**一种基于低功耗广域网和区块链的流行病密切接触者追踪方法**

**技术领域**

本申请涉及LPWAN远距离通信技术领域和区块链技术领域，尤其涉及一种基于LPWAN上报用户行动踪迹的方法。

**背景技术**

新型冠状病毒COVID-19引起的肺炎2020年在全世界流行，造成了数以十万计的无辜生命死亡，致至少数千万人感染。

目前，各国政府和科技公司都在尝试提供科学的流行病学调查辅助方法。比较著名的是中国的健康码，各个省份甚至各个城市都推出了自己的健康码，这在中国被证明是一种有效的方式。它存在几个非常重要的缺陷，第一、许多老年人、儿童没有智能手机或者即使有也在操作上有很大的障碍，上网人数有限。第二、由于工作人员不足，或是忙于测温工作，导致对健康码的检查存在漏洞。第三、由于网络环境导致APP无法调用，从而滞留大量人群引发聚集风险。第四、由于各地政府的政策不一致，导致每到一个地方就要申请新的健康码，甚至同一人到不同的省市申请到的健康码结果不同的情况，而在健康码互认的问题上更是矛盾多多。另外，在用户使用的友好程度上，现行的健康码也并不令人满意，首先就是一次出行需要反复的打开手机。其次，APP的安全性令人担忧，虽是由政府掌控个人关键信息，但是难以保证其他恶意软件通过手机上的漏洞窃取到健康码APP的内容。而且由于智能手机性能、APP权限、网络故障和人为因素导致的关键信息遗漏问题有可能大大影响流行病学调查的准确性和完整程度。

2020年五月份两大科技巨头苹果和谷歌联合推出了一种密切接触者追踪系统，工作原理仍基于智能手机和APP，系统运行时，手机就会周期性地弹出一段小的、唯一的、匿名的代码，这段代码是从手机的唯一ID中提取出来的。其他手机会接收并记住这段代码，建立一个记录他们接收到的代码和接收到它们的时间的日志。相反，设备也会接收其他设备发来的代码。为了保护隐私，这段代码还会每隔一段时间更新一次。当使用该系统的人确诊患病后，他可以选择将自己的确诊信息上传到服务器上，其他用户定期从服务器上下载确诊信息，并与本地所存储的他人代码比对，如果有匹配项，则意味着自己与确诊患者曾密切接触过，从而决定自己的下一步医治计划。但是此类系统就其防疫效果来讲是很差的。首先，要求这些甚至反对口罩的美国民众下载此APP并持续使用就是很困难的，出于文化和历史的原因，愿意花时间和精力去做防疫工作的民众并不占绝对多数，如果不是参与社交的每一个人都开启了这项服务，那整个过程的效果就大打折扣。第二、依靠患者自主上传的方式并不可靠，确诊者极有可能因为主观或是客观原因没有上传确诊信息，那整个环节就失效了。第三、即使前序流程顺利，当一名用户获知自己成为了密切接触者时，他极有可能因为是一名无症状感染者或仍存在潜伏期没有发病而拒绝前往医疗点检测和治疗，并继续参与日常社交活动传播病毒。另外，由于此系统的保密机制，只要用户不前往医院，外人甚至是政府医疗机构无法获知用户的身份和接触情况，也不能及时为其提供最佳救治方案。

其他的方法还包括借助运营商网络的，比如中国国务院、信通院与三大运营商合作的防疫大数据行程码，可以根据手机使用连接基站的情况判断持有者到访过哪座城市，甚至哪个区。此码的作用更多体现在远程出行中，并不针对特定的确诊患者的密切接触，而是从地区的风险评级上判断一个人可能的健康程度。与健康码相比，此系统似乎不需要用户的主动参与，但是在实际使用中其灵敏度不高，例如短暂停留一个城市时，并没有该城市的记录，而需要至少拨通一次电话才可以。相反，也出现了仅仅在火车上路过却被记录在案的情况。另外一个风险是，一些投机者可以利用双卡的优势，完美的避开轨迹被记录，从而给追溯带来困难。

**发明内容**

一种基于低功耗广域网和区块链的流行病密切接触者追踪方法，包括四个部分：LoRa通信部分、有线网络通信部分、踪迹区块链、风险匿名名单。LoRa通信部分包括用户设备和场所设备两个组成成分，设备与设备之间通过两种LoRa信号进行通信，场所设备和用户设备之间的LoRa信号为SF=7，场所设备和地区服务器之间的LoRa信号为SF=12，场所设备和用户设备的计算能力都比较弱，但是功耗低、成本低、数量多。有线网络部分包括地区服务器、医疗机构和地理信息服务器三部分组成，设备与设备之间通过有线网络通信，这三个组成部分的计算能力比较强、数量少，属于官方设备。

所述踪迹区块链是用于记录用户踪迹信息的区块链，只保存近十四天(336小时)内产生的区块，一条踪迹记录存储在一个区块中，包括：产生踪迹的时间、用户匿名、产生踪迹的地理位置、上传该踪迹的地区服务器的签名、上一个块的哈希值、本块的哈希值。踪迹时间是以时间戳形式记录的，精确到分钟； 用户匿名信息是在字符串“ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789”内随机挑选16个字符组成的新的16位字符串，字符可重复、有顺序差异，因此匿名信息重复的概率极低，可以忽略不计；产生踪迹的地理位置信息是字符串类型，属于官方的识别代码；签名信息以字符串形式保存，可用于验证该记录的合法性；

所述风险匿名名单是用于记录和警告用户的名单，其中记录了具有与确诊患者接触风险的用户所使用过的匿名。该名单以集合类型保存，可以保证每个匿名信息不重复，减少了数据的冗余，有利于在计算能力较弱的用户设备和场所设备使用。

所述场所设备是固定在场所中的、电源供电的设备，它监听范围内用户设备发送的匿名信息，并与地区服务器交换数据，可以收发SF=7和SF=12的LoRa信号。

场所设备和用户设备是同一种物理设备的两种模式，可以通过按键转换。场所设备模式需要由持有者向有关部门专门申请获得，以获得自身固定的地理位置信息(一种官方的识别代码)。该设备结构简单、功能简单、没有可修改性，防止了不法分子上传假数据。

在用户设备模式下(如图2)，该设备接收并识别场所设备发送的JSON打包的唤醒信息(字符串类型的专门的识别编号)，并保存伴随唤醒信息发来的风险匿名名单(16字符的字符串组成的列表)在内存中。之后该用户设备向场所设备发送JSON打包的当前匿名信息(16字符字符串)作为回复，并同时将最近14天使用过的匿名信息从存储中调入内存，与风险匿名名单进行匹配，如果匹配成功且本来用户的感染风险级别为无风险(绿色)，则更改感染风险级别为有风险(黄色)。

在用户设备模式下，风险用户(指示灯黄色)需要前往指定官方医疗机构检查并且医疗人员可以获取存储在设备中的所有近14天使用过的匿名。若用户前往医疗机构检查并确诊为患者，则医疗人员可以将设备的用户的感染风险级别更改为患病(红色)。若该用户经检查后确定没有检测出病毒，则医疗人员可以将设备的用户的感染风险级别更改为无风险(绿色)。

在场所设备模式下(如图3)，设备周期性地向周围环境发送JSON打包的唤醒信息(特殊编号的字符串)以及本地内存中的风险匿名名单，并随时接收接收范围内的用户设备发来的匿名信息(JSON打包的16字符字符串)并加上时间戳、地理位置信息作为一条踪迹信息存在内存中。

在场所设备模式下，如果设备中存有未上报的踪迹信息，设备会周期性地(周期为10秒)分部分向指定的地区服务器每次发送踪迹信息，即上报，由于LoRa包的大小限制，每次发送两条踪迹信息，并等待来自地区服务器的ACK信息以及伴随ACK信息发来的风险匿名名单。每次发送2条踪迹信息后该设备会等待ACK信息5秒钟时间，如果5秒时间后设备未收到来自地区服务器的ACK信息，则再次发送并继续等待ACK5秒钟，如此反复直到接收到ACK信息。

在场所设备模式下，当设备接收到来自地区服务器的JSON打包的ACK信息和风险匿名名单后，设备会将踪迹信息列表中的首位2条信息(最近发出并接收到ACK的2条踪迹信息)删除，并把接收到的新的风险匿名名单保存到内存中，以随后同唤醒信息一起发送给用户设备。

所述地区服务器是固定在一定地理位置上的高计算性能、高信号收发性能的设备，接收范围较大，可以接收区级行政单位范围内的来自场所设备的基于SF=12、频段为CN470的LoRa的踪迹信息，也是连接LoRa无线网通信和有线网通信的网关设备，接收踪迹信息并将该信息签名后上传到踪迹区块链上，具有验证踪迹信息、维护区块链的功能。

所述医疗机构是指每个可以对流行病病毒进行检测的官方的医疗机构，这些医疗机构也参与区块链的维护，可以上传患者匿名名单、删除风险匿名名单中的匿名信息、修改用户设备指示灯的颜色。

所述地理位置信息服务器是用于获取患者的匿名信息、查找患者的匿名信息对应的踪迹信息并以此来寻找其他风险踪迹、确认并通知其他有线网部分内的设备新增的风险匿名名单的设备，属于官方设备。

本发明的有益效益：本发明的追踪方法利用了LoRa技术，LoRa具有低功耗、远距离的优点，可以极大地降低用户设备的功耗，减少了维护所需的成本，提高了使用的便捷度。利用了区块链技术和电子签名，提高了踪迹数据的可靠性和筛选风险用户的效率，消除了不法分子篡改数据的可能性。利用匿名方法，只用官方的医疗机构才能知道匿名用户的真实身份，保护了用户的隐私权。

**附图说明**

图1为系统流程图。

图2为设备用户模式工作流程图。

图3为设备场所模式工作流程图。

图4为踪迹区块链图。

**具体实施方式**

以下结合技术方案和说明书附图，进一步说明本发明的具体实施方式。

一种基于低功耗广域网和区块链的流行病密切接触者追踪方法，图1为系统流程图，具体流程如下：

场所设备总共运行两个线程：接收兼处理线程和发送线程；

首先会向地区服务器发送基于SF=12、频段为CN470的LoRa信号的、JSON打包的、UDP形式的时间戳请求信息，从地区服务器获取当前时间戳，只有获取了当前的时间之后，场所设备才能开始正常工作，否则不能进行正常工作，即脱离了地区服务器场所设备就失去了意义；

场所设备会周期性地向周围环境发射基于SF=7、频段为CN470的LoRa信号的UDP信息，起到唤醒用户端设备的作用；

用户设备总共运行四个线程：维护匿名信息的线程、发送线程、接收兼处理线程、指示灯控制线程。会周期性地更换匿名信息，周期为1天(24小时)。用户设备会将最近14天使用过的14或15个匿名存储在设备中： 当某个匿名信息的存在时长超过14天后，会被用户设备检测出来并删除；当最新的匿名信息存在时长满24h后，用户设备会产生一个新的匿名；

当用户设备进入场所设备的范围后，便可以接收到场所设备发送的唤醒信息和风险匿名名单，用户设备接收之后便回复带有匿名信息的UDP包，用户设备回复给场所设备的信息包括该用户的16字符匿名信息、10位的int类型序列号、标识发送设备种类的字符串，以JSON的形式打包发送；

场所设备于是可以接收到用户设备发来的匿名信息，并将接收到该匿名信息的时间、该匿名信息、自身的地理位置信息代码结合在一起，构成踪迹信息放入缓存中，周期性地向对应的地区服务器发送缓存中的部分踪迹信息；

场所设备发送给地区服务器的信息包括2条踪迹信息(受UDP包的大小限制)、发送设备的种类识别、对应地区服务器的编号、10位的信息序列号。每次发送后，场所设备会等待接收来自对应的地区服务器的ACK信息，如果固定时间5秒内未收到ACK信息，则重复发送后继续等待ACK信息，直到接收到ACK信息才会发送下一部分踪迹信息，其中重复发送的信息的序列号相同；

地区服务器可以接收更大范围内的来自场所设备的基于SF=12、频段为CN470的LoRa的踪迹信息，接收成功后返回ACK、风险匿名名单、对应的序列号，如果反复接收到具有相同序列号的踪迹信息，则每次都返回ACK信息，但是只在第一次上传该踪迹信息到区块链；

地区服务器总共运行三个线程：区块链维护线程、接收兼处理线程、发送线程，是连接LoRa无线网通信和有线网通信的网关类型设备，也具有验证签名、维护区块链的功能。接收UDP踪迹信息并将该信息签名上传到踪迹区块链，最终在区块链中一个区块所包含的内容有(参考图2)：踪迹记录、上传者代码(便于匹配公钥验证签名)、签名、本区块的哈希值、上一区块的哈希值；

每次地区服务器接收到新的踪迹信息后，该地区服务器会使用自己的私钥对将该踪迹信息进行签名、加入区块链并发送给其他联网的地区服务器设备，每个地区服务器都存有所有其他地区服务器的公钥，其他地区服务器设备会验证该条踪迹信息，如果验证成功则加入自己维护的区块链中，否则丢弃该信息，通过区块链技术可以极大地提高风险接触追踪的可靠性，避免被不法分子私自利用和篡改；

医疗机构具体是指每个可以对流行病病毒进行检测的医疗机构，当风险用户来到医疗机构检查后，无论是否患病，医疗机构需要将其所使用过的所有匿名信息从风险匿名名单中删除；

当有用户到医疗机构检查并确诊后，医疗机构有权获取该用户近14天内使用过的所有匿名并上传给地理位置信息服务器，并将该患者的用户设备指示灯改为红色；

地理位置信息服务器收到来自各个医疗机构发来的新患者的匿名信息后，将这些匿名信息在踪迹区块链中进行比对，找到患者所有的踪迹记录，并将与该患者在同一时间范围内(这里为患者踪迹记录的时间前后10分钟内，因为用户可能是在上一次唤醒信息广播后到下一次广播开始前到达场所)、同一地点出现的踪迹记录筛选出来作为风险踪迹记录，提取出这些风险踪迹记录对应的匿名信息作为新增的风险匿名名单加入已有的风险匿名名单中，通知给所有地区服务器；

场所设备会接收到来自地区服务器的风险匿名名单，该名单信息会与ACK信息一起被发送给场所设备，场所设备接收后再将该风险匿名名单发送给用户设备，自己不对风险匿名名单做任何处理；

场所设备会将集合类型的风险匿名名单信息与唤醒信息一同打包为JSON通过UDP信息一起发送给用户设备，之后用户设备会将收到的风险匿名名单和自己近14天内使用过的匿名名单进行匹配，如果匹配成功并且指示灯颜色本来为绿色，则指示灯颜色变为黄色。指示灯颜色为黄色的用户有义务去医疗机构进行诊断，减少传播风险；

当患者痊愈后，医疗机构可以将该用户的设备指示灯改为绿色。

至此，本领域技术人员应认识到，虽然本文已详尽示出和描述了本发明的多个示例性实施例。但是，在不脱离本发明精神和范围的情况下，仍可根据本发明公开的内容直接确定或推导出符合本发明原理的许多其他变型或修改。因此，本发明的范围应被理解和认定为覆盖了所有这些其他变型或修改。