的巡检证明信息，包括：

通过移动终端扫描巡检地点的条形码以获取条形码中携带的巡检证明信息。

11、如权利要求 1 所述的方法，所述通过移动终端采集巡检地点的巡检证明信息，包括：

通过移动终端的 NFC 模块接收巡检地点的 NFC 设备发出的信号，以获取所述信号中携带的巡检证明信息。

12、如权利要求 1 所述的方法，所述不可逆校验信息包括：所述巡检存证信息的摘要和/或巡检人员对所述摘要进行私钥签名后的签名信息。

13、如权利要求 1 所述的方法，所述巡检证明信息携带有时间戳。

14、如权利要求 1 所述的方法，所述运行环境参数还包括时间戳。

15、如权利要求 1 所述的方法，在所述通过移动终端采集巡检地点的巡检证明信息的步骤之前，还包括：

对移动终端的系统环境的可靠性进行检测；

所述通过移动终端采集巡检地点的巡检证明信息，包括：

检测通过后，通过移动终端采集巡检地点的巡检证明信息。

16、一种基于区块链的巡检存证方法，包括：

通过移动终端采集巡检地点的巡检证明信息；

获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据；

基于所述位置相关信息和所述传感器数据对所述巡检地点进行可信验证；

当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息至少包括所述巡检证明信息。

17、一种巡检验证方法，包括:

接收检验人员输入的筛选条件，所述筛选条件用于筛选指定巡检人员在指定巡检地点的巡检存证信息;

根据所述筛选条件，查询所述指定巡检人员和所述指定巡检地点对应的巡检存证信息;

基于存证区块链中存储的所述指定巡检人员和所述指定巡检地点对应的不可逆校验信息，对所述巡检存证信息进行可信验证。

18、一种基于区块链的巡检存证装置，包括:

证明信息采集模块，采集巡检地点的巡检证明信息;

环境参数采集模块，获取采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据;

信息存储模块，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

19、一种基于区块链的巡检存证装置，包括:

证明信息采集模块，采集巡检地点的巡检证明信息;

环境参数采集模块，获取采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据;

可信验证模块，基于所述位置相关信息和所述传感器数据对所述巡检地点进行可信验证;

证明信息存储模块，当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息至少包括所述巡检证明信息。

20、一种巡检验证装置，包括:

条件接收模块，接收检验人员输入的筛选条件，所述筛选条件用于筛选指定巡检人员在指定巡检地点的巡检存证信息;

文件查询模块，根据所述筛选条件，查询所述指定巡检人员和所述指定巡检地点对应的巡检存证信息;

文件验证模块，基于存证区块链中存储的所述指定巡检人员和所述指定巡检地点对应的的不可逆校验信息，对所述巡检存证信息进行可信验证。

21、一种电子设备，包括：存储器、处理器和存储在所述存储器上并可在所述处理

器上运行的计算机可执行指令，所述计算机可执行指令被所述处理器执行时实现以下操作：

通过移动终端采集巡检地点的巡检证明信息；

获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据；

将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

22、一种计算机可读存储介质，所述计算机可读存储介质用于存储计算机可执行指令，所述计算机可执行指令被处理器执行时实现以下操作：

通过移动终端采集巡检地点的巡检证明信息；

获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据；

将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据。

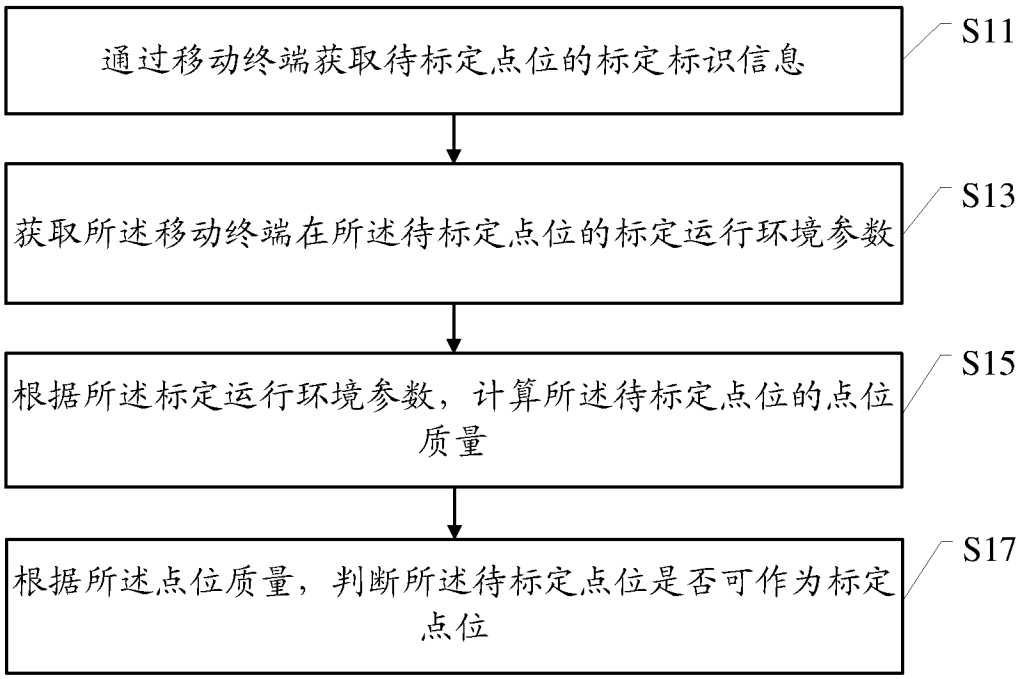

通过移动终端获取待标定点位的标定标识信息
S11
获取所述移动终端在所述待标定点位的标定运行环境参数
S13
根据所述标定运行环境参数，计算所述待标定点位的点位质量
S15
根据所述点位质量，判断所述待标定点位是否可作为标定点位
S17

图 1

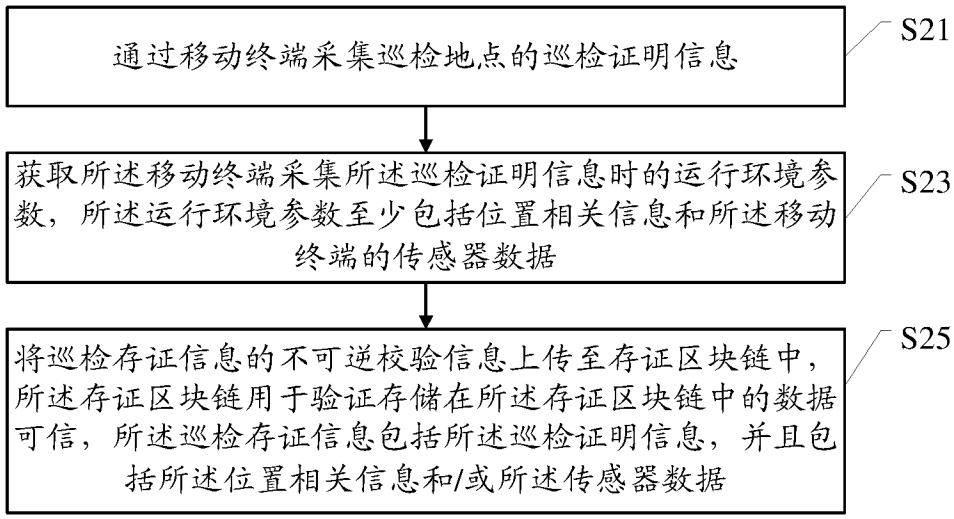

通过移动终端采集巡检地点的巡检证明信息
S21
获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据
S23
将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息包括所述巡检证明信息，并且包括所述位置相关信息和/或所述传感器数据
S25

图 2

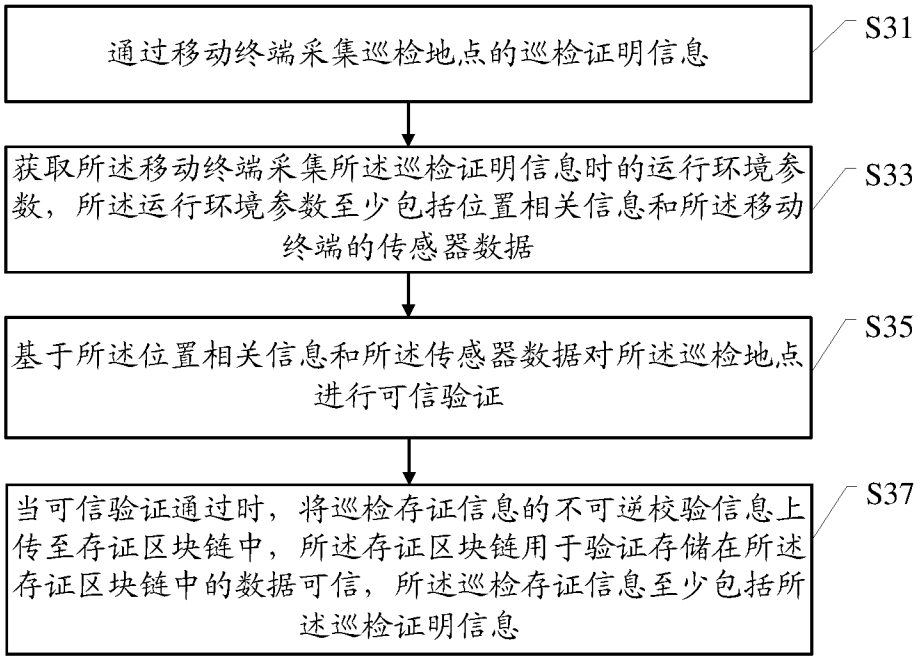

通过移动终端采集巡检地点的巡检证明信息
S31
获取所述移动终端采集所述巡检证明信息时的运行环境参数，所述运行环境参数至少包括位置相关信息和所述移动终端的传感器数据
S33
基于所述位置相关信息和所述传感器数据对所述巡检地点进行可信验证
S35
当可信验证通过时，将巡检存证信息的不可逆校验信息上传至存证区块链中，所述存证区块链用于验证存储在所述存证区块链中的数据可信，所述巡检存证信息至少包括所述巡检证明信息
S37

图 3

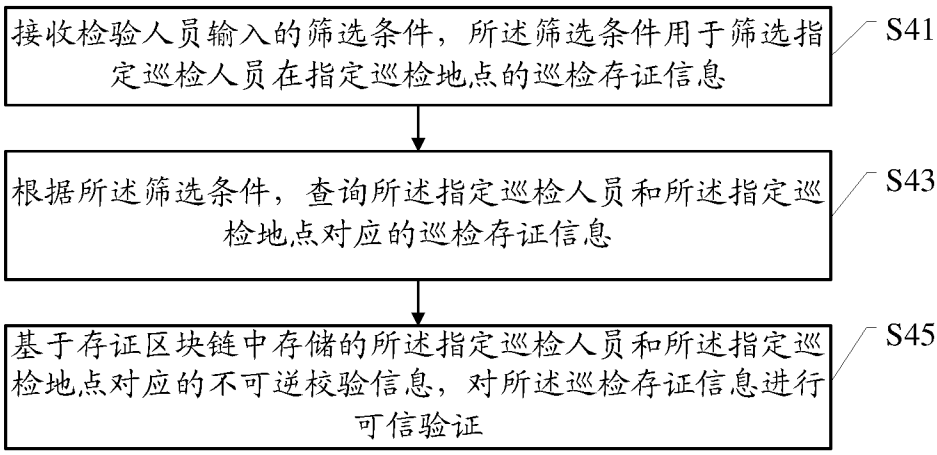

接收检验人员输入的筛选条件，所述筛选条件用于筛选指定巡检人员在指定巡检地点的巡检存证信息
S41
根据所述筛选条件，查询所述指定巡检人员和所述指定巡检地点对应的巡检存证信息
S43
基于存证区块链中存储的所述指定巡检人员和所述指定巡检地点对应的不可逆校验信息，对所述巡检存证信息进行可信验证
S45

图 4

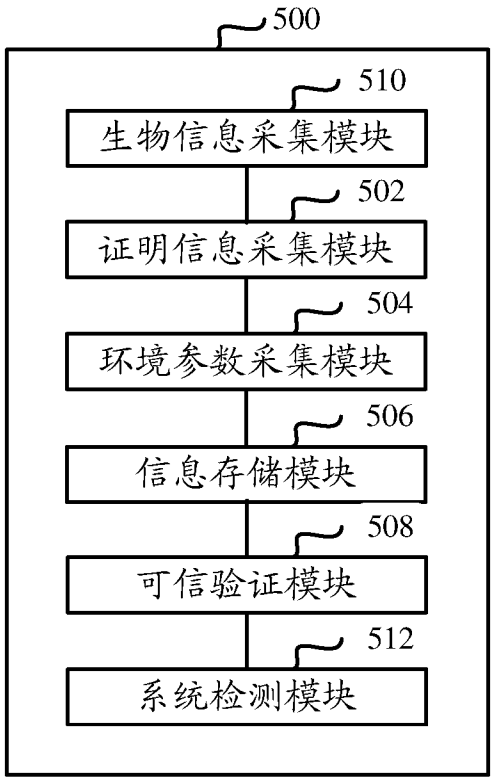

500
510
生物信息采集模块
502
证明信息采集模块
504
环境参数采集模块
506
信息存储模块
508
可信验证模块
512
系统检测模块

图 5

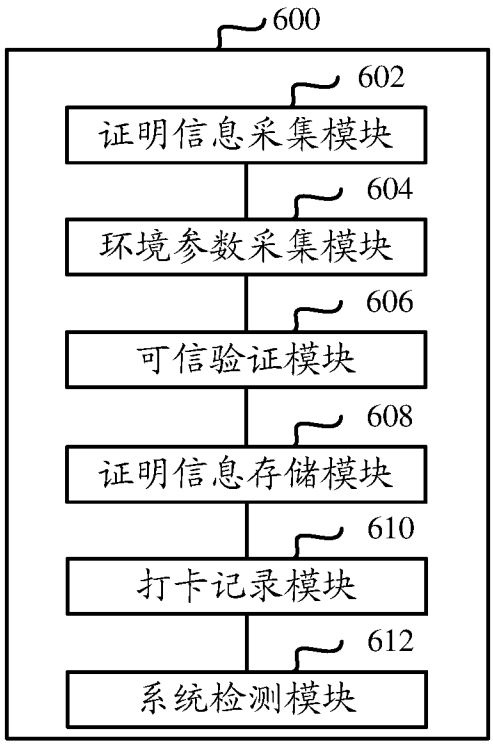

600
602
证明信息采集模块
604
环境参数采集模块
606
可信验证模块
608
证明信息存储模块
610
打卡记录模块
612
系统检测模块

图 6

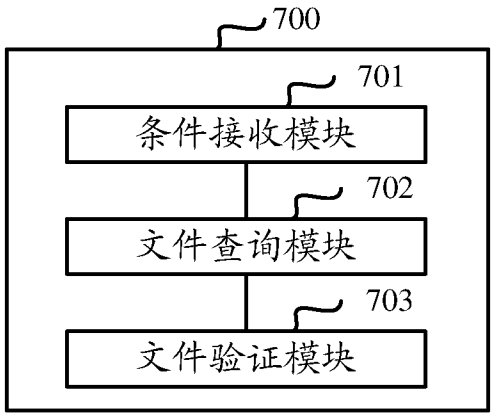

700
701
条件接收模块
702
文件查询模块
703
文件验证模块

图 7

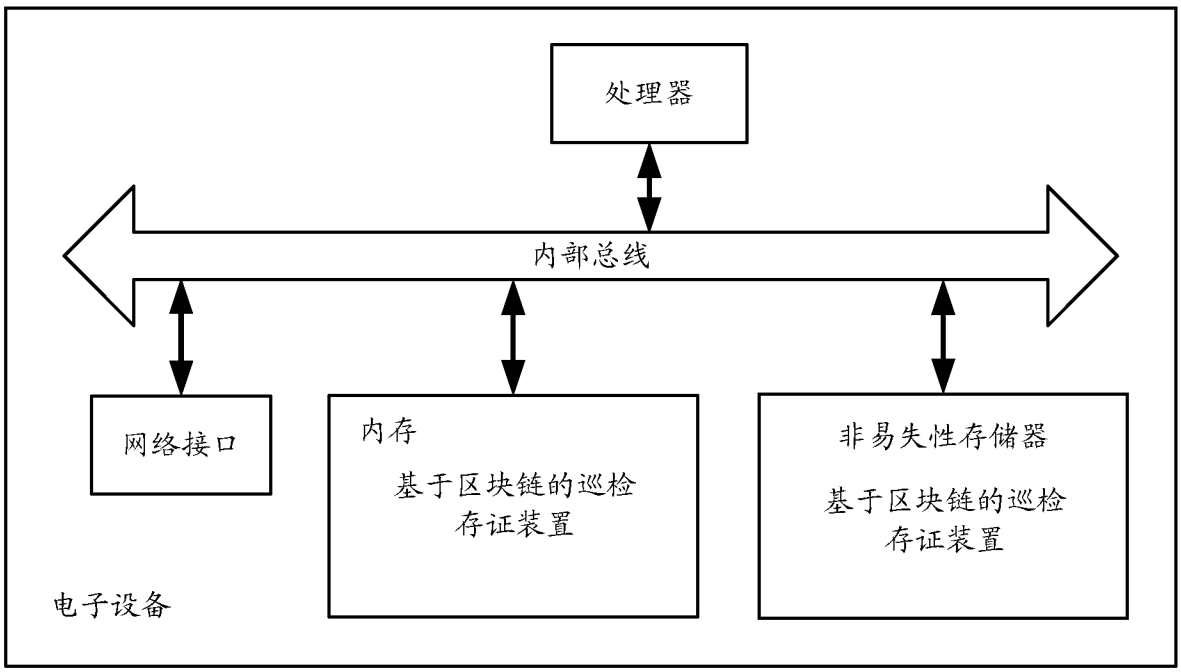

处理器
内部总线
网络接口
内存
基于区块链的巡检存证装置
非易失性存储器
基于区块链的巡检存证装置
电子设备

图 8

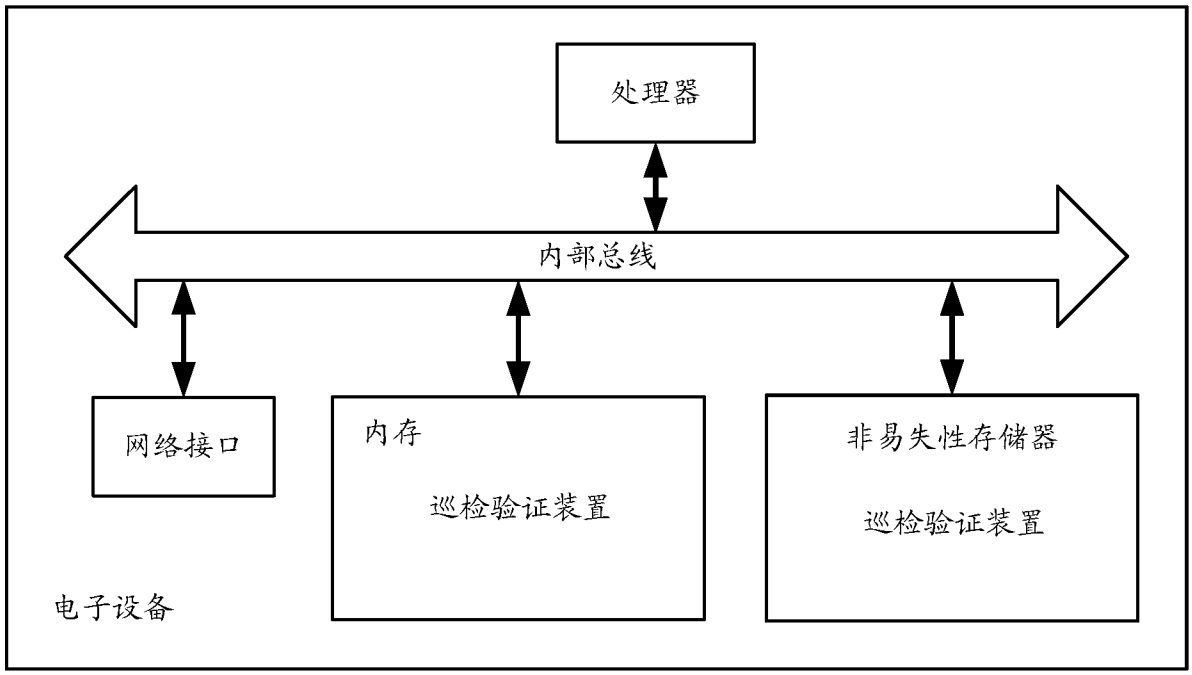


图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/071563

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00(2009.01)i; G07C 1/20(2006.01)i; H04W 12/10(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; USTXT; WOTXT; EPTXT: 巡检, 巡更, 巡视, 巡查, 巡逻, 检查, 查看, 工作, 存证, 记录, 证明, 证据, 区块链, 位置, 定位, 传感器, 环境, 温度, 湿度, 气压, 校验, 时戳, 时间戳, inspection, inspecting, patrol, proof, evidence, blockchain, position, location, GPS, sensor, timestamp

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110337104 A (ALIBABA GROUP HOLDING LIMITED) 15 October 2019 (2019-10-15) claims 1-22	1-22
Y	CN 107767478 A (ALIBABA GROUP HOLDING LIMITED) 06 March 2018 (2018-03-06) description, paragraphs [0039]-[0073], [0092]-[0110]	1-22
Y	CN 206058312 U (STATE GRID JIANGSU ELECTRIC POWER COMPANY, YANCHENG POWER SUPPLY COMPANY et al.) 29 March 2017 (2017-03-29) description, paragraphs [0022]-[0042]	1-16, 18-19, 21-22
Y	CN 109615724 A (HAOYUN TECHNOLOGIES CO., LTD.) 12 April 2019 (2019-04-12) description, paragraphs [0043]-[0063]	2-5, 17, 20
A	CN 109446830 A (SINOCHAIN TECHNOLOGY CO., LTD.) 08 March 2019 (2019-03-08) entire document	1-22
A	CN 108574734 A (SHANGHAI ELECTRIC HIGH-VOLTAGE INDUSTRIAL CO., LTD.) 25 September 2018 (2018-09-25) entire document	1-22
A	US 2005211777 A1 (GEN ELECTRIC) 29 September 2005 (2005-09-29) entire document	1-22

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 March 2020	**27 March 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/071563

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110337104 A	15 October 2019	None	
CN 107767478 A	06 March 2018	HK 1249646 A0	02 November 2018
CN 206058312 U	29 March 2017	None	
CN 109615724 A	12 April 2019	None	
CN 109446830 A	08 March 2019	None	
CN 108574734 A	25 September 2018	None	
US 2005211777 A1	29 September 2005	US 8914046 B2	16 December 2014
		US 9904274 B2	27 February 2018
		US 2015073603 A1	12 March 2015
		US 2009082039 A1	26 March 2009
		US 2012258739 A1	11 October 2012
		US 8244276 B2	14 August 2012
		US 7428419 B2	23 September 2008

国际检索报告

国际申请号
PCT/CN2020/071563

A. 主题的分类

H04W 12/00(2009.01)i; G07C 1/20(2006.01)i; H04W 12/10(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; G07C

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;CNKI;VEN;USTXT;WOTXT;EPTXT:巡检，巡更，巡视，巡查，巡逻，检查，查看，工作，存证，记录，证明，证据，区块链，位置，定位，传感器，环境，温度，湿度，气压，校验，时戳，时间戳，inspection, inspecting, patrol, proof, evidence, blockchain, position, location, GPS, sensor, timestamp

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 110337104 A (阿里巴巴集团控股有限公司) 2019年 10月 15日 (2019-10-15) 权利要求1-22	1-22
Y	CN 107767478 A (阿里巴巴集团控股有限公司) 2018年 3月 6日 (2018-03-06) 说明书第[0039]-[0073]、[0092]-[0110]段	1-22
Y	CN 206058312 U (国网江苏省电力公司盐城供电公司 等) 2017年 3月 29日 (2017-03-29) 说明书第[0022]-[0042]段	1-16、18-19、21-22
Y	CN 109615724 A (浩云科技股份有限公司) 2019年 4月 12日 (2019-04-12) 说明书第[0043]-[0063]段	2-5、17、20
A	CN 109446830 A (中链科技有限公司) 2019年 3月 8日 (2019-03-08) 全文	1-22
A	CN 108574734 A (上海电力高压实业有限公司) 2018年 9月 25日 (2018-09-25) 全文	1-22
A	US 2005211777 A1 (GEN ELECTRIC) 2005年 9月 29日 (2005-09-29) 全文	1-22

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 3月 17日	2020年 3月 27日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 李福涛 电话号码 86-(20)-28950443

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/071563

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	110337104	A	2019年 10月 15日		无		
CN	107767478	A	2018年 3月 6日	HK	1249646	A0	2018年 11月 2日
CN	206058312	U	2017年 3月 29日		无		
CN	109615724	A	2019年 4月 12日		无		
CN	109446830	A	2019年 3月 8日		无		
CN	108574734	A	2018年 9月 25日		无		
US	2005211777	A1	2005年 9月 29日	US	8914046	B2	2014年 12月 16日
				US	9904274	B2	2018年 2月 27日
				US	2015073603	A1	2015年 3月 12日
				US	2009082039	A1	2009年 3月 26日
				US	2012258739	A1	2012年 10月 11日
				US	8244276	B2	2012年 8月 14日
				US	7428419	B2	2008年 9月 23日