

基于区块链的传染病监测与预警技术

欧阳丽炜^{1,2}, 袁勇², 郑心湖³, 张俊⁴, 王飞跃^{1,2,5}

(1. 中国科学院大学人工智能学院, 北京 100049;

2. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室, 北京 100190;

3. 科罗拉多州立大学电子计算机工程学院, 美国 柯林斯堡 CO 80523;

4. 武汉大学电气与自动化学院, 湖北 武汉 430072; 5. 青岛智能产业技术研究院, 山东 青岛 266109)

摘要: 利用传染病预警技术和系统来监测传染病异常暴发趋势并及时准确预警, 是传染病早期防控的关键。现有传染病预警系统尚存在智能化程度不足、关键信息流通不畅和分布式协同决策困难等问题。基于区块链分布式计算架构, 结合人工智能、大数据和智能合约等新兴信息技术, 提出了一种传染病监测与预警技术及其实现框架。该技术可高效集中多方监测力量, 灵活集成多种预警手段, 在安全和保护隐私的前提下构建知识集成和智慧互联的分布式协同监测环境, 并以智能合约作为公开公正的、软件定义的监测代理来实时融合决策、监测疫情和自动预警, 从而兼顾预警准确性与及时性要求, 避免孤证和决策偏差。

关键词: 区块链; 智能合约; 人工智能; 传染病监测; 分布式协作

中图分类号: TP311

文献标识码: A

doi: 10.11959/j.issn.2096-6652.202015

A novel blockchain-based surveillance and early-warning technology for infectious diseases

OUYANG Liwei^{1,2}, YUAN Yong², ZHENG Xinhui³, ZHANG Jun⁴, WANG Fei-Yue^{1,2,5}

1. School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing 100049, China

2. The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China

3. Electrical Computer Engineering, Colorado State University, Fort Collins CO 80523, USA

4. School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China

5. Qingdao Academy of Intelligent Industries, Qingdao 266109, China

Abstract: The key of early prevention and control of infectious diseases is to use the early warning technology and system to monitor the abnormal occurrence and trend of infectious diseases. There are still some problems in the existing infectious diseases automated-alert and response systems, such as lack of intelligence, poor efficiency in exchange of key information, as well as difficulties in distributed decision-making. Based on the distributed blockchain architecture, a novel blockchain-based surveillance and early-warning technology for infectious diseases was proposed, leveraging emerging information technologies including artificial intelligence, big data and smart contract. The technology could aggregate monitoring forces from multiple parties efficiently, integrate various early warning technologies flexibly, and establish a distributed and collaborative monitoring environment for knowledge integration and intelligent interconnection with guaranteed security and privacy protection. In this framework, smart contract was served as a “software-defined agent” to fuse decisions, monitor the outbreak, and issue warnings in an automatic and real-time fashion, so as to meet the key requirements of accuracy and timeliness, and avoid the decision bias of single evidence.

Key words: blockchain, smart contract, artificial intelligence, infectious diseases surveillance, distributed collaboration

收稿日期: 2020-04-02; 修回日期: 2020-05-13

通信作者: 欧阳丽炜, ouyangliwei2018@ia.ac.cn

基金项目: 国家重点研发计划基金资助项目 (No.2018AAA0101401); 国家自然科学基金资助项目 (No.61533019, No.71702182)

Foundation Items: The National Key Research and Development Program of China (No.2018AAA0101401), The National Natural Science Foundation of China (No.61533019, No.71702182)

1 引言

急性传染病的暴发和全球流行将直接影响公众生命安全和经济社会发展,利用传染病预警技术和传染病预警系统实时监测传染病异常发生或增加的趋势以进行早期预警和及时干预,是防控传染病的关键策略。我国传染病预警体制和技术尚存在自动化、信息化、智能化及知识化程度不足的问题,由此导致的对早期未知疾病监测不敏感是预警延迟的重要原因之一。

结合人工智能、大数据、区块链及智能合约等新兴信息技术,有望改进我国传染病预警机制、技术与系统。近年来,在智能技术的推动下,与传染病预警技术相关的研究呈现预警数据多元化和预警模型复杂化的趋势,以症状监测、媒体监测和互联网检索等为代表的智能化预警技术,正逐步成为提高传染病暴发监测灵敏度和生物恐怖袭击早期发现能力的重要手段^[1]。区块链是一种全新的去中心化基础架构与分布式计算范式,智能合约作为其重要扩展是一种无需中介、自我验证、自动执行合约条款的计算机交易协议,两者结合将成为构建多种大规模分布式协作系统的理想数字基础设施^[2]。因此,本文提出了一种基于区块链的传染病多方决策融合监测与预警关键技术及其实现框架。该方法集成了多种预警手段和多方监测资源,具有隐私协作、安全可信、长期激励和自动预警等特点,可避免孤证偏差、决策失误和关键数据流通不畅等问题。

本文所提技术旨在融合人工智能、区块链和智能合约等技术手段与人机监测优势,一方面基于人工智能技术使智能算法具备专家级精准领域知识和探测异常的能力,减轻人为甄别与上报的压力;另一方面基于区块链和智能合约技术维护多方人工和机器直报通道,使智能合约作为软件代理全程核验、评估、追溯、对比、融合上报信息,一旦发现异常,则向社会相关部门预警,降低人工或机器预警错误和预警延迟的风险。

本文组织如下:第2节概述了当前传染病预警技术和系统的发展现状,介绍了密码学、区块链和智能合约等相关关键技术;第3节提出了基于区块链的传染病多方决策融合监测与预警关键技术,详细介绍了其基础架构、预警流程和关键组件实现;第4节讨论并分析了本文所提技术对现有系统可能带来的改进和增强;第5节对全文进行了总结。

2 文献回顾

2.1 传染病预警技术和系统

传染病预警是指通过一定的传染病预警技术,在传染病暴发前或发生早期,从传染病监测数据中发现和识别传染病发生数量超出期望常态水平的异常情况,发出警示信号,以提醒传染病暴发或流行可能发生的风险和其发生范围可能扩大的风险^[3]。传染病预警技术是传染病预警的关键,预警数据和预警模型的质量将直接影响传染病预警结果的及时性和准确性。传统的传染病预警技术是基于临床诊断和实验室确诊的病例进行监测的,采用时间模型、空间模型和时空模型等单因素模型分析数据,预警结果准确性较高,但及时性相对不足。随着互联网技术的发展,除常用的医疗卫生系统的电子健康记录外,互联网检索、社交媒体讨论、电商销售趋势、可穿戴设备监测数据等患者在医疗卫生系统外生成的及时性强的公共卫生大数据逐渐成为新的传染病监测数据来源^[4]。基于机器学习、深度学习、无监督学习等人工智能技术的具有更强数据解析能力的智能化预警技术,被用于分析多源新型传染病数据中不同因素之间的联系和变化规律,取得了良好的效果^[5]。2009年谷歌公司基于互联网检索数据预测流感趋势,预测结果与美国疾病控制与预防中心的数据呈现高相关性^[6];Odlum等人^[7]通过无监督聚类算法分析与埃博拉相关的推特短消息,监测到埃博拉病毒在尼日利亚的早期暴发,这些都是传染病预警技术的典型应用。总的来说,传染病预警技术的相关研究呈现预警数据多元化和预警模型复杂化趋势,传统监测手段和智能监测手段的结合有利于兼顾预警结果的准确性和及时性。

将传染病预警技术应用于传染病暴发或流行的长期探测,需在预警技术的基础上建立可直接应用的传染病预警系统。在传染病预警系统中尽可能地引入多种可靠智能预警技术有利于提高系统主动监测能力和实时预警灵敏度,提供多源预警依据,降低决策偏差风险,实现从电子化到信息化再到智能化的转型升级。然而,现有智能算法种类繁多,使用时有一定的专业要求,多种算法的筛选集成也需要多方监测力量的长期协作,并需要解决集成能力弱、互操作性差、关键数据流通不畅等问题才能满足多方大规模分布式协作需求。因此亟须在现有的软/硬件设施基础上,借助区块链天然的分

式架构,构建可集成多种监测技术、整合多方监测力量的分布式预警技术框架。

2.2 区块链与智能合约

区块链是众多现有技术的组合,本节主要介绍与本文技术设计和实现相关的密码学基础以及区块链、智能合约的概念、原理和应用。

2.2.1 密码学

密码学是区块链实现安全隐私协作的基础,区块链中涉及的密码学算法主要包括公钥密码学、哈希算法与默克尔(Merkle)树等。

公钥密码学又称非对称密码学,其使用一对公钥和私钥,包括公钥加密算法和数字签名算法。用户选取私钥后,区块链采用常见的非对称加密算法——RSA 算法或椭圆曲线加密算法生成相应公钥,公私密钥满足公钥加密后消息只有私钥可解,私钥签名后消息可用公钥验证,且公私密钥不可相互推导,通过验证数字签名可确保消息传输的完整性、发送者身份认证准确性和交易不可抵赖性。本文预警技术要求所有用户传递消息时按照公钥密码学对隐私消息进行加密签名或验签解密,从而保护隐私,避免欺诈。

哈希算法是能够把任意长度的输入串映射成固定长度的输出串的一种算法,具有单向性、抗强碰撞攻击等性质,相同明文经哈希算法计算后将得到相同的数字摘要,在区块链中,哈希函数可用于数据完整性验证、数据加密、共识算法工作量证明和区块链接等。

Merkle 树是一种在叶子节点中存储信息的哈希值、在非叶子节点中存储所有叶子节点合并哈希值的二叉树或多叉树。区块链采用 Merkle 树数据结构快速归纳和校验区块数据的存在性和完整性,区块头存储 Merkle 树根哈希值而不必封装所有底层数据,即可检索和确认任意一个交易,实现数据溯源和防篡改^[8]。

2.2.2 区块链

区块链是一种将数据区块按照时间顺序组合而成的链式结构,是去中心化系统中各节点共享且共同维护的分布式数据账本。具体地,区块链技术利用加密链式区块结构来验证与存储数据,利用分布式节点共识算法来生成和更新数据,利用自动化脚本代码(智能合约)来编程和操作数据^[9]。一般来说,区块链可按许可权限分为公有区块链、联盟区块链和私有区块链。其中,公有区块链面向全球

所有用户,任何人都可以在其中读取数据和发送交易;联盟区块链由若干与业务相关的机构共同参与管理,每个机构都运行着一个或多个节点,读写权限仅对联盟内的节点有限度地开放;私有区块链的读写权限由某个组织或机构控制,参与节点的资格被严格限制。借助区块链的高冗余存储特性可存储和保护重要隐私数据^[10],避免因中心化机构遭受攻击或权限管理不当造成大规模数据丢失或泄露,共识算法^[11]和 Merkle 树哈希技术可防止数据被篡改,非对称加密和多重签名技术可灵活配置数据访问权限^[12],星际文件系统(inter planetary file system, IPFS)就是一个采用区块链计算范式的分布式存储和共享文件的网络传输协议,IPFS 网络节点将构成点对点分布式文件系统,根据文件内容的哈希值进行寻址,无需网络代理即可全球共享。本文预警技术将采用 IPFS 存储预警数据、预警算法等文件,主链上共享时仅传递加密后的文件的哈希值,并记录交易记录,从而减轻主链的数据存储压力。

2.2.3 智能合约

智能合约的概念最早于 1994 年由美国计算机科学家 Nick Szabo 提出,他将智能合约定义为“一套以数字形式定义的承诺,包括合约参与方可以在上面执行这些承诺的协议”。区块链上的智能合约可被看作运行在分布式账本上预置规则、具有状态、条件响应的,可封装、验证、执行分布式节点复杂行为,完成信息交换、价值转移和资产管理的计算机程序^[13]。具体地,智能合约代码用 If-Then 和 What-If 语句预置了合约条款的相应触发场景和响应规则,智能合约经多方共同协定、各自签署后随用户发起的交易提交,经节点验证后存储在区块链的特定区块中,用户得到返回的合约地址及合约接口等信息后即可通过发起交易来调用合约。合约创建或调用交易在节点的本地沙箱执行环境(如以太坊虚拟机)中进行,合约代码根据可信外部数据源(即预言机(Oracles))和世界状态的检查信息,自动判断当前所处场景是否满足合约触发条件,以严格执行响应规则,并更新世界状态。通过将核心的法律条文、商业逻辑和意向协定封装在智能合约中,可构建各种各样运行在区块链上的去中心化应用(decentralized application, DApp)、去中心化自治组织(decentralized autonomous organization, DAO)^[14]和去中心化自治企业(decentralized autonomous corporation, DAC),智能合约将在区块链构建的虚拟

数字世界中担任各方共同信任的软件代理,安全准确地履行合约。

区块链及智能合约具有去信任、分布式、开放自治、公开可溯源、信息不可篡改等特性,它们的去中心化基础架构与分布式计算范式天然适合构建大规模多方协作系统,已在公共卫生领域中被初步应用于电子医疗数据共享^[15]、隐私敏感数据访问控制^[16]和医疗药品溯源^[17]等。本文旨在提出一种利用区块链和智能合约技术的高度扩展性和互操作性构建传染病多方决策融合监测与预警关键技术。

3 基于区块链的传染病多方决策融合监测与预警关键技术

为充分集中政府、医疗机构和社会公众三方的监测力量,长期、高效、实时、稳定地进行传染病预警和社会信息公开,本节提出了一种基于区块链的传染病多方决策融合监测与预警关键技术。该技术一方面可利用去中心化数据与组件共享市场和疫情信息协同监测市场,在安全隐私的前提下促进多源预警数据共享、多种预警技术集成以及多监测方的长期参与和协同挖掘,保证预警准确性;另一方面可将预置决策融合算法和异常探测规则的智能合约作为不停机实时监测系统,提高预警及时性。以下将从基础架构、预警流程和关键技术实现3个方面进行介绍。

3.1 基础架构

图1展示了本文预警技术的基础架构。基于区块链的传染病多方决策融合监测与预警关键技术整体构建在一条区块链上,根据用户身份、数据特征和监测模式分为利用闭源数据的政府端基于规则算法的闭环监测、利用闭源数据的医疗机构端基于联邦学习的联盟检测和利用开源数据的社会端基于开放区块链市场的协同监测3个子模块,各子模块用户通过本模块端口定制客户端,即集成了智能合约的去中心化应用,与其他模块用户或区块链进行数据交互以完成各自监测任务,交互时所有隐私文件将被加密存储在IPFS中,区块链上仅存储公开文件的哈希值和全部交互记录供验证和追溯。

系统包含智能合约权限管理组件、智能合约监测组件(开源数据)、智能合约监测组件(闭源数据)、智能合约决策融合组件和智能合约信用激励组件5个主要智能合约组件,每个组件由一组运行在区块链上相互继承调用的子合约组成,并根据功能需求设定不同的使用权限和数据可见性。预言机将作为系统中智能合约的可信外部数据源,链接经验证的链下权威站点、IPFS地址或其他指定区块链等数据源,供合约查询外部世界状态、检查触发条件和执行合约。

系统包含2个预警通道:一个是行政机构结合政府端、医疗机构端和社会端决策信息,经行政审批通过后发布的疫情预警通道;另一个是智能合约

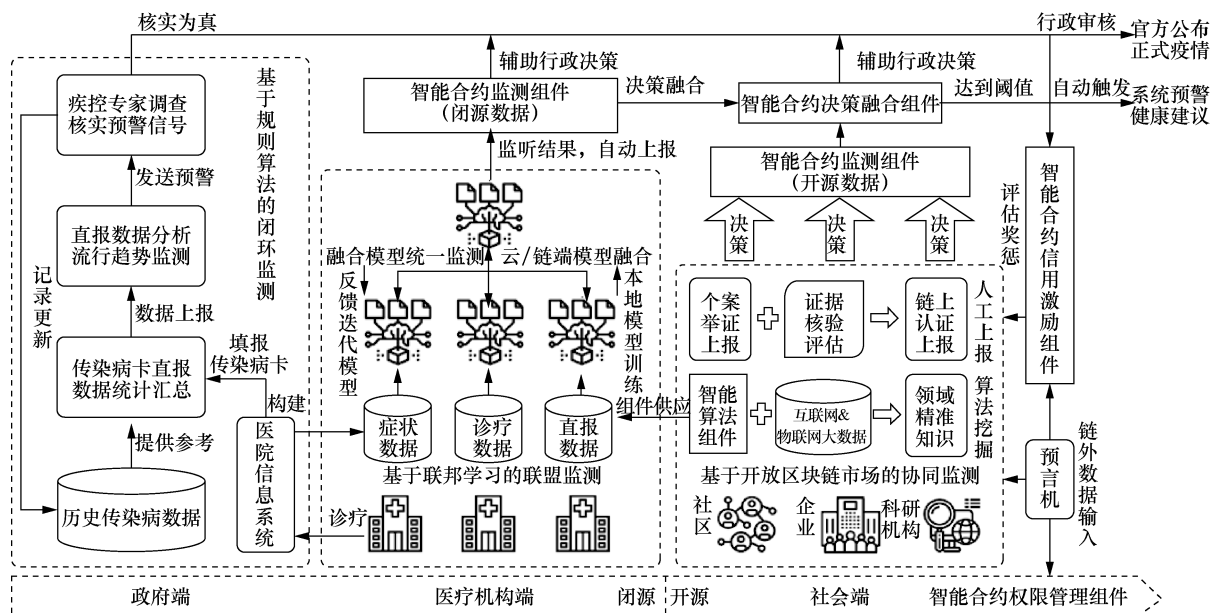


图1 基于区块链的传染病多方决策融合监测与预警关键技术框架

决策融合组件根据预置算法,融合医疗机构端和社会端的决策信息进行判断,达到预警条件后自动发布的疫情预警通道,该预警通道发布预警时将同时公开决策依据、预警级别和预警疾病模糊搜索对应的健康防护建议,从而对未知疾病起到早期防治的效果。

3.2 预警流程

本节将介绍本文预警技术的完整运行机制和预警流程,具体步骤如下。

(1) 各端口用户执行疫情监测任务

政府端提供基于规则算法的闭环监测数据接口,主要包括:规范化传染病预警技术接入接口,供社会端智能化预警技术组件简易接入和替换;政府端预警信号的响应处理信息汇总接口,以统一的格式实时汇总政府端监测到的预警信号及其核验结果,汇总接口接入智能合约信用激励组件,作为评估医疗机构端和社会端机器决策质量的参考。

医疗机构端进行基于联邦学习的联盟监测。医疗机构基于联邦学习等隐私计算架构,在不交换各自隐私数据的前提下共同训练得到统一共享监测模型,以此作为标准监测模型来反向监测各医疗机构的传染病疫情,并在发现异常后直接通过预设的内置程序上报给智能合约监测组件(闭源数据),从而减轻医疗机构端传染病人工甄别及上报压力。

社会端进行基于开放区块链市场的协同监测。社会端基于区块链构建去中心化数据与组件共享市场及疫情信息协同监测市场,以众包协作的方式获取多源监测信息。其中,系统中各用户可以自由选择去中心化数据与组件共享市场中提交、开发或验证预警数据集和智能化预警技术组件。算法组件和数据集将在按需加密后存入 IPFS,供索引寻址和全球共享,所有提交到市场的数据和算法都将被分配包含其自身详细信息的算法 ID 和数据 ID,它们的质量评分在初次提交时被初始化,并在后续监测过程中由买家评估或信用激励组件更新。政府端和医疗机构端可按需采购市场中的算法组件,从而降低数据分析难度。疫情信息协同监测市场包含人工监测和算法监测 2 种监测模式:人工监测即系统中任意用户可在市场中提交人工监测结果和证明材料,证明材料需公开存储在 IPFS 中,并支持智能合约和预言机核验与评估;算法监测即社会端

账户提供算力,自由组合不同质量评分的数据和算法,实时监测疫情并在市场中提交监测结果。人工监测结果和算法监测结果将被分别分配人工决策 ID 和算法决策 ID,并记入区块链,上报智能合约监测组件(开源数据)进行融合,最后将融合结果上报给智能合约决策融合组件。

(2) 开/闭源决策融合触发系统预警

智能合约决策融合组件按照决策质量、预警疾病和预警范围,对一段时间内接收到的智能合约监测组件(闭源数据)/智能合约监测组件(开源数据)的监测报告进行筛选和分类,根据不同疾病的特点和监测需求采用多种预警策略,最终将传染病监测决策融合结果作为系统预警进行发布,并通过模糊搜索算法匹配与所预警疾病对应的预防性健康建议。

(3) 智能合约信用激励组件反馈激励

智能合约信用激励组件将在预警全流程中实时接收和记录来自政府端的响应处理信息、来自医疗机构端/社会端的融合监测结果以及来自预言机链接权威站点的疫情信息。在实际疫情发生后,按照判断结果反向溯源,评估所有账户、机构、数据、算法的信用和质量,更新相关评分、投票权重和奖惩贡献者等,从而提供系统长期监测的激励。

3.3 关键技术实现

3.3.1 基于区块链的联邦学习

联邦学习是谷歌公司于 2016 年提出的一种用于解决数据孤岛问题、保护数据隐私的新型机器学习框架,在此框架中用户通过交换和融合本地模型参数,共同建立虚拟联邦模型,以在无需交换隐私数据的前提下聚合训练数据,提高模型精度。由于医疗机构的医疗数据一般难以共享,而相同范围的传染病监测又需要采用标准模型,因此联邦学习的架构特别适合医疗机构端的统一监测。现有框架常配置在中心化云端或服务器上,存在单点故障和数据丢失的隐患,本文系统引入基于区块链的联邦学习模式以解决上述问题。

以基于症状监测的预警技术为例,利用机器学习算法从历史诊断数据集中学习疾病特征后对未知诊断数据进行分类的过程,可转化为一个有监督机器学习分类问题。记包含 n_k 个症状的数据样本的第 k 个医疗机构的本地症状数据库为 $D_k = \{(x_1, y_1), \dots, (x_{n_k}, y_{n_k})\}$ 。本地分类模型对本地症状数据库 D_k 的经验风险,即本地分类模型目标函数可形式化为式 (1) [18]:

$$F_k(w) = \frac{1}{n_k} \sum_{j_k=1}^{n_k} f_{j_k}(w; x_{j_k}, y_{j_k}) \quad (1)$$

其中, w 为模型参数。

则由 m 个医疗机构组成的全局模型需使整体分类误差最小, 即全局模型目标函数形式化表示如下:

$$\min_w F(w), F(w) := \sum_{k=1}^m p_k F_k(w), p_k \geq 0, \sum_{k=1}^m p_k = 1 \quad (2)$$

其中, p_k 为第 k 个本地分类模型在整体模型中的权重。

每轮迭代中, 本地分类模型读取全局模型参数, 更新本地模型参数, 基于本地数据计算模型梯度后, 将加密梯度传输至全局模型, 全局模型按照目标函数聚合梯度, 并更新全局模型参数, 反复多次, 直到满足迭代停止条件即可获得理想全局模型, 将其用于患者疾病诊断则可反向监测各本地数据库。根据已知疾病的特点, 将传染病的症状监测模型训练数据分为 CT 影像数据、电子病历数据、心电图数据和网络直报数据等, 未知疾病则可用聚类模型、主成分分析、对抗网络等半监督或无监督学习方法进行异常监测。

联邦学习的交互关键在于模型参数的加密传输和融合, 基于区块链的联邦学习可将交互过程上链以避免抵赖或数据丢失, 根据各医疗机构的数据量和模型质量还可评估各医疗机构的贡献大小, 按照贡献值更新本地模型在全局模型中的融合权重来提高全局模型精度, 或反馈医疗机构经济激励, 从而鼓励更多参与者持续贡献。本文提出的预警技术支持 2 种基于区块链的联邦学习模式: 链下聚合与合约聚合。链下聚合即采用参考文献[19]中的链式联邦学习方法, 各医疗机构在本地计算模型后任意选取一个验证节点提交包含模型参数、数据量和模型运行时间的交易, 验证节点验证数据量与模型运行时间的匹配程度后打包交易上链, 医疗机构实时下载新区块内其他子模型的所有参数并在本地聚合, 验证节点根据验证任务量获得奖励。在此模式下, 本系统需建立专用联盟区块链网络, 并定期采用跨链技术将联盟链数据锚定在主链上, 以保证数据安全和训练效率。合约聚合是更简洁的模式, 医疗机构计算本地模型参数后利用同态加密技术加密, 并上传加密数据至权重聚合智能合约, 合约计算融合权重并返回结果, 同态加密技术的特点是: 对经过同态加密的数据进行某种处理后得到的输出在解密后与未加密原始数据用同一方法处理

后的输出一致, 因此合约融合权重时权重参数仍保持隐私加密。由于智能合约的计算能力有限, 合约聚合模式对模型类型和同态加密算法的要求较高。

3.3.2 开放区块链市场与决策融合算法

社会端智能预警技术的预警机制为以互联网或物联网大数据为模型输入, 通过人工智能强大的数据拟合能力对特定传染病的期望常态水平进行建模, 随后反向监测、识别和发现不符合常态数学模型的异常情况, 从而达到预警效果。高质量预警数据和可信预警模型是社会端提交的预警决策正确预警的关键。

图 2 为本文系统开放区块链市场协同监测流程, 本文所述的用户 ID、数据 ID、算法 ID、人工决策 ID 和算法决策 ID 等关键参数如图 2 所示。系统中交由 IPFS 存储的数据包括共享预警数据、共享智能化预警技术和人工决策举证材料等。所有用户、数据、算法和决策的信用/质量评分由智能合约权限管理组件初始化, 并在后续由智能合约信用激励组件进行记录和更新, 更新方式包括用户验证和系统评估 2 种。在用户验证中, 人工决策可以被任意用户验证, 数据和算法则需用户先获得使用权限才能进行验证; 在系统评估中, 系统视政府端响应处理信息、医疗机构端和社会端决策融合结果、权威站点疫情信息等为正确预警结果, 定期对市场内相关提交决策进行比对评估。所有验证和评估结果提交至智能合约信用激励组件后, 组件根据预设规则前溯奖惩相关用户和更新相关数据评分, 如对于一个正确算法决策来说, 决策提交账户、算法提交账户、数据提交账户等均可获得经济激励和信用评分提升, 相关算法和数据获得质量评分提升; 经济激励以区块链通证的形式发放和流通, 来源可包括错误决策惩罚、恶意用户惩罚和政府定期激励等。提交者可对具有信用和质量评分等量化指标的数据和算法等数字资产进行定价, 并配合相应区块链数据检索系统、需求匹配系统共同构建去中心化数据与组件共享市场。

智能合约监测组件和智能合约决策融合组件的输入数据为格式规范的结构化决策数据, 处理时可在语义层次进行判别融合, 或在数据层面进行加权融合。具体地, 智能合约监测组件和智能合约决策融合组件中一般包含决策选择算法和决策融合算法 2 种关键算法, 决策选择算法设定决策筛选规

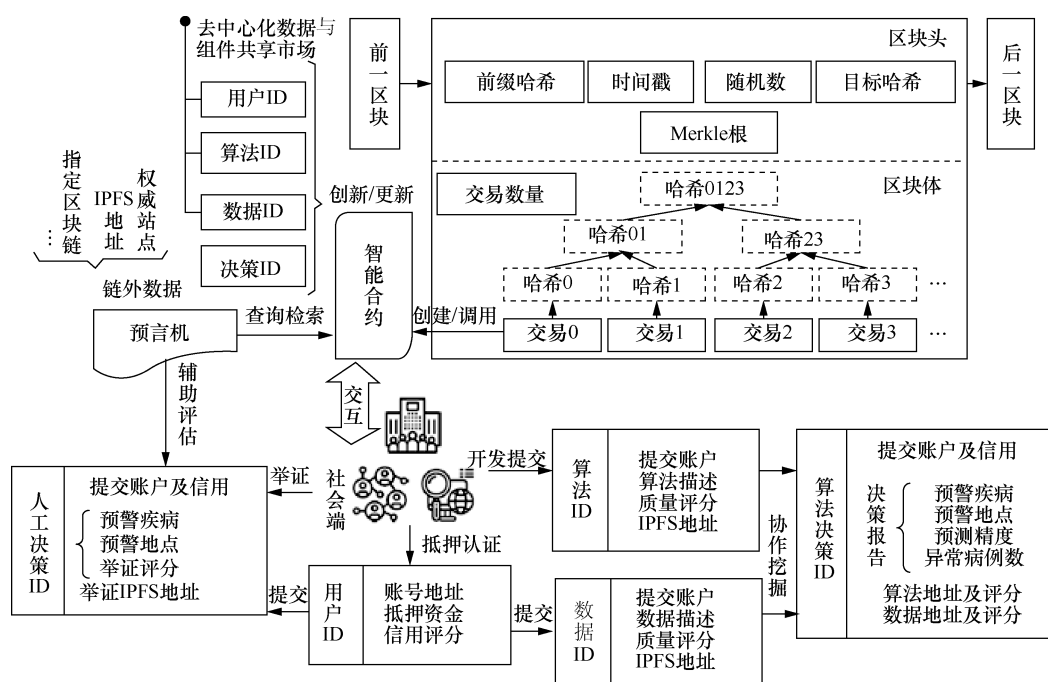


图2 开放区块链市场协同监测流程

则，决策筛选规则中可组合提交者信用、提交者押金、算法质量、数据质量等筛选指标，快速过滤海量决策中的无效或恶意决策；决策融合算法设定决策融合规则，决策融合规则根据举证评分、预测精度、质量评分等因素设定人工和算法决策的融合权重，以获得精准的共识决策。一般认为，来源于医疗端临床数据的监测结果准确性更高，而来源于社会端社会数据的监测结果及时性更好，通过调整两者的融合权重可兼顾疾病监测的准确性和及时性。

4 讨论与分析

下文从预警数据、预警技术和预警主体3个方面对本文提出的基于区块链的传染病多方决策融合监测与预警关键技术进行讨论。

(1) 预警数据：开/闭源信息融合、可信联通与隐私计算

在引入多源化预警数据时，普遍存在开源预警数据噪声大、闭源预警数据难共享和关键隐私数据流通不畅等问题。本文提出的技术在社会端构建了去中心化数据与组件共享市场及疫情信息协同监测市场，对所有用户、数据、算法和决策进行身份认证和信用追溯，从而在长期监测周期中鼓励低噪

声数据和高质量算法的共享及可信多源决策的融合。对于政府医疗数据等隐私敏感数据来说，本文采用基于区块链的联邦学习隐私计算架构，在不交换隐私数据的前提下训练共享模型，提高模型精度，统一监测标准。对于社会化疫情监测过程中关键数据信息的可见性问题来说，建议采用密码学技术和智能合约权限管理组件加密传输信息、维护联盟白名单和设定交互权限，实现选择性隐私协作。

(2) 预警技术：基于可扩展智能算法组件的多决策去中心化融合

本文提出构建去中心化智能算法组件市场：将机器学习、深度学习、自动机器学习等智能预警算法或权限管理、信用激励、决策融合等智能合约封装为可插拔式的标准化程序组件，加密存储在IPFS中，然后提交至区块链市场进行交易、共享和评估。用户只需根据自身能力和需求上传/验证数据、开发/验证组件、申请使用权限和提交决策，即可扩展更新系统和参与协同监测。同时，由于所有数据、算法和决策均可溯源、可评估、可配置，智能合约决策融合组件将通过预置决策筛选规则和决策融合规则实时筛选和融合监测周期内的全部决策，然后预警，从而避免孤证决策偏差。

(3) 预警主体：长期激励、多方大规模协作

疾病监测是长期连续地收集、核对、分析疾病动态分布及其影响因素的资料的过程，针对特定传染病数据集和传染病预警技术的高水平短期研究，缺乏及时与法定传染病预警系统整合并在其中长期发挥作用的方法和激励。同时，突发公共卫生事件应急管理通常需要大量不同学科、不同专业、不同工作背景的、地理分散的贡献者协同工作、集体决策和共同执行，而传统传染病预警系统一般由指定团队参与研发运维，其他拥有监测能力的科研单位和社会机构等难以持续投入力量。本系统基于区块链的分布式架构和通证经济激励解决上述问题，并促进构建知识集成的物联网环境^[20-21]。系统中的智能合约信用激励组件将实时收集、比对各参与方的信息和预警结果，对全体参与者和参与元素进行反向评估和贡献量化，从而提供分布式协作的长期激励，调整数据算法和决策权重，提高分布式决策精度。

5 结束语

本文基于区块链、智能合约、人工智能等多种技术手段提出了一种基于区块链的传染病多方决策融合监测与预警关键技术。该技术由政府端基于规则算法的闭环监测、医疗机构端基于联邦学习的联盟监测、社会端基于区块链的开放市场协同监测三大监测模块共同组成，可在安全隐私的前提下促进多源预警数据联通共享、多种预警技术扩展集成和多方监测力量长期协同监测，系统中预置规则不停机的智能合约将作为公开公正的、软件定义的监测代理，在监测异常时实时预警，从而有利于传染病疫情的公众防控，避免孤证决策偏差和关键数据流通不畅。随着区块链跨链技术、第二层扩展解决方案、可信计算硬件和同态加密技术的进一步发展，本文提出的关键技术架构有望应用在自主研发安全可控的区块链即服务（blockchain as a service, BaaS）上，并形成专注于传染病监测预警的智能区块链系统。

参考文献：

- [1] 熊伟仪, 冯子健. 中国传染病监测的发展历程、现状与问题[J]. 中华流行病学杂志, 2011, 32(10): 957-960.
XIONG W Y, FENG Z J. Overview on communicable disease surveillance in China[J]. Chinese Journal of Epidemiology, 2011, 32(10): 957-960.
- [2] OUYANG L W, YUAN Y, WANG F Y. A blockchain-based framework for collaborative production in distributed and social manufacturing[C]//2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). Piscataway: IEEE Press, 2019: 76-81.
- [3] 杨维中, 兰亚佳, 李中杰. 传染病预警研究回顾与展望[J]. 中华预防医学杂志, 2014, 48(4): 244-247.
YANG W Z, LAN Y J, LI Z J. Review and prospect of research on early warning of infectious diseases[J]. Chinese Journal of Preventive Medicine, 2014, 48(4): 244-247.
- [4] SALATHE M. Digital pharmacovigilance and disease surveillance: combining traditional and big-data systems for better public health[J]. Journal of Infectious Diseases, 2016, 214(suppl_4): S399-S403.
- [5] 曹志冬, 曾大军, 郑晓龙, 等. 北京市 SARS 流行的特征与时空传播规律[J]. 中国科学: 地球科学, 2010, 40(6): 776-788.
CAO Z D, ZENG D J, ZHENG X L, et al. Spatio-temporal evolution of Beijing 2003 SARS epidemic[J]. Scientia Sinica Terrae, 2010, 40(6): 776-788.
- [6] GINSBERG J, MOHEBBI M H, PATEL R S, et al. Detecting influenza epidemics using search engine query data[J]. Nature, 2009, 457(7232): 1012-1014.
- [7] ODLUM M, YOON S. What can we learn about the Ebola outbreak from tweets?[J]. American Journal of Infection Control, 2015, 43(6): 563-571.
- [8] 王化群, 吴涛. 区块链中的密码学技术[J]. 南京邮电大学学报(自然科学版), 2017, 37(6): 61-67.
WANG H Q, WU T. Cryptography on the blockchain[J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science), 2017, 37(6): 61-67.
- [9] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
- [10] 祝烈煌, 董慧, 沈蒙. 区块链交易数据隐私保护机制[J]. 大数据, 2018, 4(1): 46-56.
ZHU L H, DONG H, SHEN M. Privacy protection mechanism for blockchain transaction data[J]. Big Data Research, 2018, 4(1): 46-56.
- [11] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.
YUAN Y, NI X C, ZENG S, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022.
- [12] 钱卫宁, 金澈清, 邵奇峰, 等. 区块链与分享型数据库[J]. 大数据, 2018, 4(1): 36-45.
QIAN W N, JIN C Q, SHAO Q F, et al. Blockchain and sharing database[J]. Big Data Research, 2018, 4(1): 36-45.
- [13] 欧阳丽炜, 王帅, 袁勇, 等. 智能合约: 架构及进展[J]. 自动化学报, 2019, 45(3): 445-457.
OUYANG L W, WANG S, YUAN Y, et al. Smart contracts: architecture and research progresses[J]. Acta Automatica Sinica, 2019, 45(3): 445-457.
- [14] 丁文文, 王帅, 李娟娟, 等. 去中心化自治组织: 发展现状、分析框架与未来趋势[J]. 智能科学与技术学报, 2019, 1(2): 202-213.
DING W W, WANG S, LI J J, et al. Decentralized autonomous organizations: the state of the art, analysis framework and future trends[J]. Chinese Journal of Intelligent Science and Technology, 2019, 1(2): 202-213.
- [15] 张超, 李强, 陈子豪, 等. Medical Chain: 联盟式医疗区块链系统[J]. 自动化学报, 2019, 45(8): 1495-1510.
ZHANG C, LI Q, CHEN Z H, et al. Medical Chain: alliance medical

- blockchain system[J]. Acta Automatica Sinica, 2019, 45(8): 1495-1510.
- [16] HASSELGREN A, KRALEVSKA K, GLIGOROSKI D, et al. Blockchain in healthcare and health sciences, a scoping review[J]. International Journal of Medical Informatics, 2019, 134: 104040.
- [17] KUMAR R, TRIPATHI R. Traceability of counterfeit medicine supply chain through blockchain[C]//Proceedings of the 11th International Conference on Communication Systems & Networks. [S.l.:s.n.], 2019: 568-570.
- [18] LI T, SAHU A K, TALWALKAR A, et al. Federated learning: challenges, methods, and future directions[J]. arXiv:1908.07873, 2019.
- [19] KIM H, PARK J, BENNIS M, et al. Blockchain on-device federated learning[J]. IEEE Communications Letters, 2019: 1-4.
- [20] 王飞跃, 张军, 张俊, 等. 工业物联网: 基本概念、关键技术与核心应用[J]. 自动化学报, 2018, 44(9): 1606-1617.
WANG F Y, ZHANG J, ZHANG J, et al. Industrial internet of minds: concept, technology and application[J]. Acta Automatica Sinica, 2018, 44(9): 1606-1617.
- [21] 张俊, 李灵犀, 林懿伦, 等. 虚实系统互驱的混合增强智能开放创新平台的架构与方案[J]. 智能科学与技术学报, 2019, 1(4): 379-391.
ZHANG J, LI L X, LIN Y L, et al. The architecture and scheme of the hybrid-augmented intelligence open innovation platform based on the virtual and real systems[J]. Chinese Journal of Intelligent Science and Technology, 2019, 1(4): 379-391.

[作者简介]



欧阳丽炜（1996—），女，中国科学院自动化研究所复杂系统管理与控制国家重点实验室硕士生，主要研究方向为社会计算、区块链和智能合约。



袁勇（1980—），男，博士，中国科学院自动化研究所复杂系统管理与控制国家重点实验室副研究员，主要研究方向为区块链、商务智能、计算广告学。



郑心湖（1987—），男，科罗拉多州立大学电子计算机工程学院博士生，主要研究方向为社会计算、机器学习、数据分析。



张俊（1981—），男，博士，武汉大学电气与自动化学院教授，主要研究方向为智能系统、人工智能、知识自动化及其在智能电力和能源系统中的应用。



王飞跃（1961—），男，博士，中国科学院自动化研究所复杂系统管理与控制国家重点实验室主任，中国科学院大学中国经济与社会安全研究中心主任，青岛智能产业技术研究院院长，主要研究方向为平行系统的方法与应用、社会计算、平行智能以及知识自动化。