医院绩效薪酬核算智能化模型构建研究

文丨 杨之晗

在医疗卫生事业高质量发展的背景下，公立医院绩效薪酬核算面临涵盖范围广、核算主体多、业务逻辑复杂等挑战，传统人工模式已成为财务效率提升的瓶颈。构建智能化核算模型，通过大数据、人工智能、区块链等前沿技术深度融合，实现薪酬管理全流程数智化转型，已成为破解管理困境的关键路径。

典型案例

在某大型综合性医疗机构推进薪酬核算数智化转型项目中，面对每日产生数 TB 级的病历信息、检验报告、影像资料等海量医疗数据，核算主体涵盖院内正式职工、劳务派遣人员、院外专家顾问等多元类型，经费来源渠道涉及纵向课题经费、院内自筹资金、横向合作项目等复杂情况，税务处理规则存在工资薪金按月扣税、劳务报酬按次计算、年终奖一次性扣除等差异化情形。为此引入集成大数据融合引擎、深度学习神经网络、区块链分布式账本、元宇宙虚拟交互等前沿技术的智能发放平台，打通原本相互独立的医院信息系统、财务核算模块、人力资源管理、预算成本控制等业务单元，可以构建起包含数据自动采集清洗、智能核算分配、税务合规校验、移动端实时查询、多维度决策分析的完整技术架构，为深入剖析智能化模型关键技术体系奠定坚实的实践基础。

医院绩效薪酬核算智能化模型关键技术应用

海量数据融合的全景式薪酬核算架构

基于前述医疗机构数智化转型实践，全景式薪酬核算架构通过构建数据采集层、转换处理层、多维建模层这三级技术体系，打通原本分散在各个业务系统里的薪酬相关信息，形成统一的数据视图来支撑核算需求。数据采集层运用标准化接口技术从医院信息系统抓取门诊挂号、住院病案、手术登记等诊疗数据；从财务系统获取科室收支流水、成本核算报表等经营数据；从人力资源平台提取员工岗位系数、考勤打卡记录、职称等级等人事数据，所采集的数据覆盖院内正式职工、劳务派遣人员、院外专家顾问等全部核算主体。转换处理层采用消息队列技术来承载每秒万级的数据流量，利用分布式计算框架完成数据清洗、格式转换、缺失值填补等预处理操作，将来自不同系统的异构数据统一为标准数据格式。多维建模层基于主题数据仓库设计理念构建薪酬核算模型，核算公式为：

$$S = \sum (Wi \times Ci \times Ti \times Ai)$$

式中，S 表示科室薪酬总额（单位：元），Wi 代表第 i 类工作量积分（无量纲），Ci 为单位价值系数（单位：元 / 分），Ti 表示时间权重因子（无量纲），Ai 指质量考核系数（无量纲）。该架构将分散在各个业务模块的薪酬要素数据汇聚成统一视图，为后续智能计税处理与决策分析创造必要的数据条件。

深度学习驱动的智能计税与风险预警

在数据融合架构提供的统一数据基础上，智能计税模块采用深度神经网络算法去处理工资薪金与劳务报酬的差异化税务规则，替代传统人工逐笔判别计税的方式。卷积神经网络负责识别薪酬发放凭证里的身份证号、银行账户、经费来源、发放金额等结构化关键字段。长短期记忆网络依据员工历史发放序列数据预测个人年度累计收入的变化轨迹，在累计收入接近或者超过 6 万元法定临界值时，自动切换工资薪金按月正常扣税模式或年度一次性减免模式。针对院外人员劳务报酬计税场景，系统借助决策树算法来自动判别按次扣税及按月累计扣税这两种处理路径，要是单次劳务金额低于 800 元就会触发免税逻辑分支，而一旦超过 4000 元则会启动分段累进税率的计算流程，以此保证税务处理能够符合国家财税政策的要求。

风险预警机制通过孤立森林异常检测算法持续监测各科室薪酬发放模式，当某科室单月薪酬支出金额偏离历史统计均值两倍标准差以上时，系统就会自动向财务管理部门推送预警提示信息，辅助人工深入核查虚报工作量、重复发放薪酬等潜在违规操作行为。智能计税处理完成后，需要引入可信机制保障核算数据的真实性与不可篡改性，为此区块链

存证技术成为其中的关键环节。

区块链存证的分布式账本与透明化管理

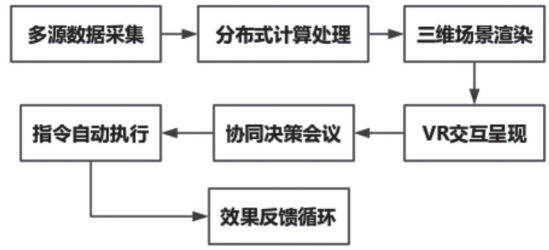
为确保智能计税结果的真实可信与历史数据不被事后篡改，分布式账本技术采用联盟链架构部署方案，医院财务部门、人力资源科、审计监察处及各临床科室作为区块链网络节点，共同参与薪酬数据的共识验证过程。每笔薪酬发放记录经SHA-256哈希算法生成唯一数字指纹标识，连同发放金额、经费来源、收款账户等交易信息一起打包进入区块链分布式账本，一旦上链完成后，任何单一节点都无法单方面修改或删除历史交易记录。智能合约模块会预先设定好薪酬发放的触发条件与执行规则，当科室绩效考核数据上链并且通过多方数字签名验证后，自动触发薪酬计算流程，同时执行银行转账指令，全程记录操作时间戳、经办人员身份标识、审批流程节点等元数据信息，从而形成完整的操作审计日志链条。

透明化管理通过权限分级访问机制设计，允许员工凭借个人私钥登录移动端应用，查询薪酬发放明细、个税扣除凭证、社保公积金缴纳记录这类个人信息；科室负责人能够追溯查看本部门绩效分配全过程相关数据；审计部门可获得全院薪酬数据只读权限，以开展合规性检查工作。区块链不可篡改的特性为薪酬分配争议仲裁提供可信的电子证据链支撑，在保障数据安全与透明的基础上，还需直观可视化决策工具辅助管理层，全面把握薪酬核算全局态势。

元宇宙沉浸式场景的交互决策平台

基于区块链技术保障的可信数据底座，元宇宙决策平台借助Unity3D游戏引擎构建三维虚拟医院场景空间。医院管理层戴上VR虚拟现实头显设备进入数字孪生环境，以第一视角在各科室虚拟区域自由漫游，并实时查看薪酬运营仪表盘动态数据。如图1所示，平台技术流程从多源数据实时采集模块启动，汇集来自HIS系统、财务系统、人力资源系统等海量业务数据，经过分布式计算集群完成数据融合清洗处理后，把科室收入构成结构、成本支出分布情况、人员绩效排名等多维度核心指标，映射渲染到虚拟三维空间的悬浮显示窗口。交互操作模块支持手势识别与语音控制双重交互方式，管理者通过空中点选操作某科室三维建筑模型，能够触发弹出该科室近3个月薪酬变化趋势折线图、与区域标杆医院对比分析雷达图、异常波动智能预警列表等多种可视化图表组件，直观地呈现科室薪酬运营状况。

协同决策功能允许多位管理者同时登录进入虚拟会议室场景，围绕全息投影展示的薪酬分配优化方案开展远程讨论交流。系统借助自然语言处理技术自动把会议讨论纪要转化成可执行的决策指令下发到业务系统执行层，形成包含数据采集、智能分析、沉浸呈现、协同决策、指令执行、效果反馈的完整管理闭环流程。



来源：南方医科大学南方医院

‖ 图1 元宇宙沉浸式决策平台技术流程

智能化模型应用评估

多指标协同的量化评估体系构建

在前述关键技术应用的基础上，量化评估体系要对智能化模型的实际运行效果进行科学测度。某大型综合性医疗机构构建起涵盖核算效率、数据准确性、系统稳定性、用户满意度这4个维度的评估框架，并且采用层次分析法来确定各指标的权重系数，最终形成多维度协同的量化评估矩阵。

如表1所示，评估体系通过设定明确的量化标准，将智能化模型抽象的效能转化成可测量的具体指标，为后续开展实证数据验证工作奠定评估基准，以此确保评估过程具备客观性与可比性。

‖ 表1 智能化薪酬核算模型评估指标体系

评估维度	评估指标	权重
核算效率	月度处理周期	0.30
核算效率	单笔核算耗时	0.20
数据准确性	计税错误率	0.25
数据准确性	数据一致性	0.15
系统稳定性	平台可用率	0.05
用户满意度	综合认可度	0.05

来源：南方医科大学南方医院

实证数据支撑的综合效能验证

基于构建的量化评估体系，该医疗机构针对智能化模型实施前后的核算运营数据展开对比分析，数据采集的周期涵盖系统上线前后各6个月时间，通过对关键参数进行持续监测来获取真实运营数据。

如表2所示，智能化模型应用后月度处理周期由8天缩短至3天，单笔核算耗时从120秒降到了30秒，计税错误比率由2.5%下降到了0.3%，数据一致性从85%提升到了99.5%，平台可用率达到了99.8%，综合认可度评分从6.8分提高到了9.2分。实证数据进行验证后表明，智能化模型借助海量数据融合、深度学习计税、区块链存证、元宇宙决策等关键技术集成应用，在多个维度都展现出了显著的综合效能。

‖ 表2 智能化模型实施前后效能对比

评估指标	传统模式	智能化模式
月度处理周期	8 天	3 天
单笔核算耗时	120 秒	30 秒
计税错误比率	2.5%	0.3%
数据一致性	85%	99.5%
平台可用率	–	99.8%
综合认可度	6.8 分	9.2 分

来源：南方医科大学南方医院

结束语

智能化薪酬核算模型通过海量数据融合、深度学习算法、区块链存证、元宇宙可视化等前沿技术集成应用，系统性破解了传统核算模式中数据割裂、计税烦琐、安全隐患、决策滞后等核心问题，实现了从人工操作向智能管理的根本性转变。随着数字中国战略深入推进与医药卫生体制改革持续深化，医院数智化转型已成为提升运营效能的战略选择，薪酬核算智能化将向跨系统深度协同、动态精准优化、全程安全可信方向持续演进。未来需加强复合型人才培养，完善制度体系建设，深化技术与管理深度融合，推动智能化模型在医院运营管理中发挥最大效能，为医疗卫生事业现代化提供坚实支撑。

作者简介：杨之晗 南方医科大学南方医院

责任编辑：杨佳宇 投稿邮箱：zhouhl@staff.ccidnet.com

（上接第94页）

数据销毁阶段，需保障数据彻底清除。并且，传统手段无法实现“数据可用不可见”的保护目标，因此迫切需要构建基于密码技术的全生命周期数据可信机制，以解决数据“变化”过程中的机密性与完整性问题。

在“行为”维度，多主体行为的责任界定存在困难。数据加工、使用及交易作为数据流通的核心环节，当前面临三项挑战：其一，行为主体由“单方”转变为“多方”，涵盖数据提供方、加工方、使用方及监管方等，责任边界较为模糊；其二，数据加工行为缺乏有效的抗否认机制，出现问题后难以追溯责任主体；其三，数据同源性溯源存在困难，无法精准追踪数据来源及流转路径。上述问题导致行为可信度不足，亟须构建具备可审计性与可追责性的行为可信体系。

密码技术协同构建新一代数字信任体系的核心路径

身份可信夯实数字信任基础。从身份可信实现路径看，新一代公钥基础设施（PKI）信任体系迭代优化是关键支撑。依据数字经济场景下“虚体”身份认证需求，以公钥密码算法为核心生成数字证书，用数字签名技术加密验证“虚体”软硬件实例的完整性与来源真实性，赋予“虚体”可信身份标识，弥补传统身份认证体系缺陷。针对物联网场景特征，构建场景化身份与密钥管理机制，将密码技术嵌入相关环节，适配其技术特性，实现“实体+虚体”的统一身份管控，解决传统PKI体系适配局限。此外，多中心分布式身份技术为拓展身份可信边界提供了重要路径。借助密码技术搭建身份信息去中心化管理架构，用户可自主控制身份数据，规避传统模式风险，构建跨场景、跨平台身份互认机制，打破认证壁垒，解决“虚体”跨场景认证难题，为信任协同提供支撑，保障数字信任体系有效运行。

在“身份可信”的基础上，数据可信是贯通数字信任链路的关键。为确保数据在流转、加工、使用、交易等动态环节中的隐私与安全，必须构建覆盖全生命周期的可信机制。传统以密码为基础的保护手段多聚焦于“静态数据”，难以应对数据在使用与加工过程中的机密性、完整性保障需求，也无法实现“数据可用不可见”的安全目标。为此，需引入以密码技术为核心的全周期数据保护体系。借助机密计算、同态加密、多方安全计算等隐私增强技术，在数据处于“变化”状态时，仍能确保可控可溯，从而在数据加工防泄露、交易保可信、销毁可验证等环节建立持续信任，真正支撑起“原始数据不出域、数据可用不可见”的现代数据流通范式。

行为可信构建数字信任闭环。行为可信的实现需要技术机制予以支撑，其首要方式是构建可信交互与证据管控机制。多种可信交互协议保证数据交易行为的可信追溯，数字签名实现行为的不可否认，密码杂凑函数可固定证据内容，区块链保障存证时序与防篡改，多者协同，共同将虚拟的数据处理行为转化为具有法律效力的可信电子证据。密码技术的协同作用，将虚拟数据处理行为固化为具备法律效力的证据链，精准界定主体责任，进而构建起完整的数字信任闭环。

本文选自：2023年度校（院）新进博士专项基金项目《人口老龄化对共同富裕的影响及对策研究》，项目号：2023BSJJ008。

作者简介：王红叶 贵州茅台酒厂（集团）循环经济产业投资开发有限公司
邵 淼（通讯作者）北京数字认证股份有限公司
黄莉群 中共中央党校（国家行政学院）国家治理教研部
梁钰林 中共中央党校（国家行政学院）国家治理教研部

责任编辑：徐培炎 投稿邮箱：zhouhl@staff.ccidnet.com