对话光大理财股票投资部总经理梁珉

“飞机装上多引擎”：理财公司靠“配置力”破风

视觉中国图片

制图/韩景丰

“如果做单一资产，就好比一架飞机只有一个引擎；多资产、多策略，就是让飞机装上多个引擎，让飞行更平稳。”光大理财股票投资部总经理梁珉这样比喻他所在部门的核心职能。

当理财行业全面步入净值化时代，低利率成为市场常态，客户的收益预期仍未脱离过往认知，现实与预期的错位成为行业共同面对的考题，而“固收+”被视为破局之法。对光大理财而言，这场转型来得更为彻底——2025年，纯固收产品全面转向“固收+”，这也推动公司向配置型机构加速转身。

锚定稳中求进的航向，光大理财在多资产、多策略的领空里，铺开两条并行的航道：一是让各类资产互为风翼，利用不同资产之间的负相关性缓解组合风险；二是在不同赛道反复下潜、细致筛选，努力挖掘资产的超额收益。

● 本报记者 程竹 李静

产品转型驱动多元配置

进入2026年，摆在理财行业面前的考题是客户预期与现实之间的错位。“理财已全面净值化，但很多客户的心态还没转变。”梁珉说，同时在低利率环境下，资产收益率在下降，这与客户收益预期形成错位，这是压力，也是机遇，“净值化，恰恰放大了专业能力的价值”。

光大理财的应对从产品转型开始。“目前，我们的理财产品类型从纯固收类全面转向‘固收+’。”梁珉透露，去年3月，光大理财正式推出全新产品序列“光盈+”，发力“固收+”赛道，全公司“固收+”产品规模从去年年初的不足千亿元跃升至目前的超3000亿元，“随着产品结构转型，公司也需要向配置型机构转型”。

这场转型不是简单的仓位腾挪，而是一套从风险预算出发的阶梯式迭代。梁珉将其概括为积极与审慎：“积极是转型的态度，审慎是对风险的把控。我们是从0含权的纯固收类理财产品，逐步向5%、10%、20%的含权比例‘固收+’产品推进，同时运用黄金、海外资产、指数增强、CTA等多元资产与策略进行组合配置，在提升收益弹性的同时努力保持稳健的投资体验。”梁珉说。

产品转型的齿轮一旦转动，多资产、多策略配置能力便不再是一道选答题。今年黄金市场剧烈波动，更是成为检验多资产组合的一次真实压力测试。“这次波动让我们重新思考，当组合中某一类资产价格大幅下跌时，该如何应对？我们将从工具储备、管理机制等维度入手，把应对极端风险内化为投资能力。”在梁珉看来，对多资产、多策略配置而言，第一位永远是风险，而非收益。“目前黄金的波动率与股票相当，它不再是避险资产，而是风险资产。我们会依据波动率进行加减仓决策。”他说。

三重目标构建护城河

这场产品转型的背后，是对多资产、多策略配置能力的深层打磨，围绕稳中有进这一投资诉求，梁珉将多资产、多策略的内核拆解为三个层次的目标：“第一，寻找多样性收益来源；第二，在风险端做好不同策略、不同资产的配置；第三，用更多手段控制回撤。”

寻找多样性收益来源，是布局多资产、多策略的第一步，光大理财的核心要求是策略的稳定性、持续性与可复制性。“无论是自主研发红利、指数增强等策略，还是筛选引入外部策略，首要标准都是阿尔法收益的可持续性，杜绝昙花一现的收益表现。在此基础上，我们会对所有策略和管理人开展全面体检，重点核查策略的清晰性与可跟踪性。”梁珉说。在策略运作过程中，光大理财会持续跟踪，一旦发现策略目标模糊、风格漂移或阿尔法收益衰减，会第一时间开展归因分析，判断管理人在对应风格下的能力是否衰退。

基于客户需求倒推风险端配置是第二层目标的核心逻辑。梁珉表示，光大理财的多资产、多策略配置是以客户的风险承受能力为出发点搭建框架。比如，在权益内部平衡价值、成长等风格暴露，在多资产层面引入黄金、海外资产、CTA等分散因子，并用风险平价或风险预算按“风险贡献”来校准权益与黄金等权重，使组合在回撤约束下更稳健、更可控。

建立系统化的流程机制，用多元手段控制回撤，是筑牢资产组合护城河的关键。“我们有三大法宝：一是用资产和策略的多样性分散风险，实现‘东方不亮西方亮’的对冲效果；二是不同于收益端预测，我们从风险端进行预测，以波动率为核心指标，一旦资产波动率过高，即便收益表现亮眼也会选择降低仓位；三是将所有风控要求体系化、纪律化，让风险管控成为投资中的‘肌肉记忆’。”梁珉强调，理财配置不求短期业绩第一，而是要在市场波动中“不下牌局”，始终保持创造收益的潜力，这也是多资产、多策略配置的核心价值：把生存率提高，才能把长期收益率做大。

借力成势

如何将多资产、多策略的理念，落地为可执行的投研体系？梁珉用手掌比喻：“我们部门就像一只手，五个指头，代表五个业务组，分别是量化组、FOF/MOM组、衍生品组、股票直投组、低波多元组。手掌，则是部门的策略中台。”各业务组在各自赛道挖掘投资机会。

策略中台则扮演“路由器”的角色，要为各组赋能，更关键的是打通策略之间的“篱笆墙”，实现投研能力的互联互通，并将分散的能力整合为系统化的配置方案。梁珉强调，理财公司的投研团队必须成为“六边形战士”——既要有专精领域，也需对各类策略具备中等以上的理解力，才能把多样化的策略真正组装起来，形成合力。

在这一架构下，光大理财采取了“委外合作+自研深耕”的双轨路径。梁珉坦言，理财公司规模体量大、需求覆盖广，但直接下沉至个股的研究人才密度短期内难以比肩成熟公募基金。“因此，我们首先要把市场上最优秀的管理人变成合作伙伴，站在巨人肩膀上，快速整合多元策略。”这种“管理人的管理人”模式，正是理财公司发挥平台优势、实现高效资产配置的关键。

这并不代表理财公司放弃自研。“除了精选市场上优秀的外部管理人，我们与基金公司等资管机构的核心差异点，其实在第二层——把多个优质资产、策略组合在一起的能力。”梁珉说，“公募基金追求的是个股阿尔法收益，而理财公司更需要回答：股票如何与黄金搭配？怎样纳入海外资产或CTA策略？这道配置题才是我们必须持续自研、不断打磨的核心。”

事实上，光大理财始终坚持并强化着股票直投团队的建设，在能力圈内，团队深耕基本面研究，持续积累认知。“唯有将外部优质投研能力与自主投研结合，才能构筑更具深度的投资能力。2025年，光大理财自主管理的权益类理财产品，收益率斩获全理财行业第一，这份成绩单离不开团队的自研能力。”梁珉介绍道。

当前，光大理财正持续挖掘新的资产类别、甄选优质策略，为多资产、多策略配置丰富工具箱。“今年将重点关注公募REITs与海外资产，这主要出于分散风险的考虑，我们需要寻找与A股、与债有不同收益来源、不同风险因子的资产，公募REITs分红稳定、属性独立，海外资产则可分散单一市场风险。”梁珉说，“只有资产还不够，还需要有策略将资产进行组合，全天候、风险平价、宏观多因子、高频动量……这些策略没有高下之分，关键是哪家机构能做得更好，以及光大理财如何更好借力，为投资者创造长期可持续的投资回报。”

龙虾闯入金融圈：一场关于效率与安全的高压测试

● 本报记者 吴杨

一只红色的龙虾正试图撬动金融业严谨的大门。近期，开源AI智能体OpenClaw（其图标为一只龙虾）凭借低代码门槛与自主执行任务的强大能力，从科技领域火爆出圈。它号称是7×24小时在线的AI秘书，能写代码、盯数据，甚至能辅助交易——不再局限于“给出建议”，而是真正开始“动手干活”。不过，记者在采访中了解到，面对这只挥舞着双钳的龙虾，大多数金融从业者并未急于尝鲜，反而持审慎的观望态度。

诱人的“生产力钥匙”

“OpenClaw具备优秀秘书的关键能力。”中信证券科技产业首席分析师许英博表示，高度拟人化是OpenClaw的核心亮点，具体体现为高效便捷的交互方式、对用户偏好的持续记忆能力，以及系统级的操作权限。

方正证券研究所金融工程首席分析师曹春晓认为，对于大量做主动投研的从业人员来说，OpenClaw可以大幅降低使用各种工具、数据以及构建量化选股策略的难度，也可以将投资者从枯燥的重复劳动中解放出来，更专注于复杂的决策、创新策略的研究开发等。而在量化投研领域，可以利用它完成因子研究、策略复现等高强度工作。

这种重塑生产力的潜力，已经催生了不少“尝鲜者”。某保险公司人士向记者分享了他的亲身体验：“龙虾在国内外社交媒体上爆火时，我就进行了部署。它确实很方便，有利于提高工作效率。”

在不少金融从业者社群中，关于龙虾的讨论帖持续刷屏，讨论焦点从“它能做什么”延伸到“我们能不能用”“什么时候能用”。一位银行金融科技部门人士向记者表示，近日同事们都在讨论它，部门内部也已组织研讨，研究OpenClaw的技术架构及其在投资辅助等场景的适配性，“即使暂时不能用，也得先搞懂它”。

隐私和安全问题令人担忧

就在OpenClaw热度持续攀升的同时，一个关键问题浮出水面：它安全吗？上述保险公司人士坦言：“养好它需要一个很长的过程。我用一部新电脑部署安装，就是担心隐私、数据泄露问题，毕竟相当于让这个智能体暂时接管了自己的鼠标。”

这种担忧并非杞人忧天。西部地区某中小银行金融市场部人士表示：“龙虾要真正发展起来，还有很长的路要走。与传统的软件不同，智能体之所以能干活，核心在于它被赋予了极高的系统权限——可以读取文件、发送邮件，甚至执行代码，它拥有的权限远超对话式AI。”

东方证券研究所计算机前瞻科技首席分析师陈超从技术层面剖析了相关风险。他表示，由于OpenClaw在权限管理上具有高度灵活性，一旦失控可能导致大规模数据泄露或系统指令误操作。作为一个具备系统级权限、能自主执行Shell命令和文件操作的框架，OpenClaw将攻击面从单纯的“对话注入”扩展到了“执行链路劫持”。这种复杂性要求安全厂商必须研发能够适应新场景的安全产品或解决方案。

监管层面，3月15日，中国互联网金融协会发布的《关于OpenClaw在互联网金融行业应用安全的风险提示》认为，OpenClaw智能体虽能提升工作效率，但其默认的高系统权限与弱安全配置，极易被攻击者利用，成为窃取敏感数据或非法操控交易的突破口，给行业带来严峻的风险挑战。日前，国家互联网应急中心也发布了关于OpenClaw安全应用的风险提示。

金融圈人士多持观望态度

面对龙虾既诱人又危险的钳子，绝大多数金融从业者选择了审慎观望。

东部地区某中小银行人士表示：“长远来看，它肯定有很大的应用空间，但因为银行是风控要求很高的机构，短期内更需要评估其风险性，不会过快在行业中全面布局。另外，它也很贵啊。”

一位业内人士道出了另一层隐忧：“AI自身的幻觉是潜在风险之一。智能体的决策始终基于模型，因此无法完全杜绝出现幻觉的可能，这需要用户在实际操作中不断加以纠正。”

因此，多位金融从业者在接受记者采访时预计，短期内将不会看到OpenClaw在金融核心业务中的大规模应用。

对于这一技术带来的挑战，中国互联网金融协会给出了明确的指导性建议：金融消费者在办理网上银行、证券交易、支付等个人金融业务的终端上应极其谨慎安装OpenClaw；如确有必要安装，建议不授予金融服务类系统操作权限，及时跟进OpenClaw漏洞修复，严控功能插件安装，不在使用时输入身份证号、银行卡号、支付密码等敏感信息。另外，此类应用在运行过程中持续调用大模型接口，可能会产生较高的Token费用，建议使用者密切关注。

从500元装虾到199元卸虾 谁在AI淘金热中稳赢

● 本报记者 李静

两周前刚花500元请人上门“装虾”（部署AI智能体）的人，现在又开始花199元找人远程“卸虾”了。烧钱、卡顿、删邮件——当打造“数字员工”的梦想撞上现实，部分AI智能体“养虾人”纷纷撤退。在这场热潮里，真正靠AI“挖金”的人寥寥无几，反倒是提供部署、教学、卸载服务的“卖铲子”群体成了赢家。

“卖铲子”的人赢了

在某交易平台上，“彻底卸载OpenClaw”的服务悄然增多，价格从几十元到几百元不等。北京上门卸载OpenClaw标价299元，基础远程卸载199元，服务内容包括彻底停止服务、清理所有配置文件、删除安装包、深度清理残留文件等。有商家甚至打出广告：“装了OpenClaw后悔了？卡顿、弹窗、API被盗刷，专业远程卸载帮您彻底清除。”

几个月前，OpenClaw横空出世，这款号称能像人手一样操作电脑、手机的AI智能体，被寄予了成为“数字员工”的厚望。近期，在社交平台晒出“养龙虾”成果的帖子层出不穷：有人用它整理会议纪要，有人让它订机票酒店，还有博主宣称“我的龙虾已学会盯盘，零代码养出一个‘数字巴菲特’”。这场“养龙虾”热潮甚至烧到了线下。美团近日在北京举办“免费装龙虾”主题快闪活动，现场有工程师免费为市民安装OpenClaw，不少人带着笔记本电脑前往体验。

然而在这场热潮中，目前真正获利的并非“养虾人”，而是“卖铲子”的人。大家忙着追逐概念，却鲜有靠这款AI智能体实现价值、“挖到金矿”的案例。在各类交易平台上，提供OpenClaw部署服务的商家随处可见，每单收费数百元，还有人兜售所谓“养虾秘籍”，靠教学、指导用户训练龙虾获利。

龙虾不好养

从争相“装虾”到扎堆“卸虾”，最直接的原因就是成本太高。

跨境电商从业者李想（化名）是第一批“养虾人”。听说OpenClaw能自动处理订单、回复邮件、监控竞品价格，他立刻花500元找人上门部署。“我原本以为，每天睡醒后，AI就已经把所有重复工作做完，我只需要做决策。”李想说，可这位“数字员工”上岗第一天就状况百出，闲置忘关了一整夜，Token消耗惊人，一晚上就烧掉近30元。

有网友晒出自己“养虾”7天的账单：部署调试23.5元，自动回复评论8.2元，写周报、整理邮件15.7元，数据抓取67.3元，闲置忘关扣费31.2元，日常办公辅助12.4元，测试新功能19.8元，一周总计花费178.1元。“最烧钱的不是对话，是后台死循环。有一次抓取任务卡住，3小时就烧掉50元。”该网友表示。

此外，想把这只龙虾训练成得心应手的“数字员工”，也比想象中困难。有用户让龙虾查询国际金价并在Excel里生成图表，折腾半小时，只调出了数据，图表始终没能生成。

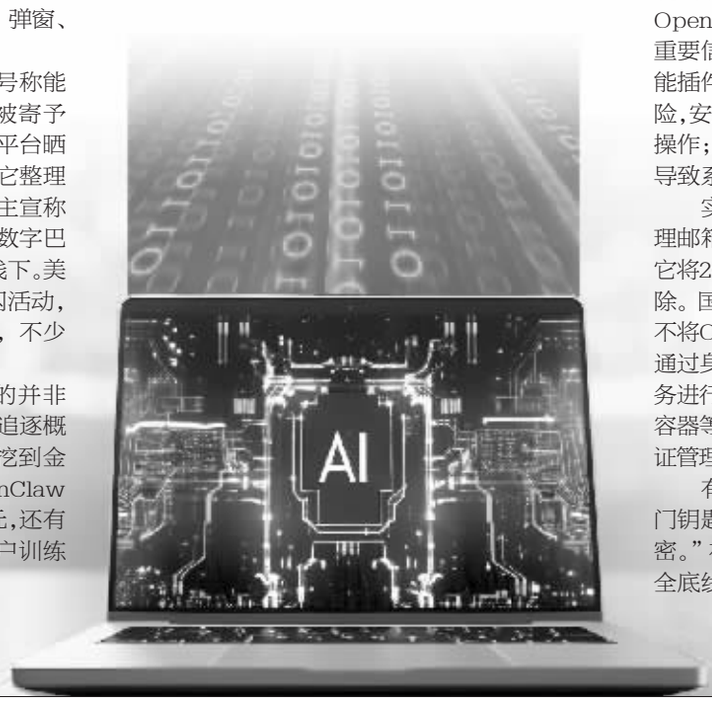
安全隐患不容忽视

更值得警惕的是安全失控。近日，国家互联网应急中心微信公众号发布风险提示：OpenClaw默认的安全配置极为脆弱，存在提示词注入、误操作、功能插件投毒、安全漏洞四大风险。

具体来说，攻击者可通过在网页构造隐藏的恶意指令诱导OpenClaw读取该网页，并泄露系统密钥；由于错误的理解用户操作指令和意图，OpenClaw可能会将电子邮件、核心生产数据等重要信息彻底删除；多个适用于OpenClaw的功能插件已被确认为恶意插件或存在潜在的安全风险，安装后可执行窃取密钥、部署木马软件等恶意操作；已曝出的多个高中危漏洞可能被恶意利用，导致系统被控、隐私信息和敏感数据泄露。

实际案例已敲响警钟。一位用户让龙虾帮忙整理邮箱，结果指令被“过度理解”——眼睁睁看着它将200多封包含合同、报价单的重要邮件全部删除。国家互联网应急中心建议用户：强化网络控制，不将OpenClaw默认管理端口直接暴露在公网上，通过身份认证、访问控制等安全控制措施对访问服务进行安全管理。对运行环境进行严格隔离，使用容器等技术限制OpenClaw权限过高问题；加强凭证管理，避免在环境变量中明文存储密钥。

有业内人士打了个比方：“这就好比你把家门钥匙交给一个陌生人，还告诉他你家的所有秘密。”在AI深入接触个人数据的同时，如何守住安全底线，仍是待解难题。



视觉中国图片