

大模型对企业数智化升级与业务经营的影响与应对

易观智慧院

2023年6月

大语言模型开启AGI时代，人工智能进入生成式阶段

什么是大模型？

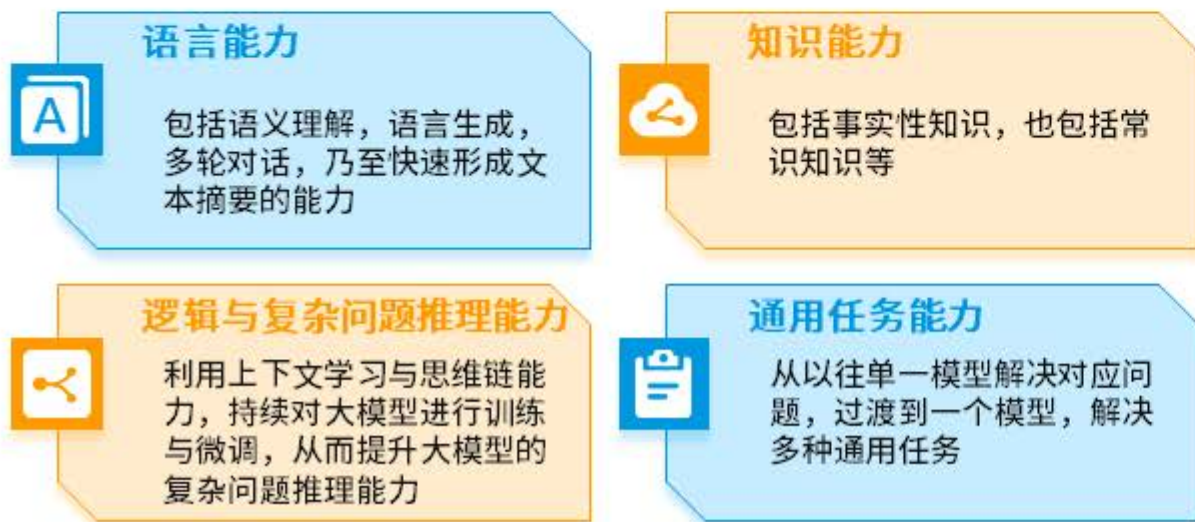
大语言模型（LLM）是建立在大量数据集上预训练的巨大大模型，包括如下关键要素：

- 海量算力与数据支撑的大参数
- “涌现”智能能力，拥有解决它从未或极少见过的问题的能力
- 预训练，仅需要少量数据的微调甚至无需微调，就能够解决多种通用型任务

大语言模型/基础模型训练过程



大语言模型关键能力



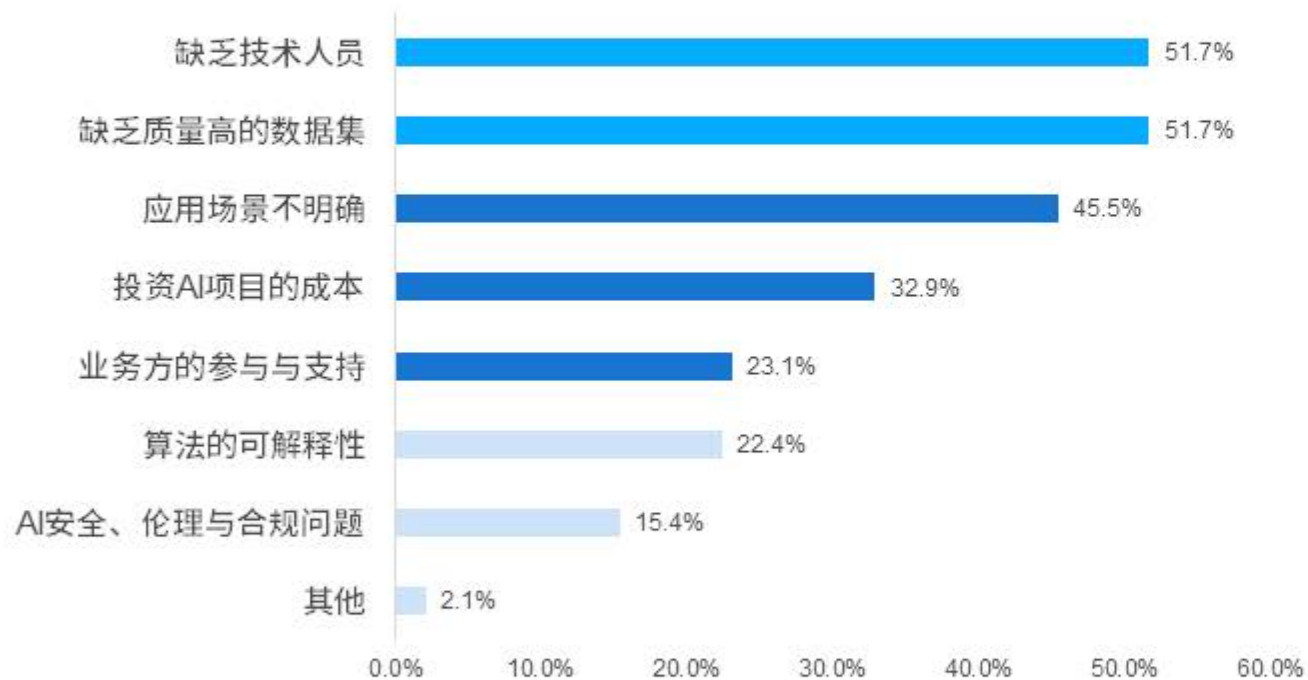
人工智能与AGI发展阶段划分



大语言模型推动企业从数字化向智能化升级

大模型对企业带来的核心价值是什么？

中国企业部署AI应用所面临的挑战



数据来源：埃森哲2020，易观整理

©易观Analysys

www.analysys.cn

01 以业务驱动的方式拥抱AI

人工智能从未如ChatGPT这般普及，超过1亿用户主动体验的背后，是业务发展需求驱动AI应用场景探索与实践的重大转变

02 降低AI开发门槛

传统的AI开发模式需要针对不同的任务和场景进行定制化开发，大模型显著降低开发复杂度，提升部署与应用的便捷度

03 增强用户体验，砸平企业数智化洼地

大模型对于人机交互方式的变革显著增强客户/用户体验与员工体验，有利于中后台赋能升级，以及员工原生数智智能发展

大模型应用尚未跨越鸿沟，尝鲜者重心在于技术突破与场景探索

企业应用大模型可能面临的挑战与风险有哪些？

技术局限尚需突破方能释放更大价值

1

- 知识更新与自主学习能力，目前大语言模型仍然为静态数据驱动的学习范式，无法实现新知识的快速学习与迭代，尤其是涉及到时效数据与专有数据的场景下存在障碍，OpenAI正在通过Plugins生态来突破这一局限
- 垂直领域泛化能力，通用任务的卓越能力已经显现，但是进入垂直细分领域与知识体系下，大模型的性能与泛化能力仍然需要增强，行业大模型训练是当前挑战的破局之道之一
- 长期记忆能力，目前正在通过增大上下文容量、数据向量化，以及AI agent等多种方式探索突破

巨大的模型训练与推理算力等成本拉低效益比

2

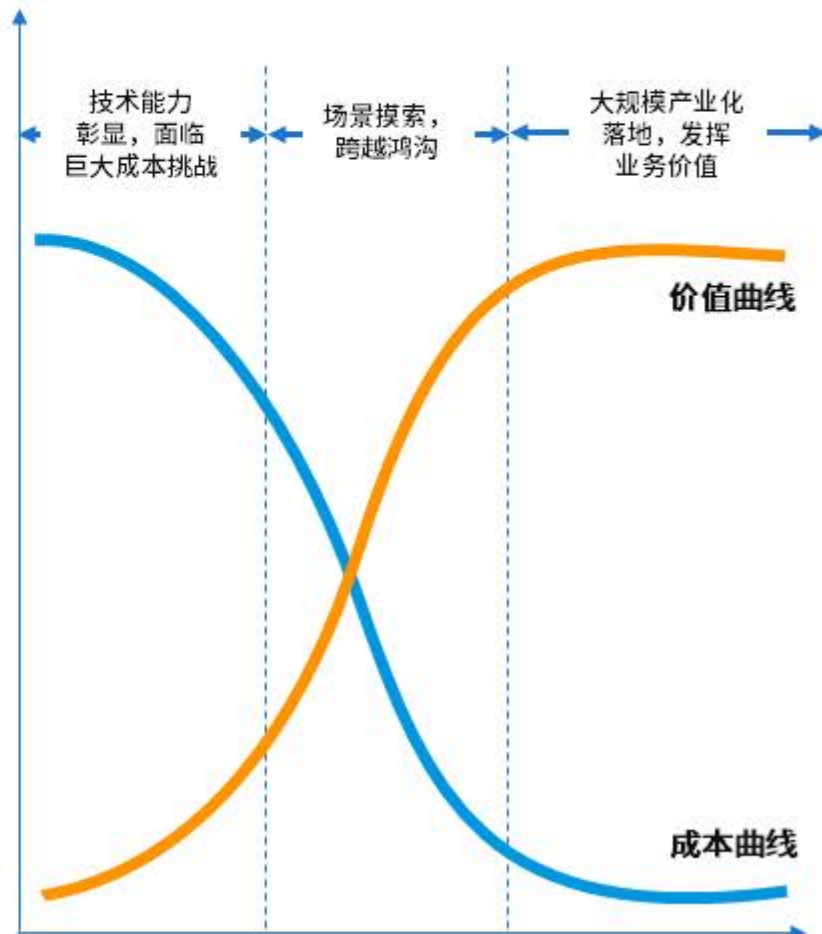
- 训练与微调成本，该训练成本仅针对企业应用基础模型结合行业知识与数据集进行训练与微调的成本，并非基础大模型训练成本，与上述“垂直领域泛化能力”相对应，该成本仍然为行业知识壁垒显著的企业必须承担的成本，开源基础模型在一定程度上可以降低这一阶段的训练成本
- 推理成本，大模型在参数体量巨大的情况下，仍然存在较高的推理成本，这方面可以通过模型压缩与剪枝等技术的发展进一步降低
- 模型能力与业务场景的适应成本，这部分成本虽然由于人机交互方式的变化显著降低，但是前期仍然需要考虑提示工程在特定场景的磨合成本

安全合规可信应用底线尚需刚性保障

3

- 模型安全与可控制性问题，这是人工智能普遍面临的问题，大模型并不能幸免，包括模型攻防、数据注入等问题；同时，模型能力来自于“涌现”，需要进行模型能力，尤其是生成结果的可控制，方能进入到生产环境
- 对齐问题，既包括人工智能与人类社会价值观保持一致，也包括与不同国家价值观，不同类型企业经营以及商业法则相匹配等，前者最为关键，这也是目前最为关注的AI不受控制的风险之一，目前在通过RLHF与RLAIF不同方式来实现
- 隐私与数据安全问题，无论是大模型的训练推理，还是对话应用的过程中，都存在过多的隐私暴露与数据安全风险，这有赖于技术突破和监管合规的进一步建立

大模型应用曲线



大模型所加速的生成式人工智能已经渗透到多个场景

生成式人工智能，到底在生成什么，应用到哪些场景？



文本

- 对话/问答
- 文档/文本/文案生成
- 内容/会议摘要等
- 语言翻译
- 文学/剧本创作等

01



代码

- 自然语言生成代码
- 代码补齐
- 生成SQL
- 生成软件测试用例
- 合成数据等

02



图像

- 图像分类/分割
- 工业设计
- 医学影像标注与解剖结果构建
- 艺术/商业作品创作
- 图像修复
- 天文观测、卫星遥感观测等

03



音视频

- 信息播报
- 语音编辑/翻译
- 影视内容分析编辑
- 视频增强/风格迁移
- 音乐/视频生成

04



3D

- 电影/游戏/动画制作
- 建筑/家居设计
- 工业制造
- 工业/艺术设计
- 医疗健康
- 虚拟现实等

05



分子发现

- 药物设计
- 材料科学
- 食品与农业
- 能源
- 个人护理等

06

大模型能力与AIGC相结合向企业经营关键环节渗透

企业可以考虑从哪些环节应用大语言模型？



企业拥抱大模型，从应用场景入手探索最佳实践再规划自建路线

如何对大语言模型（LLM）进行部署与应用？

自建MaaS能力，实现技术驱动

适用于数智技术驱动的行业，同时，企业IT投入与研发能力相对较强，能够将科技能力作为重要竞争力的行业与企业

灵活应用AI能力，赋能业务经营

适用于大多数企业，IT能力建设并非重点，但是需要利用AI能力提效降本，赋能业务经营

1

端到端自主训练大语言模型

关键考量：

- 具备高算力资源基础
- 高密度AI工程化团队
- 数据资源持续投入能力

企业实践：

以头部科技企业为主，如百度、阿里、腾讯等，不仅自主训练大模型，同时对外输出模型服务；又如三星，出于自身应用需求和数据安全考量，进行大语言模型训练，尚未披露是否对外输出相应服务

2

利用开源模型，或者与LLM供应商进行联合研发与微调，训练专有模型

关键考量：

- 算力资源基础与投入仍为必须
- 基础模型选型，或LLM供应商选型
- 自有AI团队能力图谱与拓展，实现专有模型可持续运营与迭代
- 专有数据储备沉淀与持续运营

企业实践：

行业头部企业，例如中国工商银行、Bloomberg等，进行金融行业专有模型训练，契合金融场景业务需求，实现技术驱动

3

采购或者利用开源大模型API，利用向量化方式，优化自身应用

与方式②相比，算力资源投入相对较低，同时降低对于算法能力的要求

关键考量：

- 自身应用对于AI能力的抽象与对模型的驾驭能力（Plug-in生态）
- 专有数据沉淀与向量化处理能力

企业实践：

中型企业在借力AI能力升级服务水平与平衡AI投入成本后普遍采取的方式，例如企查查通过向量数据库承载搜索引擎，将模型放在端侧进行部署，以较低成本提升产品AI功能水平与品质

4

调整目前企业应用的选型策略，提升AI能力评价权重

适用于大多数企业拥抱数智化的场景，是企业软件AI能力的整体升级

关键考量：

- 业务经营目标驱动
- 提示工程（Prompt Engineering）能力
- 更新企业软件选型标准与合作伙伴

企业实践：

钉钉接入通义千问全面升级协同办公智能化水平，变相提升企业智能协同与办公应用选型标准，包括HR、财务、客服等应用皆是如此

科学评估用例价值，进而建立高效益比的MaaS路线

起步探索最佳用例

领先头部企业自建私有大模型需综合考量，忌忽视产品与生态能力

如何对基础大模型合作伙伴进行选型与评估？

应用层



中间层

中间层生态是大模型能力的重要体现



模型层

备注：大模型产品仅为示例，未包括海外大模型企业



基础设施层



模型能力

★★★★

需要关注基础大模型的关键能力，包括语言能力（简单理解、知识运用、推理能力、特殊生成等）、安全和价值观以及通用任务能力，可以参考FlagEval（天秤）语言大模型评测体系



产品能力

★★★★

需要关注基础大模型的产品化封装与解决方案能力，包括大模型能力抽象与API化易用性、大模型训练与微调环节支撑与服务保障能力、任务场景实践能力，以及运营维护保障能力等



生态能力

★★★

侧重大模型生态发展策略以及布局情况，包括中间层生态是否完整丰富以便于模型的精调与持续运营，关键环节国产供应链布局与适配度，行业伙伴以及最佳实践案例，开源策略与协议等



可持续发展能力

★★

基础大模型非一蹴而就就需要持续投入与迭代，需要关注大模型企业战略路线与资源投入程度和专注度、人才梯队建设与核心人才情况等

选型企业应用标准被升级，AI能力权重上升

大模型能力蔓延，对于企业应用选型有何影响？



企业类型B：中小型企业灵活应用AI能力，赋能业务经营

调整目前企业应用的选型策略，提升AI能力评价权重，关键考量标准：

- 认知沉淀/行业Know-how→专有数据
- 技术应用能力→理解模型能力，并能够灵活驾驭模型的能力
- 交互协作体验→workflow整合能力

企业类型A：大型企业自建MaaS能力，实现技术驱动

规划企业自身AI策略与MaaS能力的过程中，将基础模型与应用的能力边界竞合融合纳入考量范围：

- ① 部分应用能力壁垒被大模型击穿，纳入MaaS能力范畴沉淀为中台能力
- ② 其他应用持续增强AI赋能，提升解决特定场景与任务的能力，不定期扫描

业务为纲，机制兜底，企业组织发展模式将发生深刻变革

如何规划未来3-5年大语言模型与AIGC在企业中的应用？

01 业务为纲规划人工智能上线与推广计划

“所有行业都值得用大模型重新做一遍”，前提是围绕用户与客户价值的体验升级与业务发展，相应地，人工智能与企业数智化转型一致，业务驱动是核心原则，围绕业务发展扫描数智化洼地，规划人工智能应用用例，获取业务价值，并形成迭代优化扩大AI应用范围的闭环

02 专有数据资产沉淀与管理，应对模型训练与应用

无论是自主训练大语言模型，还是围绕自身行业与业务场景进行模型精调，都需要依赖于企业过往积累的专业领域知识沉淀，进行专有数据语料的准备，从而能够让基础模型的“通才”能力发展成为具备行业属性的“专才”，专有数据是未来模型能力平民化后的重要差异化

03 设定人工智能应用合规与风险管理防范机制

生成式人工智能仍然可能出现“幻觉”、数据泄露等各种风险；同时，关于人工智能与大模型应用方面的立法与规范仍然处于意见征集与调研的过程中，企业有必要主动制定人工智能应用合规与风险管控机制，包括AI开发、应用与审核规范，数据安全规范，员工应用权限规范等等，从而“安全合规”地应用人工智能提升企业竞争力

未来组织能力围绕人工智能发展，既包括创造人工智能，也包括应用人工智能，前者是少数，主要在于提升人工智能专业与高级人才密度，并通过组织协同设计，系统化地提升人工智能科研与工程化水平。

后者是多数，也就是大部分人工智能企业更需要考虑的是，人工智能应用，尤其是生成式人工智能全面铺开过程中，对于组织架构、组织中关键角色与职能、以及对于员工的潜在影响等。

对于个体而言，普遍关注“人工智能会/不会替代什么职业”，甚至引发了对于某些职业发展方向的焦虑，一方面，积极的员工与个体正在迅速拥抱人工智能，在工作的过程中应用生成式人工智能提升工作效率，可能正在出现人工智能赋能于员工优先于组织的情况；另一方面，大众员工可能出现观望、等待甚至无所适从，“无用”内卷的状况，。

这就需求企业对于组织角色与员工发展进行整体规划，不同职能与角色人与人工智能的协同边界如何确定，组织中关键角色与员工的技能与“AI商”升级如何系统化通过培训等手段推动，都是企业系统化提升组织能力与竞争力的关键举措

组织系统协同员工能力协同进化与升级04

激发科技与创新活力

易观



数字经济全景洞察

易观千帆



金融行业数字用户
同业对标

易观方舟



全场景私域用户运营

易观社群



加入易观社群
与行业伙伴一同交流