

基于多链协同的医疗集采数据监管方案

赵楷¹, 闫俊桥¹, 胡煜环¹, 毕雪华², 张琳琳³

(1. 新疆大学计算机科学与技术学院, 新疆 乌鲁木齐 830017;

2. 新疆医科大学医学工程技术学院, 新疆 乌鲁木齐 830011; 3. 新疆大学软件学院, 新疆 乌鲁木齐 830091)

摘要: 随着区块链在医疗领域的广泛应用, 对于多样、敏感且规模持续增长的医疗集采数据进行有效监管逐渐显露出其重要性。然而, 现有的医疗集采数据监管方案由于业务关联复杂, 导致多部门协同监管过程效能低, 存在共享监管数据隐私泄露风险。因此, 基于多链提出了一种支持安全共享的医疗集采数据监管方案。构建一个基于监管中继链的多链协同监管框架, 针对医疗集采业务概括出监管元素和受监管数据对象, 形成多链协同监管与跨链交互的全面视图; 通过多链协同监管模型展示多种监管信息流, 将监管元素描述为结构化的跨部门综合监管事项清单, 以支持多部门多环节跨链监管; 在多链监管实施过程中, 将医疗集采业务产生的大量受监管数据对称加密后存储于星际文件系统(IPFS)中, 降低区块链存储负担; 引入代理重加密(PRE)技术保障对称密钥与元数据的多链间安全共享, 并结合可搜索加密算法支撑链上 IPFS 文件地址密文的检索。以医疗集采业务分析为基础, 对监管数据的流转过程进行安全性分析, 对协同监管过程中授权、上传和查询等链码进行性能测试。实验结果表明, 该方案具备安全性与高效性, 相对于其他类似方案更适合医疗领域, 能够满足多部门多环节协同监管和数据安全共享需求。

关键词: 区块链; 监管机制; 多链; 代理重加密; 医疗数据

中图分类号: TP391

文献标志码: A

DOI: 10.19678/j.issn.1000-3428.0069156

Data Supervision Scheme of Medical Centralized Purchase Based on Multi-Chain Collaboration

ZHAO Kai¹, YAN Junqiao¹, HU Yuhuan¹, BI Xuehua², ZHANG Linlin³

(1. School of Computer Science and Technology, Xinjiang University, Urumqi 830017, Xinjiang, China;

2. School of Medical Engineering and Technology, Xinjiang Medical University, Urumqi 830011, Xinjiang, China;

3. School of Software, Xinjiang University, Urumqi 830091, Xinjiang, China)

【Abstract】 The wide application of blockchain in the medical field has gradually brought attention to the effective supervision of diversified, sensitive, and continuously growing medical centralized purchasing data. However, owing to complex business relationships, existing medical centralized purchase data supervision schemes are not efficient in multi-department collaborative supervision processes, and shared supervision data carry the risk of privacy disclosure. Therefore, based on multi-chain collaboration, this paper proposes a supervision scheme for medical centralized purchase data, supporting security sharing. This scheme constructs a multi-chain collaborative supervision framework based on the supervision relay chain, summarizes the supervision elements and supervised data objects for the medical centralized purchase business, and forms a comprehensive view of multi-chain collaborative supervision and cross-chain interaction. Multiple regulatory information flows are described through the multi-chain collaborative regulatory model, and the regulatory elements are described as a structured list of cross-sectoral comprehensive regulatory matters to support multi-sector, multi-link, and cross-chain supervision. During the implementation of multi-chain supervision, a large amount of regulated data generated by the medical centralized purchase business is symmetrically encrypted and stored in an Inter Planetary File System (IPFS), reducing the storage burden of blockchain. Proxy Re-Encryption (PRE) technology is introduced to ensure the secure sharing of symmetric key and metadata between multiple chains, and a searchable encryption algorithm is integrated to support the retrieval of the IPFS file address ciphertext from the chain. By analyzing the medical centralized purchase business, a security analysis of the process flow of data supervision is carried out. Then, the performance of chain codes such as authorization, upload, and query in the collaborative supervision process is evaluated. Experimental results show that the proposed scheme is secure and efficient, is more suitable for the

基金项目: 新疆维吾尔自治区自然科学基金(2022D01C429, 2022D01C427, 2024D01C126); 国家自然科学基金(62366052, 62563036); 四川省联合基金(25QYCX0103)。

作者简介: 赵楷, 男, 副教授、博士, 主研方向为区块链、网络空间安全; 闫俊桥、胡煜环, 硕士研究生; 毕雪华, 副教授、博士; 张琳琳, 教授、博士。

收稿日期: 2024-01-03

修回日期: 2024-07-12

E-mail: zhawkk@xju.edu.cn

medical field than similar schemes, and meets the requirements of multi-sector and multi-link collaborative supervision and data security sharing.

[Key words] blockchain; regulatory mechanisms; multi-chain; Proxy Re-Encryption (PRE); medical data

0 引言

2008 年,中本聪首次提出了区块链的概念^[1],这种分布式的存储结构,将经由参与者验证的交易打包成为区块并相继链接,构成了区块链在透明性、可信性、可靠性和不变性等方面的独特优势,因而区块链技术被广泛认为是一种“颠覆性”的信息技术解决方案^[2],并在电子健康档案共享^[3]、制药溯源^[4]、大数据访问^[5]和智能检测设备^[6]等医疗健康领域呈现出广泛的应用前景^[7]。

在医疗集采业务中,医疗机构存在违规采购、采购量异常以及临床使用不合理等现象,医药器械企业断供、配送不达标和产品质量下滑的情况也时有发生,同时医保经办机构负责的报销、结算程序易出现虚报贪腐,多方利益因素都关系到医保基金的安全使用,加强监管刻不容缓。而当前医疗监管存在规范体系滞后、社会参与不足、监管流程与标准粗放、监管程序与手段有待创新等问题。在《国务院关于加强和规范事中事后监管的指导意见》^[8]中也明确要求对直接涉及公共安全和人民群众生命健康等特殊重点领域要实行全覆盖的重点监管。然而,由于医疗数据的多样性和敏感性^[9],再加上医疗、医药和医保部门之间低效的协作,以及受当前监管制度体系不健全、技术手段不完备等因素制约,导致医疗领域的综合监管面临监管权责分散、敏感数据泄露和协同能力不足等问题,因此亟需创新和完善。

对此,跨部门综合监管成为一种新的监管思路,相对于传统按行业或部门划分政府权责的监管方式,跨部门综合监管着重于市场活动的业务特性与风险类型,旨在将各层级监管纳入业务协同,以确保监管的全局连贯与一致。这代表了从众多独立管理机制向部门间集中管理的转变,关键在于集结散落的监管资源,并构筑高效的协同机制。而基于区块链的监管体系^[10],提供了一个颠覆传统的视角,建立了扁平的协同信息结构,变革了监管组织形态与流程,促进了跨部门信息流通,理顺了部门之间的协同关系,避免推诿扯皮现象的发生,提高了跨部门协同监管的效率。其中,陈纯^[11]的“以链治链”思路为区块链监管技术的发展指明了方向,将监管条例转换为智能合约以实现自动化监管将是未来趋势^[12]。

由于单链结构性能受限,多链架构应运而

生^[13]。与此同时,多链架构也带来了链间协同和多链监管的挑战。多链协同的核心在于联通不同链上相关的业务,多链协同监管则是更进一步,要求多个部门共同对分布在不同链上的关联业务进行一体化综合监管。但目前的监管方案尚未能确保各行业主体的业务操作数据与受监管的敏感数据得以有效分离,在数据可追溯性与用户隐私保护之间难以取得平衡^[14]。

基于上述的多部门多环节综合监管业务中存在的协同效能低下和医疗数据隐私泄露等问题,结合区块链应用的多链发展趋势,本文提出一个基于中继监管链的多链协同监管方案。该方案构建了一个多链模型,由监管中继链和多个业务链组成,在监管中继链中把监管行为转换为监管策略和监管任务,明确各部门的监管权责和多环节的监管流程规范,同时,监管机构对受监管业务进行灵活管控,将业务操作数据存储在各自己的业务链上,而受监管的数据和跨链交互信息则经过加密后上传到监管中继链,实现监管数据安全传输和多部门的数据共享,并把跨链交互行为纳入了监管范畴。本文的主要贡献如下:

1)构建了一个基于中继链的多链协同监管架构,对监管元素进行了概括分析,并设计监管策略表、监管任务表、业务表等结构化数据,将跨部门综合监管事项清单部署于链上,并配合相关链码和部件完成多链协同监管过程。

2)结合星际文件系统(IPFS)网络与基于高级加密标准(AES)算法的代理重加密(PRE)技术,将大量涉及隐私的业务数据加密存储于 IPFS 中,文件地址和原始业务数据需代理重加密后才能解密。此外,本文还采用基于 Hash 前缀索引的可搜索加密算法来保障链上数据隐私,并提供密文检索能力。

3)以国家医保基金监管需求为导向,搭建了医疗集采业务监管系统,包括监管类指令发布和查询,以及监管数据授权、上传和下载等功能,可实现多链协同监管和监管数据安全传输,并对相关链码进行性能测试,证明本文方案能够满足实际监管需求。

1 相关工作

1.1 区块链监管研究现状

目前,学界已经展开了一系列有关基于区块链

的监管体系的研究。区块链监管技术大致可分为 4 个发展方向,包括区块链节点追踪、公链管控、联盟链穿透式监管和以链治链^[12],后两种方案在相关文献中研究更为广泛。第 1 种联盟链穿透式监管方案包括在每个链内部设置监管节点^[15]和利用智能合约实现监管规则的数字化^[16],这种方式的优势在于监管的即时性和参与度高,但缺陷在于存在数据隐私泄露风险。此外,当不同链之间的业务相互关联时^[17],监管方可能无法有效协调,导致监管空白的出现,从而降低监管的有效性。第 2 种方案是根据“以链治链”的理念创建单独的监管链^[18-19],以适应不同行业的监管需求。尽管这种方式可以解决专业监管和数据共享的问题,但需要监管双方根据不同监管要求共同构建不同的监管链,导致操作繁琐、效率低下、资源浪费以及降低监管的实际效果。除了考虑采取何种有效的监管方式外,还需关注多链之间协同工作的跨链交互难题^[20-21],以及链间传递敏感数据的安全问题^[22-23]。

在以上各类监管技术研究的基础上,研究人员提出了面向医疗产品供应链^[24]、疫苗流通^[25]、危险废物转移^[26]、港口管理^[27]、住宅建造^[28]等应用场景的监管方案,也有利用群签名^[29]、零知识证明^[30]、代理重加密^[31]、密钥聚合^[32]等密码学技术实现具备监管能力的系统模型。然而,目前针对医疗信息的监管方案^[33]还比较少,并且更多地偏向于医疗数据共享^[9]和药品追溯^[34]等方面。综上所述,目前研究人员对涉及医疗信息的多链监管研究还处于初始发展阶段。

1.2 预备知识

本文涉及的受监管数据涵盖医疗、医药、医保等核心子行业,从患者基本信息到治疗方案、药物配方及医保赔付等敏感数据都有所包含,故在监管过程中需要保障数据安全性。通过结合 AES 对称密钥与代理重加密技术实现授权管理,并使用可搜索加密技术实现查询限制,以及利用 Hyperledger Fabric 内嵌的基于属性的访问控制(ABAC)功能实现细粒度访问保护,同时,区块链迫于高昂的存储成本、每秒事务数(TPS)限制,全数据上链显然不具现实性和效益优势,需要如 IPFS 这种更高效、更具成本效益的数据存储和处理方式。

1) 代理重加密算法。

在代理重加密(PRE)中,数据拥有者使用自身密钥加密文件得到一份密文,再结合数据接收者的公钥制造一份转换密钥,将两者交付给半可信的代理者后,被转换为可由数据接收者的私钥解密的另

一种密文。本文采用一个通用高效的基于 AES 对称密钥代理重加密算法^[35],并由区块链节点作为代理者,在密文转换的整个过程中,节点无法得到关于明文的任何信息,其算法流程为:

(1) 初始化函数 $(PK_a, Sk_a, PK_b, SK_b) \leftarrow \text{KeyGen}(G, p)$: 输入椭圆曲线密码算法 secp256k1 所需公共参数,输出共享双方的非对称密钥,其中私钥保存在双方本地,公钥可公开由对方获取。

(2) 密钥生成函数 $(Key_{AES}, Capsule_a) \leftarrow \text{EncryptKeyGen}(Pk_a)$: 输入授权人的公钥,输出 AES 密钥,以及一个携带 AES 密钥关键信息的 $Capsule_a$ 参数。

(3) 加密明文函数 $CT \leftarrow \text{Encrypt}(Key_{AES}, M)$: 输入 AES 密钥和共享数据明文,输出相应密文。

(4) 转换密钥生成函数 $RK, PubX \leftarrow \text{ReEncryptKeyGen}(SK_a, PK_b)$: 输入授权人的私钥和接收者的公钥,输出转换密钥和公开参数,转换密钥携带这两个密钥的关键信息用于代理者实施重加密步骤,公开参数用于接收者解密操作。

(5) 代理重加密函数 $Capsule_b \leftarrow \text{ReEncrypt}(RK, Capsule_a)$: 输入转换密钥和关键参数,输出对应接收者公钥关键信息的 $Capsule_b$ 。

(6) 解密函数 $M \leftarrow \text{DeReEncrypt}(Capsule_b, CT, PubX)$: 输入关键参数、密文和公开参数,输出明文,函数通过 3 个参数还原出 AES 密钥,再使用 AES 密钥解密密文。

2) 基于 Hash 前缀索引的可搜索加密。

可搜索加密是一种通过将数据文件加密后存储,并可对密文进行检索的技术。按检索准确度可分为精准搜索和模糊搜索^[36],本文实现的是基于 Hash 前缀索引的模糊查询方案,监管数据是以 $\langle K, V \rangle$ 键值对上传至链上,利用 Hash 算法将关键词转换成密文 K 值,可在不暴露搜索关键词和链上键值对真实值的条件下进行查询。

(1) $\langle word_1, word_2, \dots, word_l \rangle \leftarrow \text{Enc}(\text{Split}(\text{KeyWords}))$, 遍历明文长度为 l 的 KeyWords 字符串中每个字符,对每个字符采取 AES 加密以获取密文字符数组。

(2) $\text{IndexKey} \leftarrow \text{Joint}(\text{Hash}(word_1), \dots)$, 通过对密文字符数组中字符依次 Hash 取值后截取前 n 位,循环将所有哈希前缀拼接成密文索引字段。

(3) $\text{File} \leftarrow \text{Search}(\text{IndexKey}, \text{QueryKey})$, 在检索时需要生成密文检索令牌 QueryKey,参与检索的字符组进行步骤(1)、步骤(2)处理后生成,之后利用正则匹配以实现模糊查询。

3) Fabric-ABAC。

在 Fabric 中,可通过 Fabric CA 的身份管理接口与链码实现基于属性的访问控制,第一步对访问主体添加身份属性,后续该主体的注册证书会带上相应的属性名称和值;第二步在链码中解析身份证书中属性值,再按照设定的访问规则对比来控制链码操作权限。

4) 星际文件系统。

星际文件系统(IPFS)是一种基于内容寻址和点对点网络传输协议,集合了 DHT 分布式哈希表、Bitswap 传输协议、Git 版本控制和 SFS 自验证文件系统等技术的分布式存储方案,允许网络中的参与者互相存储、索取和传输可验证的数据。在 IPFS 中存储的数据文件具有不可伪造、全程留痕、可以追溯、公开透明和集体维护等特征。

2 多链框架

2.1 多链协同监管架构

随着医疗卫生领域“放管服”改革不断深化和技术手段不断进步,医疗卫生行业监管面临新的机遇和挑战。从重点监管公立医疗卫生机构转向全行业监管,从注重事前审批转向注重事中事后全流程监管,从单项监管转向综合协同监管,亟需建立职责明确、分工协作、科学有效的综合监管框架。本文针对医疗卫生领域提出了基于监管中继链的多链协同监管架构,通过 Fabric 通道技术构建 1 条监管中继链

和 4 条业务分链,并搭建了 1 个 IPFS 网络。具体而言主要有:

1) 监管中继链:其中有国家卫生健康委员会、市场监督管理局、医疗保障局等分管不同领域的各级监管部门,链上业务主要有发布监管指令和审查监管数据等,存有受监管业务操作数据摘要和管控跨链交互信息等。

2) 医疗链:包含多级医疗机构等医疗服务提供者,链上业务覆盖门诊预约、线上诊疗等,存储着如电子病例等核心数据。

3) 医保链:包括医疗保障经办机构、医疗保险企业和参保者,链上开展商业和社会医疗保险以及医保基金管理运用等多种业务,保存着医保费用清单等核心数据。

4) 医药链:涵盖医药和医疗器械企业以及药店等医疗用品供应者,链上记录有企业生产和商家销售数据。

5) 辅助链:包括一些如运输与存储企业、第三方可信质检机构、慈善组织等间接参与医疗业务的外围组织,链上保留仓储、运输监测数据和质量检测报告等。

多链协同监管架构设计如图 1 所示。其中,中间是 5 条链的整体交互展示,左右框图表明了各个不同链的所代表的业务类型和数据来源,中继链的监管业务则用上方框图进行了流程描绘,下方框则代表了存储的结合方式。本文将参与主体分为监管

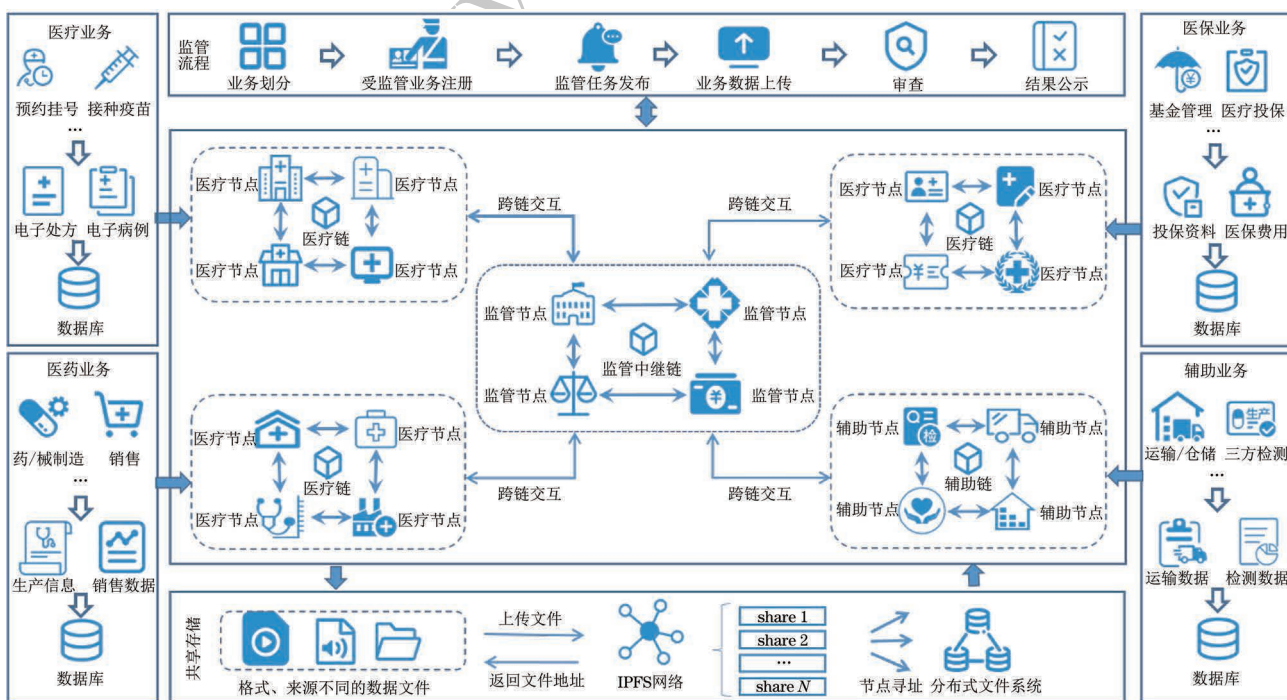


图 1 医疗信息多链协同监管架构

Fig.1 Multi-chain collaborative regulatory architecture for medical information

部门和受监管组织,将受监管对象从各企业单位整体进一步分为依法注册的多种受监管业务,以细化监管目标。受监管内容则为链上行为和链下数据,链上行为包括业务合约执行过程和跨链交互,这些行为记录分别存储在各链中和监管中继链;链下数据则是业务在日常生产经营活动中所产生和积累的数据,这些数据会被转换成电子文件并加密存储于 IPFS 中,以便按照监管要求共享给监管机构。

2.2 协同监管元素定义

为了对涉及多个监管部门并且分布于多个区块链上的综合性业务实施有效监管,需要逐一明确监管领域、监管部门、监管层级、监管事项、设定依据、监管对象、事项类别、检查方式等,以形成跨部门综合监管事项清单。基于此,本文定义协同监管元素的元数据描述如下。

定义 1 协同监管(SF), $SF = \{SFId, User, Strategy, Task, Business\}$ 表示协同监管流程实例,包含有用户、协同监管策略、监管任务、受监管业务这些监管元素。

定义 2 用户(User), $User = \{UserId, Supervise, Privileges\}$ 表示协同监管流程实例中的各级监管部门和业务执行者,其中,UserId 是 User 的唯一标识,Supervise 表示 User 参与的协同监管流程,Privileges 表示用户权限。

定义 3 协同监管策略(Strategy), $Strategy = \{StrategyId, UserId, Link[Link_1, \dots, Link_n], Files\}$

标识协同监管策略实例,其中,StrategyId 是唯一标识,UserId 表示由哪个用户创建管理, $Link_n = \{Task[TaskId_1, \dots, TaskId_n], Strategy[StrategyId_1, \dots, StrategyId_n]\}$ 表示监管流程中第 n 个环节,环节中包含有多个监管任务和子策略,用嵌套子策略体现监管层级,Files 表示设定依据。

定义 4 监管任务(Task), $Task = \{TaskId, Belong \langle StrategyId, Link \rangle, UserId, Demand, Business[BusinessId_1, \dots, BusinessId_j]\}$ 表示协同监管策略实例中的协同监管事项,其中,TaskId 是 Task 的唯一标识,Belong 表示 Task 归属于某个监管策略实例中某个环节,UserId 表示该监管任务的负责主体,Demand 表示该任务的检查方式等具体要求,Business 表示该任务包含的业务集合。

定义 5 受监管业务(Business), $Business = \{BusinessId, Properties, UserId, Parameter, Feedback\}$ 表示受监管对象,其中,BusinessId 是 Business 的唯一标识,Properties 表示业务的事项类别,UserId 表示本次监管动作的执行主体,Parameter 表示业务的参数,Feedback 表示反馈的执行结果。

目前,医疗集采作为医保基金改革的重要一环,是一种具有跨行业、跨部门特点的综合性的采办业务。故本文以监管医药集采业务为研究对象,实施多链协同监管方案,受监管业务的关键数据如表 1 所示。

表 1 医疗集采业务的关键数据

Table 1 Key data for medical centralized procurement business

业务链	隐私数据	公开数据	受监管数据
医疗链	病患资料,药品消耗数据,采购合同,基本用药供应目录,医用耗材供应目录	机构与医护人员的资质认证,处罚公示,接待人次	收费明细,药品消耗数据,采购用量和价格评估表,采购计划清单,支付账单
医保链	参保个人信息,缴费记录,医保报销单、病患诊断书	采购预算,结算账单,招标评审结果,基本医疗保险药品和器械目录	医保基金收支明细,招标评审过程文件,定点医药机构医保费用申报,参保人员医疗费用报销
医药链	产能指标,技术参数,加工工艺,原材料成本	药店销售价格,使用说明书,原材料来源、生产过程记录	出厂成本价格,临床试验资料,注册检验报告,销售数据,成品交付记录
辅助链	运输成本,订单信息,分拣,路线规划,工作监控	物流商,物流单号,运输方式、实时位置,预计到达时间,第三方考核报告	运输人员档案,运输行程,仓库地址,存储状态,第三方调查评估考核记录

3 监管机制

3.1 多链协同监管模型

多部门协同的多链监管模型如图 2 所示,首先由中继链上的牵头监管机构制定根策略,监管策

略以有向无环图形式呈现,分管各个领域的监管部门参与策略的不同环节,每个环节中都可设置多个监管任务和嵌套多个子策略。监管任务指定的多个负责单位可以共享数据资料,任务发布至各个业务链中,令业务链中企业组织等执行具体

的监管指令并提交监管数据。同时,跨链路由根据监管任务中的受监管业务所对应的监听事件,获取相关业务的执行交易编码和所在区块编号进

行打包回传至监管中继链。此外,需要多个业务链通信的跨链业务,在中继链上也留存着完整的跨链交互信息。

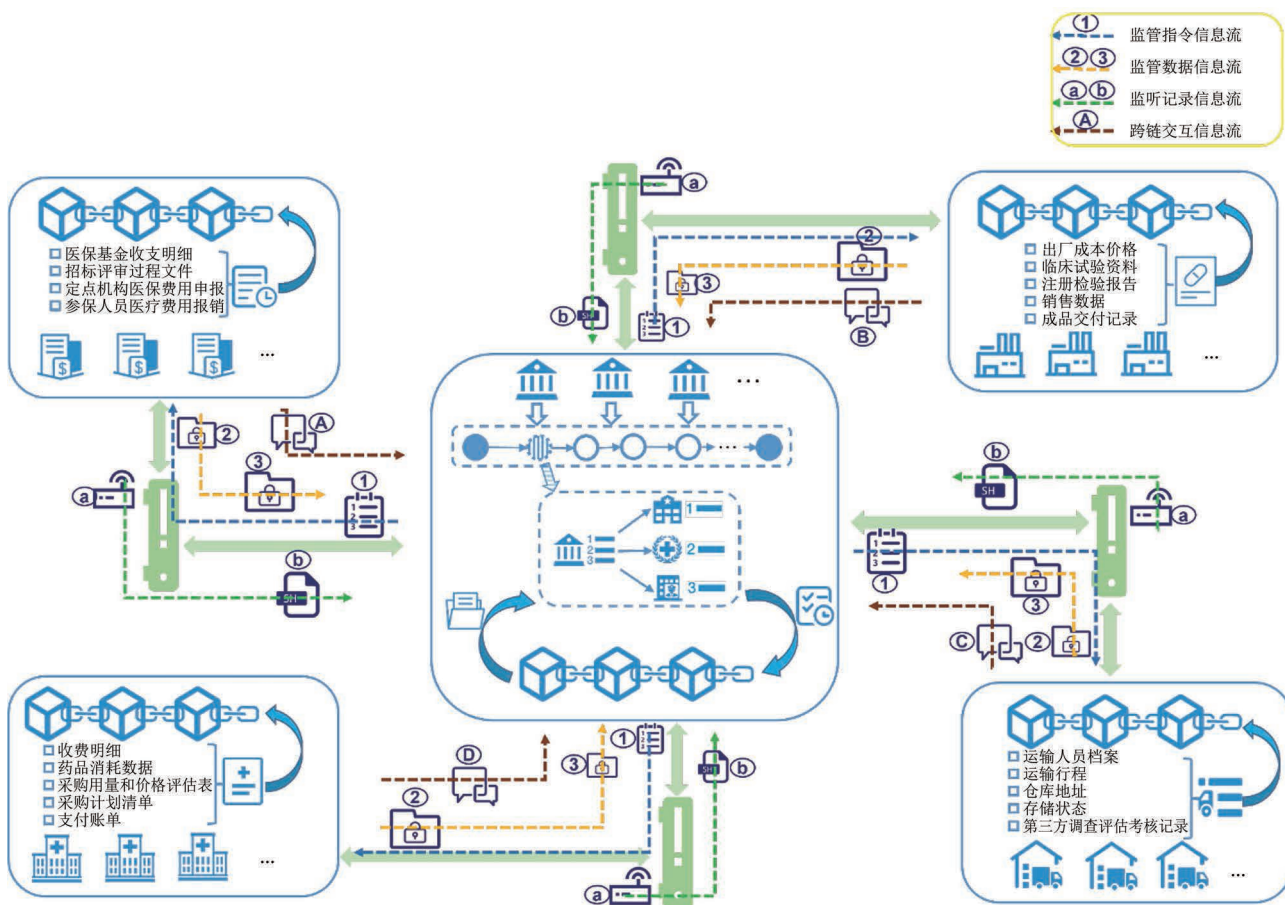


图 2 协同监管模型

Fig. 2 Collaborative regulatory model

将由政府主导的涉及多环节多部门、管理难度大、风险隐患突出的监管事项转换成链上监管工作流,行业主管部门牵头和相关监管部门配合执行各环节监管任务,受监管主体根据任务要求完成监管指令,设计了监管策略表、监管任务表和业务注册表来实现基于中继链的多链协同监管方案。其中,在监管中继链上部署协同监管流程链码,将跨部门多环节监管活动表示成监管策略表,设置管控流程和各环节的部门职责;监管任务表则明确进行协同监管的执行逻辑,根据不同监管需求来指定受监管业务编码,参与同一监管任务的多个部门则可安全共享所有上传的业务数据;此外,任何必须纳入监管范围的业务都需在监管中继链中注册,以业务注册表的形式存于链上,只有通过中继链中监管部门的合法性认证后才能分链上开展相关业务活动。监管指令所对应的数据结构设计如图 3 所示。

同时,多链监管对接的受监管业务数据具有量大、格式复杂的特点,且大多蕴含着企业隐私,

这些隐私数据泄露会对企业的市场竞争甚至发展生存产生不利影响。故本文结合 IPFS 与代理重加密技术实现受监管文件的安全传递,并采用可搜索加密技术加强链上数据的隐私性,针对受监管业务数据传递过程设计了如图 4 所示的 4 种数据结构。其中,加密密钥通过代理重加密转换完成授权操作,监管机构根据授权信息表获得解密密钥;多份受监管数据加密上传至 IPFS 后得到多个文件地址,将同批次监管文件的关键词和元数据信息封装为索引信息表;利用可搜索加密技术为每个监管文件地址制作关键词哈希串,并存储于监管文件地址表中;受监管业务链码的操作记录保留在各自业务链中,由监听器收集业务交易编码和区块哈希备份至监管中继链。需要注意的是,受监管业务根据是否需要跨链操作而分为两类,单链业务在某一条链上执行和存储,多链协同业务由两条及两条以上等多链上的链码协作完成,其交互信息通过监管中继链转换并记录。

字段	描述				
plD	策略ID				
User	创建者				
pname	策略名				
pstate	父策略编号-环节编号				
startTime	开始时间				
timePeriod	时间期限				
endTime	结束时间				
cooperateDAG[]	协同监管流程有向无环图				
link[]	监管环节集合	LinkID	环节编号		
		orgs[M]	参与单位集合		
		LinkIndex	每个环节的 活动集合索引	taskID[N]	任务编码集合
				plD[K]	监管策略ID集合
			LinkState	环节状态：准备(1/M)、执行中(1/N+K)、完成	
		File[]	监管政策公示文件集合		

(a)监管策略表

字段	描述			
businessKey	业务编码			
chainID	所在链编号			
chaincodeNmae	业务链码名称			
EventName	业务链码监听事件名			
describe	业务描述			
property	业务属性集合			
Output	输入参数			
Input	输出参数			
Enterprise	归属组织机构			
version	版本			
RegTime	注册时间			
UpdateTime	更新时间			
CrossFlag	是否属于跨链协同业务	businessID	跨链对接业务编码集合	
		TransferFunction	跨链参数和转换函数	

(c)受监管业务注册表

字段	描述			
tiD	监管任务编号			
belong	归属情况	plD	归属监管策略编号	
		LinkID	归属监管环节编号	
tstate	任务状态：准备、执行中、已完结			
regulator[]	监管单位集合			
WorkSelect[]	筛选受监管业务的条件集合			
PublicKey[]	公钥集合			
startTime	开始时间			
endTime	结束时间			
business[]	业务集合	businessEvent[]	链码事件集合，受监管业务行为监听	
		businessID[]	本次监管任务的受监管业务编码集合	
PC	批次号，上传文件的时间周期			
FileTemplate	上传文件的模版，规范上传文件数据范围、命名规范等要求的模版文件IPFS地址			

(b)监管任务表

图 3 与监管指令相关的数据结构
Fig.3 Data structures related to regulatory directives

字段	描述	字段	描述	字段	描述
capsule	原始密文	keynum	本次上传的文件数量	key	关键词密文对应的哈希串
newcapsule	重加密密文	businessID	上传文件对应的监管任务编号	IPFSvalue	文件对应的IPFS地址
rk	转换密钥	cipherKeywords	上传文件对应的关键词密文	hashkeywords	关键词哈希前缀字符串
pubX	公开参数	metadata	文件的元数据		
verifytext	加密验证密文				

(a)授权信息表

字段	描述
<Accumulator;blockHash>	<链编号, 累加器编号/区块高度, 区块哈希值>
[<workID1,[txID1,txID2...]>,...]	受监管业务的监听事件, 交易编号集
messageHash	消息包哈希值

(d)链上行为记录表

图 4 与监管文件相关的数据结构
Fig.4 Data structures related to regulatory documents

3.2 多链监管实施流程

多链协同监管策略由中继链的权威监管机构制定,按照一体化监管思路进行分配监管任务,明确各链监管执行环节与责任主体,各监管任务根据监管要求从所有注册业务中进行筛选,各链路由根据发布的跨链监管命令对本链所涉及的受监管业务的交易信息进行监听收集,同时,各受监管业务主体根据指令准备相应的监管文件主动上传。多链协同监管实施流程如图 5 所示,其具体分为以下步骤:

1)受监管业务注册。

企业机构等按照注册表中的字段要求,绑定受监管业务的责任主体,并提供本项业务的监管数据来源、类型、数量等业务描述元数据。在业务分链中

部署业务合约时节点需判定是否为受监管业务,若是受监管合约必须在中继链中注册,则取得合法认证后才可运营;在监管中继链中则由监管机构进行审核和设置业务标签属性。

2)协同监管策略设置与监管任务发布。

牵头机构设置协同监管策略表,安排各执行环节负责机构与设置政策文件等流程要求。将制定好的监管策略发布,各环节等待参与协同监管的多部门响应和提交监管任务表。监管任务表中包含受管业务编码、监管部门公钥与交付模板文件地址等关键信息,发布后由跨链路由传递到目的链。

3)监管任务执行。

将监管任务分配到对应的分链,具体的执行者为监听器和企业机构,监听器持续监听受监管业务

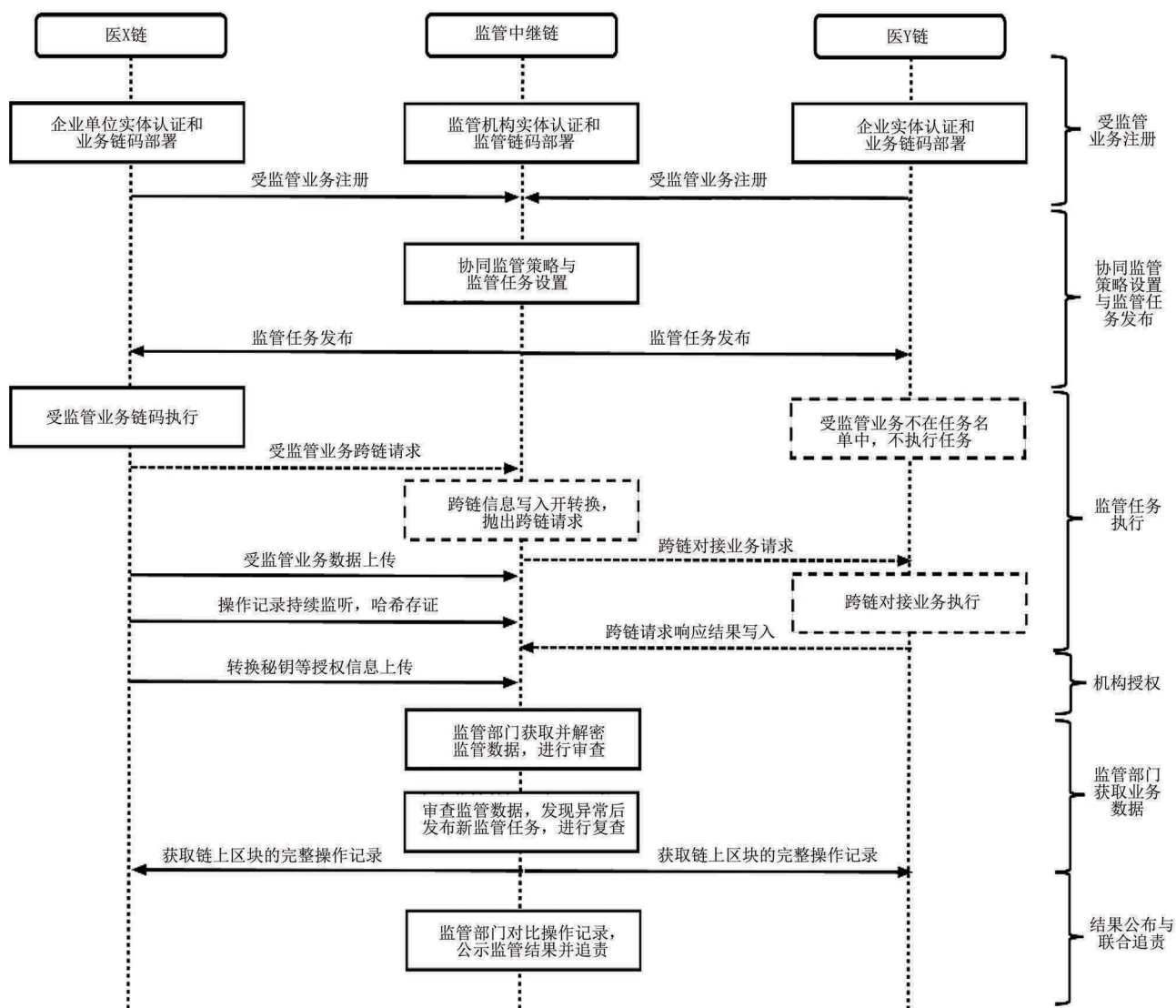


图 5 多链协同监管实施流程

Fig. 5 Implementation procedure of multi-chain collaborative supervision

在链上的操作记录,将业务交易编号和区块哈希值打包回传;企业机构将受监管业务文件 AES 加密后上传到 IPFS 中,再用同一 AES 密文加密 IPFS 返回的地址,这些密文数据结合关键词等文件元数据信息通过跨链合约上传至监管中继链。

4) 机构对监管部门授权。

企业单位利用自身公钥和 AES 密钥计算出原始密文,又通过监管部门公钥和自身私钥制造转换密钥等授权信息,最后将原始密文和授权信息上传至监管中继链,中继链中节点作为代理方便使用授权参数将原始密文重加密为二次密文并存于链上。

5) 监管部门获取业务数据。

监管部门首先获取授权信息,并使用自身私钥进行解密获取 AES 密钥,再获取索引块中的业务文件元数据信息,根据自身需求使用关键词等提示信息查询链上内容,获取 IPFS 地址密文并解密,安装

IPFS 地址下载监管文件,核对哈希值是否变化,若无错则解密开始数据审查;在审查时,当监管机构检查出异常的业务数据时,可发布监管任务获取业务链上的完整区块进行链上操作记录的复查,与监听器回传的交易编号和区块哈希进行对比,防止篡改和遗漏。

6) 结果公布与联合追责。

监管中继链管控整个协同监管流程,对比审查业务链上传的监管数据、完整区块数据以及中继链上的监听存证与跨链信息,多渠道复核定位责任主体,审查完毕后进行结果公示与问责。

对于步骤 3) 中的业务,完成监管任务的过程和跨链交互过程互不影响,各自独立执行,监听器按事件类别处理,跨链交互信息完整保存在中继链上;步骤 5) 的复查行为中发布的新监管任务挂载于原监管策略环节中。

3.3 医药集采流程协同监管示例

3.3.1 医疗集采业务流程分析

由于国家集采属于多环节且多部门参与的项目,单独某一条区块链无法满足需求,可根据每个环

节的参与者不同而部署在业务分链中,环节衔接则采取跨链通信的方式完成。在文献[37]基础上,本文对多链协同完成同一项集采业务的执行交互时序图如图6所示。

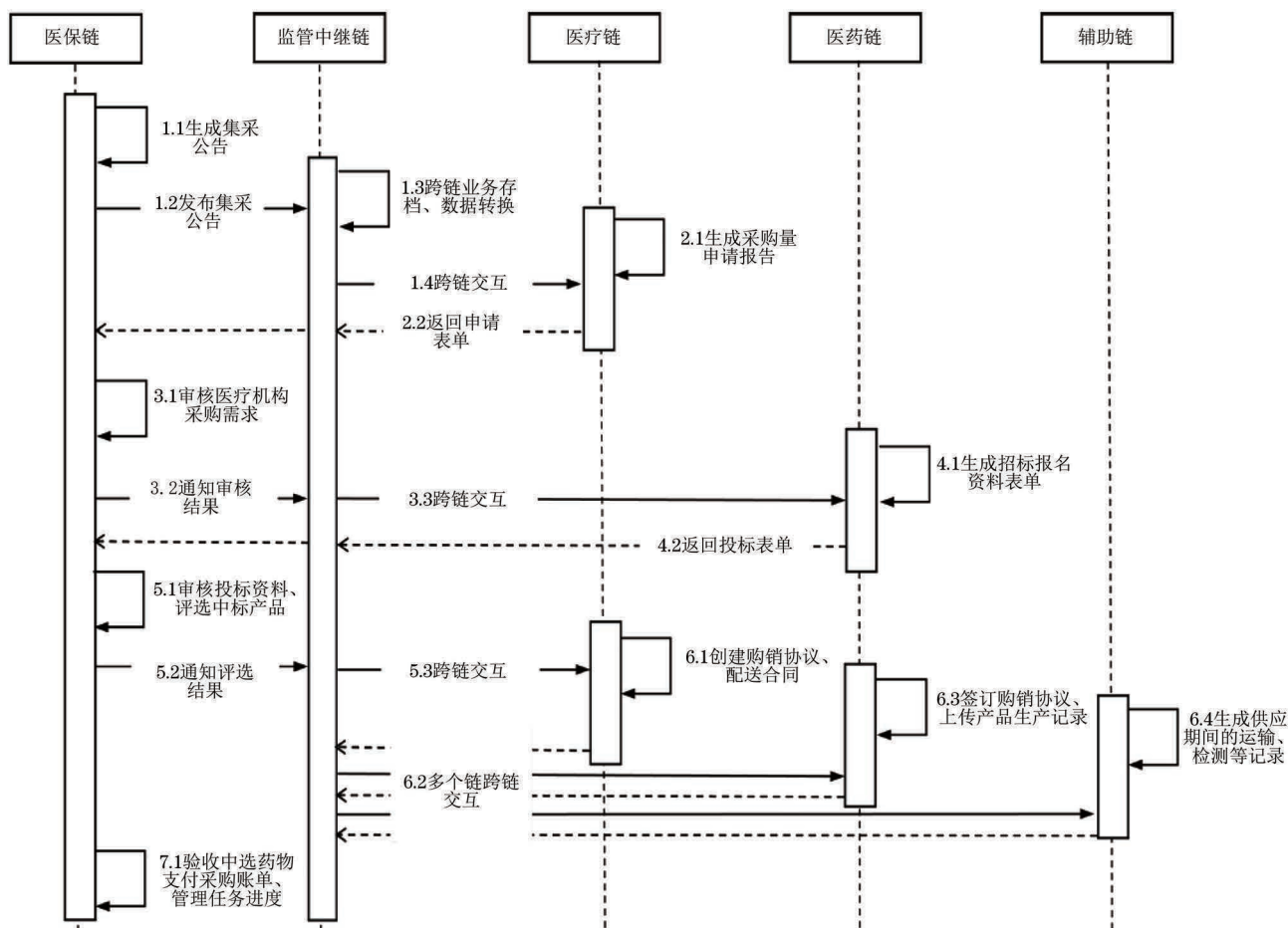


图 6 医疗集采业务交互时序图

Fig.6 Time sequence diagram of medical centralized procurement business interaction

1)医保链中的医保经办机构或采购机构调用集采公告合约,将此次药品集采的要求、时限、所需响应结果等上传,制定采购公告并跨链上传到中继链上,公告将同步至医疗链中和医药链中。

2) 医疗链中医疗机构调用采购量申请合约,填写药品采购清单,发送跨链消息经由中继链转送给医保链。

3) 医保链调用采购量审核合约, 审核药品采购清单并统计区域采购量和种类, 填写价格限制范围、数量范围、品质要求等, 完成审核后消息跨链通知医疗链和医药链。

4)医药链调用招标报名合约,邀请满足要求的合法生产商参与竞标,在规定时间内给出报价等,合约挑选一批满足基本条件的候选者,附带提交各厂家的药品清单等申报材料跨链发送给医保链。

5) 医保链调用采购招标审核函数, 履行医保经办机构职责, 随机挑选出医药专家等评审专员, 对医

药链提供的候选者进行审核打分,最终将中标者名单上传中继链,广播至所有链。

6)医药链、医疗链共同调用采购品种订单合约,达成订购意向,并与辅助链中的运输、储备、库存企业签订配送合同。

7)各分链进入采购后期管理,辅助链上由运输企业实时上传配送进度、仓储状态,以及可信第三方检测报告等。由医疗链、医药链等定期更新分配入库、药品生产状况等信息。

采购完成后医保链进行统一支付,上传支付凭证,督促医疗链及时向药品或耗材生产企业回款,双方留存结算记录;医疗链定期更新该批次集采药品的临床使用数据和集采中选药品任务量完成进度。

3.3.2 多链协同监管过程

集中采购业务涉及到多个不同的环节,并由具有利益联系的企业组织负责执行具体业务逻辑,需

要监管的关键数据呈现碎片化性质,相关机构监管困难且容易责任分属不清,导致部分环节监管缺位,同时由于部分监管机构只局限于其自身环节的监管,对前后相关环节的监管数据缺乏整体化监管意识,导致监管不连贯和监管漏洞。

监管流程如图 7 所示,首先业务受监管方通过

AES 密钥将隐私数据加密,使用监管方的公钥制作代理密钥参数,再由半可信的链节点进行代理重加密完成重加密过程,之后通过监管者的 CA 身份属性与数据获取链码提取属性进行判定,实现细粒度的访问控制,最后只有持有特定检索令牌才能查询并获取到对应加密数据。

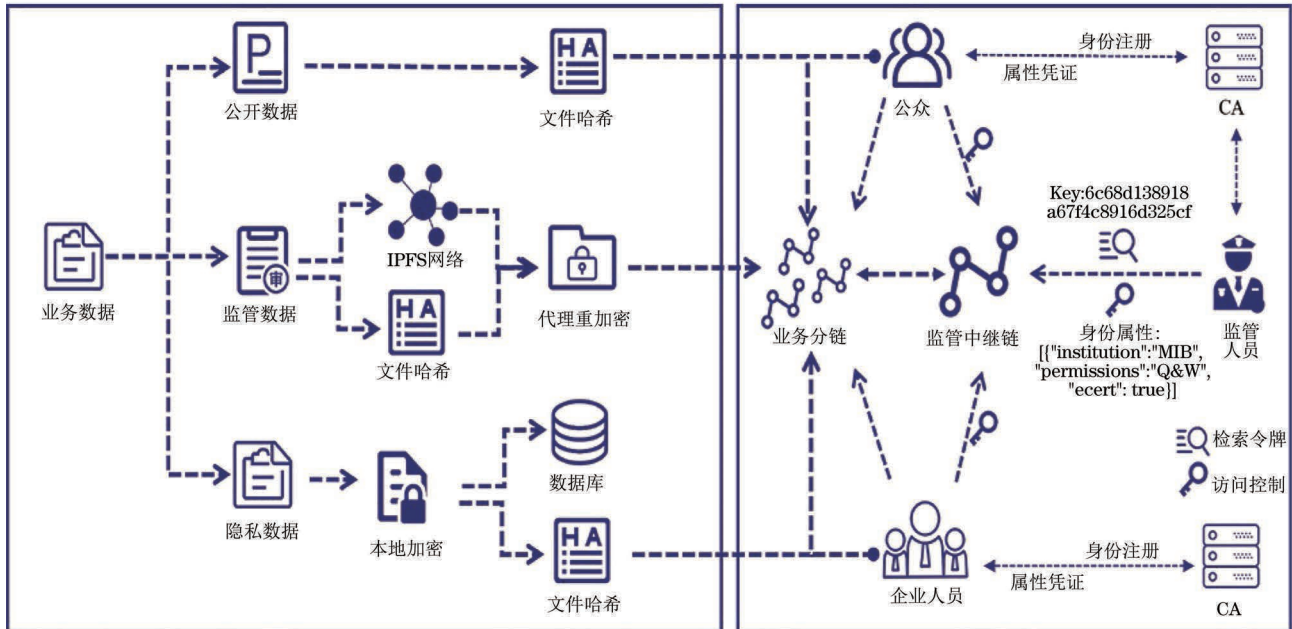


图 7 多链协同监管流程

Fig. 7 Multi-chain collaborative supervision procedure

本文基于第 3.2 节多链监管实施流程所提出的多链协同监管方案进行针对性监管,将业务场景转换为功能伪代码,其过程细节如下:

1) 受监管业务注册阶段:每个分链中的企业组织按照监管要求将受监管业务合约进行注册,如采购申请、招标和审核等关键合约,只有注册后才能配合监管指令和跨链路由完成相应监管动作,如算法 1 所示。

算法 1 受监管业务注册

输入 BusinessEnrollTable 业务信息元数据, BetRegulatory 监管机构, BetSelectLabelMap 默认标签, bID 业务编码

输出 result 注册记录

```

1. If BusEnrollTable. 标签索引 != null then
2. BetSelectLabel, BestSelectLabelMap ← {BetRegulatory, BetSelectLabelMap} // 添加业务标签
3. end if
4. BusinessEnrollTable, BestSelectLabelIndex ← BetSelectLabel
5. result ← stub. PutState(bID, BusinessEnrollTable)
6. return result

```

2) 监管策略和任务创建阶段:中继链中由卫生健

康委员会创建协同监管流程,将各环节监管权责分配至医保局、市场监管局等机构,并由各类型业务主管部门布置协同监管任务,创建过程如算法 2 所示。

算法 2 监管策略和任务创建

输入 StrategyTable 监管策略表, TaskTable 监管任务表

输出 result[] 链上写入状态集合

```

1. if cid. AssertAttributeValue(stub, "Regulatory", "true") != null then return // 访问权限控制
2. result ← stub. PutState(LinkID, Link) // 初始化策略/略各环节状态
3. TaskTable, TaskBusinessArray ← SelectByLabel(TaskTableMap) // 根据标签筛选业务
4. TaskTable, BeLongToStrategyAndLink ← (SID, LinkSequence) // 添加任务归属
5. if "判定此环节归属是否对应正确" then
6. if "监管机构响应" then
7. addLinkReplyNum(Org)
8. else if opt = "监管机构添加子策略或任务" then
9. link. IDArray ← append(link. IDArray, SID, TID, ...)
10. else if opt = "监管机构提交子策略或任务" then
11. addLinkComplete(SID, TID, ...)

```

```

12. end if
13. result←link.UpdateLinkState()
14. end if
15. return result

```

3) 监管任务执行阶段: 以医疗链中医疗机构的采购业务为例, 执行采购业务链码后, 链上操作记录在医疗链中, 并触发监听器将交易号与所在区块哈希自动回传给监管中继链。同时, 医疗机构根据监管任务的要求, 将采购药品的收费明细、消耗数据、采购用量和价格评估表、采购计划清单、支付账单等数据文件进行加密后上传 IPFS 中, 并调用跨链合约传递授权信息和 IPFS 地址等密文给监管中继链。执行阶段如算法 3 所示。

算法 3 监管任务执行

```

输入 dID 解密信息键, iID 文件元数据索引键, file 文件, keyWords 文件关键词字符串, aPubKey 医疗机构公钥, aPriKey 医疗机构私钥, bPubKey 监管机构公钥, regulatorWorkID 监管任务编号
输出 result[] 链上写入状态集合
1. capsule, keyBytes←encryptKeyGen(aPubKey)//生成 AES 密钥和原始胶囊
2. rk, pubX←reEncryptKeyGen(aPriKey, bPubKey)//生成转换密钥和公开参数
3. newCapsule←reEncrypt(rk, capsule)//重加密生成新胶囊
4. decryptInfo:= {NewCapsule←newCapsule, PubX←pubX, OldCapsule←capsule}
5. result←stub.PutState(dID, decryptInfo)
6. encrypFile←encryptByAES(file, keyBytes)//利用 AES 密钥加密文件
7. efileAddress←Ipfs.NewShell("localhost: XXXX").Add(encrypFile)//上传至 IPFS
8. result←stub.PutState(iID, Cipherindex)//写入文件关键词和元数据的索引信息
9. while _, word := range keywords do //形成可搜索加密的字符串
10. AllkeyHash←InterceptAndSplice(AllkeyHash, keyHash)//截取哈希前缀并依次拼接
11. end while
12. cipherKVs:= {enKeyHash←AllkeyHash, fileAddress←encrypFileAddress}
13. kvID←regulatorWorkID+Hash256(encryptkeywords)//精准检索 Key 值
14. result←stub.PutState(kvID, cipherKVs)//写入关键词哈希组和文件地址的内容
15. return result

```

4) 监管审核与公布阶段: 监管机构查询 IPFS

地址密文, 并利用授权信息解密获取原始数据, 对医疗机构的数据进行审查, 发现异常数据后进行追溯, 并和此业务的所有区块数据进行对比复查, 完成审查流程后更新监管任务状态, 公布违规名单, 此阶段操作流程如算法 4 所示。

算法 4 监管审核与结果公布

```

输入 dID 解密信息键, iID 文件元数据索引键, queryKey 检索令牌, bPriKey 监管机构私钥, regulatorWorkID 监管任务编号
输出 result[] 链上写入状态集合
1. 算法步骤 1 的语句//注释
2. if cid.AssertAttributeValue(stub, "Regulatory", "true")!=null then return //访问权限控制
3. capsule, pubX←stub.GetState(dID)//获取代理重加密中的解密参数
4. keyBytes←reDecrypt(bPriKey, capsule, pubX)//代理重加密中解密获取 AES 密钥
5. if iID!=null then //使用元数据索引 ID 查询
6. kvID←regulatorWorkID+Hash256(Cipherindex.encryptkeywords)//精准检索 Key
7. cipherKVs←stub.GetState(kvID)
8. else if keywords!=null then //使用关键词模糊查询
9. queryString←{"selector": {"keywords": {"$regex": ". * queryKey. *"}}}
10. resultsIterator←stub.GetQueryResult(queryString)//迭代获取所有匹配值
11. end if
12. IPFSAddress←encryptByAES(keyBytes, cipherKVs, fileAddress)//解密文件地址
13. result←Ipfs.NewShell("localhost: 5001").Cat(IPFSAddress)//获取文件
14. N, M, K←examination(result)//审查发现异常, 追溯区块数据
15. TaskTable, taskPublicIndex←taskPublicIndex{N, M, K} //N, M, K 通报名单
16. result←stub.PutState(regulatorWorkID, TaskTable)//更新链上监管任务状态
17. return result

```

4 实验结果与分析

4.1 环境配置

原型系统环境基于 go-net 客户/服务端搭建, 区块链系统基于操作系统 UBUNTU 14.04、64 位, Fabric 版本为 1.4.4, Docker 版本为 18.09, Fabric 数据库选用 CouchDB, 共识机制采用 solo, chaincode 采用 Go 编写, 测试通过 Caliper-0.50 进行, 多链环境配置如表 2 所示。

表 2 区块链环境配置

Table 2 Blockchain environment configuration

配置	值	描述
链数/条	5	监管中继链、医疗链、医保链、医药链、辅助链
组织数/个	5	每个链中存在一个相关组织
节点数/个	11	每个组织提供两个节点,CA 节点
链下存储方式	IPFS	搭建一个本地 IPFS 网络
出块时间/s	2	排序节点最晚打包出块的时长
区块交易数/个	10	区块中最大可包含的交易个数
区块容量/MB	100	区块中最大可包含的交易数据容量

4.2 安全性分析

1) 密文安全性。

本文方案采用基于 AES 对称密钥的代理重加密技术。其中, AES 加密算法作为一种块加密算法,它可使用 128、192、256 bit 密钥,其安全性可以通过它的密钥长度来衡量,密钥越长,安全性就越高,而本文采用 256 bit AES 密钥双重加密监管数据和文件地址足以保障隐私性安全。其次,本文还将业务与监管数据的对应关系利用可搜索加密技术实现隐藏,令攻击方在密文跨链传输过程中也无法劫获带有特定关键字的业务数据。

2) 密钥安全性。

在代理重加密算法中,在本地使用私钥和监管方公钥将 AES 密钥转换成可由区块链节点执行重加密的转换密文,在上传监管数据过程中,本地私钥不泄露任何信息,同时监管方也只需要提供公钥,整个过程传输都以密文形式传送。

3) 访问安全性。

本文方案通过 Fabric CA 进行身份注册,为不同主体提供不同权限的注册证书,结合 Fabric 自带的访问控制接口对监管中继链的链码调用进行属性限制,并考虑了监管任务的敏感性,防止未经授权的恶意用户提供虚假公钥以套取敏感数据,确保了监管策略和任务创建等关键链码只能由合法监管机构调用,也有助于确保监管活动的合法性和透明性,提高了监管体系的可信度和有效性。

4) 查询安全性。

区块中表示业务文件地址的交易数据键值都是通过文件关键词 AES 加密后进行 Hash256 计算得出, AES 密钥根据不同文件 and 不同监管对象进行配置,故加密后的关键词也不同,之后使用哈希计算后几乎不可能存在碰撞,搜索的精准性得到有效保障。同时,关键词盲猜等破解手段也难以突破双重加密计算,无法将业务数据与区块记录进行有效联系以达成针对性攻击,只有监管机构获取正确的

AES 密钥进行元数据解密后,才能检索到与业务相对应的数据进行监管。

4.3 性能分析

本节通过仿真实验对本文提出的基于代理重加密的多链协同监管方案进行监管信息写入与查询两方面的测试,采用 Caliper 性能测试工具,从每秒交易吞吐量、平均时延和每轮成功交易数量这 3 个指标对系统进行测试。本文系统采用 IPFS 存储各类受监管文件,只需要上传相应文件地址即可,同时采用 CouchDB 数据库以丰富查询功能。

在链上写入测试中,分别对上传授权信息和上传文件地址内容测试 11 轮,每轮工作进程 workers 个数从 1, 2, 5, ..., 70, 调整事务负载 transactionLoad 从 10 到 200, 得到每轮最高吞吐量和对应平均时延。授权信息上传后需要节点将密钥重加密后再写入链中,随着事务负载的增加,授权信息写入的吞吐量持续下降,平均时延的时长增加,当进程数达到 70 个后,由于系统性能限制,频繁并发的交易导致每个节点处理交易时出现更多的超时异常,导致吞吐量大幅下降,时延也变得 longer。加密信息写入中包含同批次的关键词与文件地址的键值对以及对应索引信息,在本实验中一次上传连续写入 15 个键值对和一组索引值。如图 8、图 9 所示,工作进程数的增加会使批量写入的效率降低,其中吞吐量稳定下降,而平均时延在进程数增加到 60 个时快速增加,说明节点面对多进程批量写入请求的响应已接近自身软硬件瓶颈。

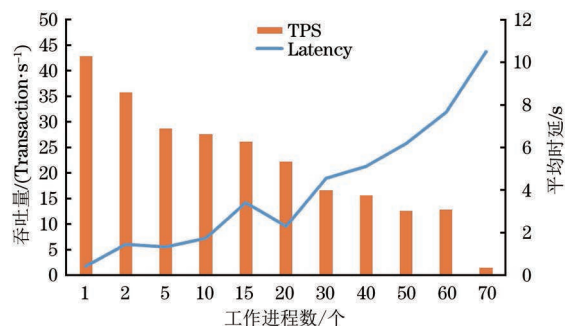


图 8 链上代理重加密写入性能

Fig. 8 On chain proxy re-encryption write performance

在对链上查询时分别对模糊查询 (EachWrokSearch)、索引信息查询 (GetIndex)、批量查询 (KVQueryByIndex) 和精准查询 (KVQueryByID) 4 个查询方式进行稳定性和负载量测试。其中,查询稳定性通过改变固定负载率控制器的起始 TPS 从 10 到 300 进行测试,并设置交易时长为 30 s,进程数为 2 个,负载量固定为 5,测试结果如图 10 所示。从图 10 可看出,在不同交易

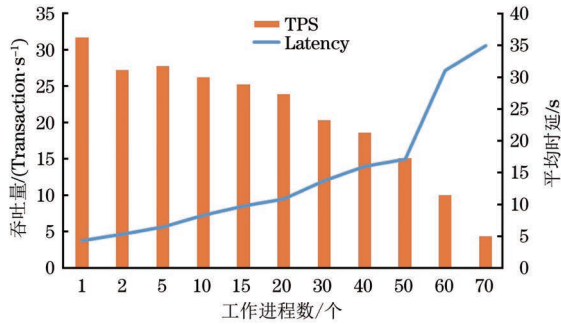


图 9 加密信息写入性能

Fig. 9 Encryption information writing performance

发送速率下,精准查询的 TPS 最高,索引信息查询稍低,但都比其他两种高一倍,因为前两种查询都是直接根据 Key 查询,查询函数无需做复杂的处理逻辑。但批量查询需先查询索引信息,获取整个批次的信息后进行循环查询每个键值对,TPS 最低的模糊查询则是使用了 CouchDB 富查询的正则匹配,故平均时延也是最长的。从整体上来看,所有查询方式的 TPS 和平均时延都保持稳定。第二个测试系统在事务积压情况下的查询性能,通过改变保持挂起的事务负载数量来检测性能极限,设置事务负载数量从 10 到 300,起始 TPS 固定为 300,其他设置与上一个测试一致。从图 11 可以看出,随着事务负

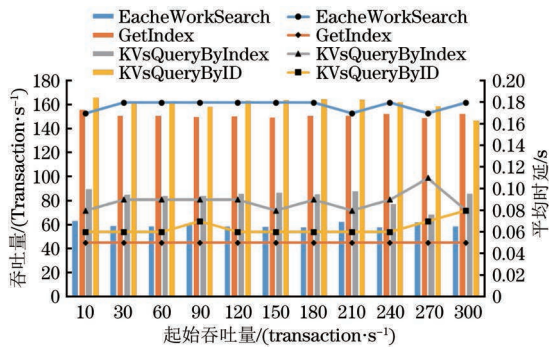


图 10 不同交易发送速率的查询性能

Fig. 10 Query performance of different transaction sending rates

载量的增加,各个查询方式的成功交易数量随之增加,到达 250 个负载量后放缓;而平均时延的时长都呈现线性增长趋势,其中模糊查询的增长最为明显,和上一个稳定性测试结果相符合。因此,4 种查询方式可以应对复杂的监管需求,并且其中的模糊查询结合可搜索加密算法能够在进一步提升安全性的同时具备良好的性能表现,适合此场景的使用。

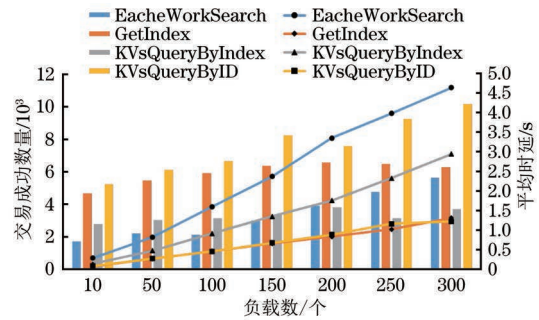


图 11 不同负载的查询性能

Fig. 11 Query performance for different workloads

4.4 方案对比

本节主要从多方面将本文方案与类似多链监管方案进行比较分析,各方案在稳定地跨链交互前提下,根据文献[38]提出的各项安全性标准,对跨链数据安全、跨链隐私安全、跨链合约安全和外部攻击安全进行比较,并从采用的安全措施进行划分,结果如表 3 所示。可以看出,本文方案跨链方式与多数方案一致,不同之处在于本文方案将中继链和监管链相融合,使监管双方直接交互从而提升效率,还可关注受监管业务的跨链行为,同时将监管范围扩展到链下数据,提高了监管的全面性。在安全保障方面,本文方案引入了代理重加密和可搜索加密技术,以确保监管数据的传输安全和保护监管双方的隐私安全,但也会导致链上操作耗时增加。此外,采用 IPFS 存储监管数据,具备较大的存储容量优势,有利于应对大量数据的存储需求。综上,本文方案相较于其他方案更适用于多链协同监管场景。

表 3 不同方案对比

Table 3 Comparison of different schemes

方案	跨链方式	监管方式	监管范围	安全措施	跨链监管时长/s	数据存储方式	安全性
文献[16]	中继链	多条监管链	链上+跨链	回滚机制	12.02	链上	中
文献[17]	区块链路由	单条监管链	链上交易+合约部署	机器学习+零知识证明校验	—	链上	高
文献[20]	混合链	公链+联盟链	链上协作流程	三次遍历双向传递机制	10.28	链上	中
文献[21]	中继链	监管链+中继链	链上+跨链	对称加密算法	19.09	链上	中
本文方案	中继链	监管中继链	链上+链下+跨链	代理重加密+可搜索加密	11.02	链上+IPFS	高

5 结束语

本文在国家药品集采的多链协同监管的应用场

景下,基于联盟链 Fabric 提出一种面向医疗信息的多链协同监管方案。该方案通过中继链方式实现多链之间的通信交互,结合代理重加密技术与可搜索

加密技术实现共享监管数据的隐私保护。理论分析结果表明,本文方案能够抵御恶意攻击,保障链上链下的数据安全,方案中的链上重加密操作、批量写入和多种查询方式的性能满足日常需求,但中继链负担较大,未来仍有一定的提升空间。

参考文献

- [1] NAKAMOTS S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2023-12-01]. <https://bitcoin.org/bitcoin.pdf>.
- [2] QIN H W, CHENG Y T, MA X Q, et al. Weighted Byzantine fault tolerance consensus algorithm for enhancing consortium blockchain efficiency and security[J]. Journal of King Saud University, 2022, 34(10): 8370-8379.
- [3] SHARMA P, NAMASUDRA S. EHDHE: enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain [J]. Information Sciences, 2023, 629: 703-718.
- [4] UDDIN M. Blockchain medledger: hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry [J]. International Journal of Pharmaceutics, 2021, 597: 120235.
- [5] GHAYVAT H, PANDYA S, BHATTACHARYA P, et al. CP-BDHCA: blockchain-based confidentiality-privacy preserving big data scheme for healthcare clouds and applications[J]. IEEE Journal of Biomedical and Health Informatics, 2022, 26(5): 1937-1948.
- [6] GRIGGS K N, OSSIPOVA O, KOHLIOS C P, et al. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring[J]. Journal of Medical Systems, 2018, 42(7): 130.
- [7] HUSSIEN H M, YASIN S M, UZDIR N I, et al. Blockchain technology in the healthcare industry: trends and opportunities [J]. Journal of Industrial Information Integration, 2021, 22: 100217.
- [8] 国务院. 国务院关于加强和规范事中事后监管的指导意见 [EB/OL]. [2023-12-01]. https://www.gov.cn/zhengce/content/2019-09/12/content_5429462.htm.
The State Council. Guiding opinions of the state council on strengthening and standardizing mid- and post-event supervision [EB/OL]. [2023-12-01]. https://www.gov.cn/zhengce/content/2019-09/12/content_5429462.htm. (in Chinese)
- [9] ZOU R P, LÜ X X, ZHAO J S. SPChain: blockchain-based medical data sharing and privacy-preserving ehealth system [J]. Information Processing & Management, 2021, 58(4): 102604.
- [10] HE Y J, JIANG R K, NI X Z, et al. Blockchain-based access and timeliness control for administrative punishment market supervision [J]. IEEE Internet of Things Journal, 2023, 10(12): 11054-11067.
- [11] 陈纯. 联盟区块链关键技术与区块链的监管挑战[J]. 科学中国人, 2019(22): 3.
CHEN C. Key technologies of federated blockchain and regulatory challenges of blockchain[J]. Science China Man, 2019(22): 3. (in Chinese)
- [12] SHEN P X, LI S Z, HUANG M, et al. A survey on safety regulation technology of blockchain application and blockchain ecology [C] // Proceedings of the IEEE International Conference on Blockchain. Washington D. C., USA: IEEE Press, 2022: 494-499.
- [13] 孙传恒, 万宇平, 罗娜, 等. 面向追溯主体的果蔬全供应链区块链多链模型研究[J]. 农业机械学报, 2023, 54(4): 416-427.
- [14] SUN C H, WAN Y P, LUO N, et al. Blockchain multi-chain model of fruit and vegetable supply chain for traceability subjects [J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(4): 416-427. (in Chinese)
- [15] 张伟航, 钟永彦, 向元柱, 等. 边云辅助下的可撤销属性加密方案[J]. 计算机工程, 2025, 51(7): 244-253.
ZHANG W H, ZHONG Y Y, XIANG Y Z, et al. Revocable attribute-based encryption scheme assisted by edge and cloud [J]. Computer Engineering, 2025, 51(7): 244-253. (in Chinese)
- [16] MAO X K, LI X H, GUO S W. A blockchain architecture design that takes into account privacy protection and regulation [C] // Proceedings of the 18th International Conference on Web Information Systems and Applications. Berlin, Germany: Springer, 2021: 311-319.
- [17] 张黔会, 袁凌云, 谢天玉, 等. 智能合约驱动的公平可验证秘密共享[J]. 计算机工程, 2025, 51(9): 177-191.
ZHANG Q H, YUAN L Y, XIE T Y, et al. Fair verifiable secret sharing driven by smart contracts [J]. Computer Engineering, 2025, 51(9): 177-191. (in Chinese)
- [18] 李莹, 瞿红红, 王佳, 等. 区块链多链防伪溯源模型设计与系统实现[J]. 湖南大学学报(自然科学版), 2023, 50(8): 172-180.
LI Y, QU H H, WANG J, et al. Blockchain multi-chain anti-counterfeit traceability model design and system implementation [J]. Journal of Hunan University (Natural Sciences), 2023, 50(8): 172-180. (in Chinese)
- [19] 经普杰, 王良民, 董学文, 等. 分层跨链结构: 一种面向区块链系统监管的可行架构[J]. 通信学报, 2023, 44(3): 93-104.
JING P J, WANG L M, DONG X W, et al. CHA: cross-chain based hierarchical architecture for practicable blockchain regulatory [J]. Journal on Communications, 2023, 44(3): 93-104. (in Chinese)
- [20] 巫光福, 余攀, 王柯柯. 双链式区块链交易监管研究[J]. 计算机工程与应用, 2020, 56(23): 116-123.
WU G F, YU P, WANG K K. Transaction regulatory research on double-chain blockchain [J]. Computer Engineering and Applications, 2020, 56(23): 116-123. (in Chinese)
- [21] 赵鲜鲜, 谭海波, 赵赫, 等. 同盟链: 一种基于多链协同的联盟链改进模型[J]. 北京航空航天大学学报, 2024, 50(10): 3283-3296.
ZHAO X X, TAN H B, ZHAO H, et al. Alliance chain: a consortium chain improvement model based on multi-chain collaboration [J]. Journal of Beijing University of Aeronautics and Astronautics, 2024, 50(10): 3283-3296. (in Chinese)
- [22] JIANG J J, ZHANG Y S, ZHU Y W, et al. DCIV: decentralized cross-chain data integrity verification with blockchain [J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(10): 7988-7999.
- [23] 邹文涛, 李传艺, 葛季栋, 等. 基于混合链的协作业务流程的隐私保护和数据监管[J]. 计算机集成制造系统, 2024, 30(8): 2897-2912.
ZOU W T, LI C Y, GE J D, et al. Privacy protection and data accountability of collaborative business processes based on hybrid blockchain [J]. Computer Integrated Manufacturing Systems, 2024, 30(8): 2897-2912. (in Chinese)
- [24] 陆艺仁, 朱友文. 基于中继链的联盟链跨链监管机制[J]. 计算机工程与应用, 2023, 59(22): 268-275.
LU Y R, ZHU Y W. A cross-chain supervision mechanism for consortium blockchain based on relay-chain technology [J]. Computer Engineering and Applications, 2023, 59(22): 268-275. (in Chinese)
- [25] WANG B, LIN Z Y, WANG M, et al. Applying blockchain technology to ensure compliance with sustainability standards

- in the PPE multi-tier supply chain[J]. *International Journal of Production Research*, 2023, 61(14): 4934-4950.
- [25] CUI L Z, XIAO Z, CHEN F, et al. Protecting vaccine safety: an improved, blockchain-based, storage-efficient scheme [J]. *IEEE Transactions on Cybernetics*, 2023, 53(6): 3588-3598.
- [26] SONG G H, LU Y J, FENG H B, et al. An implementation framework of blockchain-based hazardous waste transfer management system[J]. *Environmental Science and Pollution Research*, 2022, 29(24): 36147-36160.
- [27] GAO N, HAN D Z, WENG T H, et al. Modeling and analysis of port supply chain system based on Fabric blockchain[J]. *Computers & Industrial Engineering*, 2022, 172: 108527.
- [28] LI X, WU L, ZHAO R, et al. Two-layer adaptive blockchain-based supervision model for off-site modular housing production[J]. *Computers in Industry*, 2021, 128: 103437.
- [29] BAO Z J, HE D B, WANG H Q, et al. A group signature scheme with selective linkability and traceability for blockchain-based data sharing systems in E-health services [J]. *IEEE Internet of Things Journal*, 2023, 10(23): 21115-21128.
- [30] 宋靖文, 张大伟, 韩旭, 等. 区块链中可监管的身份隐私保护方案[J]. *软件学报*, 2023, 34(7): 3292-3312.
- SONG J W, ZHANG D W, HAN X, et al. Supervised identity privacy protection scheme in blockchain[J]. *Journal of Software*, 2023, 34(7): 3292-3312. (in Chinese)
- [31] ZHENG K N, ZHENG L J, GAUTHIER J, et al. Blockchain technology for enterprise credit information sharing in supply chain finance[J]. *Journal of Innovation & Knowledge*, 2022, 7(4): 100256.
- [32] 周昱, 于宗光. 基于 RS 和 BCH 码的 SRAM-PUF 密钥提取方法及性能分析[J]. *计算机工程*, 2024, 50(7): 187-193.
- ZHOU Y, YU Z G. SRAM-PUF key extraction method and performance analysis based on RS and BCH codes [J]. *Computer Engineering*, 2024, 50(7): 187-193. (in Chinese)
- [33] WANG W, WANG L H, ZHANG P J, et al. A privacy protection scheme for telemedicine diagnosis based on double blockchain [J]. *Journal of Information Security and Applications*, 2021, 61: 102845.
- [34] LIU X L, BARENJI A V, LI Z, et al. Blockchain-based smart tracking and tracing platform for drug supply chain[J]. *Computers & Industrial Engineering*, 2021, 161: 107669.
- [35] SHERLZ P. GORECRYPT [EB/OL]. [2023-12-01]. <https://github.com/SherLzp/goRecrypt>.
- [36] ZOU Y P, PENG T, WANG G J, et al. Blockchain-assisted multi-keyword fuzzy search encryption for secure data sharing [J]. *Journal of Systems Architecture*, 2023, 144: 102984.
- [37] YAO X, ZHAO X G, HE R, et al. A medical device management system using smart contract on blockchain[C]// *Proceedings of the 9th International Conference on Behavioural and Social Computing*. Washington D. C., USA: IEEE Press, 2022: 1-5.
- [38] 陈龙飞, 姚中原, 潘恒, 等. 跨链综述: 机制、协议、应用与挑战[J]. *计算机应用*, 2023, 43(10): 3017-3027.
- CHEN L F, YAO Z Y, PAN H, et al. Cross-chain review: mechanisms, protocols, applications and challenges [J]. *Journal of Computer Applications*, 2023, 43(10): 3017-3027. (in Chinese)

文字编辑 索书志

栏目编辑 宋 圆