

基于区块链技术的人员流动信息监管系统^①



吴源昊^{1,2}, 解 大¹, 王 宇²

¹(上海交通大学 电子信息与电气工程学院, 上海 200240)

²(华东建筑设计研究院, 上海 200070)

通讯作者: 吴源昊, E-mail: 2573925569@qq.com

摘 要: 在全球化时代, 随着人员流动频率的增加, 疫病的传播途径种类和速度都大大超过以往. 阐述了建立基于区块链技术的人员流动信息监管系统的基本原理和方法, 在重大传染病疫情发生时, 对来自疫区的人员以及确诊或疑似患者的人员流动信息实时监控, 查询人员流动历史, 寻找密切接触者, 搜索感染源, 以采取隔离等措施进行疫情防控工作.

关键词: 区块链; 人员流动信息监管; 传染病; 疫情防控; 大数据; 物联网

引用格式: 吴源昊, 解大, 王宇. 基于区块链技术的人员流动信息监管系统. 计算机系统应用, 2021, 30(2): 43-51. <http://www.c-s-a.org.cn/1003-3254/7798.html>

Personnel Mobility Information Monitoring and Management System Based on Blockchain

WU Yuan-Hao^{1,2}, XIE Da¹, WANG Yu²

¹(School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)

²(East China Architectural Design & Research Institute Co. Ltd., Shanghai 200070, China)

Abstract: At the age of globalization, as the increase in the personnel mobility rate, the transmission modes and speed of epidemic diseases go far beyond those in the past. The basic principles and methods of building the personnel monitoring and management system based on the blockchain technology were expounded. When a major infectious disease attacks, the people from the epidemic area and confirmed or suspected patients are monitored in real time. The system can inquire into the history of personnel mobility, find close contacts, and search for the sources of infection, which can support isolation measures for epidemic prevention and control.

Key words: Blockchain; personnel mobility information monitoring and management system; epidemic disease; epidemic prevention and control; big data; Internet of Things (IoT)

1 引言

近期, 我国发生新型冠状病毒感染的肺炎疫情, 根据中华人民共和国国家卫生健康委员会公告^[1], 将新型冠状病毒感染的肺炎纳入《中华人民共和国传染病防治法》规定的乙类传染病, 并采取甲类传染病的预防、控制措施.

根据 2013 年修订的《中华人民共和国传染病防治法》第四章规定, 采取甲类传染病的预防、控制措

施时, 对病人、病原携带者, 予以隔离治疗, 隔离期限根据医学检查结果确定; 对疑似病人, 确诊前在指定场所单独隔离治疗; 对医疗机构内的病人、病原携带者、疑似病人的密切接触者, 在指定场所进行医学观察和采取其他必要的预防措施. 拒绝隔离治疗或者隔离期未满足擅自脱离隔离治疗的, 可以由公安机关协助医疗机构采取强制隔离治疗措施.

与流行传染病患者密切接触的人, 自身被感染的

① 收稿时间: 2020-06-29; 修改时间: 2020-07-01, 2020-07-31; 采用时间: 2020-08-10; csa 在线出版时间: 2021-01-27

风险很高,并且有可能进一步传染他人.因此,追踪并观察这些密切接触者有助于这些高危人群第一时间得到护理和治疗,并防止病毒进一步扩展,这也是流行病控制的关键^[2].大数据能够在对接触者追踪、数据预测和流行病学传播模型建立等方面具有重要的意义.利用大数据的手段对确诊病例、疑似病例人员进行追踪、监管,在保护个人隐私的情况下,挖掘其人员流动信息,筛查同行人员,从而对密切接触人群进行重点观察和隔离预防,对防止传染病疫情扩散将大有帮助.

2月4日工信部发布《充分发挥人工智能赋能效用协力抗击新型冠状病毒感染的肺炎疫情倡议书》,2月26日国家卫健委公布《近期防控新型冠状病毒感染的肺炎工作方案》要求利用大数据等技术开展人员追踪.

基于区块链技术,以地点坐标为区块建立基础链来做数据的记录,并以被监测人员为区块建立虚拟链来做数据的校验和查询,组成双重区块链;利用用户在网络平台等环境下的动作记录来反映其位置信息,并存储在区块链中.由此建立人员流动信息监管系统,并授予公安机关和疾控中心查询权限,能高效地查到确诊患者、疑似病例或是疫区流出人员的流动轨迹和密切接触者,有效展开疫情防控工作.

在当前技术条件下,通过基站数据(手机定位)、支付数据(微信、支付宝、银联等)、出行数据(列车、航班、住宿)、城市公共安全视频监控(人脸识别)等建立大数据融合平台,通过区块链技术实现各部门各行业各地区的数据融合,充分利用物联网设备的边缘计算能力、充分利用资源.区块链技术保证了大量数据在传输过程和存储过程中的可靠性、自动化、便捷性.

2 基于区块链技术的人员流动信息监管系统的基本原理和方法

2.1 术语和定义

以大写字母 BM 表示系统协议,如代码、节点、网络及其对等交互.

以小写字母 bm 表示个人身份,即对个人身份的信息作定义,如某一个人的身份证以及所对应的护照 ID、手机号码、车辆车牌号码、支付宝账户、微信账户、银行卡号、人脸识别认证信息、所属单位一卡通等能确定个人身份的信息,确定其为区块链中的某一个人,定义为 bitman.

一个 transaction 记为 tx 表示某个人在某一确定时间的人员流动信息记录,从 A 地流动至 B 地.

txid 是 transaction ID 的缩写,即系统协议引用人员流动信息的哈希值.

某个坐标节点 (coordinate),如居住地、商场/商店、某个医院/学校办公楼的某个区域、飞机航班、高铁班次,作为一个坐标节点的地址,即为区块链 (Blockchain) 中的区块.

Yuanhao 表示某个坐标节点中 bitman 人口数量, 1 btm = 1 bm(Y).

2.2 人员流动信息记录过程

一个人员流动信息 (transaction) 的周期^[3]为:

- 1) 当某人从 A 地流动至 B 地,某坐标地发出人员流动信息交换请求;
- 2) 广播人员交换请求到 P2P 网络;
- 3) 验证人员流动信息的正确性;
- 4) 多个人员流动信息组成一个区块;
- 5) 新的区块加入到一个已经存在的区块链中;
- 6) 人员流动信息确定完成.

人员流动信息记录原理如图 1 所示.

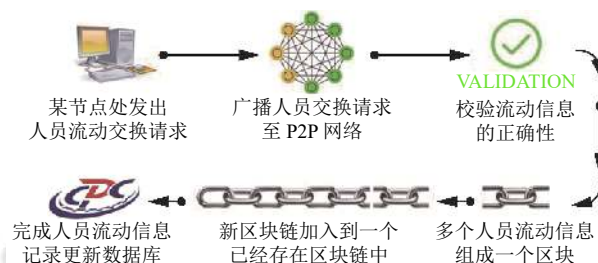


图 1 人员流动信息记录原理

2.3 人员身份证明和位置确定

记录人员流动信息时,如何确定一个人的身份,也就是如何证明“你是你”的问题.为了证明一个人到过一地方,可以把所有可以证明身份的信息,如身份证号、护照号、手机号、拥有车辆的车牌号、微信账户、支付宝账户、银行卡信息、人脸识别认证信息等,人员的这些身份信息为私钥;将这些信息全部绑定至身份证号或护照号,身份证号或护照号是区块链中的公钥;再生成一个属于个人的身份哈希,作为公钥的哈希值,也就是在区块链网络中用于保存和查询的值.不同环境的人员监控措施如表 1 所示.

当某个坐标地址 (coordinate) 读取到个人信息时,如某人在酒店用身份证+人脸识别进行登记、在办公

地出入口刷门禁卡或用身份证进行访客登记、在某商店/饭店消费时使用微信支付,此时系统会生成一个坐标地址,并在区块链系统中广播.

此系统实现的基础是监控设备(如摄像头、读卡器等)的物联网化^[4],监控设备必须是带网络地址的物联网设备,并具有一定的边缘计算能力,可以保持互联网连接状态^[5].

表1 不同环境的人员监控措施

所处位置	读取人员信息	物联网设备
跨地区收费站	车牌号	收费站摄像头
酒店	身份证	酒店身份证读卡器
航班	身份证/护照	取票机、人工录入信息设备、安检设备等
火车	身份证	取票机、安检时身份证读卡器
办公楼、住宅	工作证	门禁/电梯等刷卡器、人脸识别摄像头
学校	学生证	校园一卡通刷卡器
商场、公园等公共场所	人脸识别	人脸识别摄像头
餐饮、购物等消费场所	支付宝、微信	扫码支付终端、刷脸支付终端
手机定位	手机号	智能手机(通过基站、卫星、WiFi等定位)

2.4 人员流动信息记录

当某人从A地流动到B地,记录一个人员流动信息的tx,需由B地确认人员信息后,再由A地使用签名算法对人员流出进行确认,人员流动信息确认过程如图2所示.

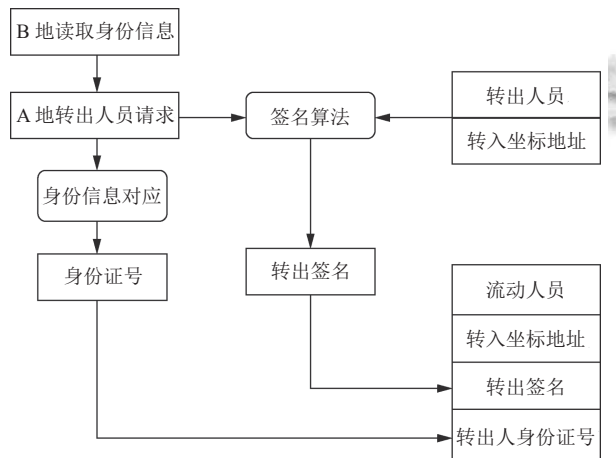


图2 人员流动信息确认过程

图2是某人从A地到B地流动时,两地对单次人员流动信息进行确认的过程. A地和B地是网络中的两个不同的位置节点,当某人从A地转移到B地时,

在转出A地时A地广播了这个消息, B地在获取此人的身份信息后在网络中查询了此人的转出地, 确认此人原先所在地是A地并请求与A地连接通信. 然后A地对B地发送此人的流出请求和流动信息, B地收到A地的信息, 且发送给A地此人流动到B地的信息.

两地发送的信息中包含了此人的身份信息(对应的身份证号)、到达时间、两地坐标信息等. 为了让A、B两地同时确认此人从A地流动到B地, 并在网络中取得认可, 需要有一个转入/转出签名和确认的过程: A地把转出人员请求、转出人员身份信息、A地坐标地址、人员转入的地址(B地坐标地址)等打包作为待签名数据, 并附上A地的转出签名, 发送给B地; B地确认后, 附上B地的转入签名, 一个完整的人员流动信息即创建成功, 该信息也可以发送给网络中其他节点进行验证.

例如人员甲, 从A地转出, 在某时某刻到达B地, 则B地和A地所发布的人员流动信息如图3所示.

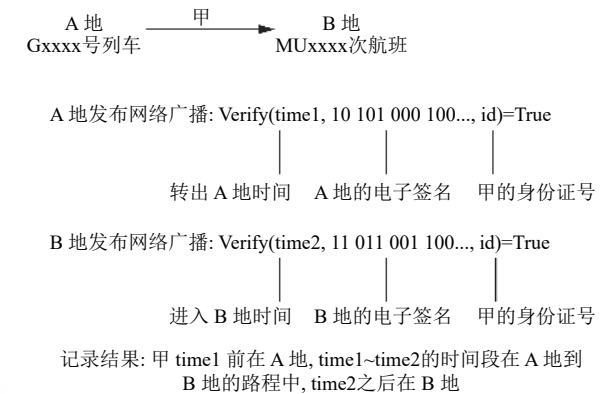


图3 人员流动信息的发布

此时, 区块链对应的相关区块会对发布的信息做校验, 如图4所示.

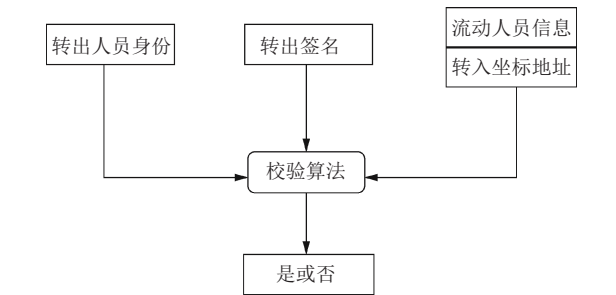


图4 人员流动信息校验

如果校验时发现人员流动信息有矛盾之处, 如A地发布的是北京到上海的列车信息且此刻列车没有到

达,而B地发布的是到达广州的航班信息,那么此次的人员流动信息是矛盾不成立的,校验失败则不能在系统中记录此次人员流动信息.如果A、B两地的人员身份一致且信息没有矛盾,则校验通过并在系统中记录这一次人员流动信息.

通过这个过程,某个人流动的单位信息在系统中建立完成.

2.5 区块链建立

传统的数字货币的区块链,区块的主体是账本,交易时是由账本的节点向全网广播交易记录,数字货币的交易也只记录交易数额.

而人员流动信息监管系统的区块链,由于查询和校验的需求,可由以坐标地点为区块的基础链和以被监测人员为区块的虚拟链组成双重区块链.

人员流动信息由坐标地点来发布,每一个具体的坐标位置,如一间办公室、一辆车、一架飞机、一节车厢甚至一个公共场所的走廊,都可以作为一个坐标位置的节点,成为在区块链中的一个块(block).每个区块需要完整记录当前地点的人员流动记录,形成一个分布式的数据库,以地点为区块的基础区块链如图5所示.当人员在某个区域内流动时,系统能进行自动记录,并进行快速的自动校验;当人员在跨区域流动时,机场、火车站、高速收费站等重点位置的设备需进行高优先级的确认校验,有必要时采用人工录入等手段.通过各地分布式数据库记录人员的位置信息,把区域内和跨地区的流动信息完整地储存在区块链中^[5,6].

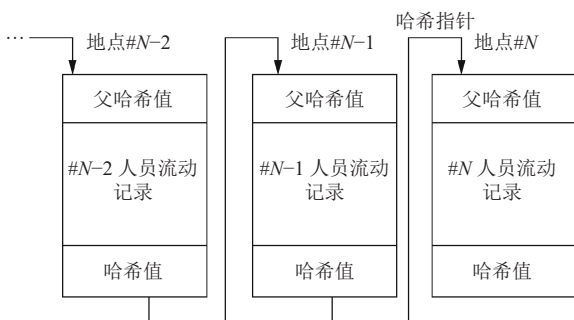


图5 以地点为区块的基础区块链

每个参与到人员流动信息监管系统区块链中的位置节点,如某个班次的高铁/航班、某个酒店/商场/办公楼等,可以由业主自行申请的,也可以是政府通过政策强制执行的.用户通过调用平台层的API,发布自己的站点服务,这是为了让系统用户能便捷地访问其他用户在系统平台上的资源.平台的系统合约由主管

部门(疾控中心或者公安机关)构建,合约必须是考虑到今后系统使用时能解决各种状况的智能合约,通过P2P网络扩散到每个节点,并存入区块链.智能合约定期进行自动机状态检查,将满足条件的事物进行验证,达成共识后自动执行并通知用户^[6].

每个节点的地点位置为使用系统的私钥,通过注册申请后,由主管部门颁发登录账号,作为登录系统的公钥,再通过公钥的哈希值,也就是在区块链网络中用于保存和查询的值,就可以生成节点所处的网络地址,整个过程中除了哈希生成坐标地址是可逆的,其他都是不可逆的,链入区块链过程如图6所示.

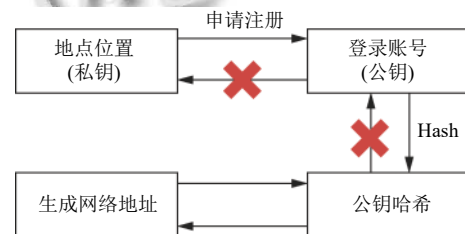


图6 链入区块链过程

此处的私钥、公钥不同于传统金融货币区块链的公钥和私钥,传统区块链的私钥是私密的,且匿名的.但本系统的私钥和公钥都是实名的,私钥被实名绑定到公钥,便于查询系统中的人员信息.私钥信息由该节点的管理者保存,并由系统的管理部门备份.系统中私钥和公钥只是一种登录系统或记录信息的工具,并不需要传统区块链的私钥和公钥之间采用SECP256K等加密方式,而是要采取实名认证的处理方式,由管理部门介入,采取必要的措施并确认.由于系统中的信息涉及公民的隐私,为了防止信息泄露和滥用,保护隐私,不仅需要在技术层面上把系统的信息安全和加密方式做好层层防护,还需要通过相关的政策法规来对系统的使用和信息进行有力监管.

此时生成一个以位置节点为账本的区块,每个区块的结构分为两部分,即区块头和区块体.

区块头包含version、prevBlockHash、merkleRoot、time和attribute. version记录了区块头的版本号,用于跟踪软件/协议的更新; prevBlockHash记录了该区块的上一个区块的Hash地址; merkleRoot记录了该区块中交易的merkle树根的哈希值; time记录了该区块的创建时间戳; attribute记录了该区块对应的节点位置属性.

区块体的内容是该区块的人员流动信息,包括人

员流动数量和人员流动数据. 区块体共分为 3 部分: numTransactionsBytes、numTransactions 和 transactions. numTransactionsBytes 记录了流动信息占用的字节数; numTransactions 记录了区块内的流动信息数量; transactions 记录了区块内保存的多个人员的流动信息.

每个区块中, 把定位、时间、人员等信息保存在区块体内, 并生成一个区块头, 用以链接前一区块和后一区块, 节点位置区块的生成和结构如图 7 所示. 当每一个新区块生成时, 都会被打上时间戳, 被保存在区块头内, 最终依照区块生成时间的先后顺序相连组成区块链, 每个独立节点又通过 P2P 网络建立联系, 这样就为信息数据的记录形成了一个去中心化的分布式时间戳服务系统^[7,8]. 区块头内还保存了 API 的版本号, 当系统发布软件/协议更新时, 可以自动更新下载. 区块体内主要记录人员流动信息的内容.

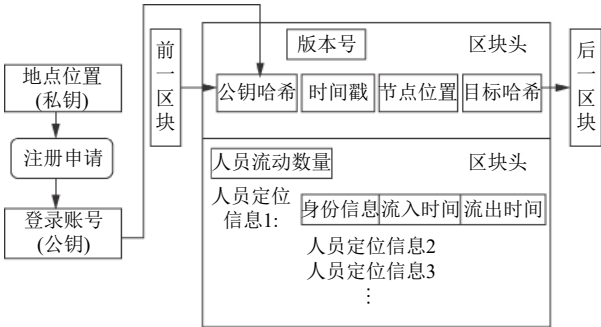


图 7 节点位置区块的生成和结构

以区、县为基础单位, 组成地区区块链; 再以省、市为单位, 组成联合区块链; 在各行业内部, 如铁路、空运、公交、商业、金融等行业, 组成行业区块链, 人员流动信息监测管理系统区块链架构如图 8 所示.

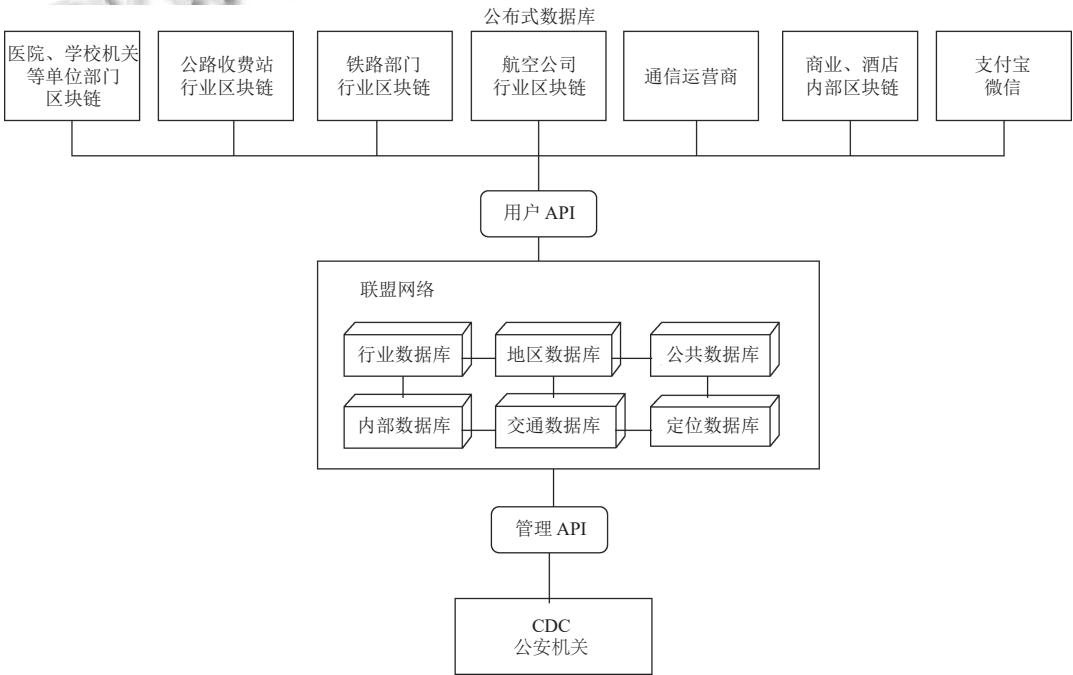


图 8 人员流动信息监测管理系统区块链架构

当不同的行业和地区产生多重区块链时, 可采用跨链技术实现跨链访问^[9], 如侧链/中继 (sidechains/relays)、以太坊联盟区块网络 (Ethereum)、哈希锁定 (Hash-locking) 等技术, 实现不同链中的信息转移和使用^[10]. 一链套一链, 一环扣一环, 形成高效的人员流动信息监管系统.

如果这个人员流动信息监管系统不是采用区块链

技术, 而是基于传统集散式的系统形式, 不仅在物理上需要建设多层级的控制中心、数据中心, 且不同行业、不同部门之间的数据协调、信息统一都需要很长时间来实现, 不同的管理部门也难以发布统一的系统.

采用区块链系统, 各单位都可以采用分布式系统, 利用已有设备进行边缘计算^[11], 不同行业和部门之间只要采用跨链技术就可以整合信息内容, 节省了大量

的建设和协调时间。

通过系统中发布的人员流动信息,以被监测人员为区块,再组成虚拟链,便于查询人员流动的路径历史,也便于人员流动信息正确性的校验。以人员不同时间段的位置信息为区块组成链,再以每个人的流动记录组成链,以人员为区块的虚拟区块链如图9所示。

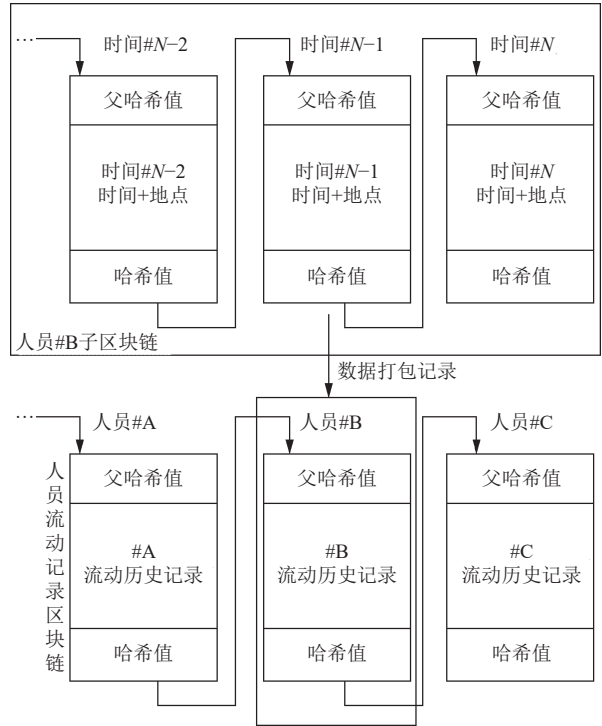


图9 以人员为区块的虚拟区块链

虚拟链的节点本身不发布信息,也没有实体的计算机节点,由只被动接受基础链的广播数据而生成,数据集中生成和保存在管理机构的系统数据库中。通过区块链的模式记录数据,是为了满足数据的可添加性,增强自我纠错能力。

在图9中,某人员#B的子区块链,以其在时间#1—时间#2—时间#3这样的时间顺序构成子区块链,人员子区块链的区块结构如图10所示。

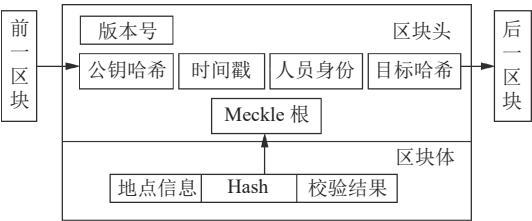


图10 人员子区块链的区块结构

图10中,区块头的时间戳直接记录了区块生成的时间,区块头还保存了人员身份信息;区块体中则记录了某一次的人员流动记录的地点信息。因此这条链的作用除了记录信息,还有校验区块链正确性的作用。

当此子区块链生成了一段时间(24h或1周)并经过校验得到了正确的链以后,可以把整条链中的人员流动信息打包到以人员为区块的虚拟区块链中进行记录(如图9),人员在这段时间的流动信息在区块体中打包,再添加区块头形成区块链结构。此区块链的主要作用是查询。记录完毕形成新的区块以后,就可把原有的子区块链删除,而每经过这样一个周期,子区块链的信息数据就被添加到人员区块链的区块体中。

在此虚拟链的区块中,人员的身份信息即为私钥,绑定至身份证件号作为区块链中的公钥;再生成一个属于个人的身份哈希,作为公钥的哈希值。以人员为区块的虚拟链区块结构如图11所示,区块头记录了时间戳、版本号、人员身份等内容,区块体内则记录了此人员在不同时间所在的地点位置信息。

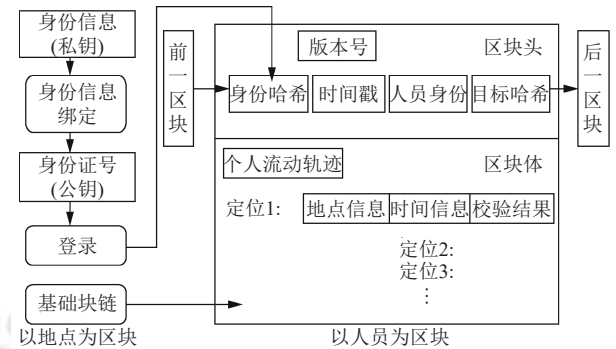


图11 以人员为区块的虚拟链区块结构

这样就生成了人员#A—人员#B—人员#C这样的以人员为区块的虚拟区块链(图9)。

2.6 区块链正确性校验

某些情况,如个人车辆被他人使用、一卡通/门禁卡借给他人、人脸识别错误等,都会产生错误的人员流动信息,为了解决这一问题,可以采用对比验证区块长度的算法,每个人员流动信息都需要广播请求到P2P网络。通过区块链中的最长链原则(the longest chain rule),验证此节点是否真有人,验证是否为真实人员所在地,这个验证过程可以通过智能合约完成。

例如,甲已经从办公室下班,甲的公司门禁卡借给正在加班的同事乙,晚上乙在办公室刷甲的公司门禁

卡, 但此时甲已经乘坐地铁下班, 通过支付宝账号在地铁站支付进出站, 并在家附近的商场入口被人脸识别摄像头探测到。在乙再次刷甲的门禁卡的相近时刻, 甲在某餐厅用刷脸支付消费, 并回家用小区门禁卡刷卡。那么甲的人员流动轨迹已经被多个区块链节点所记录, 此时乙刷甲门禁卡的动作明显不是甲本人的行为, 这个错误的人员流动信息就不能通过校验, 最长链原则校验过程如图 12 所示。

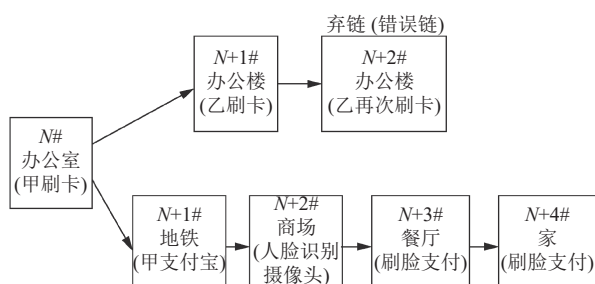


图 12 最长链原则校验过程

最长链校验的周期可以设定为 24 h, 每 24 h 确定一个人的流动轨迹是比较合理的.

考虑系统中产生错误流动信息的场景, 如果系统中收到错误的 tx 请求, 则做出如下计算论证系统准确性. 定义正确的定位请求为正确者 (链); 错误的定位请求为错误者 (链), 根据中本聪^[3] 的推导进行计算.

正确链和错误链之间的竞争可以描述为二项式随机游动. 成功事件是正确链被扩展一个区块, 使其领先优势增加 1; 失败事件是错误链被扩展一个区块, 差距减少 1. 错误者从给定差额中追赶正确者, 可以计算出错误链赶上正确链的概率.

p 为正确节点找到下一个块的概率; q 为错误节点找到下一个块的概率; q_z 为错误者从后面的 z 个块追上来的可能性, 满足:

$$q_z = \begin{cases} 1, & p \leq q \\ (q/p)^z, & p > q \end{cases} \quad (1)$$

系统将等待的请求添加到块中,并在其后链接 z 块. 系统不知道错误者的确切进度, 但假设正确的块占用了每个块的平均预期时间, 错误者的潜在进度将是具有预期值的泊松分布为:

$$\lambda = z \frac{q}{p} \quad (2)$$

为了得到错误者仍然可以追上的概率, 将其每一个进度的泊松密度乘以从该点追上的概率为:

$$f(z) = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{z-k}, & k \leq z \\ 1, & k > z \end{cases} \quad (3)$$

重新排列避免无限求和, 有:

$$f(z) = 1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} \cdot [1 - (q/p)^{z-k}] \quad (4)$$

校验计算流程如图 13 所示。

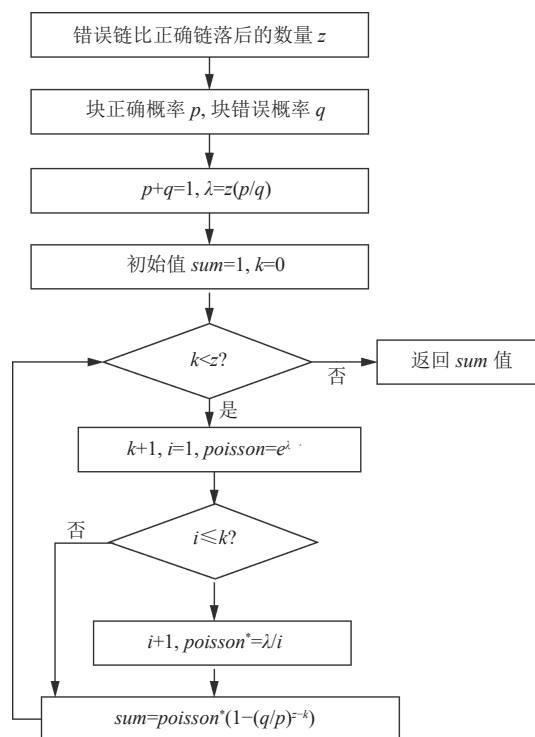


图 13 校验计算流程

系统产生错误的概率如表 2 所示, 错误的概率随 z (错误链比正确链落后的数量) 呈指数下降.

表2 产生错误块的概率 $q=0.1$ 时系统产生错误的概率

正确块比错误块多的数量 z	系统出错的概率	正确块比错误块多的数量 z	系统出错的概率
1	0.204 5873	6	0.000 2428
2	0.050 9779	7	0.000 0647
3	0.013 1722	8	0.000 0173
4	0.003 4552	9	0.000 0046
5	0.000 9137	10	0.000 0012

也就是说, 如果正确者数量比错误者数量多 10 个, 错误请求的概率是 0.1, 错误链能成功的概率只有百万分之 1.2.

但如果系统产生错误,如错误块占据数据优势时,系统需采用自动和人工的管理方式进行纠正。在数据录入时,如果物联网设备具有人工智能判断信息正确

性的能力,如某个 transaction 录入信息正确的概率很低,此时该设备应该及时发出错误警报,或给相邻或相关节点发出确认信息,再对数据的正确性做重复校验.当错误数据被区块链记录,由于区块链系统的特殊性,要再采取自动纠正就比较困难,此时就需要采用人工处理的方式进行纠正.通过人工纠正时,需要同时由转入和转出地的各相关部门确认,相关部门协调后再向系统管理部门申请修改,系统中数据的修改权限只有系统的管理部门才能持有,是系统的最高权限,能够保证系统的正确性.

2.7 提高系统性能和可扩展性

由于人员流动信息的数据量非常庞大,每一个人员流动信息如果要全网广播、全网做验证不仅难以实现,也会造成巨大的资源浪费.为保证系统的实时性和可扩展性,可采取以下几点方法:

(1) 每一个人员流动信息的验证,根据地理位置,在各区域内验证和广播.可以根据实际情况和数据量大小,以区县或者街道为范围,或以某个行业(如酒店、交通客运)为范围进行广播.

(2) 人员跨区域流动时,通过某些重要节点时,触发跨区域的广播和验证^[12],并在两个区域(省、市、区)数据库中做数据的发收和备份,例如通过高速收费站,乘坐航班,乘坐铁路列车等.

(3) 由于各行业的特殊性,不同行业的 API 通过各主管部门发布,每个行业根据自身的特点和条件建立分布式数据库,形成多个区块链网络.通过侧链技术,将不同行业的人员流动信息实现流通.

(4) 以人员为区块的虚拟链,按地理位置储存在各地区的数据库中,并在人员跨区流动时做到多地备份.分布式数据库不仅利于数据的安全性,对人员流动信息的广播、校验、记录的范围也可进行控制.

(5) 利用分片技术,将区块链网络按地理位置划分区域网络,提高系统运行速度和数据整体吞吐量.

(6) 各地区各行业的区块链形成联盟网络,定期进行数据整理,公安机关和疾控中心可以通过联盟网络全网查询数据.

3 区块链人员流动信息监控系统的应用

3.1 系统应用

举一个实际应用案例如下:

甲从武汉乘坐 2020 年 1 月 20 日的 GX0X0 号列车抵达上海,在中午 12 点离开上海火车站,通过滴滴

打车乘坐车牌号为沪 F54321 的出租车到达上海大悦城,与朋友乙一起乘坐摩天轮欣赏上海的繁华景色.然后甲发现身体不适,找到上海的朋友丙开车带其至医院检查,确诊甲已感染新型冠状病毒肺炎,甲被疾控中心采取隔离措施并进行治疗,一同来医院的丙也被采取隔离措施.此时甲的丈夫正从武汉驾驶甲的车辆(车牌号为鄂 AXXXXX)经过高速公路收费站来到河南.

此案例中,甲在系统中是以身份证号为 420100XX XXXXXX1234 的虚拟载体 bitman, GX0X0 号列车为 block 坐标节点 A,沪 F54321 的出租车为节点 B,大悦城摩天轮为节点 C,医院为节点 D,湖北至河南的某高速公路收费站为节点 E.

甲在火车站进出站检票时,节点 A 已经完成了甲的转入转出记录;甲在使用滴滴打车时,打车系统关联了甲的支付宝,并记录了其行程,完成了节点 B 的人员监测记录;甲在进入商场游玩时,乘坐的摩天轮通过微信 APP 扫码,完成了节点 C 的人员监测记录;到达医院以后,甲使用身份证就医时完成了节点 D 的记录.由于 A—B—C—D 在区块链的合约中被证实是真实有效的,甲的车辆在经过收费站时节点 E 的请求没有校验通过,在区块链中无效.

疾控中心调出甲在区块链中的节点历史,甲的历史为 A—B—C—D,各时间点的历史由区块链系统自动生成,系统通过 Merkle tree 的搜索方式,快速找到了甲 30 天内的流动历史,并确定了节点 B 沪 F54321 的出租车的司机、节点 C 中当时和甲一起乘坐摩天轮的朋友乙、节点 A 中和甲同时乘坐 GX0X0 号列车同一车厢的 50 名乘客,在区块链中共计 52 人次,成为其密切接触者.疾控中心通过区块链中记录的名单,找了这些密切接触者并采取隔离措施.

利用基于区块链技术建立的人员流动信息大数据库,建立针对目标人员的出行轨迹进行精确筛查,分析其人员流动历史轨迹.借此针对疫情防控,对接当地的确诊病例、疑似病例人员名单,政府、公安等相关部门在保护个人隐私的情况下,分析、筛选人员的出行历史轨迹,筛查到访区域,从而对这些区域进行重点观察、人员隔离和消毒处理.

3.2 系统特点

(1) 区块链系统有别于传统系统,有去中心化的特点^[13].传统系统需要层层布置,但是人员流动信息监管系统涉及的部门很多,如果需要协调公安、卫生、交

通、酒店、物业、物流等各部门、各单位系统,那么系统架设会碰到非常多的困难。而区块链系统只需要疾控中心或公安部门下发应用层的 API 并建立智能合约,通过节点把有效数据上传至互联网即可,系统架设效率高^[14],也省去了大量硬件翻新的成本。

(2) 区块链具有一致性、不可篡改性和实时性,区块链采用分布式数据库,并实时备份,只要不能掌控全部数据节点的 51%,就无法肆意操控、修改人员流动信息记录的数据,这使区块链本身变得相对安全,避免了主观人为的数据变更。这一特性极大地增强了区块链的安全性,并提高了系统响应速度。

(3) 区块链具有可添加性、拥有性和可提供性的特点。新用户只要安装管理单位下发的 API,即可链入大系统,随时投入使用。而传统系统在增加设备节点时,还需考虑总机容量和大系统的物理改造。

(4) 人员流动信息监管系统的区块链与普通区块链也是不同的:普通区块链具有匿名性,而此系统必须是实名的;普通区块链的所有用户都可以下载任意一处账本的交易记录,而此系统的数据涉及个人隐私,只有具有管理部门(如 CDC 和公安机关)授权的单位才能拥有查询权限。所以管理员的 API 和用户的 API 有所区分,用户单位只有登录和录入信息权限,管理部门才有查询权限,当系统中发生一些错误需要人工纠正时,需要多个相关管理部门确认才能得到修改权限。

4 结束语

发生新型冠状病毒感染的肺炎疫情后,监测疫区人员流动信息,隔离确诊病患和疑似病例的密切接触者的工作刻不容缓,寻找每个确诊病例的感染源对传染病防控也有重要作用。建立基于区块链技术的人员流动信息监管系统,是借助大数据信息化的手段进行信息收集的有效方式,为今后的传染病防控也能起到重要作用。

在当前时代环境下将边缘计算和区块链技术相结合,实现人员流动的监控系统。利用用户在网络平台等环境下的动作记录来反映到对应的位置信息,并存储在区块链中。利用分布式边缘计算网络和区块链技术相结合,可以充分利用边缘设备的计算能力,充分利用

资源,而区块链技术保证了数据在传输过程以及存储过程的可靠性,并在某个区域内系统自动进行记录,具有较大的便捷性。

参考文献

- 1 中华人民共和国国家卫生健康委员会. 中华人民共和国国家卫生健康委员会公告: 2020 年第 1 号. http://www.gov.cn/xinwen/2020-01/21/content_5471158.htm. [2020-01-20].
- 2 中国信息通信研究院产业与规划研究所科研管理与推进委员会. 新一代信息通信技术战“疫”应用及发展展望. http://paper.cnii.com.cn/article/rmydb_15596_290514.html. [2020-02-25].
- 3 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>. 2014.
- 4 张峻嘉, 何健豪. 人脸识别技术在智能楼宇中的应用. 智能建筑, 2019, (8): 44-47.
- 5 吴源昊. 基于区块链技术的新一代建筑设备物联网系统研究. 智能建筑, 2020, (2): 54-59.
- 6 章刘成, 张莉, 杨维芝. 区块链技术概述及其应用研究. 商业经济, 2018, (4): 170-171. [doi: 10.3969/j.issn.1009-6043.2018.04.067]
- 7 李牧阳. 基于联盟区块链的物流信息平台关键技术研究 [硕士学位论文]. 南京: 南京邮电大学, 2019.
- 8 龚玉霞, 吕家格. 一种基于区块链的数据存储系统的设计. 重庆理工大学学报(自然科学), 2019, 33(9): 190-195.
- 9 高志豪. 区块链之跨链技术介绍. 金卡工程, 2016, (11): 46-51.
- 10 刘江, 霍如, 李诚成, 等. 基于命名数据网络的区块链信息传输机制. 通信学报, 2018, 39(1): 24-33. [doi: 10.11959/j.issn.1000-436x.2018005]
- 11 陈美娟, 朱晓荣. 基于区块链的物联网设备标识研究. 物联网学报, 2018, 2(2): 18-26.
- 12 张俊. 基于混合共识的区块链冷链药品追溯系统. 物流科技, 2019, 42(12): 148-151. [doi: 10.3969/j.issn.1002-3100.2019.12.037]
- 13 Han R, Bai L, Liu JW, et al. Blockchain-based GNSS spoofing detection for multiple UAV systems. Journal of Communications and Information Networks, 2019, 4(2): 81-88.
- 14 胡卿汉, 何娟, 董青. 区块链架构下医用防疫紧急物资供应信息管理研究——以我国新型冠状病毒肺炎防疫物资定向捐赠为例. 卫生经济研究, 2020, 37(4): 10-14.