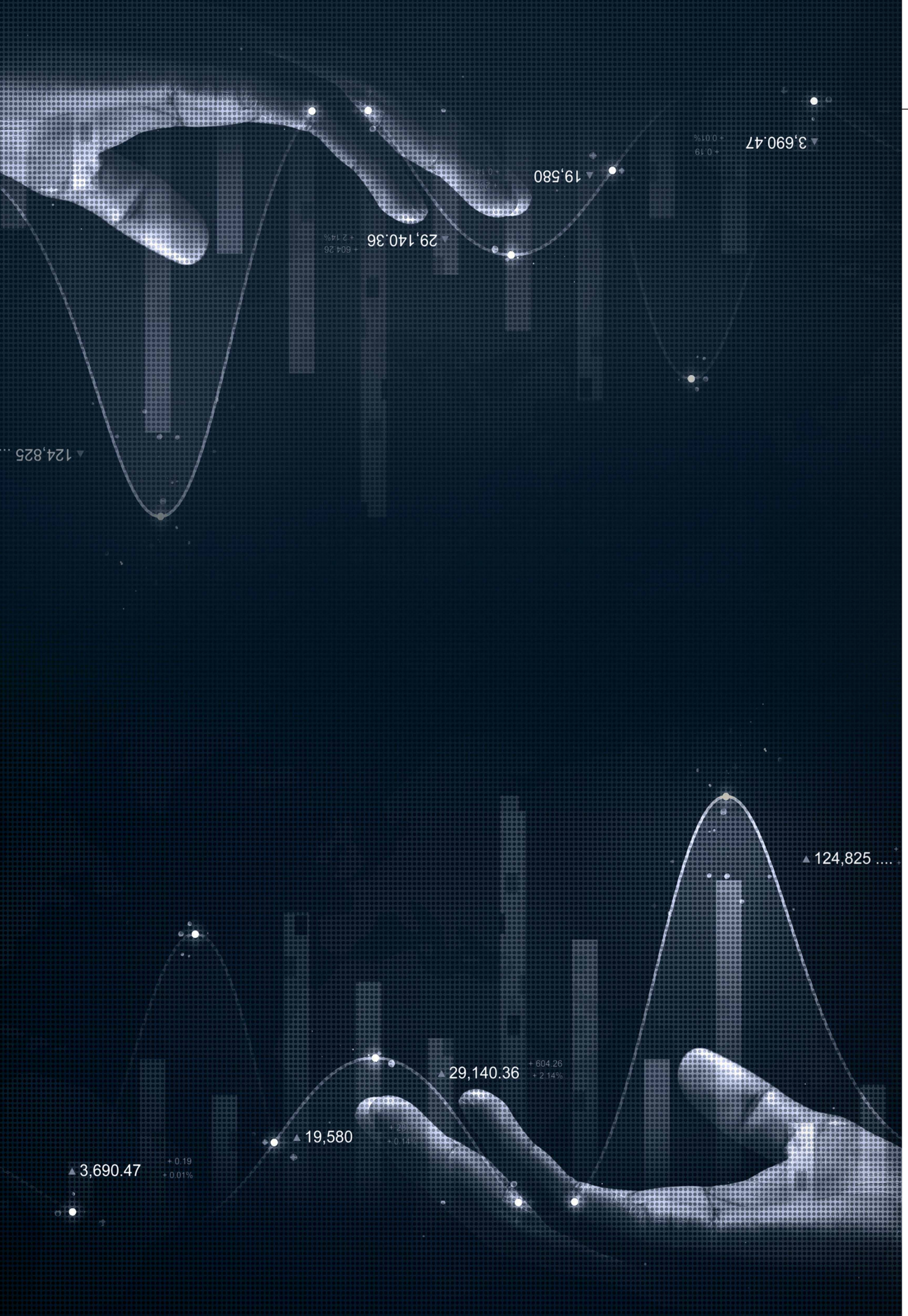
发展新质生产力
开启数字金融新纪元

大模型驱动的数字员工3.0 建设应用白皮书

中国工商银行金融科技研究院
华为技术有限公司数字金融军团
北京金融科技产业联盟
2024年9月



序言

大道不孤，众行致远。习近平总书记多次作出重要论述，指出发展新质生产力是推动高质量发展的内在要求和重要着力点。这是在世界百年未有之大变局和中国现代化建设的新阶段，对高质量发展的把脉定向。中央金融工作会议要求，金融要为经济社会发展提供高质量服务，做好科技金融、绿色金融、普惠金融、养老金融、数字金融五篇大文章。银行业应全面深化数字技术的金融应用，以人工智能为重要抓手推进产业创新和解锁新质生产力，以高质量金融服务推动经济高质量发展。

因时而变，随事而制。数字员工3.0作为人工智能大模型与银行业务深度融合的新型业务应用载体，正在重塑银行业的服务模式和创新能力。为更好推动数字金融高质量发展，助力人工智能+金融生态建设，由中国工商银行金融科技研究院牵头，联合华为技术有限公司数字金融军团、北京金融科技产业联盟倾力编撰《发展新质生产力，开启数字金融新纪元——大模型驱动的数字员工3.0建设应用白皮书》，旨在为金融机构把握机遇，应用以大模型为核心的数字员工3.0新型技术，实现金融业务高质量发展，提供全面而深入的实践参考。

创新求变，行稳致远。随着数字化与智能化转型的浪潮汹涌而来，人工智能技术的革新层出不穷。数字员工的建设与创新应紧跟技术进步的步伐，同时契合我国金融行业的发展脉络，并充分体现人机的和谐协作。本书立足于当前金融科技发展前沿，从底层的大模型技术、中间的应用范式能力构建、到上层的应用场景落地，同时融汇全域安全和全生命周期身份管理，详细描绘数字员工的技术栈和实现路径，深入探讨数字员工应用于智能客服、智能营销、智能风控、智能运营等多个实践案例以及对其管理和安全管控方面的思考，为读者提供丰富的参考。

道阻且长，行则将至。本书凝聚中国工商银行、华为技术有限公司、北京金融科技产业联盟多年来在数字员工体系建设和应用领域的思考和实践经验，是各方多年合作的智慧成果。展望未来，我们相信，通过持续的技术创新和实践探索，以人工智能大模型为核心的数字员工将成为推动银行业数字化转型的重要力量，为打造一个更加智能化、高效率、广泛覆盖的高质量金融服务体系提供强大动能。在此，我们期待与各方携手，共同打造新质生产力，迈向数字金融新纪元！

目录

目录

一.概念篇：

数字金融更上层楼，
数字员工迈入新篇

1.1 立足新发展，数字金融是数字经济发展的新质生产力

党的二十大报告中提出“加快发展数字经济，促进数字经济和实体经济深度融合”。数字经济是继农业经济和工业经济之后的主要经济形态，是以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，促进公平与效率更加统一的新经济形态。

数字金融与数字经济相伴相生，2023年中央金融工作会议提出要加速建设金融强国，做好数字金融等“五篇大文章”，提供高质量金融服务。数字金融是以数据技术双要素为驱动，推动金融产品和服务模式创新重塑，与数字经济发展相适应，全面服务经济社会高质量发展的一种新金融形态，是金融数字化转型的深化和提升。当前，数字金融正逐步融入到金融产品和服务中，实现产品、流程、渠道、营销、运营、风控等银行业务主要领域的全链路赋能，形成新质生产力，适应数字经济发展。

人工智能是发展数字金融的重要引擎，是助推银行从“数字时代”迈入“数智时代”的新动能。”中国人民银行发布的《金融科技（Fin-Tech）发展规划（2022-2025年）》，指出要重塑智能高效的服务流程，更好支撑数字化业务快速发展。2024年3月，“人工智能+”首次写入政府工作报告，为人工智能技术在千行百业的广泛应用开启新篇章。金融业作为数字化和智能化的先行者，具备人工智能应用丰富的场景舞台和技术实施基础。为高质量落实国家战略目标，金融机构纷纷加大人工智能应用布局，随着传统人工智能技术的逐步成熟和金融行业经验的持续累积，智能金融应用正在进入规模化发展新阶段。同时，生成式人工智能大模型的迅猛发展为数字金融带来新的发展方向，创造更广阔的应用前景。传统人工智能技术与新兴生成式人工智能的融合，推动数字金融向更高层次、更广范围发展，为金融行业带来前所未有的创新机遇。

1.2 贯彻新理念，数字员工是数字金融的重要应用载体

在银行业数字化智能化发展过程中，数字员工成为发展数字金融的重要应用载体，银行通过数字员工的应用将劳动力、数据、技术等生产要素按照数字形态有机融合叠加，进一步推动银行金融服务由传统生产模式向数字化智能化生产力模式转变。

数字员工，也称为数字化劳动力，是一种利用机器人流程自动化（RPA）、人工智能和其他技术来模拟人类工作行为的智能化IT系统，能在特定领域辅助或替代人类完成相关任务。值得一提的是，数字员工的设立并非是对人类员工的替代，而是让每个员工拥有贴身、智能的数字助理，提升人类员工的生产力和创造力，人机协同为企业创造更大的价值。该模式下，人类员工和数字员工共同组成协作团队，人类员工承担决策、监督、指挥的角色，数字员工围绕人类员工承担建议、执行的角色。通过上述过程，使得每个员工获得成倍的工作效能提升，进而实现生产关系的变革和生产力的飞跃式创新。

2023年大模型驱动的生成式AI技术爆发之后，数字员工也迎来全新的发展机遇——在大模型技术驱动下，数字员工拥有“智慧灵魂”，智能化能力和拟人化水平大幅提升，开启数字员工发展的新浪潮，成为推动银行数字化转型、培育金融新质生产力的新型重要应用载体。

1.2.1 从自动化到拟人化，大模型成为数字员工重要技术支撑

数字员工概念源自流程自动化技术，伴随人工智能技术的快速发展，数字员工经历基于流程自动化的1.0时代、基于RPA+传统人工智能应用的2.0时代、基于大模型和智能体的3.0时代三个发展阶段，从1.0到3.0，数字员工的智能化水平快速提升，赋能的员工范围和价值产出也越来越大。

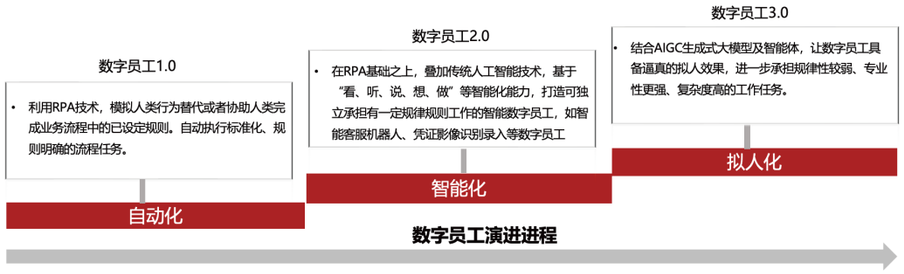


图1：数字员工的技术演进

数字员工1.0：侧重自动化，主要利用RPA自动化技术，模拟人类计算机操作行为，替代或者协助人类完成业务流程中的已设定规则、自动执行标准化、规则明确的重复性任务，如自动对账、标准化报表自动化生成等，从而提高效率。RPA应用可看作数字员工的早期形态，部分企业也将RPA自动化应用纳入数字员工范畴。

数字员工2.0：侧重智能化，在RPA技术之上，基于“看、听、说、想、做”等传统人工智能技术，打造具有面向特定工作的智能化数字员工。这一阶段的传统人工智能技术开始尝试模仿人类的感知和决策过程，基于机器学习、自然语言处理、计算机视觉、语音识别等传统人工智能技术，赋能数字员工处理相对复杂的任务，如智能问答、智能外呼、金融凭证影像智能识别录入等。从交互能力来看，该阶段出现具有数字人形象、简单语言语音交互能力且有一定人格化属性的数字员工，但受制于传统人工智能泛化能力有限，数字员工2.0往往按照人工预设脚本“照本宣科”，或基于问答对匹配知识库答案回答问题，智能化程度有限。

数字员工3.0：侧重拟人化，随着大模型和智能体技术发展演进，全能数字员工应用得以实现，该模式集成多样智能大模型的能力，包括感知、记忆、规划、执行、反馈、协同等高度拟人化能力，同时基于统一的智能体框架（如图2所示），**数字员工3.0可以融合调控数字员工1.0、2.0的各项服务能力，**如把RPA能力当成工具调度起来，实现**数字员工1.0的自动化和数字员工3.0的智能化协同；**如大小模型融合应用，**也即数字员工2.0和3.0融合。**数字员工3.0**通过自然语言交互模式，为企业中的每个员工配备一个7*24小时的智能助理，**能够通过理解目标、拆解任务、感知环境、调控工具等方式，人机协同完成规律性较弱、专业性更强、复杂度更高的工作，如市场趋势分析、资金资源调度、代码编写等。

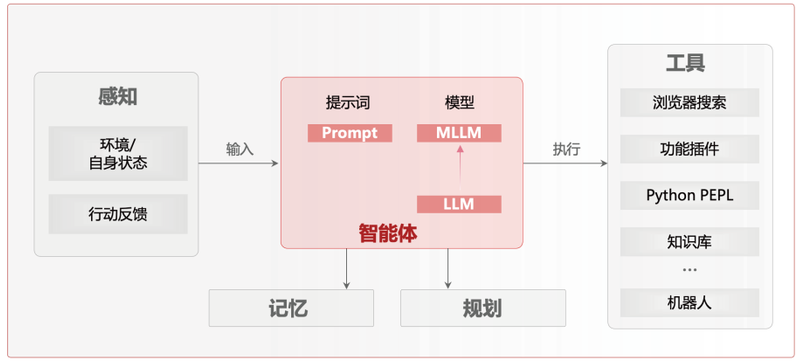


图2：智能体框架介绍

当然，数字员工3.0并非是对1.0、2.0的替代，而是在其基础之上的演进和协作共生关系。数字员工1.0、2.0擅长处理规则明确、重复性高的简单任务，算力消耗少，可解释性好，性价比高。数字员工3.0得益于大模型强大的通用问题解决能力，能胜任处理规律性较弱、专业性更强、复杂度更高的任务，但受制于大模型黑盒、计算复杂度高等因素，存在可解释性弱、成本投入大等问题。同时，数字员工3.0可以作为超级应用，无缝融合调控数字员工1.0、2.0的各项服务能力，建立基于自然语言交互、极致体验的智能化服务。因此，**不同代的数字员工互为补充，共同推动业务流程的优化和智能化创新。**

1.2.2 从简单模拟到个性交互，数智技术赋予数字员工数字人格

拟人化的数智技术发展，赋予数字员工“数字人格”。在交互能力方面，数智技术帮助数字员工模拟人类的表达方式和行为模式，尤其是伴随着人工智能大模型等技术的逐渐成熟，数字员工具备通过自然语言对话理解语境，学习和适应工作任务的沟通协作能力；在情感个性方面，通过为数字员工精心设计独特性格、知识背景和情绪表达，同时伴随着语音克隆、数字人克隆等高度拟人化技术的成熟，使得面向不同领域的数字员工展示出千人千面的类人形象和个性化服务能力。

目前，业界尚没有对数字员工的人格化标签进行标准化分类，**本文试图从人类员工工作的人力管理“员工-岗位-能力”三层关系模式出发，来综合阐述这些多元丰富的数字人格。**

一是从服务对象视角来看，数字员工分为对客服务和对内赋能两种群体。对客服务数字员工主要负责数字化的客户服务工作，如使用智能问答自动答复客户各类金融咨询；对内赋能数字员工主要服务于企业内部的综合办公、业务处理等领域，协助或替代企业员工处理各类事务，提升工作质效，激活经营活力。

二是从担任岗位视角来看，数字员工的承担岗位呈现出综合化、专业化两种发展趋势。综合化岗位数字员工通常作为员工超级助手存在，承担一个领域或者多个领域的多种岗位，通过自然语言交互，能够调控后端多种专业技能，从而具备文档编写、知识问答、程序编写、数据分析等多种能力，辅助或替代人类员工解决各类问题。专业化岗位数字员工聚焦具体岗位，旨在替代或协助人类员工处理岗位要求的一类或多类工作任务，如数据录入、交易处理、账户维护等。综合岗位数字员工由于具备较强调控能力，可通过对话交互模式调度各种专业岗位数字员工能力串联完成更为复杂的金融交易执行。

三是从胜任能力视角来看，数字员工具备“辅驾”、“代驾”两种代表性能力形态。本文结合智能体应用演进趋势，将辅驾到代驾的能力发展分为L1-L5五个等级。L1级数字员工作为工具被人类手工调用；L2级数字员工能够执行被人类分解的任务，比如RPA每天定时批量处理财务报表自动下载；L3级数字员工能自主拆解及分配任务，闭环执行，人类员工、数字员工协作完成业务工作；L4级数字员工能提供达到人类专家水平的定制化服务；L5数字员工具备自主智慧，能够独立完成工作。**当前业界的数字员工能力主要集中在L2及L3两个层次。**

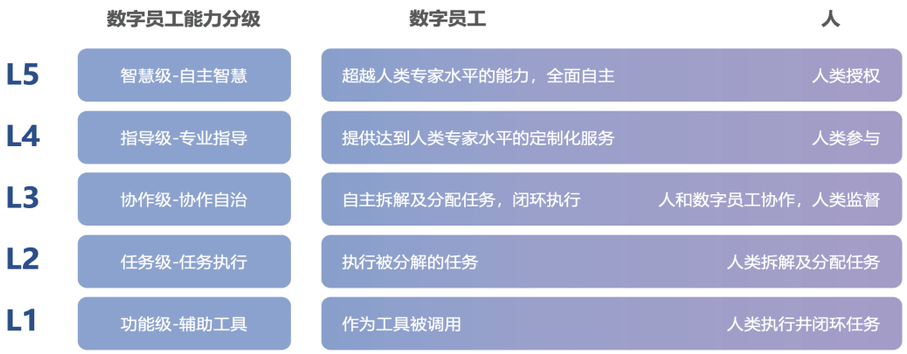


图3：数字员工的能力分级

1.3 剖析新优势，数字员工3.0助力银行迈入数字金融新纪元

数字员工3.0的核心理念是“拟人化”、“自主化”与“共享化”，这三大核心共同构建一个全新的数字劳动力模型，而不再局限于简单的任务自动化与智能化。数字员工3.0以更贴近人类的方式进行交流和互动，融合共享跨系统、跨组织的知识与资源，通过模拟人类员工的决策过程并不断自我优化，有效应对复杂业务问题。

数字员工3.0作为数字员工技术的最新发展阶段，重新定义数字员工的能力边界，将数字员工的智能化水平、任务处理能力、学习适应能力和交互能力带向新的高度，形成人机协作的新模式。

1.3.1 从判别到生成，数字员工应用出现新形态

传统人工智能在金融领域的应用主要集中于分类、聚类、回归任务，如信用评估、交易反欺诈判定、凭证影像识别、备付金准备预测等。但传统人工智能技术局限于特定的狭义人工智能范畴，能力有限。

生成式AI的出现，让数字员工具备强大的文本生成、图像生成甚至代码生成能力，为金融行业带来全新的应用场景，为金融行业数字化转型注入新动能，也壮大百模千态的数字员工生态。例如，在投资研究领域，数字调研助手可以自动生成高质量的研究报告，不仅提高效率，还能为分析师提供新的洞察角度，在产品设计方面，数字设计助手可以根据客户需求和市场趋势，快速生成创新的金融产品方案；在风险管理领域，数字风控助手可以自动预估各种极端市场情景，帮助金融机构更好地进行压力测试和风险评估，显著提升工作效率和决策质量。在生成式智能的催生下，数字员工涌现的能力可以创造出全新的、乃至人类可能未曾想到的解决方案，并催生出颠覆性的金融产品和服务模式。

1.3.2 从单点能力到通用能力，数字员工应用驶向复杂纵深领域

在金融领域，专业岗位如信贷经理、风险管理人员等，需处理大量的信息和数据，并进行深入分析和处理。传统AI在处理结构化数据方面表现出色，但在理解复杂的非结构化信息（如文本、图像等）方面能力有限，导致以往数字员工应用往往是点上的浅层次创新。

生成式大模型的出现，显著提升AI的语言理解和知识推理能力，帮助数字员工深入到智慧金融的方方面面处理和解决更复杂的任务和问题。例如在决策支持方面，研报分析助手理解和整合来自多个来源的复杂信息，包括新闻报道、社交媒体、企业公告等，从而提供更全面、更深入的市场洞察。在客户服务方面，客服机器人不再局限于简单的问答，而是能够进行深入多轮业务咨询，理解客户的复杂需求，提供个性化的金融建议。依托大模型深度理解能力的突破，数字员工将辅助金融从业人员更加得心应手地处理金融领域的复杂问题，从而提升金融机构在客户服务、业务运营、风险管理、技术创新等方面的智能化水平。

1.3.3 从+AI到AI+，数字员工助力数字金融迈入新纪元

传统的智能化金融应用往往是在现有业务流程中嵌入AI功能，即“+AI”模式，该模式下AI往往是业务流程的附属部分，并未深层次改变业务流程模式。

生成式AI的出现，推动业务应用模式向“AI+”转变，即以AI为核心重塑整个业务流程和交互方式，通过对话式交互方式串联复杂分散的业务流程，AI不再仅仅是业务流程的附属部分，更是行业创新发展的主要驱动力和调度协作中枢，使得人机交互变得更加自然和无缝，用户不再需要通过复杂的表单或菜单来操作金融系统，而是通过自然语言与智能助手进行流畅对话，即可完成信息查询、业务办理、投资建议等一系列操作，以AI+重塑业务流程，显著提升业务处理效率和体验。在AI＋的浪潮中，数字员工不仅仅是一种工具，它们与人类员工形成互补，开启人机协同的新纪元。

一是数字员工3.0的崛起，标志着“数字分身”的大规模应用成为可能，数字员工3.0将为每位银行员工提供多个“数字分身”，彻底改变人机协作的模式。员工能够创造和定制专属的数字助手，形成“1个自然人+N个数字员工”的新型智能团队。这种革命性的变革，使得每个员工能够获得成倍的工作效能提升。由此，人类员工和数字员工共同组成的协作团队，成为商业银行突破效能瓶颈的关键资源。

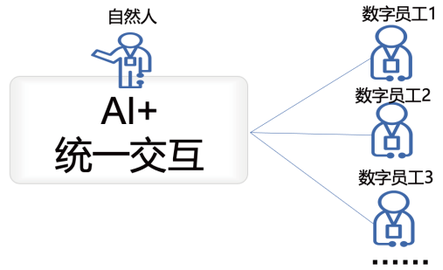
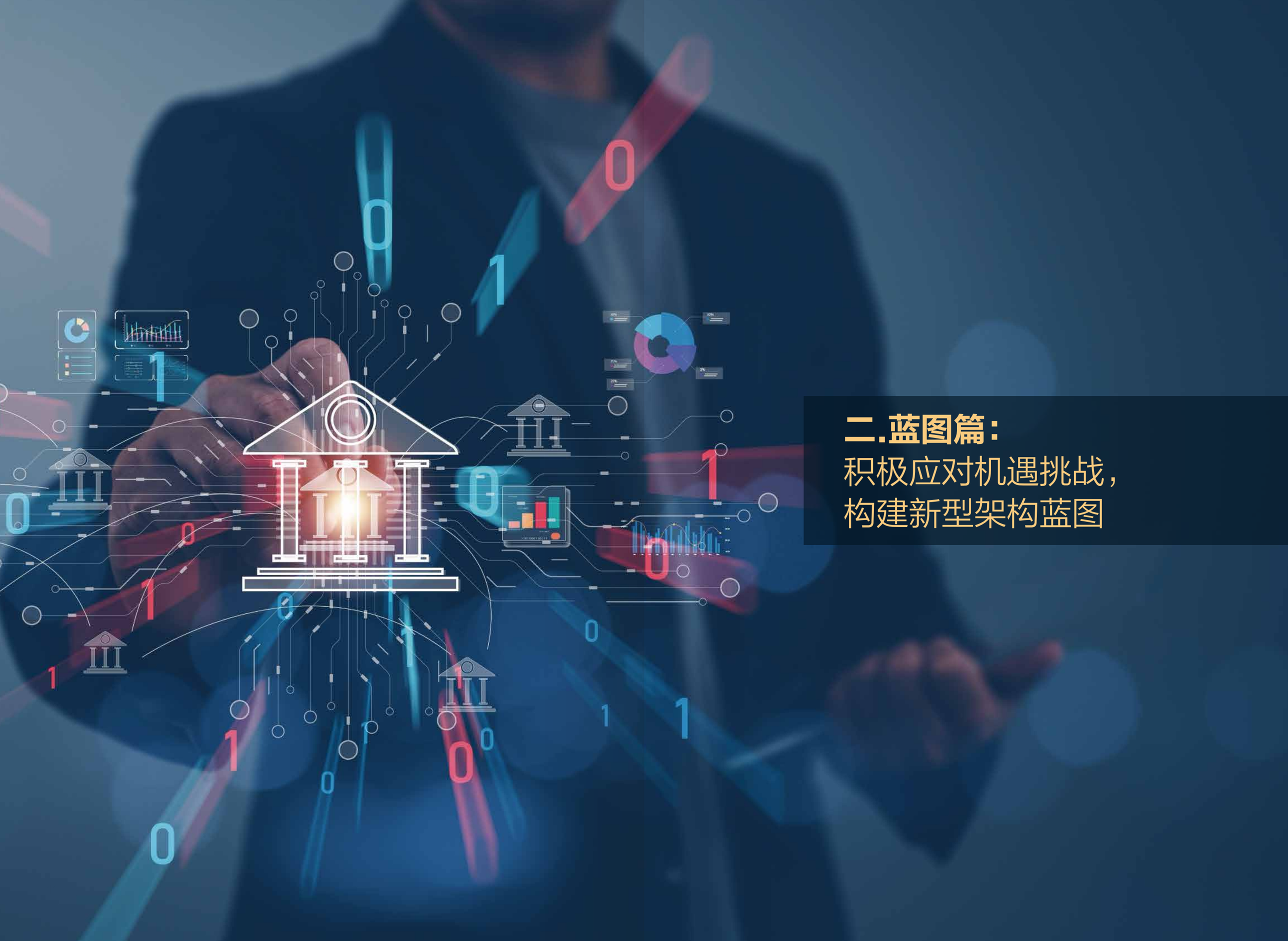


图4：AI+时代人机协同

二是传统的流程性工作和简单的非线性场景任务逐渐交由数字员工处理，这不仅提高工作质效，更释放人类员工的潜能。人类员工的工作重心随之向更高层次的领域转移，包括高阶认知、社交情感和技术创新等方面。这种转变使得人类的“高阶价值”得以充分彰显，将高精尖人才从繁琐的日常事务中解放出来，转而投入到更具创造性和战略性的工作中。这种人力资源的重新配置不仅优化银行的人才梯队结构，更促进人力资源体系改革。通过将人类智慧与数智技术有机结合，银行业正在培育和强化自身的数字基因，为未来的发展奠定坚实基础。



二.蓝图篇：

积极应对机遇挑战，构建新型架构蓝图

基于大模型的数字员工3.0，相较于传统的数字员工产生巨大的差异性，在任务胜任期望、技术支撑复杂度、人格化管理、安全可信等方面均提出新要求。从业界来看，数字员工3.0尚处于起步阶段，缺少可借鉴、可复制的行业实践和方法论指导，对标金融应用的可靠、安全、稳定、规范的高标准要求，数字员工3.0需要各银行机构从深化技术创新、规模业务应用、优化管理流程、确保应用安全等方面体系化规划，指导应用实践。

2.1 数字员工3.0建设的机遇和挑战

2.1.1 应用挑战：数字员工3.0的业务价值自证

数字员工3.0真正价值在于规模化、高效赋能业务价值创造，但数字员工3.0在金融场景的规模化应用无先例可循，挖掘高价值场景、实现场景落地解决实际问题等方面面临挑战。

一是高价值场景挖掘，业界缺少端到端的场景挖掘和智能化流程设计的业务赋能方法论。传统数字员工智能化水平有限，一般从某个具体流程痛点出发，赋能点状需求。数字员工3.0依托大模型，具备较强的感知、记忆、规划、执行、反馈、协同等能力，在涉及多重能力、多重交易的条线级和领域级赋能具备较好的可行性，因此，各银行机构需要在数字员工3.0建设应用中，从传统的点状赋能方法转向端到端的业务智能化赋能方法论，提升人工智能全链路应用业务价值。

二是场景高效高质量落地，业界缺少可解决业务实际问题的数字员工综合型应用解决方案，规模化赋能效率质量仍有待提升。数字员工3.0根据自然语言交互，调控大小模型、数据服务、业务交易等各类服务，如按照传统应用集成硬编码，研发成本高，存在功能集成难、研发周期长、方案可复制性差等痛点。因此为提升赋能质效，加速规模化效应，按照金融业务共性需求，提炼形成贴近业务、开箱即用、低门槛的综合型应用解决方案成为赋能关键。

2.1.2 技术挑战：大模型使能金融数字员工面临四大挑战

数字员工3.0的核心技术是大模型。目前大模型产业仍处于新技术发展初期，在金融大模型垂类领域更是缺少技术实践与经验积累，赋能数字员工时在算力、数据、算法、应用等方面存在挑战。

数字员工3.0需要大算力。随着大模型参数量的增加，对算力基础设施需求呈指数级增长，金融机构在建设算力底座时面临诸多挑战。首先，若进行全面体系化建设，需要大量资金投入和高技术门槛，短期难以快速实现高预期目标，需要较长周期，各类型机构需要结合自身发展制定基础设施发展策略。同时算力呈现多元异构化，如何完成多种不同类型的算力设施适配和异构算力的统筹管理调度给各机构在应用中带来挑战。

数字员工3.0需要大数据。高质量非结构化数据是数字员工3.0成功应用的基石。但所需数据量巨大且对多样性、多模态要求高，这对金融行业数据在采集、清洗、管理、使用等方面提出更高要求。同时，非结构化金融数据内容多样、解析复杂，这极大阻碍非结构化数据资产的价值实现。银行业如何在结构化数据治理基础上，进一步盘活海量非结构化数据资产，并与结构化数据形成协同增效，是数字员工3.0金融应用的关键突破点。

数字员工3.0需要强算法。数字员工3.0应用涉及多任务、多时效等特点，单个模型能力并不能覆盖需求，因此，在应用中需要充分发挥金融领域数据优势和不同类型模型的优势，大小协同，博采众长，融合应用。但目前构建多维度大模型矩阵和大小模型协作模式，业界尚未形成相关方法，需要进一步提炼形成全面、灵活、高效的人工智能模型应用方法论。

数字员工3.0需要高质效。数字员工在银行的深化应用，亟需探索形成一套面向银行业的高标准、低门槛、共享共建的应用模式，实现数字员工批量化组装、高性能运行。数字员工3.0是综合型智能应用，一是研发强调低门槛、敏捷化、贴近业务，需要将零散的数据准备、模型训练、技能研发、数字员工组装等研发工具链进行有效串联，形成低门槛的数据–智能–应用三链融合的敏捷研发能力，同时在实践中，需要形成

技术转变成金融行业生产力的范式解决方案，提升研发和赋能质效；二是应用强调共享复用，为更好达到“站在巨人肩膀上”上的应用效果，需要建立一种分层共享共建的新型研发模式，依托同一底座，在进行个性化应用的同时，确保各项研发成果之间的有机共享，共性能力提升都能带动整体赋能水平的提升，避免重复造轮子。

2.1.3 管理挑战：数字员工尚未形成体系性的身份管理机制

数字员工本质上仍是基于AI算法和编程语言设计的IT程序，缺乏人类的情感和意识，这使得对其施加人格化管理变得复杂。同时，现有的人力资源管理体系是面向人类社会建立的，由于数字员工的行为工作模式、责任归属、培训升级等需求，与人类员工截然不同，现有体系很难直接应用于数字员工。

基于上述问题，业界已开展数字员工人格化视角的管理体系研究，但数字员工的身份管理是一个跨学科、多领域协同的系统性工程，目前业界整体仍处于起步试点阶段，缺少体系化的管理机制和成熟参考案例，特别在数字员工的独立身份、分层管理、量化评价等方面亟需体系化厘清和突破。

一是需要解决数字员工独立身份的问题。目前，业界虽然开展数字员工的形象、名称、岗位、性别等人格化属性设计，但更多是便于宣传和加深用户记忆，如何将数字员工真正融入到企业人力资源体系，需要在制度、系统等层面进行配套支持并明确部门分工、岗位设置、权限管控，目前此类实践业界较少，无体系化参考案例。

二是需要解决数字员工分层管理的问题。一方面，随着基于大模型的数字员工3.0应用兴起，目前业界出现较多数字员工概念，如数字员工、数字助手、智能副驾、智能助理等，企业在构建数字员工管理体系时，需要科学厘清不同数字员工概念关系，形成统一管理话术。另一方面，数字员工按照什么维度设立，和岗位、具体工作任务间的关系怎么建立精细化管控，仍有待实践明确。

三是需要解决数字员工评价体系构建的问题。传统数字员工应用普遍围绕劳动密集型场景建设，聚焦机器换人或智能增效指标进行评价。

随着大模型技术赋能复杂的智力密集型场景，需要对数字员工评价体系进行升级。

2.1.4 安全挑战：数字员工全生命周期仍面临安全风险隐患

金融业务对于服务稳定、安全可靠、严谨审慎等方面有着高要求，数字员工的高安全性与高可靠性是金融领域应用准入的先决条件。从数字员工全生命周期来看，目前在数据的隐私保护、模型的价值观对齐、应用的抗攻击等方面仍面临安全风险。

一是数据隐私安全风险。一方面，训练大模型需要海量数据，如敏感数据未经充分脱敏，数字员工应用中存在泄露隐私数据的隐患，这就要求在数据收集和处理过程中，必须采取严格的隐私保护措施，以保障数据安全。另一方面，数字员工应用可能涉及客户信息、交易数据等敏感数据的调用和处理，存在数据泄露风险，因此，企业在应用数字员工时，必须采取严格的功能权限控制、数据访问控制和加密措施。

二是模型价值对齐风险。与传统的机器学习方法相比，大模型具有更丰富的多样性和随机性，也存在模型幻觉、涉政涉敏等算法内生风险，对数字员工的安全、公平和可信度产生影响。为确保数字员工能够生成积极、正向和合规的内容，必须在算法设计层面采取措施，从智能源头上植入正确、合理的价值观。

三是应用攻击风险。数字员工存在生成内容不合规隐患，需要对输入请求和输出合成内容进行审核，确保应用内容安全。同时，黑客可能会利用数字员工作为跳板，进一步入侵银行内的其他系统，造成更广泛的数据泄露和业务流程中断，因此，企业需要建立强大的网络安全防护体系，定期进行安全审计和漏洞扫描，确保数字员工的网络安全。

2.2 数字员工3.0架构蓝图

聚焦上述建设挑战，银行机构应着力于应用、技术、管理与安全四大领域，按照“全域场景赋能、全栈技术融合、全维人格纳管、全辖安全防护”目标，打造面向数字金融的数字员工3.0体系，实现数字员工高质量、规模化、精品化、全链路的应用建设。

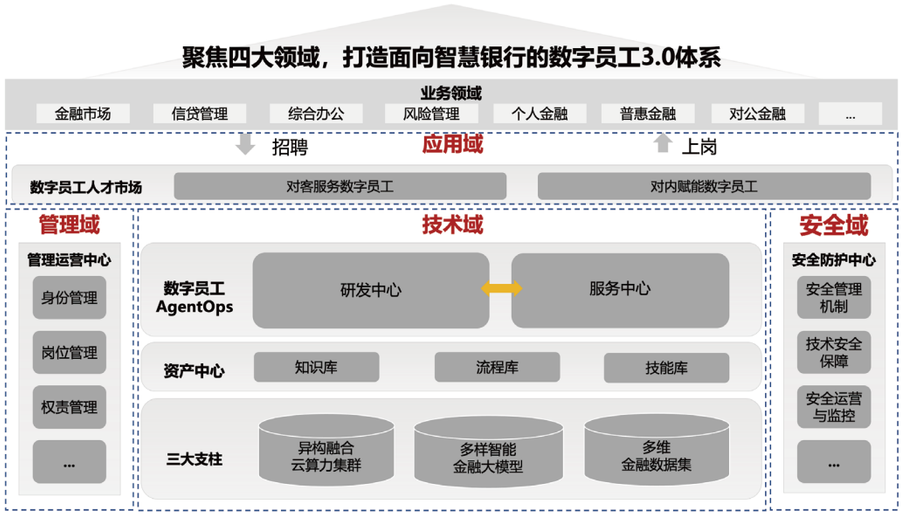


图5：数字员工3.0架构蓝图

2.2.1全域场景赋能，构建良性生态

为更好实现数字员工3.0的价值最大化，按照“方法先行、全域推广、生态共建”的思路，推进银行各业务领域的高质量赋能。

一是建立一套高价值场景挖掘和落地方法论，有效发掘并识别数字员工的高价值应用，发现堵点、挖掘爆款、重塑流程，指导业务应用。

二是实现数字员工在银行各个业务领域的端到端、规模化创新应用。对外，打造统一的对客服务数字员工，为交易查询、产品咨询、获客活客、客服答疑、辅助老年群体无障碍金融服务等众多场景提供沉浸式交互体验，进一步促进金融服务的便利性和可得性，为建设人民满意银行提供新动能。对内，建立差异化的专业业务处理的对内赋能数字员工，提升各专业业务办理和日常办公的工作质效。

三是打造开放共赢的数字员工人才市场，让业务更好触达各类数字员工能力和应用最佳实践案例，支持通过人格化的招聘、上岗等操作，实现数字员工快速赋能应用，助力增强企业的数字基因灵活创新活力，形成良性生态。

2.2.2全栈技术融合，打造全能基座

为打造百模千态的数字员工，数字员工3.0需要支持多项工作能力的融合应用，因此在技术上，整体采用全栈技术融合模式，按照“三大支柱、一条产线、全量资产”的建设思路，融汇贯通各类人工智能技术，全面满足数字员工研发运行技术支撑。

一是异构融合，夯实人工智能三大支柱。数字员工依赖的算力、算法、数据呈现多元异构特性，为保障能力的统一供给，按照云数智融合架构，构建统一的AI云原生底座，融合异构算力、异构算法、多模数据，实现AI软硬件基础设施的标准化供给，提升数字员工3.0的整体智能化工艺水平。

二是研运一体，打造数字员工一体化产线。研发态，打造研发高效的生产中心，封装数-智-用三链融合的敏捷研发能力，建立以智能体为核心的数字员工组装流水线，高效满足全领域数字员工生产。运行态，建立拟人逼真、统一标准的数字员工服务中心，实现异构智能服务的统一标准化，沉淀丰富多样的数字员工技能。

三是共享共建，建设统一纳管的资产中心。实现数字员工相关的知识、技能、工作流程的统一纳管，形成数字员工技能研发、组装的统一“零配件供应中心”。

2.2.3全维人格纳管，塑造身份体系

将数字员工作为银行机构员工体系的一部分，纳入全行人力资源管理体系进行一体化管理。在此基础上，一是参考人类员工管理模式，结合数字员工自身特点，建立针对性的管理机制和配套管理系统，实现数字员工人格化管理；二是科学设岗，从对客服务和对内赋能两方面，建立数字员工的分层分类体系，明确分工、岗位、权限；三是创新数字员

工效能评价，支持持续检验和提升其工作表现，充分挖掘并提升其工作价值。

2.2.4全辖安全防护，确保合规运营

数字员工应用的安全性与可靠性是金融应用赋能红线，不容有失。围绕数字员工全生命周期，本文建议从安全管理、安全技术、安全运营三个方向体系化建立金融数字员工安全合规能力，保障数字员工业务场景可控可用。

一是做牢安全管理。围绕数字员工生命周期的各类风险，首先，建立安全评估、安全监测、安全事件应急处置和违法违规处置等安全责任落实规范、流程，指导实践工作。其次，建立技术业务组成的数字员工安全运营团队，建立数字员工协同安全运营机制，明确各方职责工作。最后，建立数字员工安全防控的常态化安全培训，筑牢员工安全意识，强化应对能力。

二是做精安全技术。聚焦数据安全、模型安全、应用安全三大环节，通过加强采、洗、管、用等环节的数据安全性、完整性、隐私性，强化模型输出的安全性和可追溯性，构建应用输入输出内容审核能力，并建立安全防火墙机制，形成全域安全防控能力。同时，将数字员工安全检测纳入银行的红蓝攻防体系，具备常态化的数字员工应用安全攻防演练能力和安全测评整改能力，以攻验防，以攻促防，持续强化数字员工安全能力。

三是做好安全运营。通过常态化配套快速定位问题根源、制定执行处置方案、实施效果跟踪反馈三种安全问题解决措施，建立“早发现、早处置”的风险防控体系，形成高效、可靠的问题处置闭环机制，提升数字员工的安全性和可靠性，为企业数字化转型提供坚实的安全保障。

三.应用篇：
全域场景价值赋能，重塑应用百花齐放

3.1 数字员工3.0的价值场景识别

据国际数据公司IDC（International Data Corporation）预测，到2025年，超过80%的银行将建设和应用数字员工，承担90%的客服和业务咨询等服务。并随着生成式人工智能技术日益成熟，数字员工能看懂文字、听懂语言、做懂业务将成为趋势，胜任工作范围将逐步从简单重复性工作演进到决策类工作。

工商银行基于业务科技融合的实践经验，提炼出一套两阶段六步骤的数字员工业务赋能方法论，旨在指导数字员工3.0的金融业务场景高价值挖掘和规模化实施。阶段一聚焦于场景挖掘，通过深入业务一线，从岗位全旅程出发，感受真场景，理解真痛点，形成全链路赋能场景地图；阶段二聚焦于场景建设，业务深度介入方案设计、数据梳理、运营迭代，让业务人员能更直观、专业地对未来工作流进行重塑，确保数字员工3.0应用成效。

图6：两阶六步数字员工建设方法论

3.1.1 场景挖掘：科技主动前移业务一线

1、场景分析：一个原则，三种方法

“一个原则”：数字员工的应用场景挖掘必须坚持一个核心原则，始终将业务价值的实现作为首要目标，**以岗位为中心，打造数字员工实体能力，**以确保数字员工部署与业务实际需要紧密衔接。

“三种方法”：围绕价值目标，从战略分解、业务流程、行业实践三个角度识别应用机会点，绘制全场景赋能地图。

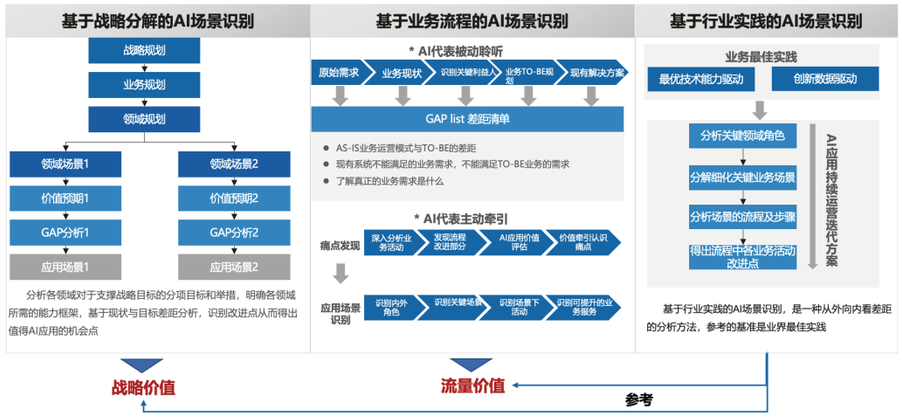


图7：三种挖掘数字员工高价值场景方法

一是自顶而下基于战略目标分解进行识别。战略规划为企业中长期发展指明方向，明确价值目标。各部门应针对战略细化目标并制定支持战略的具体措施，并通过衡量现有能力与战略目标之间的差距，识别改进和应用数字员工的场景方向。该方法包括KPI分解、业务痛点收集、现状目标差距分析、数字员工赋能方向映射四个步骤。

二是自底而上基于业务流程进行识别。该方法的核心在于识别业务流程中的痛点，有被动聆听和主动牵引两种方式。通过科技团队被动聆听业务团队需求以识别差距，以及科技团队主动牵引，利用新技术场景规划经验来发现业务流程的优化潜力，进而评估数字员工的高价值应用场景。该方法包括识别角色、识别关键场景、识别工作流、识别业务服务四个步骤。

三是从外向内基于行业实践进行识别。通过借鉴行业最佳实践并与自身现状对比，从外部视角审视并指导业务发力点的识别。无论是技术驱动还是业务创新，企业都能借助外部标杆发现并弥补自身的短板。

2、地图绘制：三个阶段，两大价值

基于上述方法，将业务部门的需求汇总后可完成场景地图的绘制。建议从全局视角落地应用价值最大化出发，**分析事前-事中-事后三阶段的用户全旅程，**归纳人员关键特征，分析形成核心痛点，以便找到真用户、真入口、真场景。

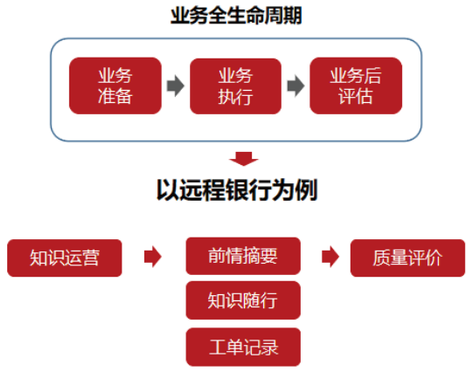


图8：绘制全场景赋能地图示例

绘制全场景赋能地图并不意味着所有场景都需要立即开发。鉴于不同场景的实现周期和复杂性差异，银行应根据**业务价值度、用户受众面两大价值维度，**将各业务应用场景进行划分，据此确定近期和中远期实施的相关业务应用场景，分阶段有序推进业务场景的智能化建设。

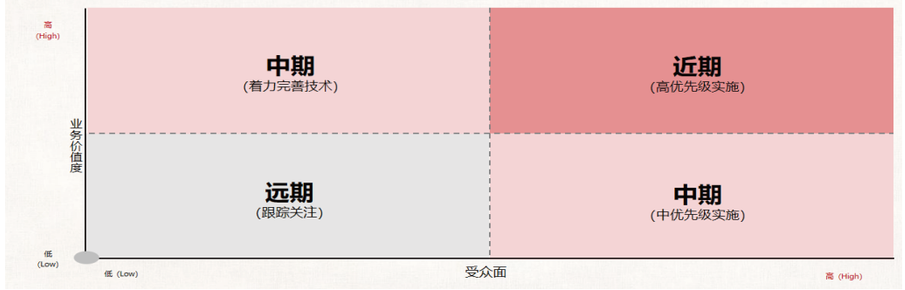


图9：数字员工应用场景选择二维象限法

3.1.2 场景落地：业务深度介入开发运营

1、方案规划：需求原型更直观

业务团队应积极介入原型设计，通过对已有应用的充分体验，设计出端到端业务模式的新原型。科技团队则通过编写交互式对话脚本来定义系统功能，并梳理所需的业务与数据服务。

2、数据梳理：知识运营更专业

业务团队提供高质量的范例数据，科技团队则利用数据合成技术扩大数据规模，同时提供智能标注工具，结合自动标注和人工复核，大幅提升

数据准备效率，高效构建业务知识体系。

3、研发部署：研发扩展更灵活

业务团队能够自助组装场景任务工作流，科技团队快速响应需求变化，实现敏捷研发。基于对话式需求脚本，科技团队设计出可复用的智能化服务，支持业务流程的灵活组合。

4、运营反馈：落地闭环更高效

业务团队通过多轮试用提供反馈，协同进行负例分析，并及时更新知识库以提升大模型的认知能力。科技团队遵循“业务体验友好，埋点精细化”的原则，实现全过程埋点，加速数据回流，以实现及时调优和深度融合协作运营。

3.2 数字员工3.0的典型应用示例

金融作为信息与知识密集型行业，随着传统人工智能领域逐步成熟，以大模型为代表的生成式AI技术的快速崛起，**让每个岗位配备专属的智能助手，每位员工都能拥有自己的数字分身，从而建立自然语言等全模态交互、人机协同的新业务模式，是大势所趋。**目前，银行机构正朝着“一岗一助手，一人一分身”的数字员工3.0方向发力。

值得关注的是，国家高度重视大模型应用安全，国家网信办《生成式人工智能服务管理暂行办法》明确“利用人工智能生成的内容应当体现社会主义核心价值观”，**遵循监管审慎要求，目前以大模型为核心的数字员工3.0相关场景需向网信办和行业监管部门报批，备案通过后方能对客服务。**

为确保技术应用的合规性与安全性，目前，数字员工3.0在银行业当前主要应用于辅助对客服务、内部赋能两大领域，通过重塑业务流程与服务模式，提升客户体验与运营效率。

3.2.1 对客辅助，质效提升的新动能

1、远程银行座席助手

（1）场景描述

远程银行作为银行业线上客户服务的重要渠道，是连接银行与客户的重要桥梁，在为客户提供便捷线上金融服务的同时，人工客服面临着工作强度大、处理和响应时间瓶颈等诸多痛点。如对座席人员业务能力要求高，针对客户多样化的问题，需要在知识库中的数十万条业务知识中搜索寻找对应答案进行解答；如转接电话体验不足，转接座席之间沟通时客户需要等待，转接后客户需要重复沟通前序问题；事后工单登记复杂，不同业务工单记录格式及侧重不同，易出现信息遗漏、错记问题。

（2）技术方案

工商银行聚焦现有远程银行客户服务的业务全流程和业务痛点，通过数字员工辅助方式重塑远程客户服务业务全流程，围绕座席通话前的了解诉求、通话中的解答问题、通话后的记录工单，分别打造转接前情摘要、知识随行、语音实时监测、工单自动填写等助手能力，实现实时通话向座席人员主动推送答复话术、知识、情绪提醒等能力。

一是在对客服务通话前环节，借助大模型语义理解和内容生成能力，通过实时总结客户与座席对话，生成前序座席与客户沟通内容的主旨摘要，转接座席在接听电话之前就提前掌握客户业务诉求，有效降低客户等待与重复沟通成本，提升客户体验。

二是在通话中环节，借助大模型知识溯源、语音情绪识别等技术实现客户诉求预判、语音实时监测、知识随行等功能。基于客户全渠道交互行为数据，精准判断客户意图，为座席提前预判客户在业务痛点、业务断点、增值服务等方面的诉求；通过构建情绪监测、敏感词监测等智能监测模型，实现全量全过程通话语音智能监测、异常通话实时干预；利用大模型语义理解、向量检索等能力，实时总结客户与座席对话，动态判断客户意图，自动进行知识检索，并实时推送给座席，省去座席手动知识检索工作，提升服务效率与业务解答精准度，提高客户远程服务体验。

三是在通话后环节，借助大模型理解和生成能力，基于客户与座席沟通情况和客户诉求，根据工单登记要求，实现工单模板自动选择、工单类别自动勾选、工单内容自动生成，座席仅需修改和复核即可成单，有效压降座席工单登记时长及信息要素错记漏记情况，切实提升座席工作质效。

（3）应用成效

远程银行座席助手重塑该群体工作模式，助力人工座席全面实现数字化“武装”，提升覆盖全渠道、全流程的客户服务能力，打造更高效、更有温度的服务体验。其中情绪、敏感词等语音实时监测，有效辅助人工座席直观感知客户沟通状态，提升服务风险意识；转接前情摘要、知识随行、知识工单的能力，大幅提升座席人员质效，在账户受控等重点场景实现使用座席通话时长压降显著。

2、网点员工智能助手

（1）场景描述

在运行管理领域，网点作为数字化转型最小作战单位，存在基层业务人员复杂业务办理难、新业务流程不熟悉、自助终端菜单多功能深操作不便等痛点问题。例如，复杂业务不会办，在日常业务处理中，新员工面对外汇等复杂问题，以及老员工处理不常见业务时，往往不能即时获得有效解答，这不仅影响业务处理效率，也影响客户体验。自助终端操作复杂，导致客户不会操作，经常需要现场客服经理辅助办理，这导致客户自助办理占用厅堂资源多，同时一定程度影响客户体验和效率。

（2）技术方案

工商银行聚焦网点日常服务运营中遇到的制度查询不便、复杂业务处理困难、客户体验不足等痛点，打造集业务问答、外文翻译、客户菜单导航等三大功能为一体的网点智能助手，构建网点智能化对客服务新模式。

一是业务问答，基于大模型技术提供对话式搜索体验，能够深度理解用户搜索意图，结合多轮对话能力，针对复杂的业务办理、专业术语解释以及新业务流程熟悉等问题，智能化地生成操作流程和术语解释，大幅节省制度查找时间，提升网点员工的业务处理效率和服务质量。

二是外文翻译功能，利用大模型翻译能力提供英、德、法等多语言在线翻译能力，解决网点面向外籍客户、处理外汇业务等场景下外文翻译难、翻译不准的痛点问题。

三是客户菜单导航，通过大模型技术，客户可语音与助手对话，调控智能终端服务，支持业务菜单轻松找、账户数据快速查、简单业务便捷办等场景，解决客户到店柜面排队久、自助服务操作难的痛点，为客户提供便捷、易用的金融服务体验。

（3）应用成效

网点员工智能助手面向客服经理、客户经理、运营主管、网点负责人等各岗位20余万一线员工，切实为网点人员赋能减负。其中网点业务问答，以溯源的方式形成可信的问答知识，回答网点员工业务操作、规章制度等问题，节省制度查找时间，提升网点员工业务处理效率与服务质量。外文翻译提供在线文本翻译功能，并支持输入内容语种识别，帮助网点员工更好地应对涉外业务场景。客户菜单导航有效提升客户业务办理效率，缩短网点智能终端用户平均等待时长。

3、对公营销智能助手

（1）场景描述

做好对公业务是银行服务实体经济的重要工作之一，服务好对公客户、及时获客、活客是一线营销人员的职责，然而一线营销人员也面临着对公产品业务知识全面掌握难、获客方式传统、文案工作耗时长、经营指标数据获取不便捷等工作痛点。如对公客户根据自身业务需要，提出不同的金融服务复杂需求时，客户经理需要检索对公产品的介绍或产品对应的案例，找出适合当前客户业务场景的产品进行推荐。因对公涉及的产品类型较多，产品本身也较为复杂，在该服务过程中，对客户经

理的对公业务专业知识储备要求较高，且客户经理检索适合客户的产品时间较长，整体服务效率较低，影响客户的体验感。

（2）技术方案

工商银行聚焦对公客户服务日常工作痛点，利用大模型“对话式”交互、智能检索、数据分析等技术能力，融合小模型、大数据分析成果，以对公营销通平台为统一入口，打造对公营销通“数字专家”新模式，支持一线营销人员一站式检索产品知识，获取营销机会，查询营销进展，定位系统功能联动业务办理等，提升发现、挖掘、跟进、转化客户服务和管理能力，提高对公客户营销服务质效。

一是利用大模型知识检索技术构建结算金融智能顾问能力，提供交互式、可溯源的对公产品推荐及产品知识检索咨询服务，依托数字专家“快速、准确、全天候”的优势，解决一线营销人员“查找资料困难、不会办”的痛点问题，为营销减负，为基层赋能。

二是利用ChatBI技术打造对公数据交互式分析能力，结合数据中台沉淀的近千个对公营销数据指标，提供自然语言交互式的数据查询服务，更有针对性地服务好用户。

（3）应用成效

对公营销智能助手面向全行10万+对公营销人员，与传统的“人工检索”、“专业分析师分析数据”模式相比，对公营销智能助手应用大模型技术提供“智能问答”、“对话式查数”功能，大幅提升对客服务效率。自应用以来，对公结现产品营销时长压降明显，产品签约测试上线准备时间大幅缩短。

4、网络金融运营助手

（1）场景描述

随着互联网经济的蓬勃发展，线上渠道的运营管理日益重要，高质量的运营工作不仅有助于业务人员达成特定的业务目标，同时也是用户获取权益及产品信息的重要途径之一。当前，银行业面临用户属性多

样、产品逻辑复杂以及客户接触渠道多元化等挑战，这要求业务人员必须具备数据分析、灵活运用内部运营工具、制作宣传海报及宣传文档等多样综合技能，运营工作综合性强、难度大。同时，鉴于互联网服务水平存在地域性差异，将企业内优秀的运营工作经验有效地在各分支机构之间进行传播，对于提升整体运营服务质量及用户服务体验也尤为必要。

（2）技术方案

工商银行围绕解决运营过程中客群圈选和路径决策困难，运营方案缺少大数据分析支持、内容物料准备耗时长、效果跟进缺少个性化工具等业务痛点，依托大模型技术打造网络金融运营助手，在运营工作各个环节提供智能决策、效果分析、总结规划等能力，提升运营人员工作效率，为手机银行等互联网用户提供更适配的个性化运营方案、触达内容，从而提升银行运营工作效果，加速客户服务质效提升。

一是在客群圈选环节，利用大模型+智能中枢应用模式，大模型调用传统小模型完成客群圈选工作。运营人员通过“对话”交互模式输入运营目标，运营助手将结合当前运营目标决策建群方式与路径，并解释说明推荐原因，解决一线人员建群方式选择难点，降低工具学习成本。

二是在活动部署环节，综合利用知识检索、智能中枢、文档编写等大模型应用范式，整合历史运营活动经验，协助运营人员串联部署运营工作中各个环节，为用户推荐权益方案、触客方式，并完成触客内容撰写工作，以结果为导向实现银行内运营经验共享，提升运营工作部署效率。

三是在用数分析环节，利用ChatBI打造自然语言交互式数据分析能力，赋能运营人员分析地区、客户群体、运用活动转化结果、业务表现等多方面数据诉求，降低运营人员用数难度，明确数据挖掘工作方向。

（3）应用成效

网络金融运营助手，辅助工作人员精准开展运营工作，为运营活动提供客户精准触达能力。模型通过对用户的全生命周期与使用习惯进行

数字化沉淀与加工，将用户消费习惯反哺到运营工作中，实现数据对业务的即时赋能和数据驱动智能化决策，有效提升客户营销服务的质效。

5、投诉处理智能助手

（1）场景描述

银行业高度重视消费者权益保护工作，把客户投诉处理工作做的好不好作为践行金融工作政治性、人民性的重要检验标准。银行在客户投诉处理过程中，还面临着一些困难和痛点。例如，银行受理客户投诉分派处理时，一旦工单首次分派不准确很容易引发处理时间较长等情况，影响客户服务体验，甚至导致客户再次进行投诉。再如，员工投诉处理工作量较大，投诉处理过程中需逐一联系客户并撰写处理报告，耗费大量时间与精力，且人工撰写报告容易出现信息遗漏等问题。

（2）技术方案

工商银行利用人工智能大模型技术对投诉处理流程进行重塑，打造集问题智能分类、知识智能检索、报告智能撰写三大功能为一体的投诉处理智能助手，辅助员工提升对客服务能力，为基层员工减负、为投诉处理赋能，推动客户投诉处理数字化、智能化转型。

一是联系客户前，对于外部机构转办的投诉，借助大模型语义理解能力准确判断客户意图，精准进行问题分类，推动相关投诉根据分类情况准确分派至相应分支机构，有助于相关纠纷得到快速受理。

二是联系客户时，借助人工智能技术对员工通话过程的情绪、语速、敏感词等进行实时监测，利用大模型语义理解、向量检索等能力，动态监测客户反映的问题，实时进行知识检索，并及时推送给相关员工，提升服务效率与业务解答准确率，不断提升客户体验。

三是联系客户后，借助大模型理解和生成能力，通过实时跟踪客户与座席对话，生成与客户沟通情况的相关总结，员工仅需要简单修改和复核即可形成投诉处理报告，减少报告撰写时长，同时解决信息错记漏

记的问题，有效为员工减轻工作量。

（3）应用成效

投诉处理智能助手面向总行、一级分行、二级分行、支行和网点等各层级机构的投诉处理人员，有效辅助员工提升对客服务能力。其中问题智能分类，通过对外部机构转办投诉准确进行识别分类，推动纠纷快速受理，有利于提升客户满意度，有助于提高投诉监测质效与投诉管理水平。知识智能检索，帮助员工更加快速、规范化解纠纷，有助于及时解决客户业务诉求，提升基层分支机构投诉处理能力与处理质效。报告智能撰写，有效减轻工单处理压力、显著提升投诉处理效率、真实还原纠纷处理过程。

3.2.2 对内赋能，辅助决策的新帮手

1、金融市场交易助手

（1）场景描述

金融市场外汇交易是企业重要的金融工具，企业可以通过外汇衍生品如远期合约、期权等工具来对冲货币风险，实现套期保值。这有助于企业降低因汇率波动带来的不确定性，保护企业免受不利汇率变动的影响。

银行可以为客户在银行间市场进行风险对冲，其中询价交易模式可以为企业客户提供更好的服务和优质的价格，因此询价交易成为众多企业客户选择外汇业务的首选交易渠道。传统银行的询价交易，需要先线下电话沟通，再线上流审批、报价，存在交易效率低、体验差等痛点，难以快速为企业客户锁定市场报价。

（2）技术方案

工商银行打造金融市场交易助手ChatDealing，创新交互式智能询价的解决方案，以对话框为统一入口，使用大模型自动识别对话信息，完成交易要素提取、录入、风险识别等交易全流程，通过群聊交互对话

完成客户背景审查、对话交易、知识问答、菜单导航、询价进度等关键流程，实现询价交易全流程效率提升，有效解决以往总分行人工询价存在的交易效率低、体验差等痛点问题。

一是对话式体验，支持支行、分行、总行多方交易员在同一交易对话框中通过对话完成价格磋商，运用大模型识别用户意图，并智能识别交易话术，生成交易意向单达成交易。

二是数字人实时审计和质检，防范交易、操作风险。在交易对话全过程中，ChatDealing自动提取关键要素，完成反洗钱检查、价格偏离度控制、客户背景审查等，满足事前事中的风险控制要求，节省客户经理跨系统操作的时间。

三是智能询价助手引导式辅助业务办理。ChatDealing具备客户画像生成、价格行情实时查询、报告辅助编写、智能报价等能力，为交易决策提供技术支撑，真正达到沟通在线、业务在线、风控在线的组织状态。

（3）应用成效

金融市场交易助手ChatDealing通过AI重塑业务模式，实现支行、分行、总行多方交易员在同一交易对话框中通过对话完成价格磋商，运用大模型智能识别交易话术，生成交易意向单达成交易，改变原有先通过线下沟通，再流程逐级询价、报价的业务模式。这是AI介入业务开展的一种尝试，重塑业务流程，大幅缩短代客询价交易时间，有效提升工商银行报价的市场竞争力。目前已服务全行2万余名交易员和客户经理，覆盖即期结售汇、远期结售汇、即期外汇、远期外汇等业务产品，对客交易效率提升显著。

2、对公信贷风控助手

（1）场景描述

在信贷业务中，信贷客户经理、审贷员等业务人员涉及尽调报告、

审查报告、贷后检查报告等大量文档编写工作。传统的报告编写主要依赖于专业人员手工操作，存在以下具体痛点：一是报告编写耗时，业务人员需要花费大量时间收集、整理和分析内外部数据信息，再将其转化为一份详尽的报告。二是信贷风险分析受人为因素影响大，不同信贷人员由于其经验、专业水平、风险偏好等差异，对风险的评估判断会存在不同的标准和结果。

（2）技术方案

工商银行积极探索大模型在对公信贷领域的智能化应用，围绕信贷全流程，打造集信贷制度查询、报告编写、数据分析等能力于一体的专属信贷风控助手，运用大模型在自然语言处理、逻辑推理方面的优势能力，提升业务效率和风险管理水平。

一是信贷制度查询，基于检索增强RAG技术、视频内容理解、信息抽取等技术，支持对文档类、视频类等各类信贷制度、教材的快速问答和定位，提升信息收集效率。

二是报告编写，综合利用传统NLP小模型和生成式AI大模型技术，自动抽取关键信息，应用财务数据生成财务结构分析报告初稿，按模板自动生成尽调报告初稿等文档。

三是数据分析，利用ChatBI技术，通过自然语言对话模式，自动转为查数SQL，快速生成可视化分析图表，实现便捷用数。

（3）应用成效

依托人工智能大模型对海量素材的深度理解能力，能够自动遵循既定大纲完成报告初稿的撰写，提升信贷全流程各类文档编写过程中的资料查找、数据分析、内容编写的便捷性和智能化程度。业务人员仅需对文稿进行审核和补充完善，便可完成报告的编制工作，有效提高工作效率，使业务人员从重复而繁重的流水线作业中解脱出来，转而投入到更具价值的工作中去。

3、商户审核智能助手

（1）场景描述

商户审核是银行和支付机构在开展收单业务过程中的一项重要工作，主要目的是确保商户的经营活动真实、合法，防范业务风险。然而商户审核业务存在耗时耗力的痛点，每逢营销旺季，总行、分行会接到大量的商户审核任务，对于每个商户的建档申请审核，审核人员需要审阅大量文字和图像审核资料，包括各类证件、账户证明、商户收单业务申请书、调查审批表、征信信息查询和使用授权书、商户经营影像和风险信息等。同时，结合外部信息和业务经验对商户风险进行判断，决策商户准入和管控策略，工作具有一定难度。

（2）技术方案

针对商户审批过程中需筛查核验大量文字和影像资料相关痛点，工商银行基于OCR、多模态大模型的大小模型融合技术，打造商户审批智能助手，实现实时智能生成商户预审批报告。

一是针对营业执照、商户证件等证件类照片，利用OCR模型进行精准识别，快速抓取并解析证件照上的关键信息；再与商户录入的信息进行比对，确认信息的一致性，最后生成证照比对结果。

二是针对企业经营照、门头照等，结合图片和文本相关的审核数据，使用多模态大模型对商户经营情况进行分析推断，基于多模态大模型的图片理解能力，对商户现场照片进行合规性检查，生成商户经营审核结论。

三是综合外部新闻和舆论数据，借助大模型的摘要生成能力将业务采集的法人、授权经办人等外部风险信息生成商户风险提示。

（3）应用成效

自推出商户审批智能助手以来，有效解决商户审核业务耗时耗力的痛点，降低商户审批成本，提升商户审批质效。

4、综合办公服务助手

（1）场景描述

综合办公服务是企业提高工作效率和团队协作能力的重要保障，对银行业而言亦是如此。传统的办公服务模式下，员工在使用各类办公工具开展工作时，面临着协同成本高、交互操作繁琐等痛点。例如在会议场景中，在参加国际化会议时经常需要有配套的翻译服务，以便更好理解与会各方的发言，会后也需要花费大量时间进行会议纪要的整理；例如在差旅场景中，员工在提交出差申请、预定机票酒店、填写报销单据等环节，需要花费大量的时间；又如在文档编写场景中，员工需要寻找合适的文档模板、查阅各种参考文档、拟定文档大纲等，整个过程费时费力，而写出的文档质量也参差不齐。

（2）技术方案

针对日常办公所面临的协同成本高、人工操作繁琐等痛点，工商银行以办公数字员工“工晓伴”建设为主线，以智能中枢应用范式为核心，采用大小模型协同模式，构建智能化交互新范式，为每一名员工配备专属贴身的数字化、智能化的办公助手，围绕会议、差旅、文档等典型办公场景进行重点赋能与创新进化，简化日常工作事务操作路径和时间，提升员工日常办公的质效。

一是打造智能会议。会前，通过与工晓伴对话即可完成会议预定，并与办公系统打通，实现会议通知即时发送与提醒，提升人机交互体验；会中，通过语音转写及大模型翻译能力，实现实时字幕与实时翻译，显著提升参会体验；会后，通过大模型摘要总结能力，实现会议纪要初稿智能化编写，有效提升会议效率。

二是推出智能差旅。事前，支持自然语言交互模式提交出差诉求，智能采集出差信息并提交出差申请；事中，通过工晓伴实时推送行程提醒；事后，主动提醒用户进行差旅报销，并协助收集报销所需的各项票据数据，替用户填写并完成报销。

三是建设智能文档。推出“帮我写作”功能，支持快速撰写公文、邮件、通讯稿等常见文档。同时，提供智能大纲写作模式，通过大模型生成文档大纲，并基于大纲快填充形成全文初稿，提升日常办公文档编写效率。

四是提供信息搜索，快速获取行内外资讯。对接知识检索底层技术能力，与行外互联网知识与行内网讯、规章制度等知识库对接，搜索用户目标问题，结合大模型的语言润色能力，为用户整合关键信息，组合问题答案，生成用户搜索问题的回答内容。同时，建设查人找人能力，结合知识图谱的图谱问答技术，关联用户信息，支持按姓名、统一认证号、机构、手机号、电话等多种方式找到用户，满足日常办公查人找人需要。

（3）应用成效

工晓伴依托大模型、智能体、自然语言处理等各项AI技术的综合应用，为员工提供找人、创建会议、提交出差申请、知识问答、文档辅助编写等40余项智能服务，增强数字员工在银行办公产品体系内的辨识度，助力综合办公、人力资源、财务管理等领域的数字化转型。

5、金融研究智能助手

（1）场景描述

金融研究工作是商业银行进行战略决策、谋划战略转型的重要基础，在传统的金融研究工作中，研究人员需要通过各种渠道获取大量的研究数据作为参考，再通过对海量数据分析形成相应的观点研判，并汇总输出相应的研究报告。在过程中，由于研究所依赖的信息通常较为分散，需要花费大量的时间精力进行搜索，同时编写研究报告时也面临缺少好的创作思路、成稿费时费力等痛点。

（2）技术方案

工商银行依托千亿级大模型，建设面向研究人员的金融研究智能助手，面向研究人员提供智能推荐、智能搜索、智能创作等能力，实现研究工作的全流程智能化升级，推动研究工作从信息化向智能化升级。

一是智能推荐，通过整合内外部全量研究信息和研究成果，基于大模型文本分析能力进行自动打标与分类，面向不同研究人员、不同研究方向进行智能推荐，为研究人员和管理人员提供丰富、专业、高质量的研究信息参考。

二是智能搜索，基于大模型提供对话式素材收集、问答体验，按照“精准、高效、全面、智能”标准，打造智能搜索引擎，支持传统关键词检索和自然语言语义搜索，提供快速精准的文字、图片、视频等多模态、全类型的研究数据搜索服务。

三是智能创作，应用大模型为研究人员自动生成研究报告大纲，支持灵活调整，再根据大纲自动生成研报内容初稿，并提供纠错、改病句等能力，切实提高研究报告的创作效率与编写质量。

（3）应用成效

金融研究智能助手上线后，有效赋能研究人员，实现宏观、行业、同业等多领域研究信息的智能推荐、智能搜索，以及金融研究报告的智能创作，建立起“AI+数据+研究员”的研究新范式，实现以数字化手段提升研究质效的目标。

3.3 打造开放共享的数字员工人才市场

数字员工3.0作为一种新型劳动力，重构金融行业的生产关系，催生金融机构经营模式、服务方式和决策流程新形态。需要构建一个开放、共享、共建的市场平台、运营机制，吸引技术提供者、应用开发者、业务需求用户等共同参与，共同推进数字员工3.0创新应用。

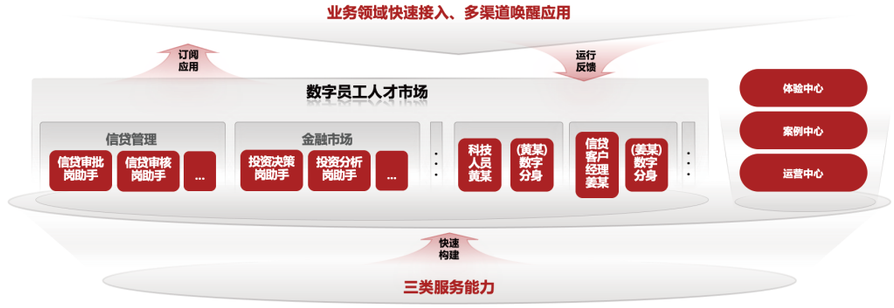


图10：数字员工人才市场框架

一是打造能力体验中心，为技术和应用者搭建桥梁，支持技术开发者分享开箱即用、类ChatGPT对话式全能力智能技术服务，激发应用开发者创新灵感。

二是打造共享共建的应用案例中心，通过分享应用案例、可视化展示等手段，实现全领域优秀应用实践案例共享借鉴。

三是建立动态反馈的运营机制，从技术、应用双视角实现数字员工人才运行监测、评价迭代，逐步推动数字员工3.0应用准入和低效退出的机制，提升应用质效。

四.技术篇：
全栈融合百模千态，建设敏捷创新工厂

4.1 技术框架：“三大支柱、一条产线、全量资产”

数字员工3.0不仅具备多项工作能力，更能通过不断学习提升自身技能，贴合匹配银行业务流程的工作任务。其“多面手”特性，已成为商业银行突破效能瓶颈的关键资源。优化数字员工的生产打造和调度配置，也因此成为实施数字员工建设的重要目标。为实现数字员工3.0的规模化推广，按照中台模式，建设技术标准化、研发便捷化、能力拟人化及资产共享化的数字员工工厂，降低开发和应用门槛。

一是技术标准化，建设算力、算法、数据“三大支柱”。通过对异构算力的融合调度、多样智能的融合应用、多维数据的融合治理，实现金融大模型基础支撑能力的标准化供给，为数字员工构建智慧大脑。

二是研发便捷化和能力拟人化，建设研运一体的“一条产线”。通过低代码/零代码的创新工厂模式，标准化生产组件，封装AI建模能力，实现敏捷化开发，降低开发门槛。服务中心作为智能枢纽，提供拟人逼真的数字员工3.0能力组件，按需组装，面向业务应用人员，提供分层分级、贴近业务应用的综合型智能化解决方案。

三是资产共享化，建设全量资产管理“资产中心”。统一管理知识、技能、流程等数字员工的各项技能和资产，通过能力的共建共享提升数字员工的业务能力，促进其持续演进。

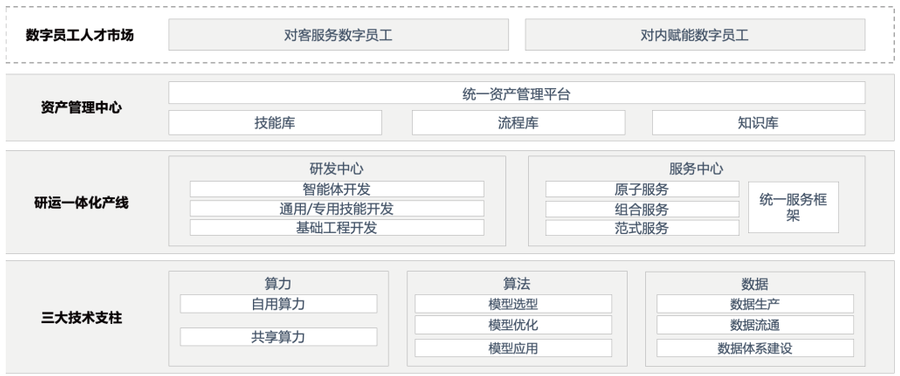


图11：数字员工技术架构

4.2 三大支柱：技术融合，夯实数字员工智慧基石

4.2.1 算力：异构算力融合，按需开展算力利用和建设

大模型作为数字员工3.0的智力基础，其参数量的激增对算力基础设施提出更高的要求，大模型全面体系化的建设需要大量资金投入和高技术门槛，各类型金融机构应结合自身发展制定基础设施发展策略。

一是对于大型机构，建议加快推进新一轮算力规划和布局，开展面向通用人工智能的大规模算力技术设施规划与建设，根据“绿色低碳、高效协同、云智融合”的思路统筹规划，构建企业级智算中心。

- **绿色低碳：**打造符合国家“双碳战略”的绿色新基建，短期内，考虑到液冷机房建设周期长，优先采用高密风冷机柜部署风冷AI算力服务器模式推进建设；中长期来看，目前，AI算力服务器随计算能力增长带来单机耗电功率快速增长，传统风冷技术难以满足制冷需求，液冷技术因其更高的热传导性能和更低的能耗成本，成为智算中心散热的必然选择。
- **高效协同：**大模型的训练和推理通常需要多卡甚至多机运行部署，需要使用高性能AI服务器、RDMA高带宽网络、多级高效存储系统等设施，组建规模在千级AI算力芯片及以上的算力集群进行大模型训练和推理，推动算网存高效协同赋能，建设高效的大模型算力集群。
- **云智融合：**硬件层面，支持IaaS弹性部署，具备云化资源池化供给能力，支持CPU、GPU、NPU、MLU等异构AI算力混合部署，形成大规模异构算力集群，支撑不同场景的AI任务算力需求；软件层面，基于PaaS容器化能力，通过云化算力调度引擎支持AI算力的池化调度、弹性伸缩和存储加速等能力，实现AI算力的统一调度，并利用算力虚拟化技术提升算力利用率；运维层面，形成资源统一纳管、统一监测、统一运营的标准化流程，支持分租户资源隔离、训练推理集群资源隔离，并建立故障快速诊断、故障预测预警、断点续训等能力，满足AI算力大规模集约化应用。

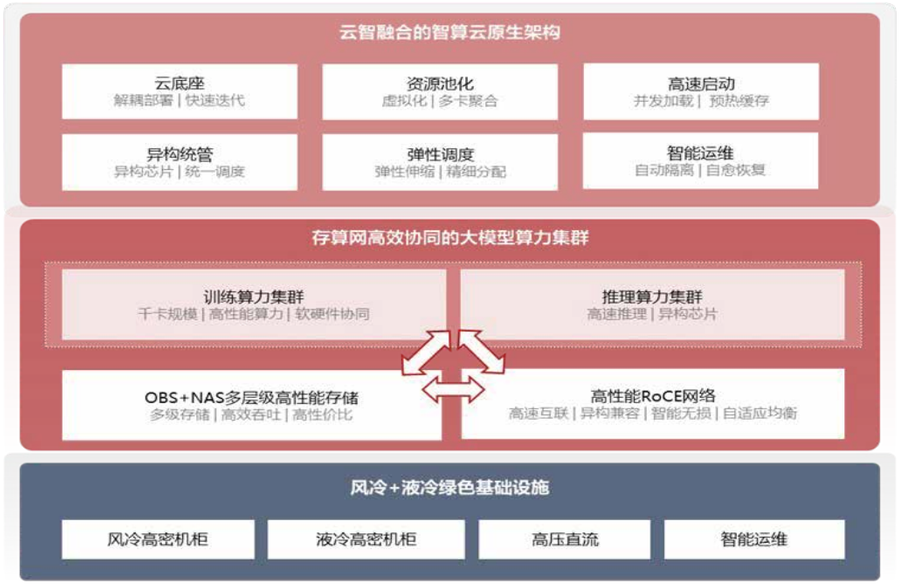


图12：大规模算力基础设施架构

二是对于中小机构，可优先建设推理小集群满足业务应用，并视金融场景适配情况建设小规模的训练资源满足模型微调需求。这种算力部署模式相对轻量，面向实际应用需求，优先支持物理机形态或PaaS小集群模式，灵活部署相关数字员工应用的AI服务能力，快速赋能。同时，轻量化设计意味着集群可以快速扩缩，可快速适应不同的工作负载和业务需求。

场景层 工程化服务套件	**网点助手**	**客服助手**	**办公助手**
模型层 大模型+RAG	**RAG平台** 向量数据库　OCR　语义搜索大模型		
	L0基础大模型		
平台层 轻量化	**AI轻量化管理平台**		
底座层 十卡~百卡	**算力**　**存储**　**网络**		

图13：轻量化算力基础设施架构

4.2.2 算法：多样智能融合，赋能数字员工生产力跃升

1、传统小模型与大模型并存共进，“选、育、用”三维发力模型能力建设

金融业务场景复杂多样，涉及多任务、多时效等要求，单一的大模型虽然知识面广，但难以全面覆盖各类应用需求。大模型和小模型各有优劣，以生成式AI为主的大模型具有“大而强”的特点，性能强大且有很好的泛化能力，但在训练部署灵活性、结果可解释性、反应速度方面尚有提升空间；以判别式AI为主的小模型具有“小而美”的特点，尽管泛化能力弱，但具有轻量级、高效率、易于部署优化等优点。

因此，在数字员工3.0的构建中，需要充分考虑大小模型的融合，通过模型选型引进、训练优化、共建应用三个维度，融合“多样智能”，建设数字员工3.0的全能算法库。

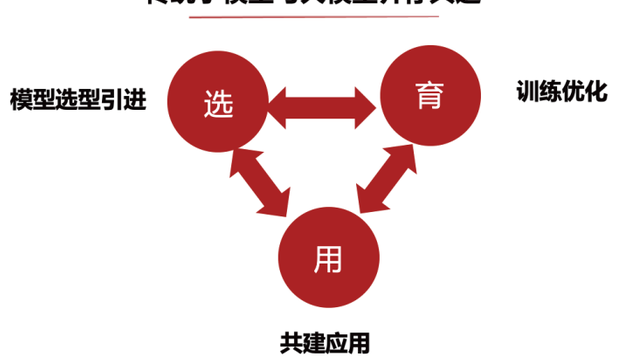


图14：模型“选、育、用”三维建设思路

2、“选”：紧跟技术发展，持续引进先进模型

2023年以来，国内外头部科技公司竞相发布大模型，形成“百模大战”的业态格局。为保持大模型能力的持续领先，银行机构应建立大模型的持续优化与科学选型机制。

一是建立金融大模型能力测评标准测。从技术能力、应用能力、安全可信能力等维度，面向通识理解和金融实际应用，建立涵盖世界通识、金融行业通识、金融专业认知、实际金融应用任务的金融大模型能力测评标准，做到能力测评有据可依。

二是持续建设完善、丰富的测评数据集。根据业务场景特点，建设覆盖文本、语音、视觉、图文多模态等模态，包含理解、记忆、仿真、问答、生成、推理、计算、调控、安全等方面的面向商业银行具体业务的金融测试集，并建立测评数据集常态化更新机制，支撑模型能力选型。

三是构建自动高效的模型选型测评流程。通过自动化评测工具，自动评测大模型，并通过大模型辅助审核方式提升测评效率。

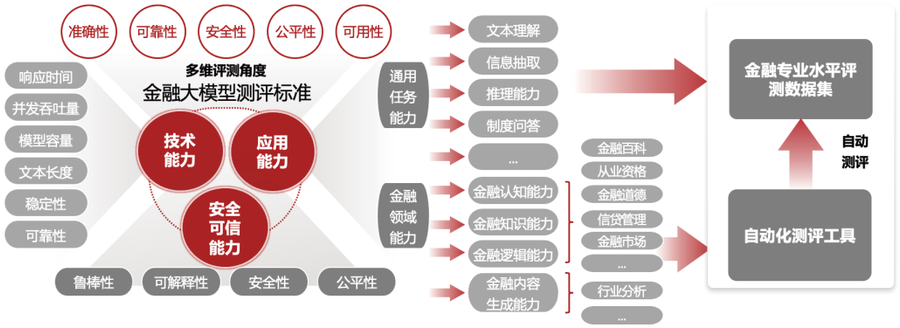


图15：大模型测评框架

3、“育”：建设多模型能力协同矩阵，持续优化模型效果

通过打造多维度大模型矩阵，形成全面、灵活、高效的模型发展路径，针对不同场景提供定制化解决方案，提升模型在金融各个细分领域的表现。以工商银行为例，构建横向多模态/多参数，纵向多层次、大小协同的金融千亿级大模型算法矩阵，满足不同场景的模型应用需求。

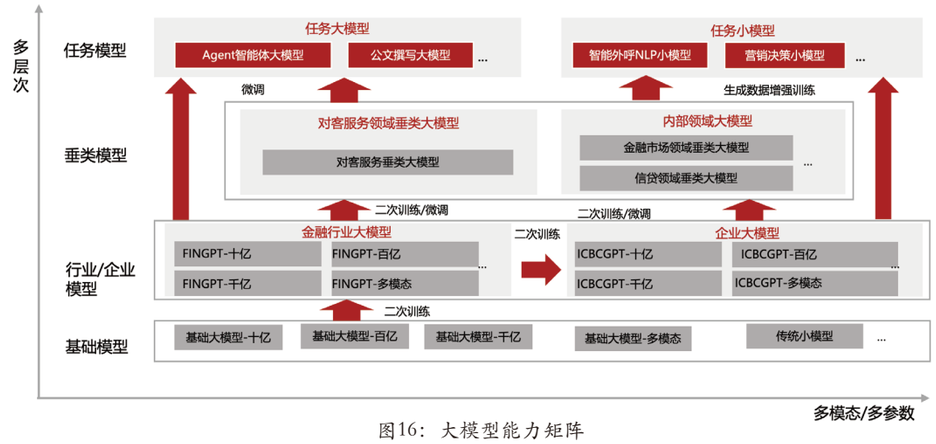


图16：大模型能力矩阵

1）纵向多层次模型

一是在通用模型基础上训练行业/企业大模型。行业/企业通用大模型要求“大而全”，即模型参数规模较大，能力多样，能够满足金融行业通识知识问答、数据分析、财报分析等涉及海量金融知识、难度较大场景的需求。训练策略方面，通过引入大量金融领域专业数据和知识，对能力优秀的基础通用大模型进行针对性二次训练，形成具有深度金融知识理解能力的行业大模型，并在此基础上融入企业特有的知识数据，训练形成企业专属大模型。

二是针对企业特定场景，在通用/行业/企业大模型基础上进行垂直领域或任务模型的构建，扩展模型的专业领域覆盖面和任务处理能力。面向特定领域或任务，模型能力要求“小而精”，即能够在特定领域和任务上提供精准、高效的服务，并能满足高并发下的推理性能要求。训练策略方面，通过模型蒸馏、微调、数据蒸馏等方案，在对客服务、金融市场等特殊的垂直领域或具体任务，打造专精的垂直领域或任务大模型，保证在专项任务效果的同时节省算力资源开销。

2）横向多模态多参数模型

针对不同的任务，需要调用不同模态、不同参数的模型满足需求。多样模型协同的数字员工才能够更好发挥场景价值。

一是以多类模型协同实现能力互补，提升整体运行效率。例如，自然语言处理大模型擅长语言理解与生成，具备问答、文案、编程等多功能，适用于金融制度/操规问答、营销话术生成、财报分析等金融文本理解/生成类场景。预测大模型专长结构化数据的聚类、分类、回归，适用于客户流失预测、资金流预测等决策分析类场景。多模态大模型融合文本、图像等数据，理解跨模态信息，适用于包含大量电子影像文档的信贷智能审核、远程银行通话语音质检等场景。

二是根据应用场景需求，选择相应参数规模的大模型。传统小模型适用于需要强解释性的场景，十亿、百亿级参数满足低时延、低成本推理需求，适用于知识问答、摘要生成、数据分析等场景。千亿级参数大模型，能力较强，适用于复杂分析任务，同时可生成合成数据供其他模型做数据蒸馏增强训练。

银行机构应根据自身情况制定响应的模型能力建设策略。对于数据充足、场景丰富、技术能力强的大型银行，可参考建设全体系模型能力。对于中小银行，短期内可采用金融知识库+基础通用大模型融合应用模式，快速满足知识问答等通用场景应用需求，中长期，随金融业务数据积累、技术应用能力增强，可考虑针对特定领域进行大模型的二次训练或微调，进一步适配场景广度和深度。

4、“用”：降低模型使用门槛，打造协同生态

随着大模型技术逐步成熟，大模型逐渐进入规模化应用阶段。为让大模型能够更好地适配场景需求，应从模型推荐、高效研发、易学易会等方面降低使用门槛，打造协同生态。

一是按场景进行模型的适配和推荐。在已建成大模型矩阵的基础上，建设模型调控引擎，根据各场景的不同需求，推荐合适的大模型。同时，提供包括OCR、语音、知识检索、文档生成、数字人等不同AI能力的沉浸式体验，从拟人化组合成人的视角，促进应用。

二是建设开放的高效微调流水线。面向差异化场景，应用推广中逐步开放大模型微调能力，综合考虑算力消耗和场景价值，建议优先利用

LoRA等高效微调技术构建支持文本、图文多模态等大模型建模流水线，加强对特定场景的模型适配能力，降低建模资源整体消耗。同时构建高效的推理方案，实现同一基座大模型挂载多个LoRA模型的高效推理，支撑长尾场景高效推理。值得一提的是，LoRA是一种高效的微调方法，它通过在预训练的大模型中引入少量的低秩网络层来实现。这些额外的层具有远小于原始模型参数量的参数，允许模型在保持大部分预训练权重固定的同时，通过训练这些新增的参数来适应特定领域的数据。通过该模式，LoRA可以将需要训练的参数数量减少到原模型的千分之几，大幅度减少所需的计算资源和内存占用，使得对大模型的微调变得更加可行和经济。

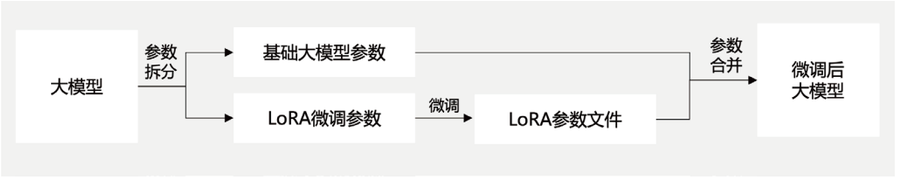


图17：LoRA微调原理图

三是构建易学易会的大模型知识体系。围绕模型接入、提示词优化、模型选择、模型微调、模型上线等常见问题构建完整的知识体系，并搭建自动化的选择和问答工具，降低大模型使用门槛。

4.2.3 数据：全模数据融合，激活数字员工认知核心

商业银行数据呈现形态多模化、质量多维化、内容多元化、来源多样化等特点。为夯实人工智能的数据基础，一是建立企业级金融数据知识体系，对内丰富模型训练数据，对外建立金融专项知识库，内外协同，提升数据的可获得性和利用性。二是建立智能化的非结构化数据治理能力，在结构化数据治理的基础上，进一步盘活海量非结构化数据资产。

1、“5+1”架构数据知识体系，增强数据的可获得性和利用性

图18：5+1数据知识体系

为更好积累沉淀高质量、多维度、海量的金融数据，各银行机构可从“基础-行业-企业-领域-任务”五层模型体系及外挂知识库增强诉求入手，配套建立“5+1”金融大模型知识工程体系，提供各类知识分层管理、新旧迭代、内容可信监测等能力，确保数据的多样性、通用性和准确性。

一是建立世界-行业-企业-领域-任务五层知识架构，灵活纳管全领域、全模态金融数据。同时，分层训练对应类型的大模型，通过二次训练+微调实现金融知识高效继承复用，增强各类模型的金融认知能力。其中，世界层，集成全球资讯、百科等通用知识，提供宏观视角；

行业层，专注金融行业数据，如监管政策、企业财报、投研分析等，提供行业视角认知；企业层，细化至银行内公共数据，包括资讯、公文、业务知识，提供企业视角统一认知；领域层，针对金融具体专业业务领域沉淀专业知识，其中，建议针对对客服务知识进行统一归口建设，避免二义性；任务层，针对具体金融任务，沉淀场景定制化知识数据。

二是实时更新的外挂知识库，为大模型提供知识“外脑”。外挂知识库通过实时数据流和自动化更新，保持信息时效性，结合细粒度访问控制和安全措施，确保数据安全。利用检索增强生成RAG技术（Retrieval-augmented Generation）将大模型与语义检索以及向量数据库结合，满足内容精细化检索的需求。同时，通过Graph RAG进一步提升对文本语料库的全局理解，实现基于知识图谱的检索增强。

2、4种智能化数据治理能力， 盘活非结构化数据资产

结合工商银行大模型数据工程实践，本文建立利用AI4Data技术从数据“采集、清洗、管理、应用”四方面提升非结构化数据处理生产效率，盘活非结构化数据资产。

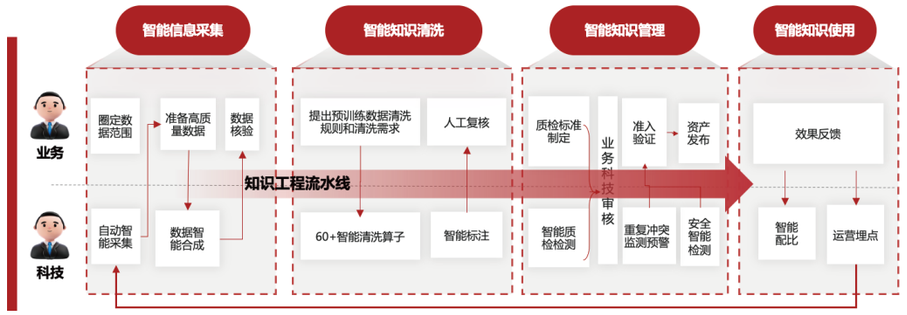


图19：智能化数据治理流水线示意

一是夯实数据采集之“基”，打破数据孤岛。对内，通过建立企业级数据中台方式，形成统一集中纳管的数据资产。对外，通过开源加联创、专项采购等方式，持续丰富通用的互联网新闻、书籍等外部数据。内外结合，建立数据的全面采集机制，为金融大模型的构建引来源头活水。同时，**利用合成训练数据技术，为填补数据缺陷提供创新路径。**银行机构可以探索利用生成式AI技术合成训练数据，重点强化对合成数据的生成技术、质量评价能力和效率。合成数据可以作为现有文本数据集的有效补充，全面提升智能金融应用的效果。

二是持续提升数据处理清洗之“器”，降低数据处理门槛，提升质效。建议通过建立专家清洗规则库+多种智能清洗模型方式，解决异常值等常见数据质量问题，并满足内容矫正补齐等复杂数据清楚处理诉求。同时，考虑到大模型的金融微调数据人工投入大、标注难度大等痛点，建立基于大模型的AIGC辅助标注能力，智能生成文章、观点、逻辑链等复杂标注数据，辅助人工提升效率。通过AI提升数据清洗能力，有效消除数据冗余、清除数据偏见，确保数据的质量和准确性，并通过工具支撑，持续扩充金融专属数据集，以便完成企业内专有模型训练。

三是加强训练数据的高质量管理之“术”，守牢大模型数据合规安全。重点增强知识冲突检测能力建设，可训练智能专项模型提供知识相似度、矛盾等监测能力，并制定知识质检标准，建立业务+科技双审核机制，提供各类知识新旧迭代、内容可信监测等管理能力，避免知识重复、冲突。同时，重点加强大模型数据安全管控，在数据安全管控过程中，优先保障社会主义核心价值观、金融从业要求、企业文化，通过敏感词检测、非法数据过滤、安全测评、人工审核等处理安全手段，提升数据质量和安全可控能力。

四是建立数据应用的运营之“道”，实现大模型的数据闭环。训练阶段，通过十亿模型数据最佳配比，推断百亿、千亿大模型的数据智能配比推荐，解决百亿、千亿大模型多样化数据配比难度大的痛点，提升性能。应用阶段，建立以业务场景为单位，大模型迭代为目标，通过规范运营埋点数据、建立运营团队、持续分析bad case、优化模型等方式，确保大模型应用的数据运营闭环，推动大模型持续优化。

4.3 一条产线：研运一体，革新数字员工研发模式

数字员工3.0的研发本质，是将复杂的多技术融合成“人”，是业务服务需求与人工智能技术的深度融合。考虑到金融行业领域多样，业务需求众多，对数字员工的技能要求复杂，银行机构宜在夯实三大支柱基础上，建立分层共享共建的研运一体产线，打造全链路安全、敏捷、易用的研发工作站，将以往“树烟囱、大应用、高代码”的作坊式研发朝“重共享、大底座、低代码配置”的工厂化流水线研发模式演进，实现数字员工3.0研发模式的变革。

图20：研运一体产线框架

新的研发模式围绕 “敏捷化、标准化”，打造面向开发态的研发中心和面向运行态的服务中心。

一是打造数-智-用全链路整合的AI研发中心，满足数据、模型、智能体的低门槛研发。其中，基于三大支柱底座，面向AI能力开发，打造低门槛的数据工程和模型工程两个基础工程流水线，形成数字员工的智能核心的标准化供给；向上，打造多样化、全能力的通用/专业AI能力构建流水线，构筑数字员工丰富多样、开箱即用的智能化技能；面向应用，构建配置化的智能体组装流水线，分钟级构建金融数字员工。

二是建设标准化的智能服务中心，面向不同的服务需求，以分层解耦的构建思路，实现原子服务、组合服务、范式服务等异构AI能力的统一接入、统一管理；同时构建统一的管控框架，提供服务的统一输入、能力的快速组合、服务的快速调用。

4.3.1 建设创新工厂，以敏捷化研发中心打造数字员工能力基石

按照零代码、低代码研发思路，打造全链路安全、敏捷、易用的研发工作站，沉淀数据与模型两大基础工程能力，组装通用/专用AI技能流水线，并建立智能体开发流水线，三者结合，实现数字员工的模型构建流程化、服务组装积木化、数字员工生产工业化，大幅提升研发效能。

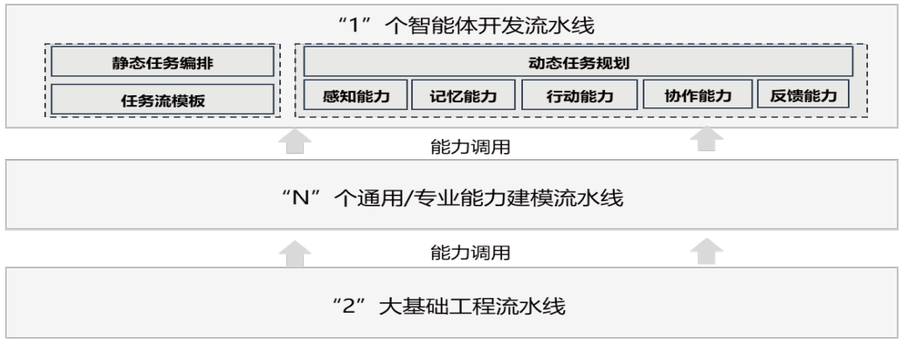


图21：数字员工三层开发流水线框架

1、基础工程流水线：融合用数赋智能力，提升模型训练效率

数字员工在金融行业的能力提升依赖于持续的学习和训练，需要不断利用大量的人类行为数据和专业知识进行浇灌，以便更好地模拟和理解人类员工的行为方式以及金融行业的专业技能。为此，围绕数据和模型两大基础核心能力，建设基础工程流水线，沉淀数据引入、数据清洗、数据标注、算法选择、模型训练、模型评估、模型部署等用数赋智的通用技术模块，规避公共组件重复建设。通过DataOps和LLMOps的工程化融合，提升数据工程的效率，降低模型训练的技术门槛，确保数字员工在金融领域应用的快速迭代和优化。

2、通用/专业技能流水线：多样化AI技能生产线，为数字员工3.0提供拟人化能力支撑

数字员工的建设，需要运用智能决策、知识图谱、OCR、生物识别、语音合成、语音克隆、自由式对话、知识检索、数据分析等多种“看、听、想、说、做”智能化技术，并根据业务需求提供定制化组装。为此，结合领域特色，建立通用+专用结合的全领域AI技能流水线，支持开箱即用以及按需求灵活组装，为智能体开发提供智能化技术支持。

其中，机器学习流水线为数字员工提供基于结构化数据的决策能力；计算机视觉、语音识别流水线为其提供配合神经中枢处理非结构化数据的感知能力；自然语言处理流水线为数字员工提供认知计算和交互决策能力；数字人及语音克隆技术为其提供交互形象及语音输出能力；机器人流程自动化以及各种工具插件为数字员工提供行动执行能力。

3、数字员工组装流水线：多技术融合与规划编排，将“AI技术组合成人”

对标数字员工3.0高拟人度要求，从“AI技术组合成人”的视角，需要打造数字员工组装流水线，将感知、记忆、行动、协作、反馈五维能力以及规划编排等能力进一步优化升级，以提升数字员工3.0处理复杂和创造性问题的能力。

1）智能能力融合：五维协同，夯实数字员工能力调控引擎基础

数字员工的运行基础在于构建一个高度集成的多技术融合体系，这一体系通过感知、记忆、行动、协作以及反馈的五维协同能力，使数字员工3.0应用得以向更复杂、更深入的领域拓展。

图22：五维协同智能体能力

一是多模态感知能力。除传统的视觉、语音、文档感知能力，数字员工3.0需要在多模态融合感知能力上有所增强，使得数字员工自行感知用户或者环境的状态信息。通过视觉文档处理、屏幕处理、系统信息对接、语音解析、传感器感知分析等组件，来打造增强的多模态语音/视觉信息获取等能力。

二是长短记忆能力。数字员工通过构建长短期记忆能力，能够跟踪用户、学习历史经验，并提取价值知识，实现记忆的有效复用，进一步提升规划和行动的依据。短期记忆可通过缓存技术存储最近的交互内容。长期记忆可通过向量数据库等用于快速检索和无限检索，使得数字员工更好地理解上下文。

三是执行能力。数字员工通过建设技能插件和工具库组件，完善手脚行动能力，实现大脑与外部服务和工具的联动，扩展大模型边界，实现复杂场景的任务执行。

四是多协作能力。面对复杂任务，数字员工的交互对象从单体扩展到多体，需要协调和调度多个小模型，将复杂金融任务分解为子任务，分配给适合的小模型。有三种模式：一是串行模式，大小模型分工协作，例如大模型进行预处理和后处理，小模型执行精确评估计算。二是分流模式，大模型分流任务至小模型，如客服场景中基于意图的理解分发任务。三是协调模式，大模型协调各模型，汇总结果生成综合方案，如投顾场景中的风险分析和投资建议。

图23：大小模型协同的三种模式

五是反馈自学习能力。数字员工通过集成反馈循环机制接收和解析用户的反馈信息，评估自身行动的效果和准确性。一方面利用自然语言处理技术分析用户的输入反馈，实现自我调整策略和行为，确保服务的持续优化和个性化。另一方面反馈数据作为下一轮训练的输入，不断迭代和提升其决策和交互质量。

2）规划、编排能力建设：动静结合，强化数字员工规划核心

数字员工通过规划及编排能力将复杂分散的业务流程串联起来，从而具备解决综合性问题的能力。规划、编排能力是数字员工的调度协作中枢，是实现自主性和目标导向行为的关键，目前业界主要有动态任务规划和静态编排两类技术。

一是动态任务规划。使用大语言模型作为智能体的决策核心，通过提示词的方式规范大模型对任务的理解。利用大模型将复杂任务自主分解成更小的子任务，并持续根据任务执行情况和外部反馈动态调整任务计划以接近设定目标，直到任务完成。这种模式针对非预设的任务具有更强的智能化、泛化性，但该模式需采用较大规模参数模型，以满足对复杂任务的理解和规划，由此带来大量的算力消耗。同时多轮交互任务对大模型的记忆能力及指令遵从性要求较高，当前仍有较大提升空间。动态规划当前适用于如远程银行信息查询等无固定流程且交互轮次较少的场景。

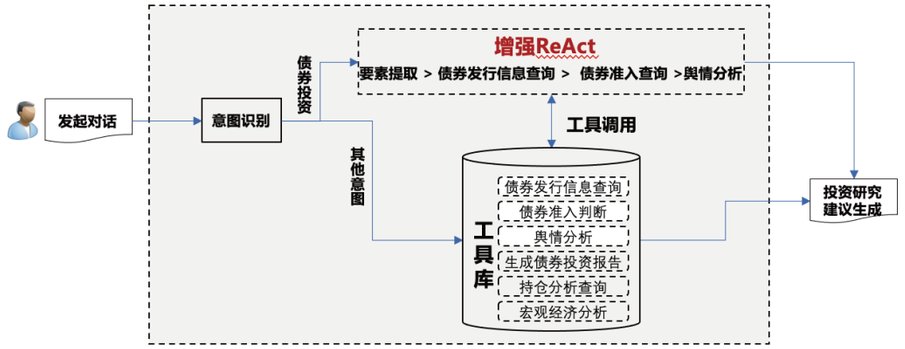


图24：动态规划流程图示例

二是静态工作流编排。由于当前动态规划在场景应用上的能力不足，且金融行业大量业务场景复杂、流程固定，对流程执行的严谨性要求较高，当前业内普遍发展大模型结合静态编排模式进行能力的建设和落地。静态编排利用流程编排框架定义好工作流的各个步骤和执行顺序，并且在工作流运行时严格按规划执行。大模型在其中负责与用户的交互，理解用户意图并引导用户完成参数填充，从而进行执行分支选择。这种模式虽然交互相对固化，但能确保任务按照既定的标准操作程序执行，保障金融任务执行的严谨性和准确性，当前适用于如金融市场投资交易等流程长、任务严谨的金融场景。

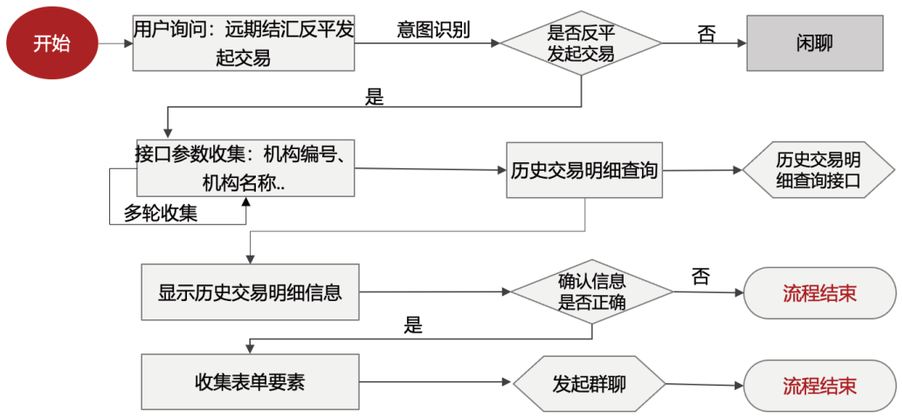


图25：静态编排流程图示例

在数字员工的规划编排能力建设中，应考虑动态规划和静态编排结合，通过静态编排增强场景规划的准确性、可回溯性；通过动态规划提升场景规划的灵活性、自主性。在动态规划过程中，根据用户反馈提炼沉淀静态工作流，提升规划的一致性；同时静态编排能够为动态规划提供结构化的框架，提升规划的稳定性。

3）零代码\低代码数字员工组装：低门槛开发，促进数字员工共建共享

在数字员工组装方面，业务和开发人员技能水平参差不齐。根据应用场景，提供无代码和低代码模式智能体编排开发模式，打造低门槛工程化解决方案，促进数字员工开发共建，实现生态共享。**一是零代码数字员工组装。**面向建模人员和业务专家，通过零代码配置，完成身份人设、知识、技能插件、工作流等信息组装。**二是低代码数字员工开发。**该研发模式通过打造拖拉拽、可视化的工作流编排流水线，基于多种组件实现数字员工技能的自由编排，扩展性强，相关工作流可作为数字员工的技能进行复用，也可直接发布单一技能的数字员工应用。

图26：数字员工编排流程图

4.3.2 建设能力枢纽，以标准化服务中心加速数字员工上岗运行

从将各种拟人化能力组合成人的视角出发，打造建设数字员工智能服务中心，通过基于智能体技术建设的统一智能服务管控框架，实现原子服务、组合服务、范式服务三类服务的统一封装、统一管理、统一编排与统一调控，解决异构AI服务的标准不统一、管理难度大等痛点，同时模拟人的行为模式，沉淀共享拟人逼真、丰富多样的AI服务能力。

1、统一的智能服务管控框架，实现服务插件化、管理集中化、编排流程化、调控统一化

数字员工服务能力涉及多个异构系统，需要通过统一、便捷的方式与大模型整合成为可运行的智能体。同时还需确保各类异构服务能够灵活组装、衔接流畅，可根据业务需求被智能体快速调用。因此，建设基于智能体技术的统一的智能服务管控框架，实现服务插件化、管理集中化、编排流程化、调控统一化。

一是服务插件化。建立可插拔的架构，将各个系统能力以标准化模式封装为插件的形式，以智能体单一分支行动为最小化单元进行插件的封装。插件信息采用标准化JSON进行定义，包括插件名称、插件用途、URL等，确保功能描述规范化、接口标准化，以便于模型理解和调用。当插件被调用时，同样可基于标准化JSON进行参数定义，以便于数字员工基于不同分支选择对应的最小化单元插件完成任务。

插件描述

```
{
  "arguments": [
    {
      "default_value": null,
      "description": "地区信息",
      "name": "location",
      "required": false,
      "type": "",
      "visible": true
    }
  ],
  "auth": {},
  "description": "能够根据地区信息查询天气",
  "headers": null,
  "logo": "",
  "method": "get",
  "name": "天气查询",
  "response": [],
  "url":
"https://xxx.xxxxxxxx.xxx/v3/weather/now.json?key=x_xxxx
```

插件参数定义

图27：插件定义示例

二是管理集中化。围绕智能服务资源申请到智能服务发布的全流程，实现资源申请流程、测试流程、上线部署流程、运维流程的标准统一，并且可根据数字员工忙闲、工作负载，以数字员工为运维单位，弹性扩缩容数字员工智能服务，降低运维和准入验证人力投入成本。服务上线后，建立通用服务和领域专用服务统一管理视图，面向业务侧提供服务目录检索、服务信息查看等能力，实现各类智能服务跨部门、跨产品、跨业务条线的共享使用、运行监控。

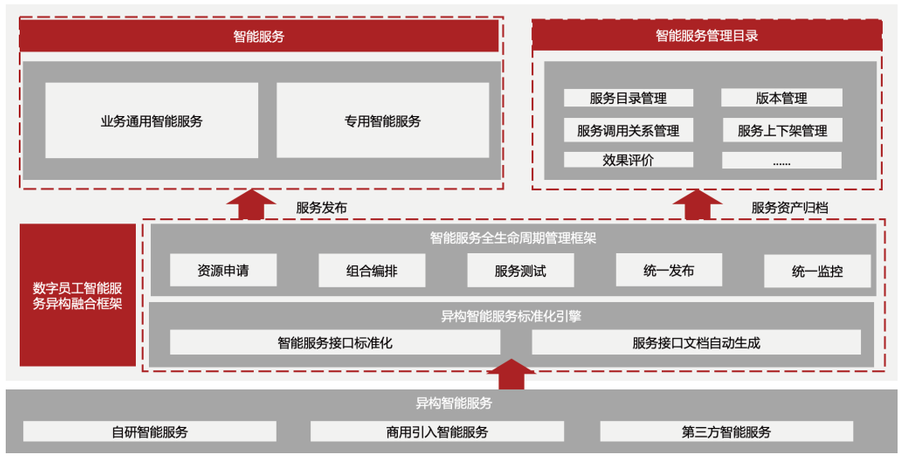


图28：数字员工能力统一管理框架

三是编排流程化。按照“积木式组装”思想，打造低代码理念的组合服务可视化编排流水线。以人的行为模式为参照，支持用户通过拖拉拽方式实现多技术融合的拟人化智能服务分层组装，将原子服务组装为组合服务，并进一步封装为面向场景的工程化解决方案范式，最后总结提炼形成具有业务含义的数字员工智能服务策略。

四是调控统一化。封装好的插件统一通过数字员工的智能体框架进行调控。将各插件以及插件能力以格式化文本的方式进行统一描述，便于大模型进行统一识别。当任务执行时，由大模型进行对话意图识别，判断需要调用的插件，再由主框架完成插件的调用和执行。

图29：基于智能体的数字员工服务调控框架

2、沉淀百模千态的数字员工智能化服务能力

一是原子服务能力发布。服务中心提供一系列拟人逼真的原子服务能力。包括传统小模型的能力，如OCR、人脸识别等，还包括仅通过提示词即可获得的服务。这些服务通过标准化的方式供上层快速调用，既可直接应用，同时也可通过组装服务更为复杂的场景。

二是组合服务能力发布。在原子服务的基础上，服务中心能够发布组合服务能力，这些服务由多个服务组合而成，以满足更复杂的业务需求。例如合同审核需要“看”OCR文档识别、“想”自然语言理解等服务的组合。远程银行双录质检需要“看”视频识别、“想”图像内容识别、“做”结果反馈等智能化服务的组合。

三是范式服务能力发布。金融应用领域多样，各场景多元化个性化需求，以不变应万变。根据技术成熟度和场景，可优先聚焦于知识检索、数据分析、文档编写等场景，总结提炼，打造工程化解决方案，促进规模化、规范化金融应用创新。例如多模态知识检索范式，依托知识库、大模型等技术，提供知识管理、知识搜索、答案生成等能力，支持各业务、科技人员通过零编码方式搭建专属知识库，只需上传制度、规范等文档，即可实现文档内容检索问答，并给出可信来源，提升专业知识获取效率。例如数据分析范式，提供对话式数据分析解决方案，帮助用户一句话实现报表查询、SQL生成、指标查询、图表绘制等，提升数据分析效率、降低数据分析门槛。

图30：原子-组合-范式三层服务

4.4 全量资产：统一纳管，使能数字员工持续进化

4.4.1 打造全面高效的资产中心，持续供给数字员工生产资料

数字员工的生产资料主要是员工技能、领域知识、业务流程等。通过构建一个资产标准化和共建共享的资产中心，整合技能库、知识库、流程库等资源，形成数字员工技能研发、组装的统一“零配件供应中心”，为全行数字员工提供持续学习和能力升级的共享资源尤为重要。

1、技能库资产：数字员工行动能力的工具箱

技能库资产是数字员工执行多样化任务的能力基础。数字员工通过调用各种业务系统、AI能力、工具等插件，极大地扩展行动范围和效率。**一是建设通用插件库，**面向知识问答、代码生成、数据分析等通用应用，集成知识检索、代码解释器、知识检索、ChatBI等通用插件，实现通用能力的共享复用，确保资源的最大化利用。**二是建设专用技能插件库，**包含针对特定业务需求和行业应用的专业工具和算法，以支持数字员工更好地适应各种复杂的业务场景，提供定制化的服务和解决方案。例如调用客户画像插件进行客户偏好分析和营销策略推荐，调用行业资讯库插件进行市场趋势分析等。

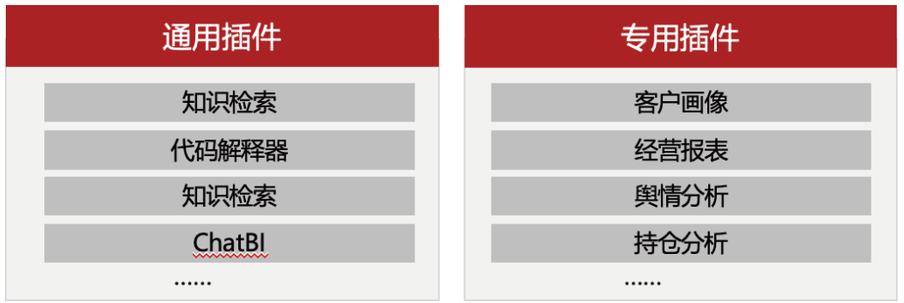


图31：插件库资产示例

2、知识库资产：数字员工分析与决策的支撑

知识库是数字员工获取信息和数据的主要来源之一。知识库为数字员工提供外部信息库，不仅扩展智能分析能力，还提供长期记忆能力。为提升知识库的建设与使用效率，需要从以下方面重点考虑。

一是知识的多样性。1）知识形式的多样性，知识库不仅要包含文本信息，还应该包括图像、表格、视频等多媒体内容，以提高信息的可访问性和理解性。2）知识内容的多样性，知识库的建设应覆盖广泛的主题和领域，包括但不限于实时更新的国内外金融监管政策、金融市场分析；详细的产品介绍、条款说明；业务领域专用的信贷评估标准、反洗钱规则等，以满足不同背景和专业领域用户的知识需求。

二是知识的可回溯性。随着知识的不断积累和更新，信息往往会被细分并重新整合到不同的应用场景中。为维持知识的准确性和一致性，需要建立知识管理框架，支持知识的存储和检索，以及知识的生命周期记录，包括创建、更新、审核和废弃等各个环节，确保每个知识点都可以追溯到其原始的上下文和来源，在引用时能够提供完整的背景信息，避免因断章取义而产生的误解或歧义。

三是知识的可隔离性。在商业银行中，业务领域的专用知识信息，例如信贷评估的标准和产品定价策略，以及大量的客户个人信息通常属于敏感数据，需要严格控制访问权限。通过为不同级别的用户设定相应的权限，从而确保只有授权人员才能访问特定的知识资源，保证敏感信息的保密性和合理流通。

3、流程库资产：数字员工自动化作业的引擎

流程库资产是数字员工在自动化执行金融业务中的核心引擎。流程库资产聚焦于将复杂的金融业务流程转化为可由AI代理执行的任务序列。流程库资产建设主要包括四类资产沉淀：

一是静态编排流程文件。将常规且标准化的业务流程转化为一系列明确的操作步骤，并形成详尽的流程文件。这些文件作为数字员工执行任务时的指导手册，确保每一步操作都按照既定的最佳实践进行，从而提高工作效率和准确性。


```
  - name: "历史交易信息查询"
    activate: "{{data.code}} == 0"
    input:
      serialNo: "{{获取一个随机字符串生成随机编
号.output.data.msg}}"
      productId: "103"
      branchId: "{{数据收集.output.XXX号}}"
      agmtNo: "{{数据收集.output.XXX号}}"
      cptNo: "{{数据收集.output.XXX号}}"
      userId: "{{数据收集.output.XXX号}}"
      actType: "5"
      serviceName: "queryContract"
      language: "zh_CN"
    prompt: "###工具调用###当前任务:
《{{Operation.name}}》\n请你帮我调用
`transactionDetailsQuery`这个工具，相关参数信息如下:
{{Operation.input}}"
    next:
      - "信息查询成功"
      - "信息查询失败"
```

图32：静态编排流程.yaml文件示例

二是动态规划提示词和指令。在大模型进行动态规划时，需要根据提示词和指令来帮助其理解任务需求，同时确保它能够根据不同的应用场景和实时数据做出适应性响应。提示词文件应包括角色的定位概述、所具备的关键技能、遵循的行为准则与规范，以及面向具体任务的解决方案和实施步骤。通过沉淀不同语境下的提示词模板资产，引导数字员工更准确地识别不同场景任务的上下文、目标和预期结果，从而提高其执行任务的效率和准确性。

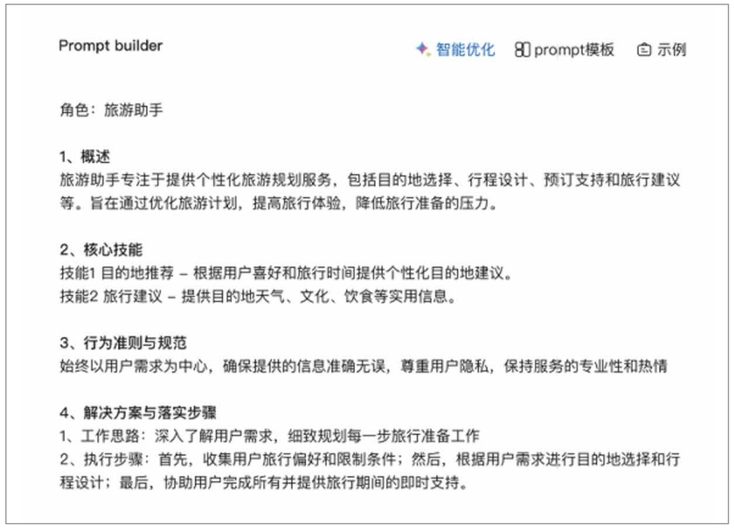


图33：动态规划提示词示例

三是流程测试集。从流程遵从性、异常任务处理、流程执行性能等方面，面向金融通用场景及金融特定任务创建测试集，以验证流程的正确性和效率，确保数字员工在各种情况下都能稳定运行。

4.4.2 构建共建共享的运营机制，全面推进数字员工快速发展

金融机构应构建标准化的管理平台和共建共享的机制，以充分发挥资产中心的作用，激发数字员工3.0的智能化能力。通过构建标准化的管理平台，可以实现资产的统一管理和高效利用。建立共建共享的机制能够鼓励不同部门、团队甚至不同机构之间的合作与知识共享，促进资源的优化配置，避免重复劳动，提高整体的工作效率。

一是资产统一管理。构建标准化管理平台，将各类资产统一注册并集成到统一的界面中。按照业务领域对AI资产进行归类，编制AI资产目录，构建面向业务领域的AI资产视图，统一查询入口。依托自然语言处理与知识图谱等AI技术，构建“模型、样本、场景、算法、服务”五维关系网络，建立可查询分析的资产血缘分析能力，强化资产溯源分析，提升资产的可见可得共享能力。

二是资产统一模板。在完善的AI资产视图基础上，进一步将资产按照能力粒度，提炼面向各业务场景的资产模板，形成可复用的能力组件，并与开发流水线对接，实现跨部门、跨机构相似场景的快速研发，降低能力共建的门槛。

三是资产统一体验。建设可视化、典型业务场景植入的数字员工智能化能力体验中心，覆盖智能搜索、文本创作、以图生文等典型的场景，并提供建设最佳应用实践，加速数字员工和智能场景建设。

四是资产统一运营。从版本管理、服务发布、调用授权、服务监控、预警告警、效果评估等资产运营全生命周期维度，对数字员工能力资产进行管理和优化，从而提高资产的利用率，确保资产价值的最大化发挥。

五.管理篇：
遵从劳动分工本源，创新数字员工管理

1776年，亚当.斯密在《国富论》中最早提出并强调劳动分工论，多维度论述劳动分工对提高劳动生产率、增加国民财富的促进意义。分工论在企业治理中已是一种重要的管理模式。商业银行在引入数字员工时也应基于协作分工原则，建设数字员工配套的管理体系。

结合工商银行实践，本文建议数字员工管理体系参考人类员工管理模式，从独立身份、权责清晰、专业设岗、统一纳管、数字运营五个方面进行建设。一是建立数字员工身份认证制度，构建数字员工统一运营管理平台，实现数字员工全流程管控。二是明确数字员工建设各方职责，包括企业级数字员工发展与指导、数字员工技术能力建设、数字员工管理体系建设等，在企业内部形成自上而下的全面建设体系。三是明确对客服务和对内赋能两大类数字员工的岗位设计，建议从现有人力岗位序列的具体工作任务切入，参照设置数字员工岗位。四是综合考虑数字员工呈现出综合化、专业化两种发展趋势，采用融合策略，按照“统一数字员工品牌、差异化岗位数字助手建设”的模式推进数字员工分层管理。五是建立数字员工的评价体系，实现数字员工工作的精细化运营管理。

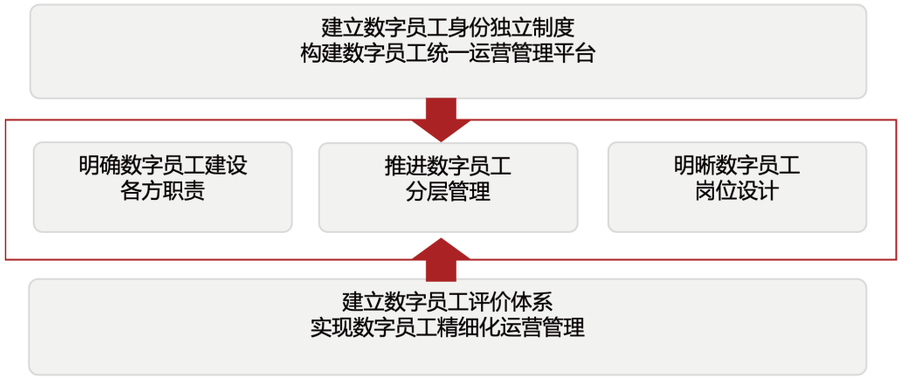


图34：数字员工管理体系

5.1 独立身份，赋予个性人格

数字员工身份独立有两方面优势。一是在内部管理上，数字员工与人类员工实现权责分离，可确保人机协同运转，保障运行安全可控。二是在外部宣传上，独立人格化、形象化的数字员工有利于提升客户体验，助力形成品牌效应，形成新的获客引流热点渠道，扩大影响力。

银行机构可从管理制度制定、人格化设计、配套系统支撑三个方面推进数字员工的身份独立设计。

一是管理先行，制定数字员工管理制度。明确数字员工设立、身份权限管理、部门间职责分工、日常管理、风险防控等机制流程，方便各部门根据管理制度，合理设置部门内的数字员工岗位，并对数字员工开展人格化属性设计、业务系统的权限分配、风险防控措施制定等工作。同时，在操作流程上，建议比照企业内的人类员工招聘入职审批流程，建立签发数字员工身份的工作流程，为数字员工分配独立员工编码和形象，使数字员工具有唯一身份标识和个性外观，方便数字员工识别和沟通，增强数字员工人格化属性。

二是规范设计，形成数字员工人格设计的统一标准。银行机构应制定数字员工人格化属性设计的标准化规范指引，具体从姓名、人格特征、语言风格、人物形象、交互设计、行为模式等方面形成设计标准，避免造成命名不规范、形象侵权等问题。

三是系统配套，建设数字员工运营管理平台。为更好实现对全行各机构数字员工统一管理，以及工作岗位、工作绩效等要素的综合展现，建设配套的数字员工运营管理平台。首先是从人员管理视角，建立数字员工运营管理平台的管理流程，形成数据员工身份的申领、分配、建设、上岗、管理、应用和评价的闭环管理新模式，并与人力资源管理系统打通，联动实现数字员工身份签发、冻结、注销等全生命周期管理；其次是统一采集数字员工评价指标，并利用可视化分析技术，打造各专

业条线的“多维度、可钻取、可量化”的可视化管理工具，让数字员工的成效实现业务侧可感知、可评价；最后是加强数字员工培育和数字员工监控，形成数字员工知识管理、健康管理、合规管理等能力，确保数字员工能力的安全可信、持续进化。

5.2 权责清晰，明确组织管理

为简化管理流程和不增加额外的管理成本，建议复用现有项目研发模式，采用“人力统筹、专业主管、科技实现”的思路明确相关部门职责，明确数字员工的需求分析、人格化设计、能力建设、准入评估、运营评价、持续迭代的全生命周期管理流程。

- **人力统筹：**由人力资源部门制定数字员工管理制度，明确数字员工的设立、身份权限管理、日常使用管理等机制流程，并负责签发数字员工身份证，统管数字员工人力信息。
- **专业主管：**由业务主管部门主导辖属的数字员工建设工作，其中，考虑对客服务的统一性，建议将对客服务数字员工统一归口到一个业务部门统管建设；内部专业数字员工则由对口业务部门负责建设，确保业务专业性。
- **科技实现：**科技部门牵头数字员工的技术支撑能力和系统建设实施工作，夯实IT平台功能。

5.3 专业设岗，实现任务专办

银行数字员工可按对客服务和对内赋能出发进行岗位设计。

对客服务方面，以提升客户服务体验为宗旨，打造数字客服、数字远维等对客服务的数字岗位体系，重点从事客户服务、主动触达等工作，实现产品咨询、客服答疑等场景的沉浸式交互自助服务，助力提升金融服务的便利性和可得性。在岗位设置上建议“少而精”，如数字客服岗、数字远维岗等，服务于电话银行、手机银行、网上银行、网点设备等渠道，提供业务咨询、投诉受理、业务办理、产品推荐、客户关怀等服务。为更好强化客户认知，统一用户体验，对客服务岗位数字员工必须统一对客服务的形象、知识话术等信息。

对内赋能数字员工方面，各业务部门可参考部门内的现有人力资源岗位体系，结合自身业务数字化转型需求，打造领域内的数字员工专业岗位。在岗位设置上，可以按照“具体条线具体分析，具体岗位具体设计，具体事项具体实施”工作思路，基于各部门相关岗位工作要求，以具体工作任务为切入点，从实际任务替代/辅助出发，合理设置数字员工岗位及配备相关数字助手。该设计，宏观层面实现数字员工岗位和人类员工岗位体系的完整对照、微观层面实现与具体工作事项关联，有效提升数字员工管理和实施的精细化水平。

表1：数字员工设岗示例

分类	岗位	任务	岗位说明	数字员工类型
对客服务数字员工	数字客服岗	客户服务	24小时在线客服，回答场景问题，处理简单的客户咨询。	代驾
		业务咨询	提供业务流程咨询，帮助客户了解银行业务和操作流程。	代驾
		交易处理	辅助或自动化执行标准交易流程，如转账、支付等。	辅驾
	数字远维岗	投资咨询	提供基于算法的投资建议，辅助客户做出投资决策。	辅驾
		产品营销推荐	根据客户资料和行为分析，推荐适合的银行产品和服务。	代驾
		客户反馈分析	收集和分析客户反馈，用于产品和服务的改进。	辅驾
对内赋能数字员工	智能陪练岗	辅助员工培训	提供在线培训资料，辅助员工职业发展和技能提升。	辅驾
	风险辅助分析岗	风险辅助预警分析、处置	评估和量化银行业务风险，提供风险评估报告。	辅驾
	.....	.....	.....	.....

5.4 科学管理，分层统一纳管

考虑到很多银行已建设多种类、多数量的数字员工队伍，建议综合考虑数字员工呈现出综合化、专业化两种发展趋势，采用融合策略，按照“统一品牌、差异建设、协同调度”的模式推进数字员工分层管理，厘清数字员工的多样化概念，形成统一标准话术，避免出现数字员工过度建设，及用户同时对接过多独立数字员工造成体验不佳、服务不均和使用复杂等问题。

一是统一数字员工品牌。对外服务，由对客服务牵头部门统一负责，按照个人或家族模式，建立统一的对客服务数字员工品牌，建立形象、姓名等统一标准的人格化属性，规避客户理解偏差。对内，建议按大的业务领域或条线整合，由相关专业部门牵头，其他部门配合，人力资源审批，建立对公业务、个人业务、综合办公等专业领域的对内赋能数字员工品牌，形成统一专业化品牌管理。

二是按岗位差异化建设百模千态的数字助手。建议参考人类员工“人员-岗位-任务”三层工作关系，在对应数字员工品牌之下，建设方以具体岗位-任务为切入点，按照自身业务需求和业务属性，对照岗位要求，建设实际负责干活的专业型数字助手，并赋能相关业务场景，形成“统一数字员工品牌-N（N个差异化岗位数字助手）-X（X个差异化业务场景赋能）”的数字员工建设新模式。

三是通过数字员工统一入口协同调控各类岗位数字助手能力。打造多助手协同框架，用户通过一键“@”方式在统一数字员工对话窗口快速唤醒所需的数字助手能力进行交互，通过自然语言的简单指令精准响应用户需求，避免原菜单点选模式下多个系统、多个助手查找/切换/执行的繁琐操作，实现一人+N个数字助手的协同工作模式。

5.5 数字运营，持续提升能力

数字员工的常态化运营对于数字员工服务能力的提升至关重要。聚焦数字员工评价指标体系建设、数字员工能力运营两个方面，建立数字员工运营保障支撑体系，实现数字员工工作成效可评价、能力可提升、运营有抓手的长效化机制，保证数字员工工作质量和水平，激活数字员工的工作潜力和业务价值。

5.5.1 数字员工评价指标体系

参考人类员工KPI评价方式，围绕业务成效、业务成本、劳动质量、应用能力、风险安全等维度构建统一的数字员工评价指标体系，银行机构可以科学量化和评价数字员工的表现，促进数字员工能力的持续提升。同时，通过“标准值”等对照策略或漏斗策略，由运营人员提出体验建议，可以针对性开展优化，不断完善评价管理体系。其中，“标准值”对照策略是指将数字员工评价指标与预设的标准值进行比较，以此来判断数字员工的表现是否达到既定的标准或目标。漏斗策略是指将数字员工服务的全过程分解为一系列的阶段，通过分析每个阶段被服务对象的流失或转化情况，识别出数字员工服务过程中的瓶颈。

一是业务成效方面，旨在对数字员工的服务量、客观的业务效果以及客户的主观评价进行评价，主要包括业务量评估、效果评估、客户评价等指标类别。二是业务成本方面，旨在对数字员工的日常运营的各项成本进行评价，主要包括运营成本等指标类别。三是劳动质量，旨在对数字员工服务的准确性、及时性、完整性等方面进行评价，主要包括准确性评估、响应速度评估等指标类别。四是应用能力，旨在对数字员工的技能和能力进行评估，主要包括知识丰富程度、专业技能覆盖度、应用灵活性等指标类别。五是风险安全，旨在对数字员工的系统安全性和数据安全性方面进行评估，主要包括安全保障、数据保护等评估指标类别。

表2：数字员工评估指标体系（示例）

指标维度	指标类别	指标项
业务成效	业务量评估	交互量、会话量、服务客户量、点赞量、评论量等；
	效果评估	完成量（率）、分流量（率）、转化率、成功办理量（率）等；
	客户评价	满意度、投诉量、好评率等；
业务成本	运营成本	运营人员成本、系统资源使用成本、IT技术成本投入等；
劳动质量	准确性评估	转写准确率、识别率等；
	响应速度评估	平均响应时长等；
应用能力	知识丰富程度	知识量、学习新任务所需迭代次数等；
	专业技能覆盖	覆盖专业数量、算法丰富性等；
	应用灵活性	上线灵活性、智能调度能力等；
	功能完备性	功能完备性、功能灵活扩展能力等；
	工作量承载能力	工作量承载能力、扩展能力等；
风险安全	安全保障	系统稳定性、生产问题数量等；
	数据保护	数据安全性等。

5.5.2 数字员工能力运营

数字员工能力运营可助力银行持续提升数字员工的服务效率、改善用户体验、降低服务成本、提供个性化服务、增强市场竞争力、提高客户响应速度和满意度。为做好相关工作，以数字员工的运营评价和能力持续迭代为目标，建立以数字员工服务能力为中心的数据闭环智能化运营体系，提升数字员工能力的持续迭代和应用的量化评价能力。

一是规范数字员工运营埋点数据，将数字员工应用场景信息、服务信息、交互信息等数据作为关键埋点，实现埋点数据的统一、全面和标准化采集。同时，实现数字员工运营埋点数据全入湖，并基于埋点数据加工形成数字员工运营指标，为数字员工能力迭代提升数据依据。

二是强化数字员工运营数据监控分析，按照对客服务数字员工、对内赋能数字员工等分类预置数字员工运营指标模板，实现技术指标、业务指标的统一监控，并基于可视化分析技术能力生成各类数字员工的运营评价报告，供各业务部门持续提升数字员工能力提供重要数据依据和指导。

三是建立常态化数字员工知识库运营机制。知识库运营是保证数字员工服务效果的重要资源，智慧银行需要基于集中、统一搭建知识库，并按照数字员工维度，组建专业团队负责统一运营，负责知识收集、知识清洗、知识分类和标注、知识库管理、更新和维护、质量控制等工作，支持全行数字员工服务场景共享复用。

四是实现数字员工训练调优运营常态化。数字员工的能力需要通过训练不断优化提升，训练内容包括语音识别能力、语义理解能力、语音合成能力、数字员工表情动作仿真能力。训练方法包括提取客户交互过程、标注客户交互过程中的错误或缺陷、分析问题原因、优化程序或语音语料等流程。银行应组建科技和业务融合的专业团队，确保训练结果的准确性和业务反馈结果的及时性。

六.安全篇：

科技向善坚守本心，
安全可信夯实根基

数字员工从最初简单流程自动化，到如今借助大模型打造的智能化、拟人化，数字员工的能力边界不断拓展，应用场景日益丰富。随着数字员工的广泛应用，其体现出高效、稳定、精准等诸多优势，但同时也蕴藏着数据安全风险、模型算法风险、输出内容风险、业务权限管理等多方面安全风险。数字员工在处理敏感金融数据、执行关键业务流程时，若缺乏有效的安全管控，极易成为不法分子攻击的目标，从而导致操作失误，造成严重数据泄露和业务中断，带来金融信誉和经济损失。

为更好处理技术创新和监管合规之间的平衡，银行机构应将“安全可信”作为数字员工发展的核心原则和使命担当，通过从安全管理、安全技术、安全运营构建起全方位、多层次的企业级数字员工智能安全合规框架，才能真正发挥数字员工的价值，实现数字员工数据安全合规、模型安全可信、应用风险可控三大安全目标和“科技向善”的愿景。

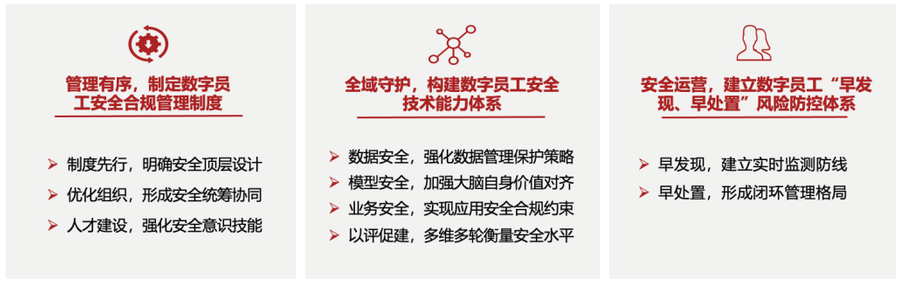


图35：数字员工安全体系

6.1管理有序，制定数字员工安全合规管理制度

为防范化解人工智能技术及数字员工应用风险，提升科技创新治理水平，银行机构可从制度流程制定、组织架构建设、人才建设三个方面着手，形成自上而下、重点明确、责任清晰的安全管理框架和相关组织保障，有效降低安全风险，为数字员工的持续创新发展提供坚实的制度保障。

6.1.1 制度先行，明确安全顶层设计

管理制度方面，构建并持续完善全方位、多层次的安全管理体系。

一是覆盖数字员工全生命周期。围绕需求分析、规划设计、系统建设、部署设置、监控评价、优化扩张、集成协同、维护升级、闲置报废等，建立安全评估、安全监测、安全事件应急处置和违法违规处置等安全责任落实规范、流程。

二是提前制定详细的应急响应预案。针对数字员工可能发生的数据泄露、恶意攻击等常见安全事件，制定详细的应急处置流程、资源调配和人员分工，明确应急处置流程、资源调配和人员分工。

三是完善数字员工使用授权机制。严格规范数字员工的账号管理、权限分配和访问控制，确保其只能在授权范围内执行操作，防止越权行为，防范内部风险，增强数字员工操作的可追溯性和合规性。

6.1.2 优化组织，形成安全统筹协同

组织保障方面，建立数字员工协同管理机制。

一是明确科技、人力、业务等各部门在数字员工安全管理中的职责，在此基础上形成日常跨部门协作机制，定期召开会议，分享安全最佳实践，讨论潜在风险并制定应对措施。

二是设立专门的安全部门、安全团队或跨部门的安全管理小组，负责数字员工的安全策略制定、执行、监控和持续改进。

三是在安全团队的人员构成上应包含高层领导、安全专家和相关部门负责人，在对内部组织架构、制度设计充分了解的基础上实现安全管理政策的稳健制定和坚决执行。

四是团队成员应具备算法理论、数据结构、密码学、网络安全等相关知识背景，对人工智能算法的安全特性、漏洞类型、攻击手段、防御策略有深刻理解，常态化针对数字员工应用定期组织安全测评、攻防测试和应急演练等活动，确保数字员工持续提升安全能力。

6.1.3 人才建设，强化安全意识技能

人员培养方面，持续开展数字员工研发和应用的安全培训。

一是筑牢员工安全意识，定期为科技和业务人员提供有关数字员工的安全培训，包括安全意识教育、安全操作规程、应急预案等，提高安全意识和操作技能，通过案例分析、模拟演练等方式协助员工充分了解潜在的安全风险。

二是帮助员工熟悉安全技术规范，通过安全操作手册、小视频、现场培训等多种方式提供详细的安全操作细节，使员工掌握应对安全事件的正确方法，确保具备专业素养和应对能力。

6.2全域守护，构建数字员工安全技术能力体系

数字员工的安全技术能力是保障数字员工安全建设的核心能力，主要涉及数据安全、模型安全、应用安全以及安全测评等技术维度。其中，数据安全技术用于满足数据安全监管要求；模型安全技术用于提升数字员工原生安全合规应用能力；应用安全技术用于识别是否存在各类违规风险、全面保障服务安全；安全测评技术用于保障数字员工的安全稳定运行。

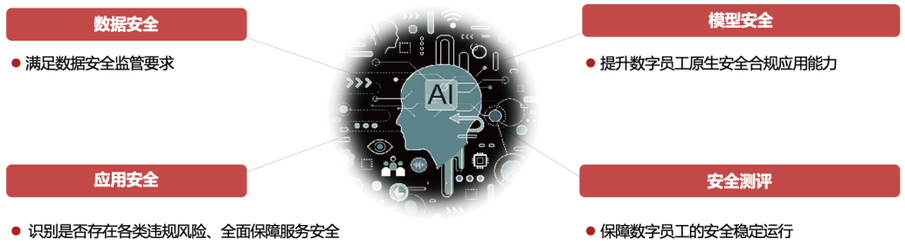


图36：数字员工安全技术能力体系

6.2.1 数据安全，强化数据管理保护策略

数据是数字员工运行的基石，而在数字员工接收并处理数据过程中，存在数据泄露、滥用等风险。同时，数字员工的模型构建也依赖于海量多元数据进行训练。为提升数据安全，需在数据全生命周期的安全管理采集、访问、传输和存储等环节采取措施保障数据的合规性与安全性。

一是采洗源头防控，确保数据来源和内容的合规性。在数据引入时严格审查数据的来源和授权，确保数据来源合法、合规，针对训练数据通过语料脱敏清洗、自动化安全评估和人工抽检机制，从源头上实现不良信息治理，剔除毒害信息。

二是管理精确防控，实施数据使用最小化访问权限。在数据管理上对

数字员工的数据进行分类、归档和设置相应的访问权限。通过遵循数据最小化原则，实施细粒度的访问控制，如基于角色、属性的访问控制以及动态授权机制，实现对数据访问的精确管控，确保数字员工只能在合法授权情况下访问和使用数据，以有效降低数据泄露的风险。

三是存取使用全程可控，确保数据传输和存储的安全性和完整性。数据存储时，采用强加密标准对存储和传输的数据进行加密，以防止数据泄露。数据使用时，使用数据掩码、伪匿名化和数据合成等数据脱敏技术来隐藏敏感信息，确保个人隐私和商业秘密不被泄露。

6.2.2 模型安全，加强大脑自身价值对齐

模型算法是数字员工技术的核心，决定数字员工行为的可预测性和可信度。相较传统机器学习算法，生成式人工智能大模型输出具有多样性和随机性，存在新型的算法和模型风险，如AI模型幻觉、知识侵权等，极大影响数字员工的安全、公平、可信。因此，从加强算法内生安全入手，引导数字员工生成积极、正向、合规的内容。

一是开展引入模型评估工作，确保基模安全。通过评估模型备案情况以及构建通用和金融领域特色安全测试集，确保遴选的基础模型安全、健康、向上向善，严格遵从国家法律法规。

二是构建金融正向价值观数据，提升模型内在价值安全。综合金融业、企业价值观要求，通过构建多元化的正向的价值对齐数据基础，使用大模型对齐技术进行强化学习训练，例如人类反馈的强化学习RLHF（Reinforcement Learning from Human Feedback）、直接偏好优化DPO（Direct Preference Optimization）等，引导大模型的能力和行为跟人类的价值、真实意图和伦理原则相一致，增强人类和人工智能协作过程中的安全和信任。

三是构建数字员工行为可解释能力，提升模型透明性。构建算法层面的模型可解释能力，综合利用特征重要性局部可解释算法、基于知识图谱的可解释等方案，为风控、营销等可解释诉求紧迫的场景，强化对数字员工行为及结果的可解释能力。

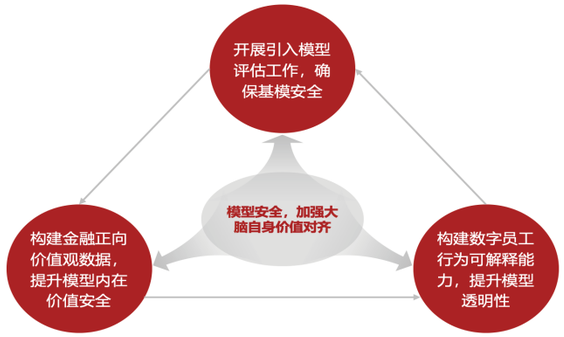


图37：模型安全体系

6.2.3 业务安全，实现应用安全合规约束

数字员工在对外提供服务时面临未经授权的访问利用、输入输出可能存在不合规合法内容、恶意利用造谣诈骗等潜在风险。为保障数字员工生成内容的安全性，需要从内容审核、机制设计等方面采取措施。

一是强化数字员工权限管理，确保授权内访问操作。智慧银行可参考现有人力资源体系的权限管理要求，按照使用数字员工从事具体业务的员工和机构所具备的最小授权限制数字员工在该次任务中所能访问的业务系统和操作权限，确保数字员工只能完成符合业务流程规范的系统操作，避免出现一手清等风险隐患。同时对于数字员工完成的业务准确记录其操作日志及调用数字员工能力的人类员工信息，做好台账管理。

二是建设输入输出内容审核能力，保障数字员工响应内容合规。输入内容审核方面，通过自动审核用户输入，对提示词攻击、违反价值观等内容进行拒答处理；对涉及敏感且无法拒答的内容，通过检索红线知识库进行作答。输出内容审核方面，通过自动审核模块对输出内容的安全合规进行检验，如存在安全风险，数字员工将基于固定话术生成一段无公害的描述，从而实现生成内容的安全控制。另外，还应关注数字员工服务请求拒答率等外界反馈数据指标，及时采取措施，避免对用户体验产生影响。

三是建立防伪审核机制，阻拦恶意利用。针对对抗样本、深度伪造等新型攻击手段进行对抗技术研发，对于人脸识别、OCR识别等广泛应用

的关键服务，应使用活体检测等安全技术进行加固，提升安全能力，保障金融应用的可靠可用。随着攻击手段的不断演变，安全防火墙机制也应持续更新和优化，定期评估现有防护措施的有效性，并根据实际情况进行调整和改进。

6.2.4 以评促建，多维多轮衡量安全水平

安全测评是确保数字员工长期安全稳定运行的关键。通过建设系统化、标准化、常态化的安全攻防演练能力和安全测评整改能力，可全面体系了解数字员工的安全状况，及时发现和修复潜在的安全隐患，为持续针对性改进优化提供依据。

一是建立自评体系，满足动态高频高效评测需求。通过构建多样化测评数据集和评测工具，支撑多维度全面评估。数据方面收集和整理相关业务领域数字员工的各类型数据，形成完整的数字员工安全测评数据集，既包含涉黄、涉暴、涉政、涉密、知识产权、伦理价值观等多源全面的通用模型安全评估测试集，亦包括银行领域特色的常见违规问答和操作内容，为安全测评提供坚实数据基础。使用自动化测评工具衍生出反向诱导、提示词注入、越狱攻击不同攻击样本，提升数据全面性，并支持多维度指标评分自动计算，简化评测过程，提升评测效率，直观呈现安全状态，形成上线准入评估结果和短板提升建议分析。

二是建立数字员工安全攻防体系，开展红蓝演练。根据收集的漏洞清单，开展进行排查分析，开展基于黑客视角开展模拟攻击检测，挖掘算法模型安全漏洞，识别潜在算法安全风险，通过开展常态化的攻防对抗，发现应用系统、算法模型及基础架构中存在的安全隐患或者薄弱环节，促进算法安全能力螺旋式提升。

三是积极参与业界权威安全测评，获得客观评价。通过参与权威的安全测评，了解业界的安全标准和最佳实践，带来新的测评视角，获得独立客观的评价，发现数字员工的安全差距和不足，也能获得专业的意见和建议，有助于发现内部评估可能忽视的问题，进一步指导改进和优化数字员工的安全措施。

6.3 安全运营，建立数字员工“早发现、早处置”风险防控体系

数字员工的安全建设需要久久为功，在日常运营中持续优化和完善。建立健全的风险防控体系，实现对安全威胁的早期发现和快速处置，化被动应对为主动治理，形成高效、可靠的问题处置闭环机制，最大限度降低安全风险，确保数字员工的稳定运行和持续发展。

6.3.1 早发现，建立实时监测防线

为实现对数字员工运营过程中潜在风险的早期识别，在已有自动化网络安全、数据安全等监测基础上，通过客户反馈、业务人员监看、科技指标报警以及跟踪外部舆情政策监控等能力，建立全面的数字员工应用监控能力，形成可量化的安全态势感知，从而为治理和优化提供数据支撑。

一是建立全面的安全态势感知平台，在强化业务应用中大模型内容安全监测能力。业务系统监测运营方面，打造人机协作审核模式，对于机器审核的结果，由业务人员及时进行漏判、误判和纠错判断，对于机器策略不当情况，由业务人员及时开展回访和应急。科技监测运维方面，在数字员工服务运行期间，利用设定的关键性能指标和阈值，持续监测问题拒答率、违规内容生成率等，当问题拒答率和违规率超阈值时，立即触发报警机制，并通过短信、邮件等方式通知相关人员介入。

二是跟踪外部舆情政策，主动搜寻潜在的威胁。密切关注与数字员工相关的政策变化、技术突破、安全资讯等外部信息，为数字员工的合规性建设提供情报支持和研判分析，并基于分析结果形成应对预案，确保数字员工能够及时适应新的法规要求和适应外部技术发展情况。

三是建立使用反馈机制，及时响应客户需求。建立多渠道的客户反馈机制，通过点赞点踩、在线客服、问卷调查、电话访谈等方式，收集客户的反馈信息，及时了解数字员工在实际应用中出现的问题和风险，提升用户体验。

6.3.2 早处置，形成闭环管理机制

对于潜在安全风险，快速而精准的处置能力是确保数字员工安全的关键第二步，在事中以高效高质响应将安全事件的影响降到最低，从而保障生产安全和客户体验，在事后基于运营数据，持续优化安全策略，实现抗风险能力持续迭代提升。

一是快速定位问题原因，识别薄弱环节。通过部署全面的监控系统，实时收集和分析数字员工的运行数据、日志数据，综合利用日志检索、机器学习、数据挖掘等技术，建立异常检测模型，增强安全威胁的自动识别和定位，并追溯问题发生的源头，为快速处置提供有力支持。

二是制定执行处置方案，转化改进措施。根据客户、业务、外部的多渠道安全事件，设定对应应急处理策略方案和长期模型优化措施，优先保障客户诉求满足，降低风险和损失，再针对问题的根本原因，制定长期的改进计划，防止类似问题的再次发生。

三是效果跟踪反馈，确保闭环有效。在处置完成后，对实施效果进行跟踪和评估，并收集用户对处置效果的反馈意见，及时调整和优化处置方案，确保处置措施达到预期效果。通过闭环管理，使数字员工在面对不断演变的安全威胁时，始终持续演进，保持高度的抗风险能力。

七.展望篇：

数字员工未来已来，
技术革新稳中求进

在大模型等生成式AI技术的带领下，数字员工从自动化走到拟人化，已成为生产力中最活跃的因素之一。根据麦肯锡预测，2025年，全球数字员工市场规模将达到6.7万亿元。本章我们将展望数字员工在技术趋势、应用潜力、人才发展、风险合规等方面的未来前景，便于各银行机构提前布局谋划。

7.1 数字员工应用广阔，层次多元潜力深远

未来10年，大模型会遵循点、线、面、体法则，加速在智慧金融领域深化应用。在智慧金融的浪潮中。数字员工正逐渐成为金融机构的核心竞争力。其应用范围之广，层次之多，潜力之深，将给客户带来全时空、专享化、拟人化的极致体验金融服务。

一是数字员工突破时空限制，为客户提供随时随行的金融服务。从零售银行到投资银行，从保险到资产管理，银行将通过数字员工为客户交易支付、投资咨询、贷款融资等各类金融服务，极大化金融的可及性普惠性。

二是应用数字员工，金融机构将真正实现以客户为中心的“千人千面”的专享化客户服务。例如，数字员工能够识别并快速响应特殊需求群体，通过精准分析客户数据和行为模式，为小微企业主、大学生、老年客户等传统银行服务难以惠及的客户，打造专属的“口袋银行”。

三是数字员工以其拟人化形象和高级交互技能，为客户提供多元服务。结合多模态、具身智能等技术，数字员工在智能咨询、银行品牌宣传、实体和虚拟网点等对客服务领域和渠道将展现更为重要的价值。

同时，在银行的内部运营中，数字员工的作用也将日益凸显。一是拥有自然语言入口的数字员工将成为银行IT系统的统一入口，这将极大优化银行内部资源配置和运作效率。二是以数字员工为辅助，银行全员自助分析时代即将到来。大模型驱动的数字员工3.0，不仅可以缩短BI分析

的报表设计、数据建模等交付周期，更可以自动生成最佳决策方案，实现“问答即洞察”，帮助所有人从数据中获取价值。三是数字员工在智能化决策和管理层面上展现出巨大潜力。比如：在智能体等技术加持下，数字员工通过与先进的风险预警系统集成，能够实现风险监控的动态化和智能化，提高风险管理的精准度和响应速度。

7.2 紧跟技术创新趋势，需求驱动动态升级

数字员工的技术创新与人工智能技术的发展和进化密不可分，未来算力、数据、算法将进一步夯实数字员工发展的基石，同时具身智能、多模态、多智能体、端云协同等技术创新，将数字员工演进成一个高度智能化、成本效益优化、与人类思维高度对齐的金融伙伴。

1、算力等基础设施发展将进一步降低数字员工的应用成本。例如目前大模型推理算力投入较大，业界正在采用以存代算等新技术方案降低算力开销，通过将大模型推理结果存储到高性能存储系统中，已处理过的问题优先从存储系统中匹配回复，减少AI芯片的算力开销，提升响应速度，并大幅增强数字员工“长记忆”能力以支撑处理复杂任务。又如，考虑到异构AI算力演进快速，需要推动业界推进同厂商不同型号、不同厂商异构算力的兼容性适配建设和治理，通过提升算力集群异构芯片的兼容性、高中低性能AI算力混合部署等方式降低整体算力投入成本，实现数字员工更高效、更经济的规模化应用。

2、数据合成技术将助力数字员工突破上限。数据是数字员工能力进一步提升的核心要素，数据合成技术的发展将为数字员工提供更加丰富和多样化的信息输入，突破真实数据用尽的限制。比如在需要复杂金融任务推理且真实数据不足的场景中，合成大量长序列、高质量的思维链数据，可显著提升数字员工自动理解并完成长周期规划和推理的高阶复杂任务能力。

3、超大规模模型和强化学习技术推动数字员工向通用人工智能水平逼近。随着模型架构、训练方法、推理形态、知识密度等手段的持续完善，通过思考学习、人类监督、AI辅助和主动对齐等方式最终“控制”人工智能主动向人类对齐，使其行为具有伦理性、可解释性、透明度和可信性。可以预见，未来“超级模型”将数字员工智力提升至类人脑水平。

4、多模态AI帮助数字员工凿穿物理和数字世界。传统上。受技术限制，我们主要依赖结构化等低维度数据进行分析和决策。多模态AI技术的飞速发展，通过利用自各种传感器、摄像头和其他物联网设备的文字、图像、视频、音频等，打破物理和数字世界之间的界限，让数字员工能够有效地理解和交互于复杂的现实世界。

5、具身智能让数字员工从虚拟走向实体。具身智能为数字员工提供“身体”，使其能够在物理世界中执行任务，如客户服务、交易处理等，实现更加直观和人性化的交互体验。

6、多智能体让数字员工更加稳健高效地参与业务协同。智能体是模型的分身，根据用户提出的目标请求，多智能体会调用多个大模型分析推理，并选择最佳路径完成用户任务，实现成本效益最大化。

7、端云协同让数字员工为用户打造个性化专属智能服务。端侧计算的优势在于响应速度快，数据处理在本地完成，避免数据上传至云端可能带来的延迟。如利用端侧AI进行文档智能分类、自动摘要或是日程管理，不仅能快速响应用户需求，还能保护数据隐私，避免敏感信息外泄。同时，通过端侧智能和云上智能的协同，为探索更复杂的金融数字员工应用打下坚实基础。

7.3 强化人才队伍建设，人机协同和谐发展

我们预计数字员工将掀起生产力变革浪潮，人机协同的工作模式将成为企业人力资源发展的重要方向。在这一浪潮冲击下，银行的人员结构、管理模式和组织架构都将发生深远的变革。一是人机协作模式将成为银行的主要工作方式，例如，数字员工可以处理数据统计和报告生成，人类员工则基于这些报告进行战略规划和决策。二是数字员工将与人类员工相互促进、共同进化。一方面通过与数字员工协作，人类员工也能学习到新的技术知识和工作方法。例如：数字员工可以作为人类员工的陪练，指导人类员工掌握算法和数据处理技术，启发人类员工创新灵感等；另一方面通过与人类价值和行为对齐，数字员工的人格将更为完善；三是数字员工将推动银行全面升级员工技能需求和人才梯队建设。这促使银行重塑人才策略，培养数字化复合型人才，强化人机协作能力，以适应数字金融时代的新挑战。

在上述冲击下对于未来的银行业而言，强化人才队伍建设和促进人机协同至关重要，我们认为银行机构应当尽快布局人才梯队建设，构筑人机协作下的智慧银行数字基因。

第一，银行应当规模与质量双并重，构建“人工智能+金融”人才布局，尤其应当聚焦“技术核心、应用范式、场景赋能”三种人才的选育。其中，技术核心人才聚焦算力、算法、数据、平台、安全等技术支撑能力研究和建设；应用范式人才聚焦业务共性需求，提炼业务综合解决方案；场景赋能人才聚焦金融业务具体需求，业务科技融合实现赋能。

第二，银行应当强化数据要素价值，着力打造数字化人才队伍。一是研发测试人才，建立高效科技人才队伍，实现需求、研发、测试一体化端到端全流程的数字员工研发模式；二是业务运营人才，与数字员工开展协同联动的业务运营支持；三是产品运营人才，在数字员工的协助下加大对客户对同业赋能力度。

第三，银行应当加强内部人才培养和外部人才引进。对内，围绕数据科学、数据安全、数智产品、数据治理等领域建设数字化人才队伍；对外，通过与高校、科研院所、各地区行业的人工智能基地合作，挖潜青年骨干，同时提供多样化的职业规划、发展路径、培训机会、资源支撑，吸引顶尖人才。

7.4 做好安全风险评估，完善监管合规机制

随着数字员工在金融领域的应用日益广泛，我们必须清醒认识到其潜在的应用风险和监管挑战。这些风险如果处理不当，可能对金融稳定、客户权益和社会公平造成严重影响。

一是数字员工依赖的生成式人工智能技术存在固有风险，如算法歧视、数据安全、幻觉现象等问题，将导致输出结果不可控、服务质量不稳定、可解释性和可审计性不强等情况，造成操作风险、声誉风险、法律风险等隐患。同时，也要防范外部黑、灰产利用技术缺陷给银行带来业务风险，如伪造身份欺骗数字员工形成交易风险、引导数字员工做出不当言论等声誉风险等等。

二是系统性风险不容忽视。比如，广泛使用训练有偏的信贷审批助手可能会导致金融领域风险评估和信贷决策的同质化，为系统性风险的积累创造条件。一旦发生极端风险事件，人工智能可能会迅速扩大和传播整个金融系统的冲击，并削弱政策应对的有效性。

三是传统的监管框架可能难以应对数字员工带来的新问题，比如，对于数字员工应用的伦理准则和责任界定，以及银行数据安全和隐私保护等，制定适应性强、前瞻性强的监管政策成为当务之急。

为应当上述风险带来的不确定性和冲击，银行和监管机构需要采取积极措施：

第一，在银行机构内部，应当建立针对数字员工全面风险治理体系，包括但不限于：1）建立强大的数据治理框架，确保数据安全和隐私保护；2）定期审核和优化算法模型，消除潜在偏见；3）增强系统的可解释性和透明度，提高决策的可追溯性等。

第二，在金融机构之间，应当针对数字员工进一步打磨最佳实践和行业标准，对于数字员工的应用成本、隐私保护、系统性安全防范、对客服务风险等问题需要进一步凝聚行业共识，协同解决。

第三，监管机构应统筹发展和安全，根据行业共识制定针对数字员工的监管框架。数字员工的发展需要平衡创新与风险控制，既不能扼杀技术创新，又要确保金融稳定和消费者权益，如科技风险和业务风险如何审核，数据运营机制和体系如何构建等。

7.5 结语

大模型开创的人工智能2.0时代正在重塑千行百业，这是启蒙运动以来未有之大变局。以大模型为核心的数字员工3.0引领的智慧金融革命浪潮，将为银行业带来前所未有的机遇与挑战。

在这场变革中，商业银行唯有勇立潮头，方能把握先机。银行业应当积极拥抱新技术，深入探索数字员工的应用场景，不断扩大其应用范围和深度，并建设适应智慧金融纪元的人才梯队，培养能够与数字员工协同工作的复合型人才，打造人机协作的新型金融服务模式。在此过程中，我们也需要高度重视风险管控，建立健全的监管机制，确保数字员工的应用合规、安全、可控。

我们相信，通过持续的技术创新和实践探索，以大模型为核心的数字员工3.0将成为推动银行业数字化转型的重要力量，为打造一个更智能、更高效、更优质的金融服务体系提供强大动能，高质量落实金融五篇大文章，助力金融强国建设。