

# 区块链智能合约技术在医疗废物监管领域的应用

刘 晋

王 晖

(武警北京总队医院 北京 100600)

(山东大学软件学院 济南 250101)

〔摘要〕 介绍医疗废物监管信息化存在的问题及对策、区块链技术核心价值、医疗废物监管信息系统优化路径,详细阐述区块链智能合约技术在医疗废物监管领域的应用方案设计,包括医疗废物处置流程、医疗废物监管创新应用、医疗废物监管区块链架构等。

〔关键词〕 区块链;智能合约;医疗废物监管

〔中图分类号〕 R-058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2021.12.010

**Application of Blockchain Smart Contract Technology in the Field of Medical Waste Supervision** LIU Jin, Beijing Armed Police Corps Hospital, Beijing 100600, China; WANG Hui, School of Software, Shandong University, Jinan 250101, China

〔Abstract〕 The paper introduces the problems and countermeasures of medical waste supervision informatization, the core value of blockchain technology, and the optimization path of medical waste supervision information system. It expounds the application scheme design of blockchain-based smart contract technology in the field of medical waste supervision in detail, including medical waste disposal process, innovative application of medical waste supervision, the blockchain architecture of medical waste supervision, etc.

〔Keywords〕 blockchain; smart contract; medical waste supervision

## 1 引言

### 1.1 研究背景

医疗废物含有大量病原体、重金属和有机污染物,具有潜伏性传染、空间传染以及急性传染等特点,做好医疗废物分类管理、回收、处置是维护公众、医务工作者健康的有效保障,应严格按照标准进行医疗废物分类收集和无害化处理。2020年5月国务院发布《关于开展医疗机构废弃物专项整治工作的通知》,开展多部门联合专项整治行动。在此

背景下全国多地制定了推进医疗废物监管信息化建设,提升医疗废物监管全程化、智能化、规范化水平的工作方案。

### 1.2 医疗废物监管信息化存在的问题及对策

1.2.1 存在的问题 目前医疗废物监管信息化仍处于起步阶段,虽然部分省市已建立医疗废物监管信息系统并投入使用,但是尚未形成较为完善、可大规模推广的解决方案,现有方案仍存在突出问题,主要包括:现有医疗废物监管信息系统采用传统数据库存储,致使其数据来源、完整性保障能力弱,存在被篡改和伪造的风险;医院内部和外部的医疗废物监管机构分属不同监管部门,传统中心化架构在数据协同共享方面存在劣势,不利于跨部门

〔修回日期〕 2021-07-15

〔作者简介〕 刘晋,中级职称,发表论文17篇。

协作；医疗废物从产生到处置存在大量中间环节，如收集、搬运、暂存、运输、处置以及监管等，由于缺少责任者绑定机制，在交接过程中出现不经称重和清点就签字交接，且在出现问题后无法追溯到具体环节和责任者等情况，存在风险；采用人工称重、录入信息的形式存在引入错误或误差的风险，目前虽然已引入扫码器、蓝牙秤等设备，但是尚未实现完整、防篡改、能够绑定设备与使用者的自动化采集与存证。

1.2.2 对策 为解决上述问题，本文提出基于区块链智能合约技术<sup>[1-4]</sup>的医疗废物监管信息系统。通过建造该系统，可以有效利用区块链可追溯且不可篡改的数据存储功能，使监管信息从信息原生处上链，尽可能确保信息数据的客观性和真实性，开放公众自主查询，大幅度提升监管公信力和效率。

1.2.3 基于区块链智能合约技术的医疗废物监管信息系统优势 (1) 数据安全且不可篡改。医疗废物处理流程的关键节点数据上传到区块链保存，上链数据脱敏，核心数据采取加密哈希值上链，同时兼顾数据的隐私安全性及不可篡改性。(2) 适合多角色主体参与。医疗废物收集、转运、处置过程中，各参与主体之间相互独立，没有隶属管理关系。与传统中心化系统相比，基于区块链数据汇集的多中心体系结构兼顾效率与安全，适合多角色主体的应用场景。(3) 责任绑定。绑定账号与相关责任人的客观属性并做摘要签名上链，数据采集的时间地点(GPS经纬度)同时上链。时间、地点、人物、操作和结果同时上链锁定，不可抵赖。(4) 自动化采集与存证。通过提供不可否认的非对称加密签名机制，实现完整、防篡改、设备与使用者的自动化采集与存证绑定。

## 2 区块链技术

### 2.1 内涵与核心价值

2.1.1 内涵 区块链是由多独立节点参与的分布式数据库系统<sup>[5]</sup>，可记录节点上发生的所有交易信息，交易过程高度透明，数据高度安全<sup>[6]</sup>。其核心在于通过密码学、分布式网络及分布式共识机制等

技术建立起相互之间的信任关系，实现在不可信网络中进行信息传递交换的可信机制<sup>[7]</sup>。区块链具有去中心化、不可篡改、数据透明、共同维护等特性，更适用于医疗废物监管。

2.1.2 核心价值 区块链系统核心价值是建立信任<sup>[8]</sup>，这种独特的数据结构完整、真实地记录了行为主体签名认可的授权行为<sup>[9]</sup>。区块链的实施要避免类似传统系统越过行为主体的授权操作，应使行为主体在做出授权之前，认识到其授权行为可能面临的风险并及时做出应对<sup>[10-11]</sup>。

### 2.2 医疗废物监管信息系统优化

结合智能合约核心技术特点和优势，可从以下几个角度优化医疗废物监管信息系统。一是透明度，医疗废物监管各参与方可访问合约的条款和条件。二是精确性，避免手动填写大量表单导致的交易错误。三是安全性，采用高级别的数据加密技术。四是速度，优化传统业务流程，快速执行交易。五是存储备份，将医疗废物关键流程及个人等相关信息记录到合约中永久存储，以供查询、共享。

## 3 医疗废物监管过程分析

### 3.1 医疗废物监管信息化发展现状

目前推动医疗废物监管信息化的需求较迫切，但是医疗废物监管信息化仍处于起步阶段，尚未形成一致认可并得到广泛应用的方案，以及面向医疗废物监管信息化的国家标准和行业标准。医疗废物监管信息化处于起步阶段，在设计和开发中可以充分发挥区块链技术优势，优化现有尚未实现信息化的工作流程，在推进信息化建设的同时实现流程再造。

### 3.2 医疗废物处置流程

在医疗废物处置流程中，通过合约记录节点上所发生的一切交易信息，使过程高度透明，具体流程如下：护工人员与科室人员当面对医疗废物进行称重封装，护工打印标签，科室人员进行标签扫描确认的同时交接数据上链。护工人员将医疗废物运送到暂存点，与暂存点管理人员进行面对面对称重交

接。确认废弃物重量无误后生成箱子二维码，交接数据上链。由医院暂存点管理人员进行废弃物分类、扫描进箱操作。运输人员与医院暂存点管理

员进行箱子称重交接，扫描确认箱子重量无误后，交接数据上链。运输人员和销毁点人员对车辆称重，确认接收后交接数据上链，见图1。

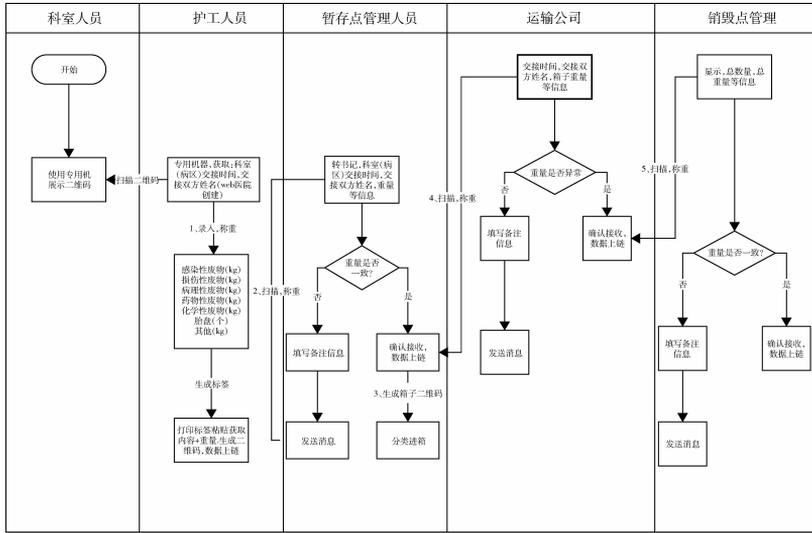


图1 医疗废物监管业务流程

### 3.3 医疗废物监管创新应用

3.3.1 概述 新型医疗废物监管模式主要是在实现完整的废弃物处理过程基础上，包括收集、搬运、储存、运输、处理以及监管，应用区块链智能合约技术和二维码<sup>[12-13]</sup>，射频识别（Radio Frequency Identification, RFID）<sup>[14-15]</sup>和近距离无线通信（Near Field Communication, NFC）等物联网技

术<sup>[16-19]</sup>，对于系统各区域节点产生的关键追踪处置信息，均按照在区块链上的合约记录到区块链中，通过系统查看各医疗机构废弃物的产生情况，各环节的处理时间、处理人、处理结果等，有效地实现信息自动化监管，通过对节点监控促进医疗废物按时、按线路运送，提高医疗废物处置的规范化管理水平。业务逻辑架构，见图2。

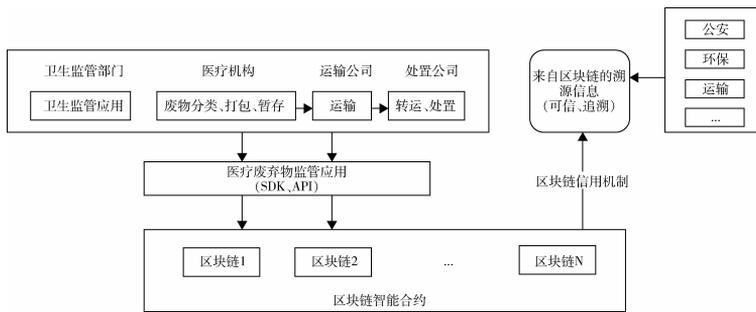


图2 业务逻辑架构

3.3.2 网络匹配 如果对于区块链组网节点没有特殊网络环境要求，采用互联网、局域网等方式进行组网均可；对于需要通过互联网提供服务的组网节点则接入互联网并启用Web服务，从而使非组网设备与区块链平台能够利用互联网进行互操作。对

于非组网设备，如电子秤，位置传感器，个人数字助理（Personal Digital Assistant, PDA）和其他业务终端等，一般通过互联网访问某一可信组网节点实现数据上传和读取。

3.3.3 部署方式（图3） 在医疗废物中间环节

中,工作人员即普通用户通常采用 PDA 等设备进行数据采集和提交等操作,由于 PDA 设备本身计算能力有限,并非时刻保持在线而是按需联网,不适合直接参与组网。因此采用节点代理模式,即用户无需直接参与组网及操作,而是通过所属机构提供的,应用服务生成密钥对、导出证书、签名交易提交等功能。机构用户可以对普通用户进行注册、管理和审核,在提交签名交易时,应用服务需通过机构用户私钥对交易进行签名。提交数据的签名交易上附有普通用户自身私钥签名以及机构用户在提交交易时的签名,数据上链后不可篡改且不可否认。

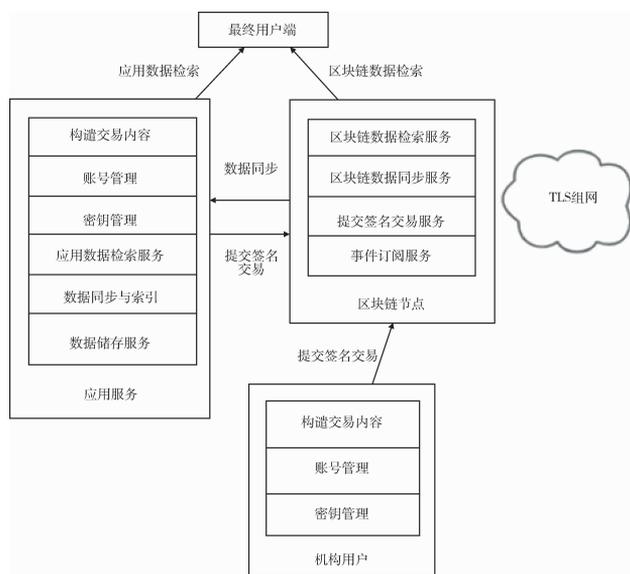


图3 部署方式

3.3.4 数据上链 (1) 医疗废物交接信息上链数据格式设计。1次行为拥有1条链上记录,格式通用、数据互通。追踪到医疗废物最小包装单位,装箱及装车仍然可持续追踪,确保闭环。交接双方数据各自上链,无状态、无依赖,通过链上数据做校验核对,见表1。(2) 上链数据分类。分为面向账户权限的上链数据和面向业务的上链数据两类。面向账户权限的上链数据主要包括用于账户权限管理而上链的各参与主体的数字证书,其中各参与主体可利用账户管理合约按需为负责具体业务活动的自然人建立账户,将其数字证书以相同形式上链。面向业务的上链数据具体可分为基础信息数据和全过程追溯信息数据两类。基础信息数据主要为与医

疗废物转运处理环节无关的数据,包括但不限于:医疗垃圾基本信息(分类、重量、个数)、医疗机构基本信息、科室基本信息、医废暂存点信息、医废转运车辆信息、医废销毁点信息、各类人员信息。其中输入参与主体的信息与其数字证书及身份绑定。全过程追溯信息数据主要是医疗废物从产生到分类、打包、暂存、院内转运、院外转运、最终处置等各环节产生的动态数据,主要包括但不限于:打包追溯码、医疗垃圾分类标签、称重信息、存证照片、交接信息、运输过程轨迹信息、监控视频存证信息(哈希码)。(3) 形成追责机制。涉及单一参与主体的数据在上链过程中需要参与主体用其数字证书对应的私钥进行签名,保证参与主体对该数据负有不可否认的责任。涉及多方参与的交接活动所产生的数据,需要多方参与者利用其数字证书对应的私钥签名后才能上链,保证参与各方认可数据是真实可信的。通过这种机制能够有效解决追责困难问题。(4) 关联数据记录。对于上链信息还需通过唯一标识引用的方式建立数据记录之间的关联关系。另外通过在交接步骤中产生的上链数据中记录前序步骤的标识符使各个环节形成闭环,还可以将前序步骤的关键信息通过数组等集合结构冗余地保存在最新链上状态中,以便实现状态快速查看。(5) 建立公共账本。利用区块链分布式记账特点实施医疗废物管理,建立客观公正的数据体系,即公共账本,为管理提供支撑。首先,研发具有上链能力的专用智能设备,在医疗废物的产生、交接和处置环节可以实时客观地采集数据并将数据指纹上链存证形成公共账本。上链过程由程序代码来保障其客观性并经公开检查和验证。其次,每次上链过程需要交接双方共同签名才能完成,确保上链数据指纹所代表数据是获得双方认可的公共账本,避免事后追溯产生异议。在医疗废物产生环节采取专用包装袋并粘贴追溯二维码,做到医疗废物交接流转过程中可以低成本识别医疗废物流向,为上链数据建立关联提供保障。最后,所有双方签名后的上链数据经过加密后备份,相应数据指纹会基于区块链协议同步到各参与方独立管理的服务器上,从而使各参与方都保存统一的公共账本,确保上链数据的充分安全和共享,并且不能单方面修改公共账本的链上数据。参与方包括医院、运输公司、医疗废

物处置单位以及卫健委、交通管理和环保等监管部门。在客观公正的区块链数据体系之上，运用数据分析和数据挖掘技术发现问题环节和违规事件并及时通报给监管单位，实现有效监管。

表 1 数据格式设计

名称	类型	描述	说明
PackageId	String	废弃物包装袋编号	废弃物的最小单位
BoxId	String	运输箱编号	废弃物打包后装箱
VehicleId	String	运输车编号	废弃物装箱后装车
MW_Type	String	废弃物类别	明文
MW_Weight	String	废弃物重量	-
Op_Role	String	上链角色类别	(1) 医院；(2) 运输；(3) 处置
Op_UnitId	String	操作人员单位 ID	-
Op_MemberId	String	操作人员编号	-
Op_MemberDigest	String	操作人员信息摘要哈希	-
Opation	String	操作行为	(1) 初始打包/确认；(2) 装箱/确认；(3) 装车/确认；(4) 入库暂存/确认；(5) 回收处置/确认
Oth_MemberId	String	交接人 ID	-
Op_DateTime	String	操作时间	时间戳
Op_Location	String	操作地点坐标	传统经纬度格式
Op_RFIDInfo	String	RFID 位置坐标信息	-
Memo_Photo	String	照片摘要哈希	-

### 4 医疗废物监管区块链架构

医疗废物监管架构共分为联盟链平台基础层、医疗废物监管应用层两层，从底层到上层分别是数据存储层、组件层、应用接口层、医疗废物监管应用层，见图 4。数据存储层：分为文件存储和数据库存储。文件存储主要是存储区块分段文件；数据库存储是对区块、交易索引以及合约状态进行存储。组件层：提供网络传输、验证机制、合约运行引擎、共识机制等组件，为应用接口层提供基础服务。应用接口层：提供外部接口，医疗废物监管信息系统以 Restful 形式与区块链系统进行交互。应用接口层提供交易提交、交易和区块检索等基本功能。应用层：通过用户密钥安全管理进行安全性验证，结合医疗废物监管业务流程，从收集、存储、转运、处置 4 个方面，基于应用接口层实现合约和接口应用管理。用户层：医疗废物监管信息系统用户包括卫生监管部门、医疗机构、运输部门、运送公司、环保部门、处置公司等。

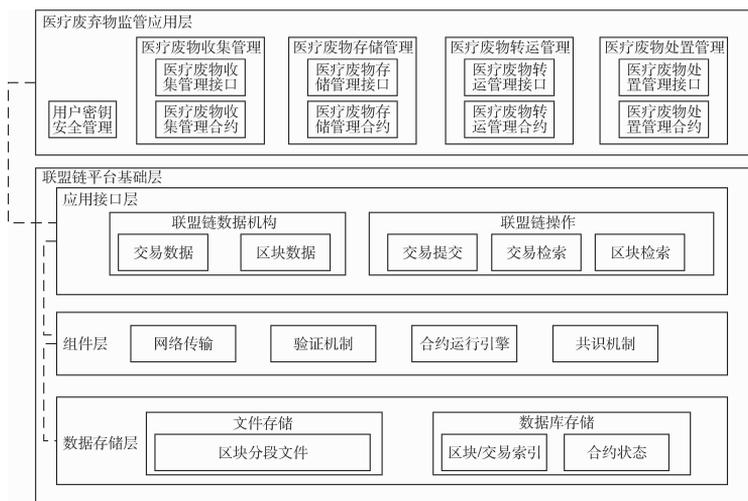


图 4 医疗废物监管架构

### 5 结语

在医疗废物监管领域，本文提出基于区块链智

能合约技术的应用方案，通过区块链、智能合约等技术应用有效地解决了传统医疗废物监管过程中数据隐私安全问题、各参与主体之间相互独立问题、监管溯源问题和自动化采集存证问题，有助于现有

传统医疗废物监管模式进行转型升级。

## 参考文献

- 胡凯, 白晓敏, 高灵超, 等. 智能合约的形式化验证方法 [J]. 信息安全研究, 2016, 2 (12): 1080 - 1089.
- 黄涵禧. 应用智能合约的简易承兑汇票实践 [J]. 金融科技时代, 2017 (2): 38 - 44.
- Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things [J]. IEEE Access, 2016 (4): 2292 - 2303.
- 陈志东, 董爱强, 孙赫, 等. 基于众筹业务的私有区块链研究 [J]. 信息安全研究, 2017, 3 (3): 227 - 236.
- Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy - preserving Smart Contracts [C]. San Jose: Proc. of the 2016 IEEE Symp. on Security and Privacy (SP), 2016.
- 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究 [J]. 软件学报, 2017, 28 (6): 1474 - 1487.
- 工业和信息化部信息化和软件服务业司, 中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书 (2016) [EB/OL]. [2016 - 10 - 18]. <http://www.cbdforum.cn/index/dd/7>. do.
- 李春晓, 陈胜, 郑龙帅, 等. 响应式许可链基础组件——RepChain [J]. 软件学报, 2019, 30 (6): 1670 - 1680.
- Neisse R, Steri G, Nai - Fovino I. A Blockchain - based Approach for Data Accountability and Provenance Tracking [C]. Reggio Calabria: Proc. of the 12th Int' l Conf. on Availability, Reliability and Security, 2017.
- Micheler E, Von Der Heyde L. Holding, Clearing and Settling Securities through Blockchain/Distributed Ledger Technology: Creating an Efficient System by Empowering Investors [EB/OL]. [2021 - 05 - 01]. [http://www.onacademic.com/detail/journal\\_1000040514042610\\_dcfcd.html](http://www.onacademic.com/detail/journal_1000040514042610_dcfcd.html).
- Jang H, Lee J. An Empirical Study on Modeling and Prediction of Bitcoin Prices with Bayesian Neural Networks Based on Blockchain Information [J]. IEEE Access, 2018 (6): 5427 - 5437.
- 陈扬扬, 宓永迪. 二维码与 RFID 和 NFC 技术在图书馆中的应用 [J]. 科技情报开发与经济, 2013, 23 (5): 46 - 48.
- 文斌, 梁鹏, 罗自强. 基于 QR 二维码和数据聚合的农业产品追溯服务系统设计 [J]. 小型微型计算机系统, 2014, 35 (2): 261 - 265.
- 王卉. 基于 RFID 的蔬菜质量追溯系统的设计与实现 [D]. 南京: 南京农业大学信息科学技术学院, 2013.
- 颜波, 石平, 黄广文. 基于 RFID 和 EPC 物联网的水产品供应链可追溯平台开发 [J]. 农业工程学报, 2013, 29 (15): 172 - 183.
- 林宇洪, 林敏敏, 林承操, 等. 基于物联网的肉产品质量安全信息的追溯 [J]. 华北科技学院学报, 2015, 12 (5): 98 - 102.
- 刘凯, 吕璐. 基于物联网技术的产品可追溯系统研究 [J]. 湖北理工学院学报, 2015, 31 (2): 27 - 30.
- 赵震, 张龙昌, 韩汝军. 基于物联网的食品安全追溯研究 [J]. 计算机技术与发展, 2015, 25 (12): 152 - 155.
- 张丽, 杨怀卿, 刘晓亮. 基于物联网技术的化肥质量安全追溯系统 [J]. 物流技术, 2015, 34 (15): 244 - 246.
- Duan J, Zhang C, Gong Y, et al. A Content - Analysis Based Literature Review in Blockchain Adoption within Food Supply Chain [J]. Int J Environ Res Public Health, 2020, 17 (5): 1784.
- 贺超, 刘一锋. 融合区块链的新型供应链模式研究 [J]. 管理现代化, 2020, 40 (1): 84 - 87.
- 李志宏, 乔贵鸿, 唐洪婷, 等. 区块链技术与社区知识分享 [J]. 科技管理研究, 2020, 40 (15): 199 - 208.
- 张亮, 刘百祥, 张如意, 等. 区块链技术综述 [J]. 计算机工程, 2019, 45 (5): 1 - 12.
- 付永贵. 基于区块链的供应链信息共享机制与管理模式研究 [D]. 北京: 中央财经大学, 2018.
- 陈伟利, 郑子彬. 区块链数据分析: 现状、趋势与挑战 [J]. 计算机研究与发展, 2018, 55 (9): 1853 - 1870.
- 杨扬, 石相团. 基于区块链技术的“澜湄区域”跨境物流运作模型设计 [J]. 科技管理研究, 2020, 40 (5): 139 - 145.

(上接第 54 页)