No. 2606

研 究 报 告

IMI

人工智能赋能金融——效率提升与风险治理

吴轲

人工智能赋能金融——效率提升与风险治理[1]

一、为什么金融尤其需要人工智能？

当前，我们正处于人工智能技术飞速发展的历史节点。2022 年 11 月 ChatGPT 问世，标志着通用人工智能迈出历史性一步，开启了大模型在金融非结构化信息分析上的新可能；2025 年初 DeepSeek-R1 发布，将高质量推理成本降至学术可承受范围，体现出中国 AI 研发的韧性与创造力。与此同时，通义千问开源系列大模型持续迭代，多模态处理与文本嵌入能力不断提升，为中文金融文本分析提供了有力的基础工具。从国家战略层面看，中央金融工作会议明确提出建设金融强国、做好科技金融与数字金融等“五篇大文章的目标”；2025 年 8 月国务院印发“人工智能+”行动意见，推动智能体在金融、商务、法律等领域的广泛应用；央行《金融科技发展规划》亦将 AI 列为核心技术，推动风险管理从“人防”到“智控”的转变。

在产业实践层面，AI 已从概念验证进入规模化落地阶段。中国银行计划未来五年为 AI 全产业链提供不低于 1 万亿元专项金融支持；工商银行完成 DeepSeek 本地化部署，赋能 200 余个业务场景；北京银行启动“All in AI”战略，落地 90 余个金融应用；腾讯云联合沪深交易所、中国银行等将 AI 大模型落地超 100 个金融场景，智能资讯分析效率提升 30 倍，信贷尽调周期由 10 天缩短至 1 天。Swift 联合 13 家国际银行进行 AI 模型试验，欺诈识别准确率提升 100%，交易审查处理由数天缩短至几分钟。截至 2025 年底，中国金融科技专利申请量达 46419 件，居全球第一。

与此同时，AI 正经历从“Chat”到“Agent”的范式转变。2026 年初爆发式流行的开源 AI 智能体框架 OpenClaw，发布数日即获得 GitHub 10 万+星标，截至 2026 年 3 月突破 25 万，并在我国迅速完成 DeepSeek 和微信的本土化适配。AI Agent 不再是对话助手，而是能自主执行任务、调用工具、操作计算机的“数字员工”，在金融领域可自动化执行交易策略、管理投资组合、生成合规报告。然而，热潮背后的安全风险不容忽视：2026 年 2 月 Hudson Rock 检测到 OpenClaw 配置被恶意软件攻陷，API 密钥与对话历史泄露；Cisco 发现第三方技能存在数据窃取和提示注入攻击；同年 3 月 Claude Code 因 npm 包误带 source map 暴露大量源码，随后引发伪造仓库和恶意软件传播。2026 年 3 月，我国已限制国有企业和政府

[1] 作者：吴轲（中国人民大学财政金融学院应用金融系主任、教授）

机关在办公电脑上运行 OpenClaw 应用，以防范潜在安全风险。

金融行业天然适合 AI，其核心在于信息处理。5000 余家 A 股上市公司的年报、公告、研报、专利总量以亿字计，传统分析师团队只能覆盖有限比例。大语言模型使得系统性“阅读”全市场文本、提取经济信息并转化为可量化金融变量的新范式第一次成为现实。但 AI 本身存在前瞻性偏差、幻觉和过拟合等风险，若不加以审慎处理，也可能误导决策。因此，近期研究同时关注 AI 如何提升效率、辅助风险识别，以及 AI 应用本身需要警惕的风险。

二、人工智能如何重塑行业边界：基于大语言模型的 A 股上市公司行业分类

在学术界，基于大模型的金融研究进展迅速。在语义分析与市场预测方面，Lopez-Lira 和 Tang（2023）率先证明 ChatGPT 新闻情感信号能预测股票收益；Siano（2025，Management Science）表明 LLM 能从财报电话会议中捕捉传统方法难以识别的细微语义信号；Jha 等人（2024a，2024b）展示了 ChatGPT 从电话会议中提取资本支出和宏观展望信息的能力。在风险管理领域，Pele 等人（2026）提出了 LLM-VaR 和 LLM-ES 方法，以零样本方式估计在险价值和期望损失。在企业网络构建方面，Breitung 和 Müller（2025）利用 10-K 年报构建了上市公司全球商业网络。

行业分类是金融实证研究的重要基础设施（McGahan 和 Porter, 1997），但 A 股现有的多套行业分类标准存在三大不足：一是更新滞后，对并购重组或业务转型通常存在 1-2 年的滞后期；二是细分赛道区分不足，组内公司同质性低；三是方法不透明、难复现。中国上市公司协会分类严格参照国标，首要目标是统计和行政监管而非金融研究；申万、万得分类虽更贴近市场，但编制方法不公开。Hoberg 和 Phillips（2016，JPE）利用美国 10-K 年报产品描述文本构建了动态 TNIC 行业分类，但这类数据驱动方法在中国市场一直处于空白状态。

本团队的核心思路是：两家公司在年报中描述的业务内容高度相似，则归为同一行业。这一分类体系追求三大目标——客观性（分类方法公开透明，可复现，可根据具体研究需要调整）、准确性（聚类准确，能够捕捉相似企业，组间差异大，组内差异小）和实时性（及时反映企业业务转型）。研究收集了 2007 至 2023 年间沪深两市全部 A 股上市公司的 52702 份年报“管理层讨论与分析”（MD&A）文本，采用“嵌入—聚类—命名—测试”四步骤方法构建分类体系。

第一步：嵌入。使用 Qwen-text-embedding-v4 文本嵌入模型将每份 MD&A 映射为 2048 维语义向量。考虑到模型输入长度限制，首先将每篇 MD&A 文本划分为若干段落，分别计算

各段落的嵌入向量，再以段落嵌入向量的均值作为该篇文本的整体向量表示。为增强嵌入对行业语义的捕捉能力，研究在调用模型时加入任务指令（Prompt）以提升模型信息提取能力。最终对每个 MD&A 文本生成一个 2048 维语义嵌入向量，用于描述该公司的业务模式。

第二步：聚类。基于 52702 个嵌入向量，研究采用层次聚合聚类（Agglomerative Hierarchical Clustering）方法，配合平均链接（Average Linkage）准则和归一化欧氏距离，自底向上构建三级分类体系。这一方法完全由数据自下而上驱动，避免了预设行业定义可能带来的先验偏差。在归一化前提下，欧式距离和余弦距离存在单调映射关系，归一化欧氏距离的平方根特性在聚合过程中能有效压缩极端样本对的惩罚权重，使聚类算法对 MD&A 文本中的局部噪声更加鲁棒。具体而言，三级分类的构建过程如下：三级分类层面，先将全部向量聚合为 300 类，再通过动态小簇合并机制将簇内少于 5 个点的微小簇并入最近的大簇，得到 271 个三级行业；二级分类层面，基于三级聚类结果构建簇间距离矩阵，继续聚合至 150 类后将少于 30 个点的小簇合并，得到 102 个二级行业；一级分类层面，在二级结果上继续聚合至 50 类后将少于 300 个点的小簇合并，得到 26 个一级行业。动态小簇合并机制的创新性引入，既解决了传统层次聚合聚类容易产生大量极小孤立簇的缺陷，同时也保证了分类体系的完全嵌套关系——若任意两家上市公司归属于同一三级行业，则它们必然也归属于同一个二级行业和一级行业。

第三步：命名。研究创新性地采用基于大语言模型的两阶段命名策略——“局部摘要-全局命名”，避免人工命名带来的偏好偏差。首先使用具备长上下文处理能力的 Qwen-Long 模型，对各行业抽样读取 MD&A 文本，生成详尽的行业业务画像总结；然后使用 Qwen3-Max 模型将所有行业的业务摘要整合为单一输入进行全局对比分析，赋予符合中国 A 股市场通用术语的行业名称（如“基础化工”“食品饮料”“高端装备”等），名称长度严格控制在 2-6 个中文字符，确保名称互斥。二级行业命名时还显式引入一级行业信息作为先验背景，使二级名称体现出对一级行业的从属或细分关系。

第四步：测试。构建分类体系后，研究从行业间差异性、行业内相似性和资产定价三个维度，将 LLM 分类与申万三级分类、万得四级分类及中国上市公司协会分类进行系统比较。评价指标选取了营业利润率（OpMargin）、资产回报率（ROA）、营业收入增长率（RevGrowth）和资本支出增长率（CapxGrowth）四个在相同业务公司间高度相似的财务特征指标。衡量逻辑是：一个好的分类标准应该把最相似的公司放入同一个类别中，使得类内差异最小、类间差异最大。

最终形成的“人大-新华”分类体系涵盖 26 个一级、102 个二级和 271 个三级行业。26

个一级行业包括：高端装备、食品饮料、医药生物、电子元件、软件服务、农林牧渔、基础化工、种子农业、交通运输、电力设备、公用事业、纺织服装、文化传媒、建筑材料、商业零售、房地产、综合转型、交运能源、金融服务、家电部件、旅游酒店、轨道交通、造纸包装、高速公路、石油化工和环保水务。聚类层次完全嵌套。数据显示，综合转型行业从 2007 年的 294 家骤降至 2023 年的 3 家，电子元件行业则从 71 家扩张至 766 家，生动反映了中国产业结构的动态演变——高新技术产业和先进制造业快速扩张，而部分传统行业则面临调整或增长瓶颈。

在行业间差异性方面，研究计算了各分类体系下不同行业在四个核心财务指标上的标准差，标准差越大表明行业间财务特征差异越显著。结果显示，在同等类别数量粒度下，LLM 分类体系在多数指标上均优于同级别的申万、万得分类。以营业利润率为例，“人大-新华”三级分类的标准差为 0.266，而申万三级仅为 0.131——LLM 行业区分度约为传统分类的两倍。在一级分类层面，LLM 分类标准差（0.113）同样显著高于申万一级（0.064）、万得一级（0.097）和万得二级（0.079）。在二级分类层面，LLM 二级（0.188）显著超过申万二级（0.102）与万得三级（0.098）。

在行业内相似性方面，研究采用行业哑变量回归的 R^2 作为衡量指标，R^2 越高表明同一行业内公司在该指标上越趋同。结果显示，LLM 分类在多数指标上均具有更高的 R^2 解释力。以营业利润率为例，“人大-新华”三级分类的平均 R^2 为 0.144，高于申万三级的 0.102 和万得四级的 0.095。更高的 R^2 意味着同一行业内企业在关键特征上更相似，LLM 分类能更好地实现“类内相似、类间差异”的分类目标。

在资产定价检验中，研究基于 Hoberg 和 Phillips（2018）的行业“领先-滞后”效应，结合 Du 等人（2025）关于 A 股高价股动量更显著的发现，构造了对冲投资组合。具体方法为：每月末在收盘价不低于 10 元且流通市值位于市场前 70%的股票池中，计算过去 11 个月（排除最近一个月）同行业公司平均累计收益率作为“领先-滞后”特征，采用双重独立排序——按收盘价（前 10%与后 10%）和领先-滞后特征（前 20%与后 20%）独立排序后取交集，做多“高价股+高领先-滞后”组，做空“高价股+低领先-滞后”组。结果表明，“人大-新华”二级和三级分类产生了统计显著的正收益（月均收益分别为 1.29%和 1.53%，T 值分别为 2.43 和 2.81），而其他分类体系的对应组合均未产生显著正收益。经 Fama-French 五因子模型调整后，LLM 三级分类的等权 Alpha 为 1.60%（T=3.00），经中国四因子模型调整后等权 Alpha 为 1.80%（T=2.84），均高度显著；而申万和万得体系在多数设定下均未能产生统计显著的 Alpha。Fama-MacBeth 横截面回归进一步证实，“人大-新华”二级分类交乘项系

数为0.0148（t=2.05），加入资产增长率、公司规模、账面市值比和毛利率等控制变量后仍在5%水平显著，其他分类体系均不显著。

“人大-新华”A股上市公司行业分类数据集已于2026年3月正式发布并在新华财经数据终端上线，可供金融从业者和研究人员使用。

三、人工智能如何识别风险链条：基于生成式AI的公司关联网络

企业间的关联网络对于理解系统性风险至关重要。2018 年东方园林债券违约表面仅为单一公司信用事件，但迅速引发蒙草生态、铁汉生态、道氏技术等多家公司股价大跌，累计损失市值超150亿元。Acemoglu 等人（2015）系统揭示了这一机制：关键企业的微观冲击可通过供应链、信用链层层放大，引发宏观波动。在中美科技竞争背景下，出口管制和关税变化可能通过隐性关联网络传导影响大量表面上无直接关联的企业。

现有描述企业关联的方法大多局限于单一维度——供应链联系（Cohen 和 Frazzini，2008）、行业竞争（Hoberg和Phillips，2016）、地理位置（Parsons等人，2020）、技术专利（Lee等人，2019），共同问题是依赖结构化数据、更新频率低、覆盖范围有限、难以捕捉多维度隐性关联。

我们团队正在推进的国自科面上项目，试图利用大语言模型从企业年报文本中挖掘多维度隐性关联，再结合图神经网络（GNN）整合为复合企业网络结构。方法分为三步：第一步,将年报按段落拆分为文本单元,由大模型评估每个单元与特定经济概念(产品市场竞争、产业链上下游、技术创新、市场风险暴露、地理关联等）的相关度并赋分（0-100 分）。例如，“天然气消费量为4930亿立方米，同比下降12%”这一文本，在风险关联性维度获85分，主营业务关联性获70分，技术关联性为0分，体现了大模型精细化的多维度语义理解能力。第二步，在每个概念维度上提取各公司得分最高的文本段落，用嵌入模型转化为语义向量，通过余弦相似度构建企业间邻接矩阵。第三步，用GNN通过消息传递机制融合多维度网络，能够动态学习节点间关联权重，并通过多层结构捕捉间接关联——因为风险传导往往层层传递。

基于所构建的网络，研究计划在三个核心场景中检验其价值：股票收益率预测、股价风险预测（NCSKEW、DUVOL和下行Beta）以及参数化投资组合优化方法（Brandt，Santa-Clar和Valkanov，2009）。研究将在中美两个市场同时进行检验，分析不同制度环境和市场结构下网络效应的异质性。

四、人工智能应用的关键约束

AI 赋能金融的同时，其应用本身的风险同样不可忽视。前瞻性偏差是当前几乎所有使用大模型进行金融预测的研究都面临的系统性风险。大模型训练数据涵盖互联网海量信息，分析某一历史时点的企业年报时，模型可能无意中利用了后来才出现的信息（Glasserman 和 Lin，2023；Ludwig 等，2025）。比如：让大模型分析 2015 年小米公司年报，由于模型“知道”小米来来涉足电动汽车，可能使用未来信息判断小米主营业务已涵盖汽车行业。学术界提出的主要应对方案是文本匿名化——通过 NER 技术去除公司名称、人名、地名等标识信息（Kim 等，2024），或利用 LLM 对原始文本进行实体替换和改写（Engelberg 等，2025），使大模型无法判断文本属于哪家公司、哪个年份。

然而，我们团队最新完成的研究论文《Anonymization and Information Loss》揭示了匿名化方法的重要局限。核心发现包括五个方面：其一，匿名化导致情感信号解释力显著下降，R^2 从 0.132 降至 0.124，对比回归中标准化系数从 2.331 骤降至 0.775；其二，信息损失主要来源于数字和机构名称的移除，地名移除影响相对较小；其三，信息损失在文本不确定性高、企业透明度低时更为严重；其四，信息损失可能大于前瞻性偏差，截止日前后两个时段比较，原始文本对匿名化文本的信息优势没有显著扩大；其五，上述发现在多种任务、多个模型、多类文本中均广泛稳健。这项研究对整个“AI+金融”领域提出了重要的方法论警示：匿名化不应被视为万全之策，更合理的做法是同时使用截止日前后的样本进行对比分析，区分偏差消除和信息损失两种效应。

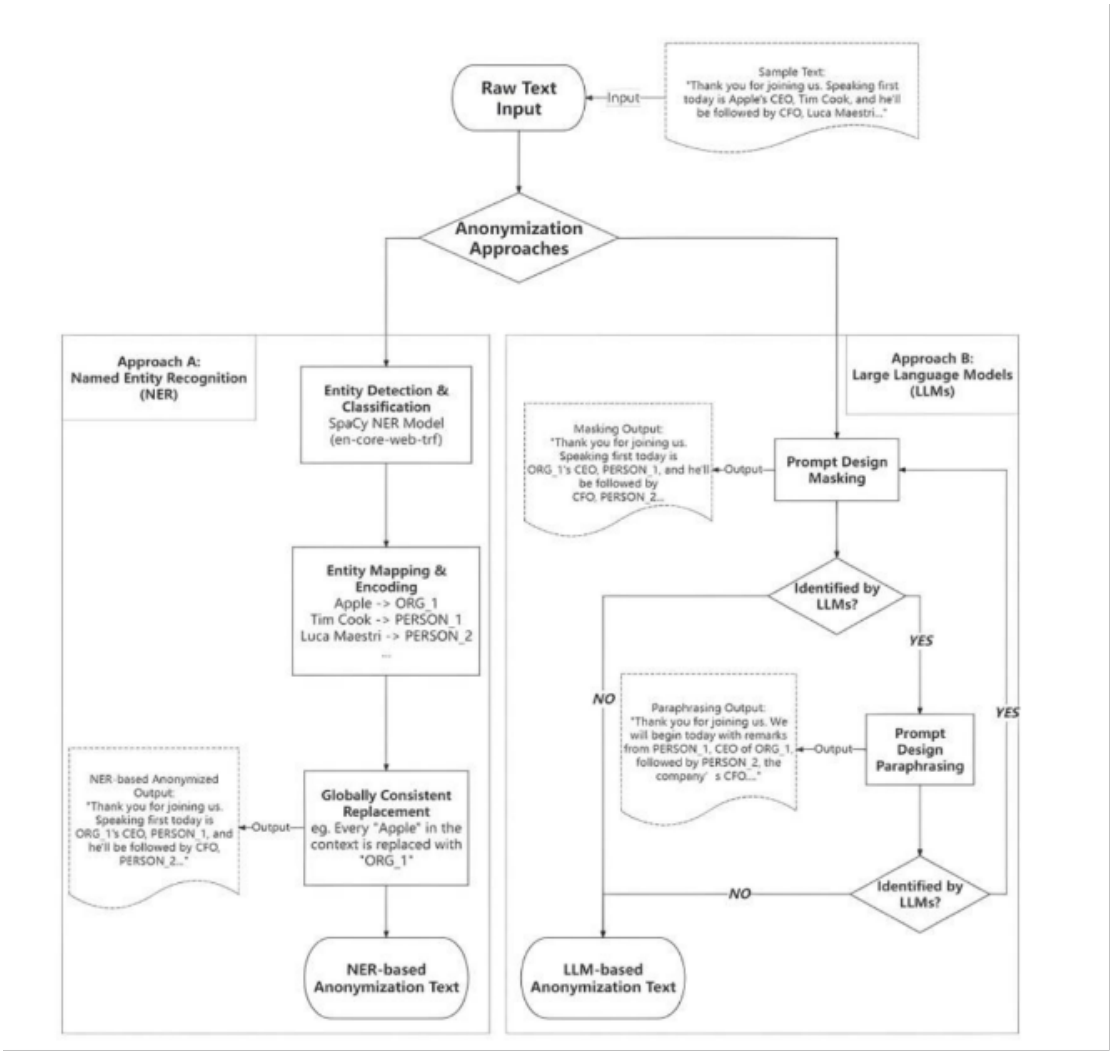

Figure 1: Anonymization Pipeline (Wu et al., 2026)

此外，AI 金融应用还面临多重风险。在过度数据挖掘方面，Harvey 等人（2016）分析 316 个因子后指出大量显著性为数据挖掘产物，AI 大幅降低“发现”新模式的成本，加剧“人工愚蠢”效应。在算法合规方面，大模型可能自发“发现”违规但有利可图的策略，全国人大 2025 年已将 AI 立法列为预备审议项目，欧盟 AI 法案已生效。在版权风险方面，2026 年 1 月斯坦福和耶鲁研究团队发现主流 LLM 深度“记忆”版权书籍内容，部分可复现 70%以上。在 AI Agent 安全方面，API 密钥泄露可能导致未授权交易，提示注入可能操纵投资决策。在通用模型金融专业性不足方面，“负债”在金融语境中可能为中性甚至正面，“做空”在专业领域是常规对冲手段，通用模型存在系统性偏差。

AI 对全球劳动力市场的结构性冲击已从理论走向现实。世界经济论坛报告指出到 2030 年全球将有 9200 万个岗位因 AI 被淘汰，高盛估算约 3 亿个全职岗位受生成式 AI 实质影响，2026 年 3 月 AI 已成为美国企业裁员的首要原因（占月度裁员的 25%）。对金融行业而言，数

据处理、报告撰写、合规审核等规则性岗位面临直接替代风险，大规模就业替代还可能通过消费萎缩等渠道产生系统性影响。如何在推进 AI 应用的同时妥善管理劳动力市场的转型阵痛，已成为政策制定者和金融机构必须正视的重大课题。

五、总结与展望

报告围绕“效率提升”与“风险治理”两条主线，系统探讨了人工智能如何赋能金融。基于 LLM 的 A 股行业分类全面优于传统标准，实现了数据驱动、透明可复现、年度自动更新的范式转变。多维度概念赋分与 GNN 融合构建的复合企业关联网络，覆盖收益率预测、风险预测、投资组合优化三大核心场景。前瞻性偏差与匿名化信息损失的权衡揭示了匿名化非万全之策，数据挖掘、合规伦理、版权记忆、Agent 安全和劳动力冲击等问题同样需要审慎治理。展望未来，2026 年“十五五”开局之年，随着金融专属大模型持续演进、多模态数据融合、监管框架完善以及 AI Agent 从 Chat 到 Action 的跃迁，人工智能将在市场定价效率提升和系统性风险治理中发挥越来越核心的作用。

编　号	名　称	作　者
IMI Report No.2605	更加积极有为：“十五五”开局年的政策协同与新范式	高昊宇 李戎
IMI Report No.2604	AI 时代金融机构智能化转型与本体论轻量化落地方案	张鲲
IMI Report No.2603	国际货币体系与主权债务面临的危机和挑战	Anoop Singh
IMI Report No.2602	欧洲的地缘政治与经济挑战	David Marsh
IMI Report No.2601	全球视野下的中国跨境支付体系变迁	仇乙彤
IMI Report No.2535	地缘经济风险对中国的宏观影响	IMI
IMI Report No.2534	美元稳定币加快发展带来深刻警示	王永利
IMI Report No.2533	稳定币的经营模式、发展影响与监管框架	朱太辉
IMI Report No.2532	稳定币的发展历程、成败叙事及其对中国的启示	柏亮
IMI Report No.2531	关税博弈维度下的人民币汇率波动与趋势研判	陆利平
IMI Report No.2530	从“参与者”到“定价者”：人民币债市国际化如何乘势突围?	宗良
IMI Report No.2529	AI、大数据与区块链：财富管理的未来已来	田力
IMI Report No.2528	传统中国思想精英对货币形态本质特征及其功能的长期追问	何平
IMI Report No.2527	离岸金融视角下沪港国际金融中心协同发展思考	邓志超
IMI Report No.2526	低利率时代金融机构的韧性重塑之路	高昊宇
IMI Report No.2525	人民币汇率波动与美联储政策预期	管涛
IMI Report No.2524	人工智能如何重塑金融业	姜富伟
IMI Report No.2523	新时代全球财政债务管理如何破局?	Anoop Singh
IMI Report No.2522	稳定币的风险、挑战与中国对策	邓建鹏
IMI Report No.2521	现实世界中的货币流动性分析	王剑
IMI Report No.2520	地缘经济风险与全球产业链供应链格局再调整	IMI
IMI Report No.2519	人民币国际化指数（RII）：最新走势与世界货币格局变更	IMI
IMI Report No.2518	地缘经济风险对人民币国际化的深刻影响	IMI
IMI Report No.2517	金融制裁、地缘经济风险与全球支付体系	IMI
IMI Report No.2516	2025 人民币国际化课题成果发布稿：不断深化的地缘风险	IMI
IMI Report No.2515	银行报价基准利率的未来：基于 LIBOR 弃用的反思	IMI
IMI Report No.2514	提振消费如何发力扩内需	王微

中国人民大学国际货币研究所
INTERNATIONAL MONETARY INSTITUTE OF RUC

地址：北京市海淀区中关村大街 59 号文化大厦 605 室，100872　电话：010-62516755　邮箱：imi@ruc.edu.cn