



(2025 年第 4 期，总第 201 期)

中国证券投资基金业协会

2025 年 7 月 7 日

基金行业人工智能大模型应用及建设探索

【编者按】基金行业数据量大、应用场景多、监管及日常操作繁杂，拥有人工智能（AI）驱动的天然属性和需求。当前基金行业 AI 技术建设尚处于初级阶段，需要加强对基金行业 AI 大模型技术的应用场景、潜在风险、技术治理等关键问题的深入研究。本文基于基金行业 AI 大模型的应用实践，系统总结基金机构建设 AI 大模型的全业务流程场景、主要功能模块及技术实现方式，对大模型全生命周期的系统性管理提出相关解决方案及系统建设要点，从无到有、从少到全，助力基金机构逐步实现 AI 大模型落地应用，推动行业投研智能化转型、营销服务创新、风控体系升级、运营效率提升，实现人工智能从“效率工具”到“战略能力”的转变。

一、前言

在科技创新驱动提高社会生产力的背景下，金融科技快速发展，场景化、智能化和个性化金融服务不断催生人工智能新技术应用落地。基金行业不断加大科技资源投入，积极拥抱人工智能带来的行业新变革。

在国外，贝莱德核心系统阿拉丁与 eFront 风险管理系统构建一个“共同驾驶员”，客户可以使用贝莱德的大模型语言技术从阿拉丁中提取信息。富达资产管理公司从海量数据分析和投资决策支持入手，利用人工智能进行市场预测、提高投资效率和风险管理水平。桥水基金使用 AI 工具进行基本面分析、资产配置和风险管理。

在国内，多家资管机构设立专门 AI 工作组，平台先行，研究业务融合大模型方案；同时本地化部署 DeepSeek，用以辅助投资研究、知识问答、客户服务等。某大型基金公司利用模型分析用户行为数据、了解用户投资偏好，实现精准营销。有基金公司自主搭建直销柜面智能录单系统，借助大模型，在业务服务方面实现创新升级、提升柜面效率。一些机构将人工智能运用于系统运维中，实现故障根因分析、异常自动处置等。

从基金行业看，无论规模大小，都在积极拥抱 AI，尝试将新技术新算法融入业务领域。总体情况上，基金行业的 AI 布局还处于初级阶段，前景广阔但同时存在各类潜藏风险和困难点，需要技术适配性、业务融合度与生态开放性等多方面的协同发展。

二、基金行业 AI 应用场景及潜在风险

基金行业数据海量、专业程度高、市场环境复杂、监管力度强，AI 大模型异军突起，其卓越性契合行业复杂需求，行业大模型应用场景丰富，但也隐藏特定的技术风险。

（一）基金行业 AI 应用场景

1. 智能投研

投研领域核心诉求是通过数据发现市场规律、挖掘投资机会，利用 AI 实现数据驱动的高效决策。大模型通过分析海量市场数据（如研报、信披、舆论等市场数据），精准解读金融资讯、提取有价值信息、预测市场走势，辅助投资决策。

在投资交易过程中，利用算法评估投资组合，根据实时监测的市场变化，优化算法交易、提示交易风险；后续 AI 自动生成投资报告、评价考核标准、复盘交易过程等。

2. 智能销售

大模型通过分析用户的风险偏好、财务状况、投资目标、行为数据等信息，同时分析市场信息，提供个性化的基金投资建议、资产配置方案，实现精准营销。另一方面，在投教营销物料的内容及样式生成过程中，使用 AI 软件能够大幅提升效率。

此外，销售领域可以开发智能柜台、智能客服、智能投顾等客户服务系统，实现极大程度整合现有渠道客户资源的提质增效。

3. 智能合规风控

当前大模型对语言理解能力卓越，对金融分词、内容相关性等能够实现秒级搜索，通过训练已能较精确解读政策法

规、制度规范等。在建立相关文档库基础上，可对输入的具体案例、交易数据进行智能评判及合规建议。

风险控制上，通过分析预测，能对市场风险、信用风险、流动性风险、操作风险等各方面进行实时甚至事前识别；事后，也能对交易行为等进行检查、评估、自动生成相关报告。

4. 智能运营/运维

AI 技术支持整个运营过程的提质增效。TA 及 FA 岗位通过人工智能实现清算及数据校验的自动化，资金清算上能够对异常数据稽核修复。此外，支持各维度数据报表精确推送业务人员并能用自然语言查询相关数据。

运维方面，人工智能运维（AIOps）概念持续火热，故障自愈、智能告警、日志识别、趋势预测等技术日趋成熟，技术人员使用 AI 工具能有效避免操作风险、运行风险。

（二）潜在技术风险及应对

人工智能技术在基金行业的使用场景逐步广泛，新形式的风险随之增加。除了社会治理、伦理道德类的风险需要完善立法及引导外，主要还存在以下四类技术风险：

一是管理类风险。管理制度提供规范化解决方案，确保基金运作在系统辅助下顺畅衔接；旧版本制度流程无法完全套用 AI 驱动下的人员协作、无法适应 AI 带来组织人员新架构。此外，碎片式运用场景落地，也将提升管理复杂度。没有与时俱进的流程制度更新，人工智能运用会产生推进困难、协同不畅、职责不清等情况，进而增加实施成本。

二是安全类风险，涵盖数据安全及生产运行安全。人工智能技术高度依赖大量数据（包括市场数据、客户信息、交

易记录等），使用过程极易产生过度采集、存储不当、生成内容违规，数据安全关系运营稳定性、合规性以及投资者信任。生产运行安全则涉及业务连续性，大模型大数据在训练及运行过程中需要持续迭代、调整参数，整个过程对资源需求大，系统的稳定运行及可用性将受到挑战。

三是架构类风险。复杂 AI 系统模块多、数据处理链路长（数据采集—数据清洗—模型推理—结果反馈），导致响应缓慢影响使用预期。此外，架构上也会产生与现有系统融合难度大、数据质量不高、与模型适配繁琐等问题，以此需要业务系统进行架构调整。

四是数据类风险。人工智能的算法歧视和不透明性，加上训练及使用过程中极易引入失效数据，最终会使推导结果产生不公平对待用户及人工幻觉现象。该类现象一旦产生，很难进行算法解释和责任鉴定，并且也不可能对异常情况事件进行全方位数据复盘。

针对基金行业 AI 技术风险，有必要进一步强化管理，比如：制定基金行业人工智能发展指引；对各家人工智能进行问卷调查及算法分级备案；现场检查及第三方准入机制等。同时，基金公司应加强算法内控，通过管理及技术手段识别和防范相关风险，例如使用检索增强生成（RAG）减少模型幻觉、部署哨兵系统检测异常输出、人工反馈强化学习（RLHF）增强任务适应性等。

三、行业机构 AI 技术实施路线

（一）制度先行，打造人工智能共同体

人工智能技术引进应建立健全制度流程，以“目标、责任、安全”为宗旨，以此形成自上而下的推动方式。第一，确定人工智能目标。将各阶段需要达成的效果当作考核依据，明确技术开展的优先方向，制定架构平台的长期规划。第二，加强全局统筹领导。人工智能技术已从效率提升转向业务流程重塑，主动转型过程需考虑业务协同。第三，确定各专业条线在具体实施工作中的职能，防止跨专业间出现推诿不作为表现。第四，保障安全、长期规划，在确保数据及运行安全的前提下打造全员共同参与新模式。

（二）系统基建，完善大模型运行体系

AI 作为上层建筑，需建立在有效的大模型运行体系上。行业内已提出大模型运维（LLMOps）概念，专注于管理大语言模型的整个生命周期。有效的大模型运行体系，需要一系列拥有基础功能的系统支持。

一是作为数据来源的数据中心。有效的大模型的基石是其训练数据的质量和多样性，数据收集和预处理、数据标记和注释、数据存储和组织、数据有效性及合规性贯穿于整个大模型的使用过程，健全数据管理机制是减少大模型产生幻觉和歧视的有效方式。

二是高效的模型管理工具。从头开始训练基础模型复杂、耗时且昂贵，资管机构可选用开源或专有模型（例如 DeepSeek）作为已经完成预训练的基础模型，再进行 Prompt、微调、蒸馏以适配下游任务。一个高效模型管理工具能够对基础模型的全生命周期、Prompt 版本、训练数据、参数微调、

测试用例进行全方位管理，并支持大模型的持续集成和交付。

三是持续跟踪线上运行的哨兵系统及监控平台。大模型部署上线后，需不断跟进用户反馈及资源利用率。运行过程中产生的监控数据是后续模型调优的关键依据，通过对监控数据分析可以精确找出性能瓶颈进行针对性优化。

（三）由点带面，迭代人工智能新场景

根据现有模型支持情况，通过局部试点，逐步扩展应用范围并实现人工智能技术升级。可以优先支持预期回报较高、较快的应用场景，循序渐进推广 AI 应用。例如，本地化部署大模型支持单元知识库查询、文件解读，后续接入到智能客服领域等。

（四）安全高效，打造人工智能业务新领域

人工智能正在重塑资管行业，从量化交易到智能投顾，从风险预警到精准营销，AI 技术显著提升基金业务的效率、精准度和安全性。随着技术进步，IT 人员需要逐步从基于数据集的应用开发转向基于模型的人工智能应用，并能够组合多个模型协同工作，构建“安全高效”的 AI 基金业务体系。

四、行业 AI 大模型建设实践

（一）智能研报法规解读大模型

根据实施路线，打造大模型场景应用，综合成本收益，应当优先选择高价值、低风险的场景，例如选择搭建文本解读类的研报法规文件大模型场景。



图 1 智能研报法规文件解读模型架构

文本解读类的大模型架构建设可拆分成四个主要步骤：

1. 基础数据采集

集中研报数据、行业趋势、财务数据，法律法规、合规文件，以及各类知识文档。基础数据采集注重自动化、标准化，将采集数据以一定格式存放，数据的时效性和完整性直接影响模型训练和使用效果。

2. 数据处理

采用大数据技术，对基础数据进行数据清洗、数据标注、结构化、指标设计、特征工程等，转化成模型易读的方式存储。对于文件类原始数据，需要向量化存储，同时标注文件时效性。数据处理后需对数据集划分，使用合适方法划分为训练集、测试集、验证集供大模型调用。

3. 模型处理

对于应用场景不同，需要选择相适应的大模型进行训练。例如 DeepSeek-R1 的推理能力适用于研报解析，LawGPT 擅长法规类文件解读。大模型下载完成，使用处理的数据进行训练。源模型经过大量训练，可以有效避免数据偏移、缩小领域差异。训练过程耗时较长，可使用工具软件对全过程进行监控。后续对模型进一步优化，针对文件解读知识问答类大模型功能，特别地使用知识蒸馏、Prompt 工程将极大地提升使用效果。最后，将模型导出部署，使用 API 或 gRPC 方式对外提供服务。

4. 应用场景

智能研报法规及知识库系统的登录前端包装为统一入口，根据用户权限控制提供对应服务。使用者首先输入问答信息，系统通过自然语言处理对其意图识别，后续调用大模型进行知识库检索、研报解析、法规解读等。

（二）基金全业务流程大模型架构

人工智能技术正在深刻改变基金行业运作模式和发展轨迹，且已从单一场景向全流程覆盖扩展、从技术工具向战略能力转变。在此基础上，需要对实现目标提前规划，确定发展重点，掌握各阶段资源需求。

图 2 是大模型在资产管理业务中的技术架构与应用：



图 2 基金全流程业务大模型技术架构

1. 基础设施

良好的硬件保障是算力运行和预防模型偏移的重要支撑。主要的基础设施包含计算资源（CPU、GPU、内存等）、存储资源（高速存储、磁盘阵列）、网络资源（低延迟网络、防火墙等）。

开源模型下载后进行再训练，所需的具体硬件要求取决于模型规模、训练方式、数据量。训练和运行过程中，对硬件使用情况实时监控，并使用资源管理工具进行资源的及时调配。

2. 数据工程

资产管理机构普遍建设数据中心项目，可将其用作大模型数据源，对数据再进行清洗、标注、增强后适配加载给相

关模型，成为相对应的训练集、验证集、测试集。对于 PDF 类文件型数据，搭建文档中心，再采用结构化、向量化方式存储和加载。数据工程同时承担数据展示、数据权限、数据血缘、数据安全职能，在前期建设数据中心时提前统筹规划。

3. 模型工程

技术架构核心部分，包括模型开发、测试、运维整个大模型生命周期的管理。

模型开发遵循“模型下载—模型设计—模型训练—模型评估”过程，同时需要模型库及代码仓库将完整的训练数据存储下来以便追溯、审查。经过专门训练（微调、领域适配）的模型相比原始下载大模型而言，专业问答的准确性提升 20% 以上，部分极端情况下甚至更高。

模型测试主要对训练后的模型进行功能、性能、安全、伦理四方面测试，测试前根据用途制定相关指标及案例。选择自动化测试工具模拟调用，运用压测工具进行性能排查，以及使用大模型专业评测工具（例如 OpenCompass）对模型进行测试。专业评测工具拥有全面的指标分析能力，可以对大模型的基础语言能力、推理计算能力、安全与伦理、具体行业、性能与效率等进行有效评估。

模型运维旨在对生产环境中模型的部署、运行、监控、维护及迭代进行系统化管理，确保模型持续稳定、高效地服务于业务需求。监控工具可使用开源 Prometheus、Zabbix，根据资源使用趋势进行弹性扩缩容。整个运维过程需要遵守 ITIL 管理规范，并逐步引入 SRE 及自动化运维理念。

4. AI 应用平台

基础设施、数据工程、模型工程组成了 AI 大脑，此基础上，可以设计各大模型应用平台。平台框架可以是常见的 WEB 容器，通过前端交互，后台使用 gRPC 或 HTTP 方式调用大模型。

应用平台的持续落地，将有效支撑投研智能化转型、营销服务创新、风控体系升级、运营效率提升，实现 AI 从“效率工具”到“战略能力”的转变。

（三）大模型运营平台工程

大模型使用初级阶段，可以引入 Dify、LongChain 等开源工具进行模型的开发管理，此类工具类似于百度千帆系列。当 AI 应用建设到一定规模后，由于模型版本多、语料数据广、使用场景增长快，需要搭建能够系统化管理所有模型整个生命周期的平台。

1. 大模型运营平台系统概述

大模型运营平台是全业务流程应用落地的关键基础，是管理大模型整个生命周期的工具链，通过充分利用第三方工具应用，使平台具备从数据处理、模型开发到模型部署的一站式能力，还可以通过全栈优化加速企业 AI 应用落地，同时契合审计要求。

2. 大模型运营平台系统功能

大模型运营平台系统功能主要满足以下五方面需求：一是大模型开发与版本管理，提供预训练大模型库，支持自定义微调再训练。二是大模型的测试与评估，包括测试用例维护和自动化测试方式。三是大模型的运行维护，可充分利用第三方应用进行迭代上线及监控。四是数据语料的预处理及

分级，同时能够对数据进行安全保护。五是大模型数据的安全与审计，使用环境隔离、权限配置确保安全性，将操作日志、再训练参数等进行版本管理和留痕。

3. 大模型运营平台系统建设

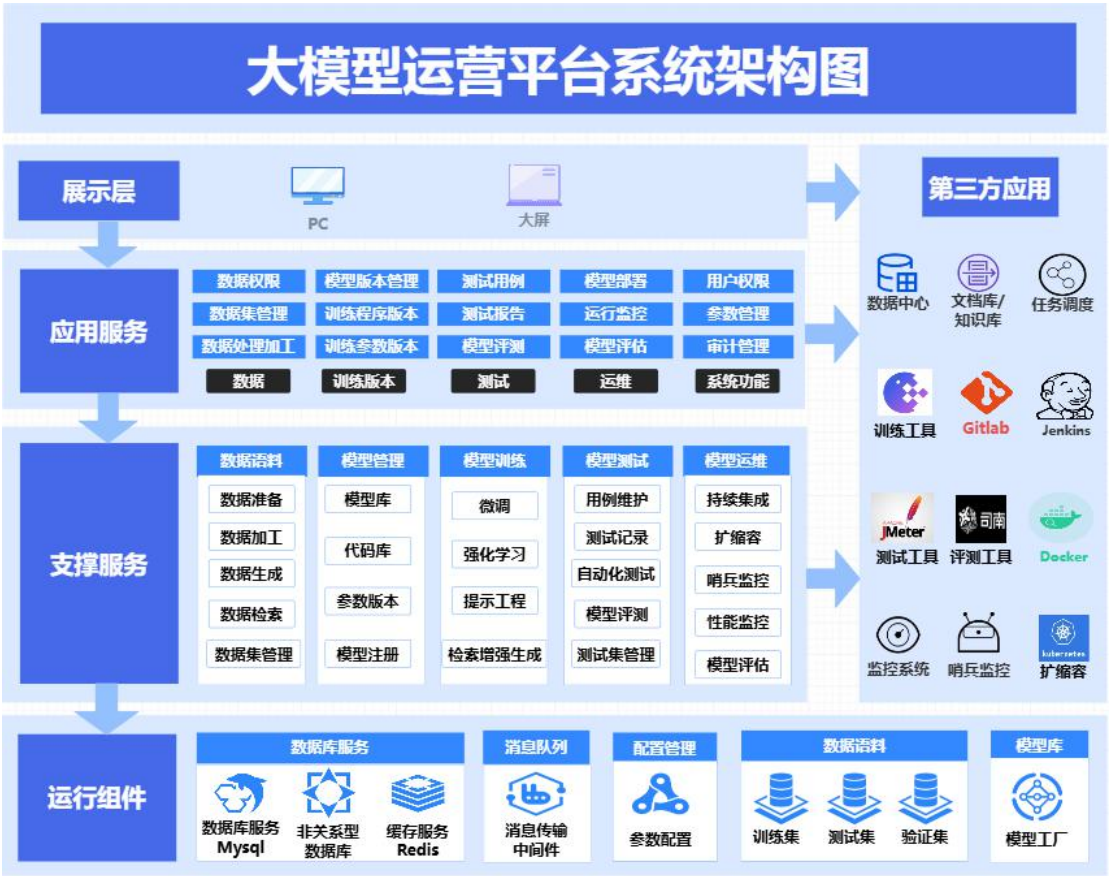


图 3 大模型运营平台系统架构

（1）运行组件

用于平台运行的数据持久化、服务解耦和运行参数配置。关系型数据库和非关系型数据库分别存储系统信息及操作流水信息，同时建设相关训练数据集存储单元和模型工厂。

（2）支撑服务

大模型训练及运行的核心部分，主要分为五大组件集：一是使用大数据技术的数据语料管理，对训练数据进行准

备、加工、生成等。二是模型管理，可以便捷加载模型工厂中的注册模型，并对相关代码及参数进行版本管理。三是模型训练，整合 python 的 AI 训练库及外部三方应用。四是模型测试，能够维护测试用例、操作测试流程、生成测试报告。五是模型运维，拥有上线后监控、扩缩容、持续迭代、使用评估报告的功能。

（3）应用服务

将支撑服务的各项组件进行整合，以功能菜单模式进行展现，使用人员可以根据不同阶段不同操作进行大模型的管理。同时，平台应该具有权限分配、用户审计等系统管理功能。

（4）第三方应用

为减少重复建设的成本，可使用开源或采购相关平台工具，用作模型管理过程中一部分的服务需求。例如 Git 负责代码托管，JMeter 用作性能和自动化测试，Jenkins+Docker+K8S 完成持续迭代及扩缩容功能。

【本文由联博基金管理有限公司信息技术部陈慧卿供稿，中国证券投资基金业协会编辑审校】