

超越 MLOps

解析 LLMOps 的新范式

刘喆

个人简介

2010 年	百度大数据	SRE
2011 年	人民搜索	运维部总监
2013 年	AdMaster	大数据平台负责人
2021 年	白海科技	联合创始人兼技术负责人

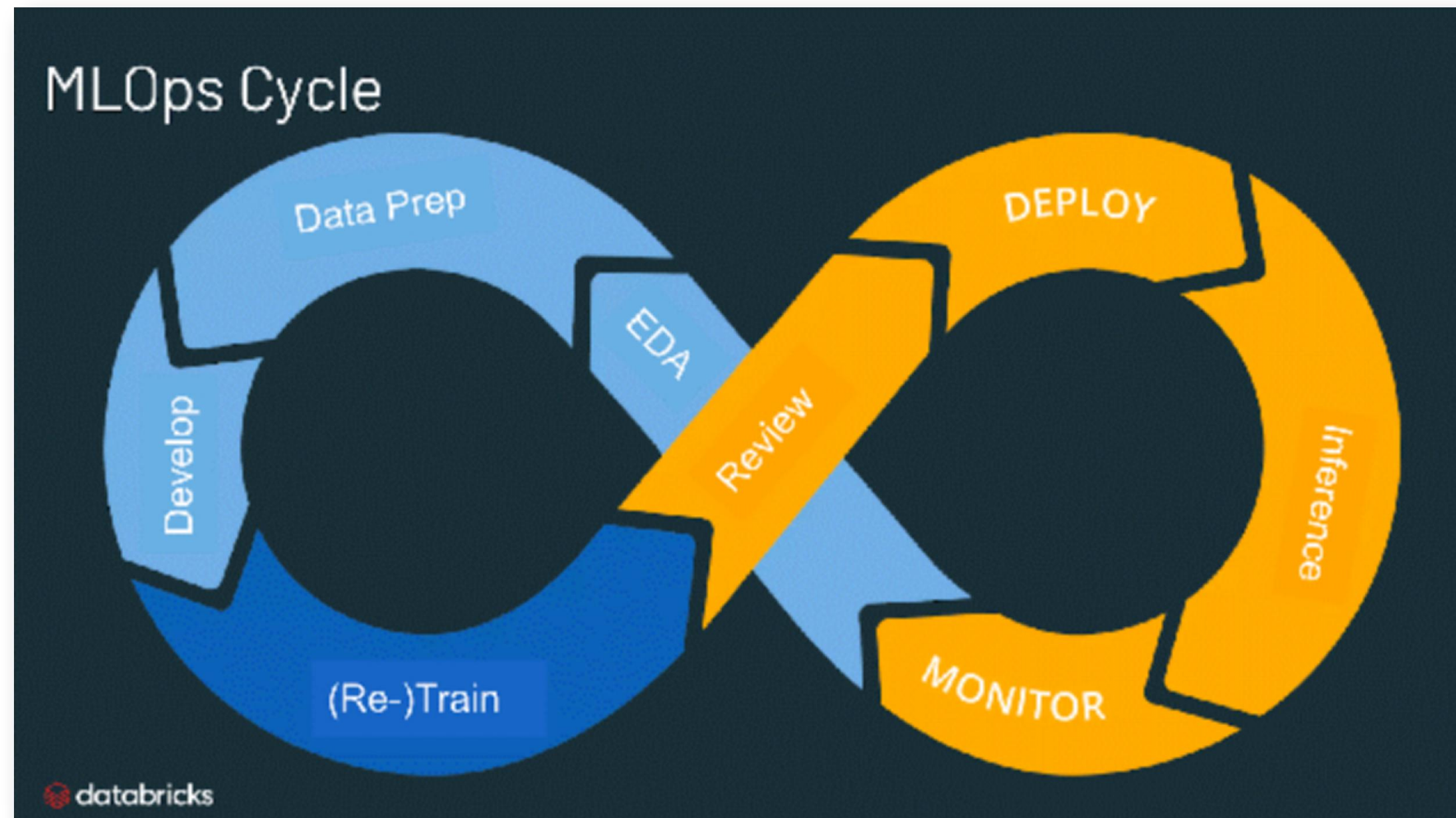
2014 - 2019 年在 51CTO、Qcon、Spark 峰会等作过几十次演讲

主要内容

- *LLMOps 概述: 概念、起源、与 MLOps 的异同*
- *白海科技 LLMOps 实践分享*
- *面向未来: LLMOps 的应用前景*

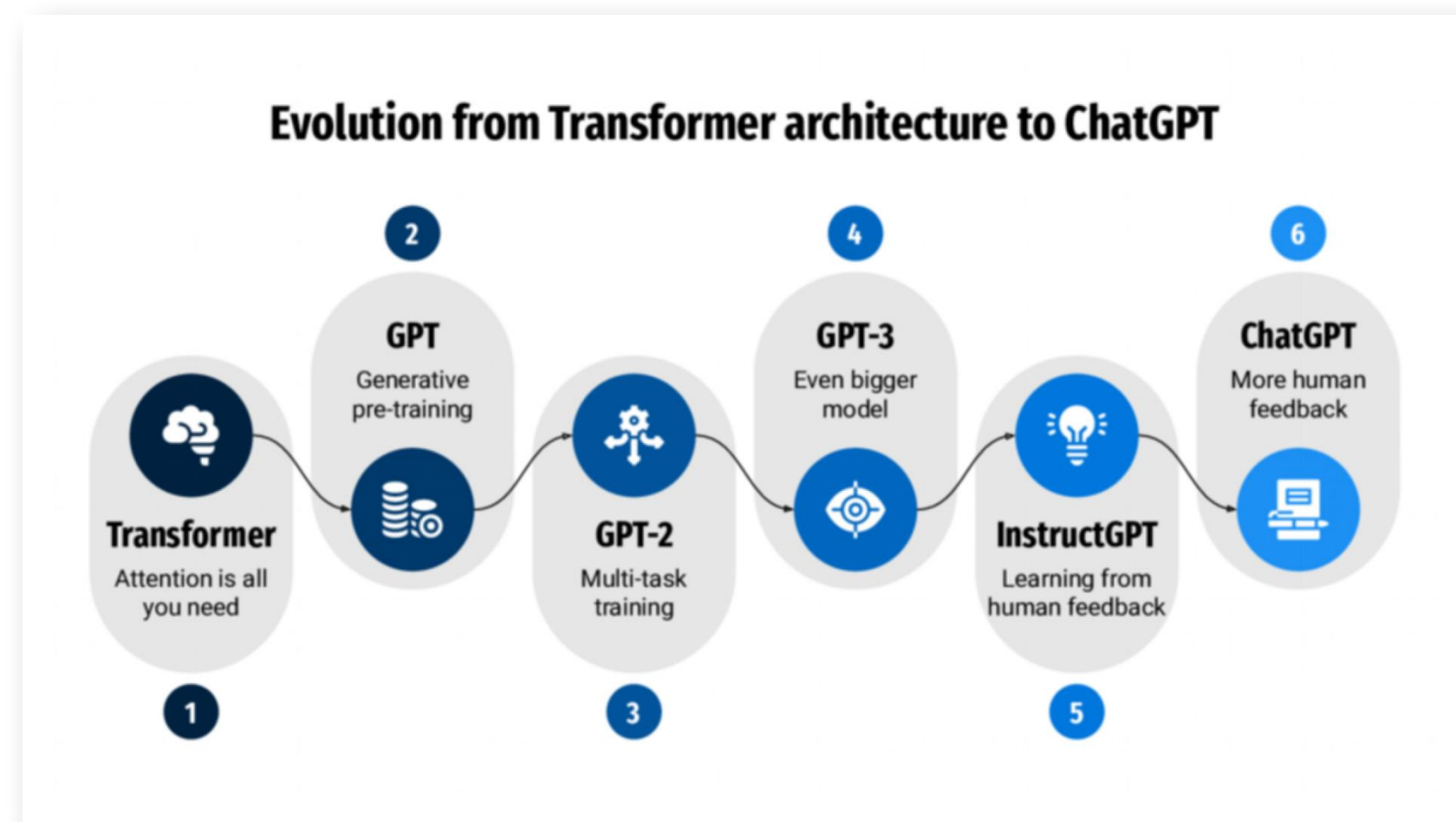
LLMOps 概述：概念

- Ops for LLM
- MLOps
- 指导路线
 - ✓ 标准化
 - ✓ 自动化
 - ✓ 智能化

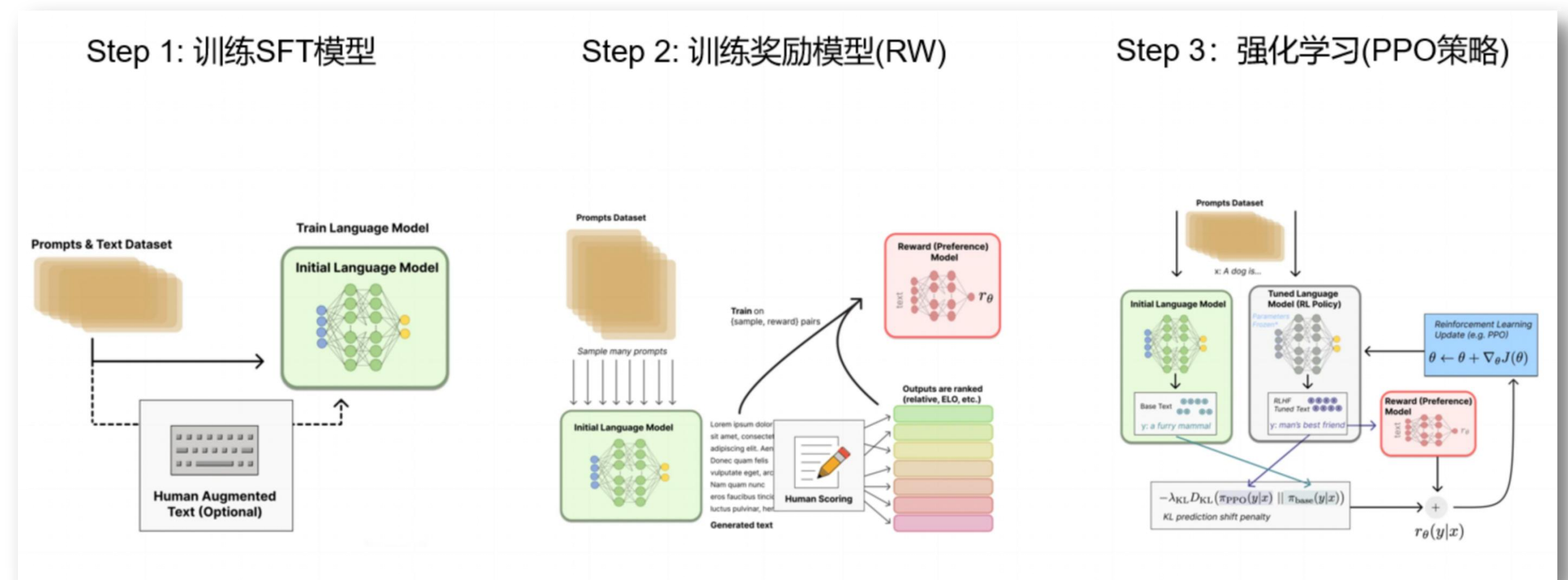


LLMOps 概述: 起源

- 2022 年 12 月 ChatGPT 出道
- 2023 年 2 月 LLaMa 参数泄漏
 - ✓ 从“造模型”到“训模型”
- InstructGPT RLHF方法论

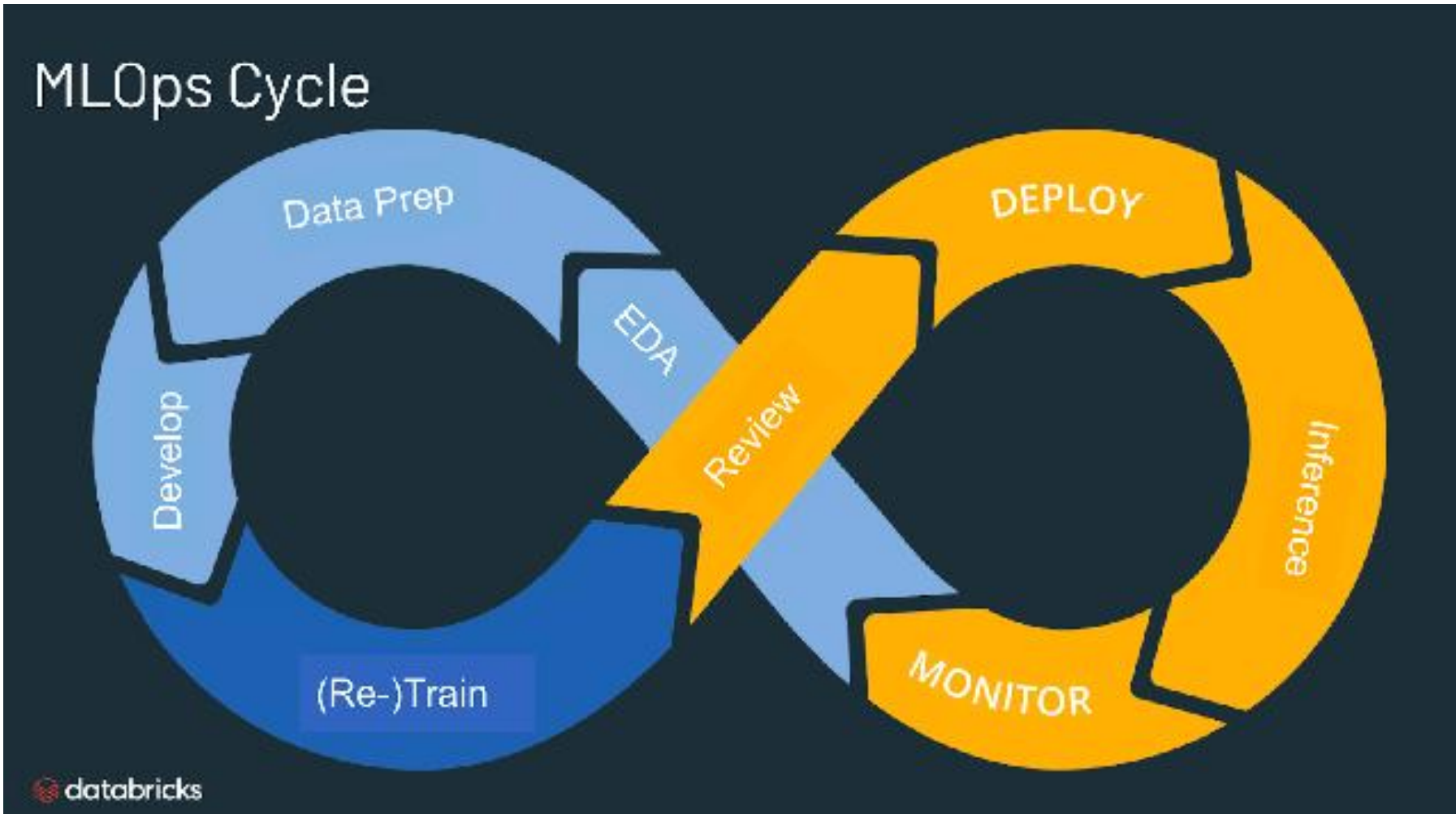


GPT发展历程



RLHF技术

LLMOps 概述: 与MLOps 的异同



步骤	MLOps	LLMOps
EDA	数字、分布、画图	文本
Data Prep	转格式、清洗（数字）	转格式、清洗（文本、图片）
Develop	设计模型、可视化、写代码	多数情况选模型
(Re-)Train	数字运算居多、环境简单、单机就够	文本图片居多、环境复杂、依赖复杂、GPU、多节点
Review	标准很明确，很容易量化，测试周期短	标准太多，不好评估，测试周期长
Deploy	软件标准化、硬件需求简单，容易标准化	硬件复杂，软件环境更复杂、较难标准化
Inference	快	慢
Monitor	故障点少	故障点多



白海科技 LLMOps 实践分享

1

背景和目标

2

方案落地

- 架构设计
- 数据处理
- 模型训练
- 模型评估
- 服务部署



LLMOps 实践分享：背景和目标

背景：为什么是我们？

- 大数据处理经验
- LLMOps 踩坑实战
- 云原生资源管理平台



目标：达成什么效果

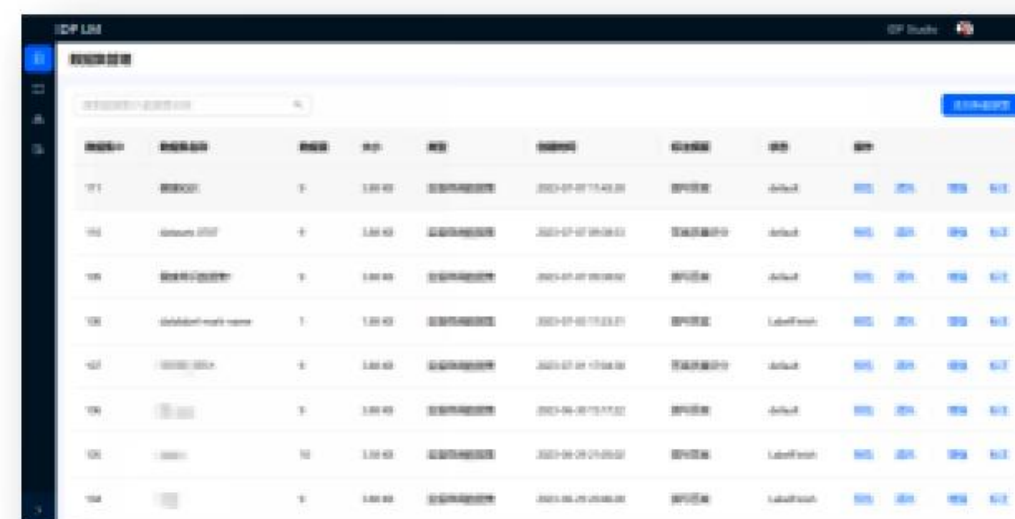
- 几乎零代码使用 LLM
- 全流程支持
- 可视化
- 个性化



LLM Ops 实践分享：背景和目标

· 成果鸟瞰

数据集管理及数据预处理



数据集ID	数据集名称	数据集类型	大小	状态	创建时间	最后更新时间	操作
101	数据集1	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
102	数据集2	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
103	数据集3	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
104	数据集4	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
105	数据集5	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
106	数据集6	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
107	数据集7	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
108	数据集8	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
109	数据集9	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
110	数据集10	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除

数据集上传



数据集上传

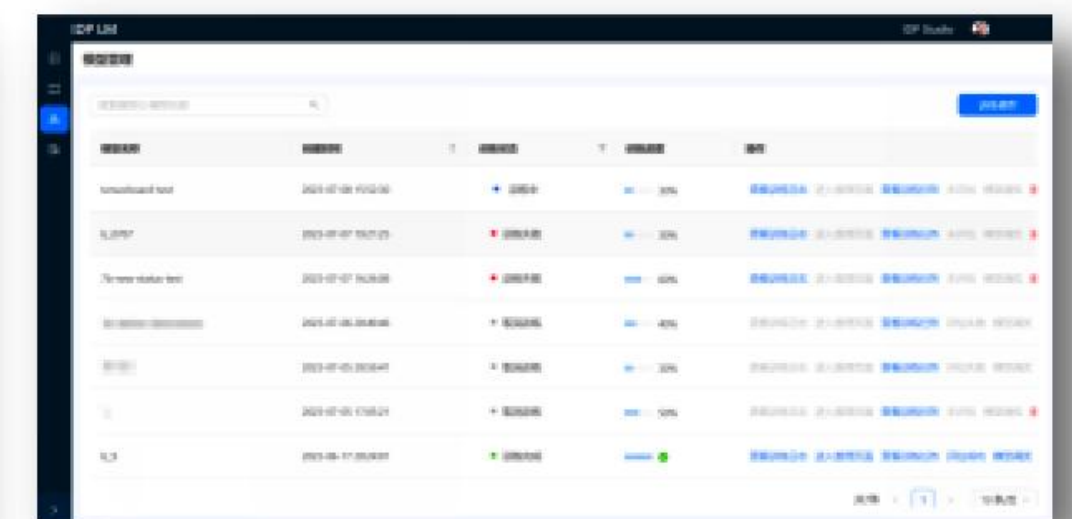
数据集名称:

数据集类型:

数据集大小:

上传数据集

大模型构建及管理



模型ID	模型名称	模型类型	大小	状态	创建时间	最后更新时间	操作
101	模型1	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
102	模型2	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
103	模型3	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
104	模型4	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
105	模型5	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
106	模型6	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
107	模型7	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
108	模型8	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
109	模型9	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
110	模型10	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除

大模型推理



大模型推理

模型名称:

模型类型:

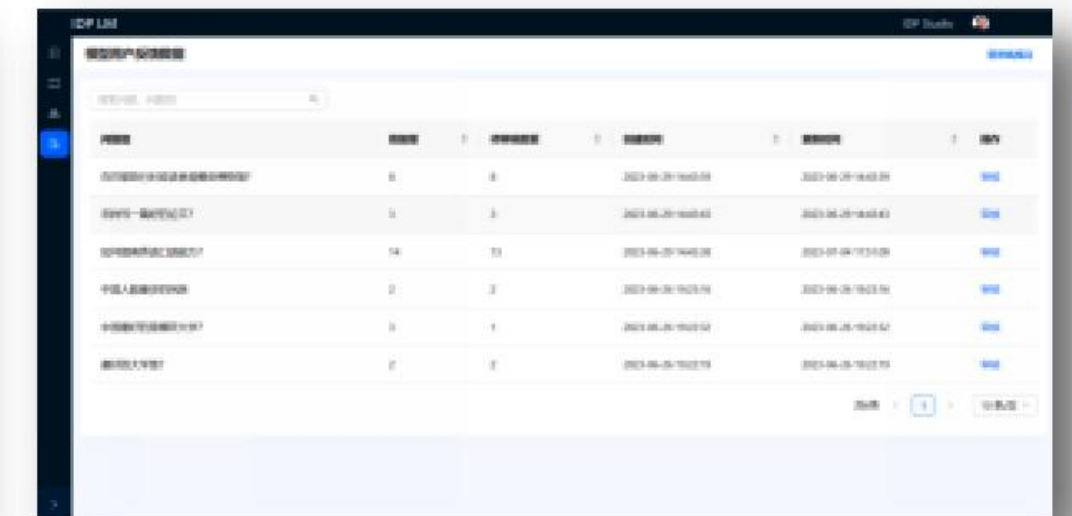
模型大小:

推理

大模型通用评估

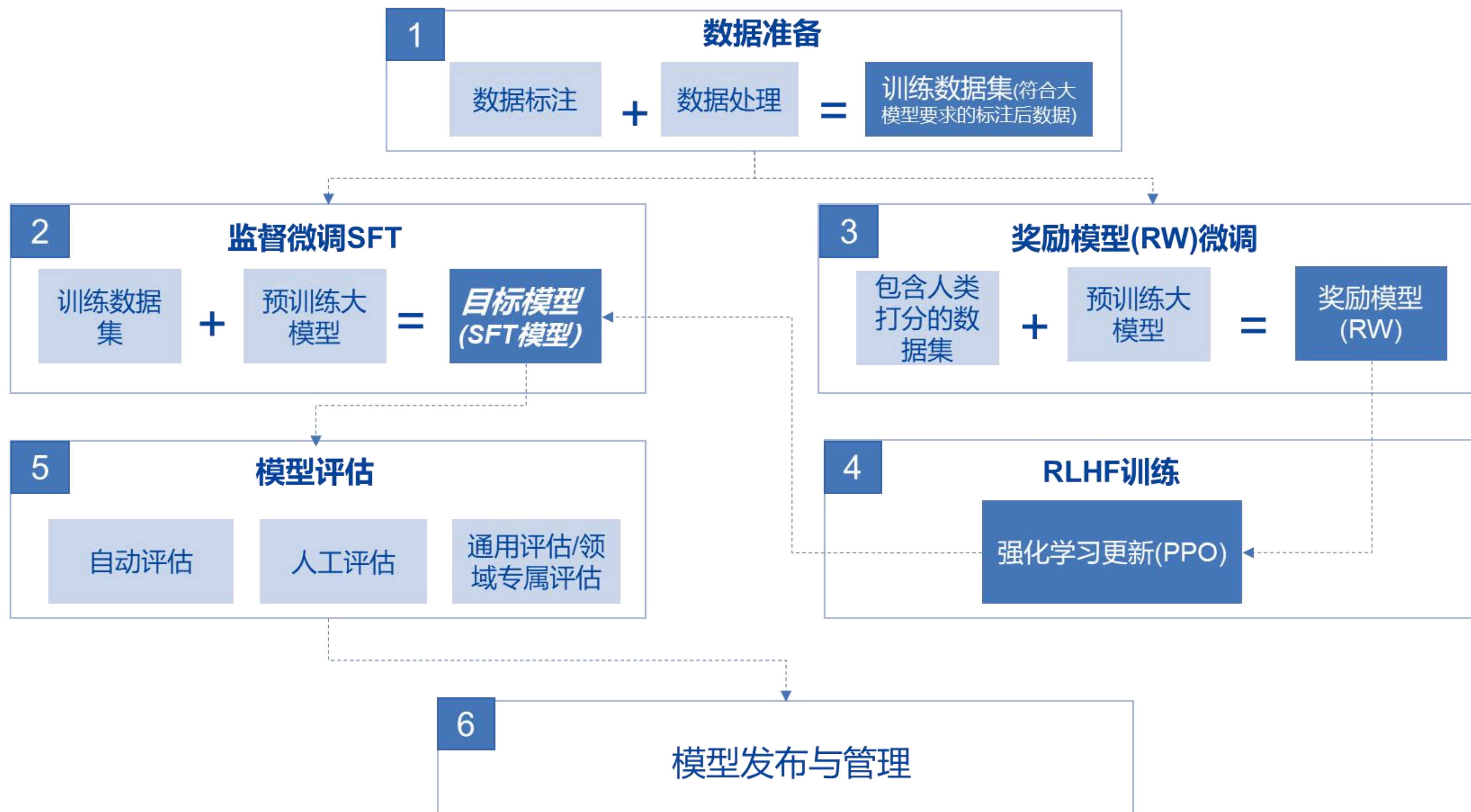


反馈数据回流审核



反馈ID	反馈名称	反馈类型	大小	状态	创建时间	最后更新时间	操作
101	反馈1	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
102	反馈2	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
103	反馈3	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
104	反馈4	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
105	反馈5	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
106	反馈6	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
107	反馈7	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
108	反馈8	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
109	反馈9	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除
110	反馈10	文本	1.0M	已上传	2023-07-07 10:00:00	2023-07-07 10:00:00	删除

LLMOps 实践分享：架构



LLMOps 实践分享：数据处理

开源数据集

私有数据集



质量



挑选
格式转换

LLMOps 实践分享: 训练

- SFT
- Reward Model
- PPO
- DPO

步骤1: 微调GPT-3.5

从提示词数据集中获取提示词示例

标记者(Labeler)书写期待的回复

被标记的数据用来微调 GPT-3.5



步骤2: 搜集对比数据, 训练奖励模型

采样, 列出所有提示词和模型输出

标记者(Labeler) 对模型输出质量进行排序

用排序结果训练奖励模型(Reward model)



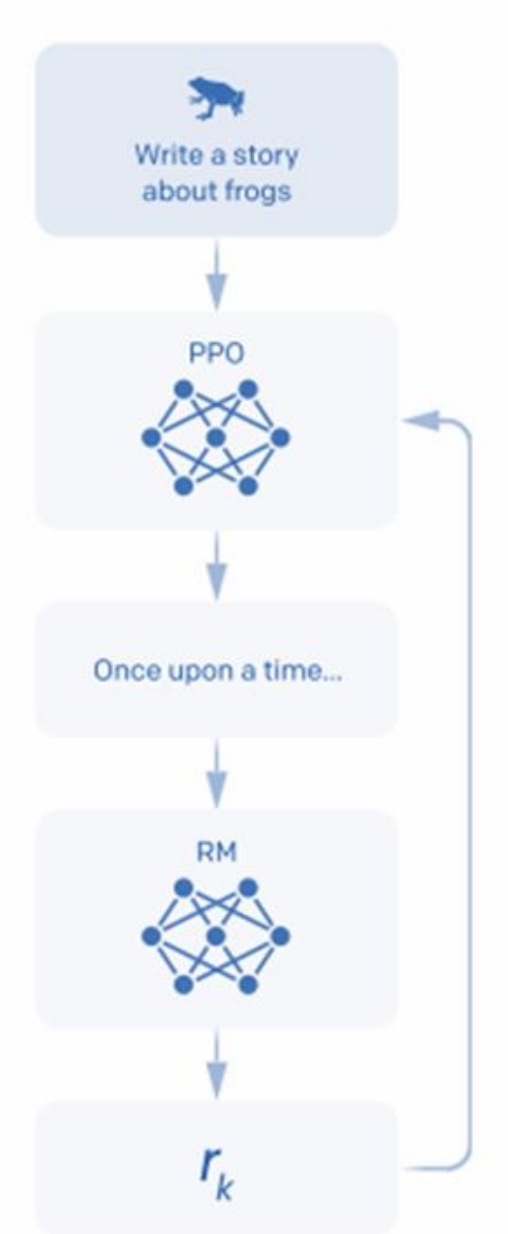
步骤3: 基于强化学习优化微调模型

抽样新的提示词

生成结果

奖励模型为上述生成结果计算一个奖励结果

奖励结果被用于更新模型策略, 通过 PPO(proximal policy optimization)

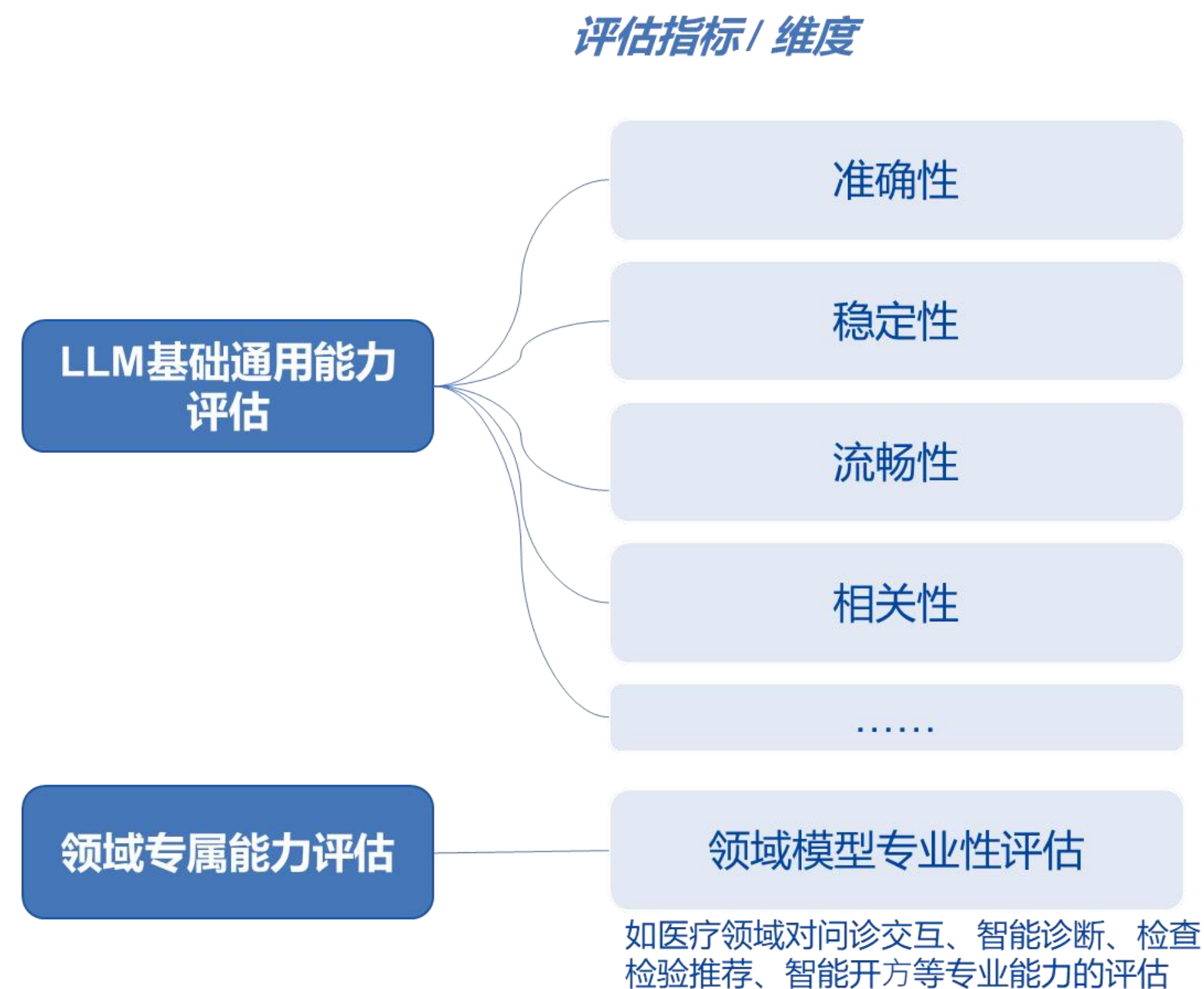


资料来源: OpenAI 《Training language models to follow instructions with human feedback》

LLMOps 实践分享: 评估

- ▶ 公开数据集
- ▶ 领域数据集
- ▶ 人工
- ▶ evals

IDP LM 模型评估体系

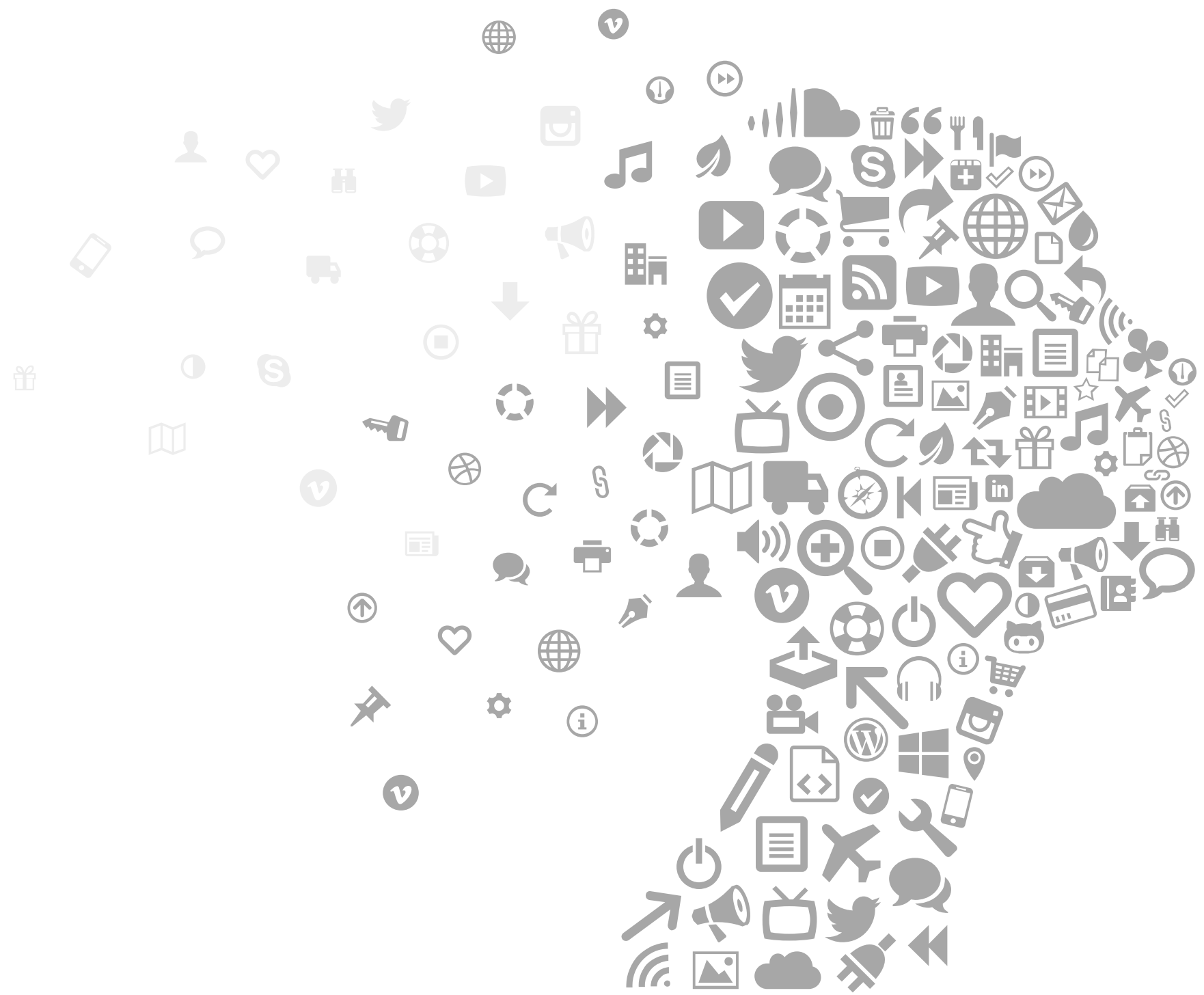


机器评估

IDP LM模型自动评估
ChatGPT评估

人工评估

LLMOps 实践分享：部署



- 量化：效果和成本的权衡
- GPU 资源管理
 - 异构 GPU
 - 生命周期
 - 队列

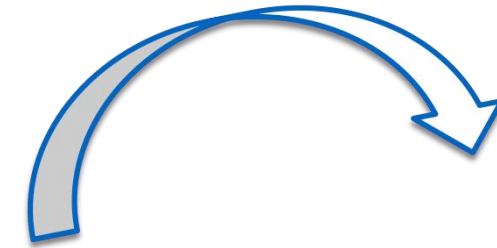
面向未来：LLMOps 的应用前景

- 垂直化
- 平民化、个性化
- 成本越来越低、功能越来越强，参考“手机发展史”



面向未来：AI 平台建设

新鲜事物，判断原则 **ROI**



只是想测试一下

- 手工测试即可
- 租借成熟平台亦可（比如白海）
- 自己搞，不划算

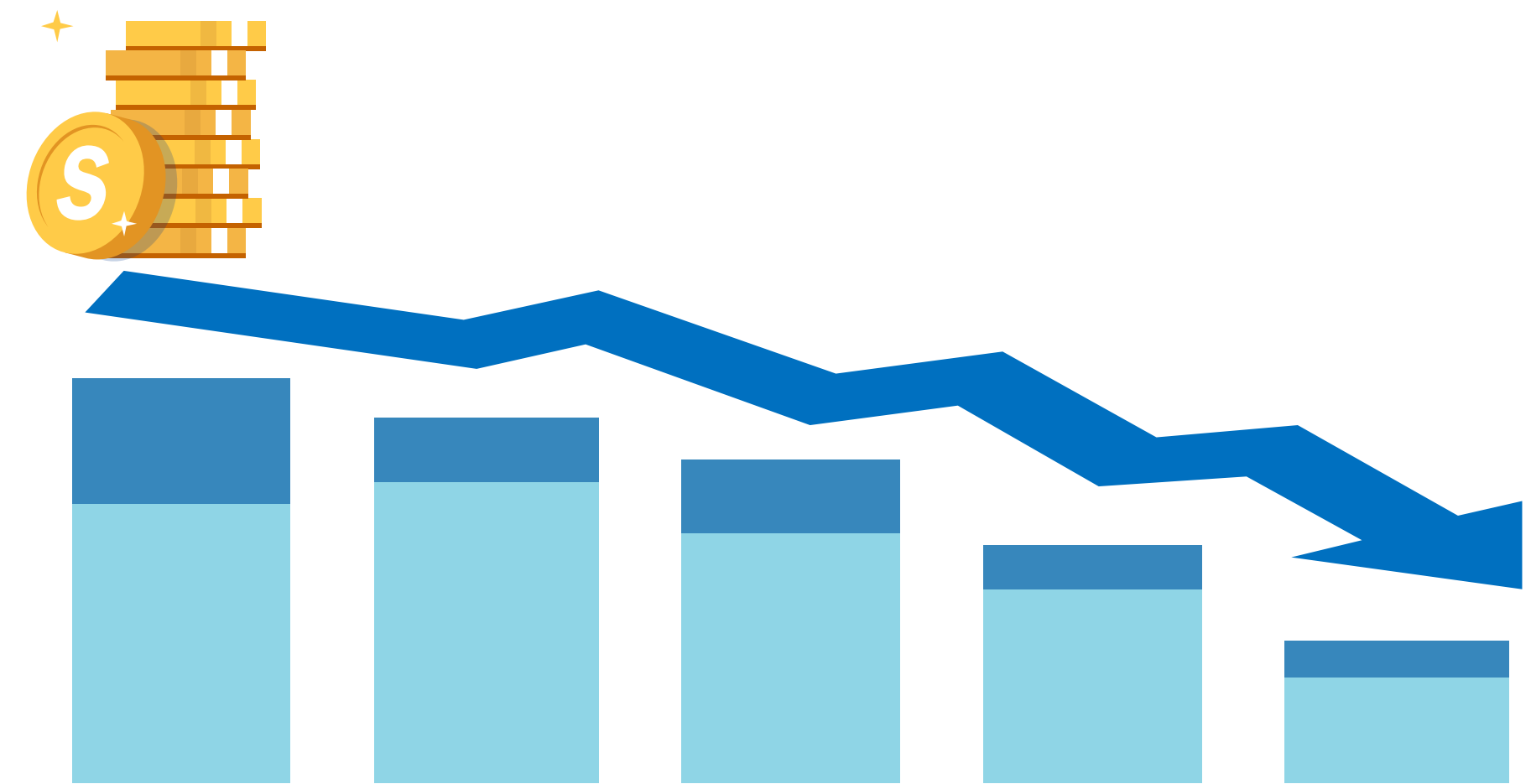
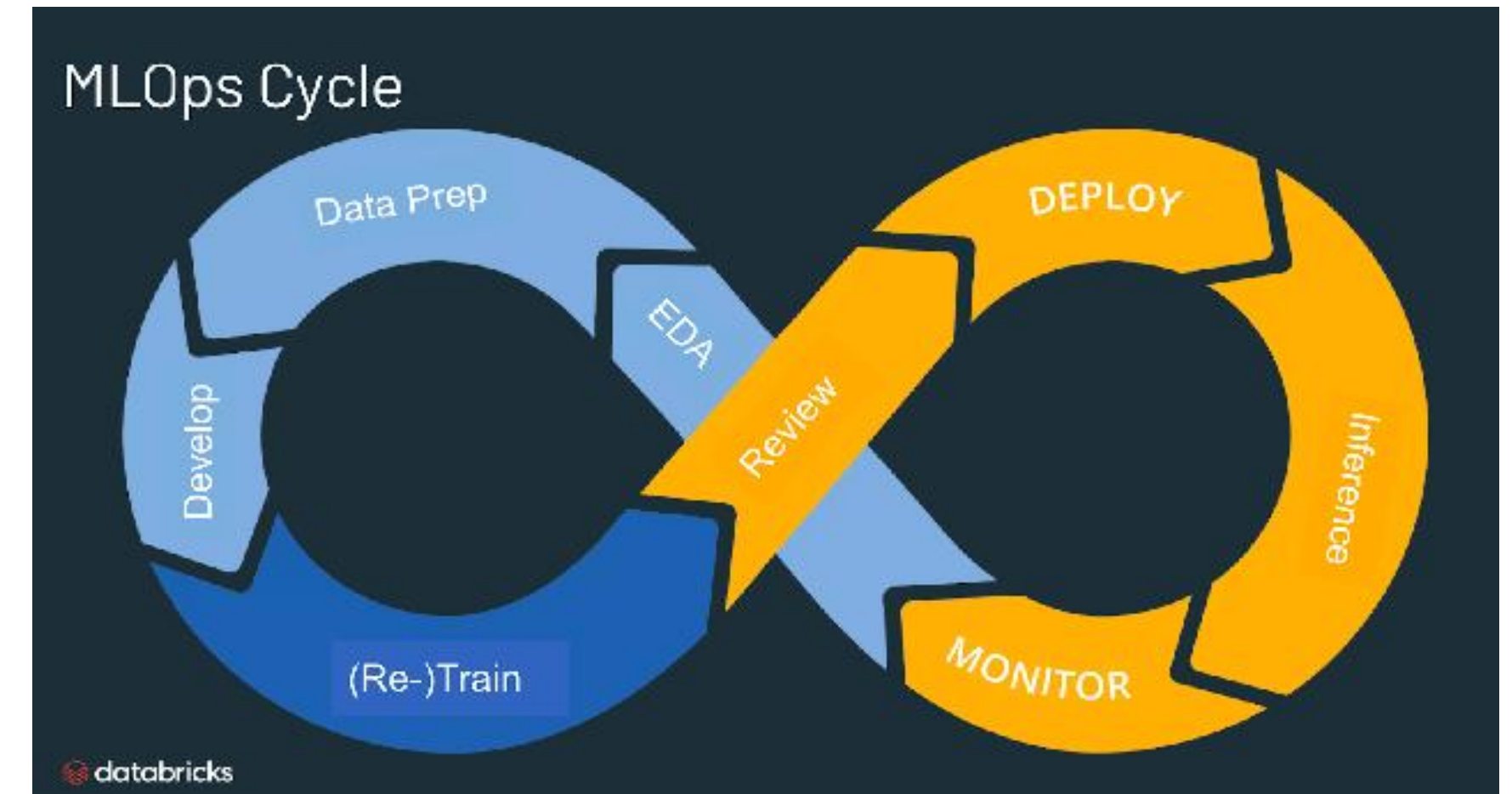
测试效果不错，要继续迭代

- 租借成熟平台
- 同步自己研发或服务方联合开发

面向未来: MLOps --> LLMOps

问题: 已经有 **MLOps**, 还需要 **LLMOps** 吗?

- ✓ 是功能的扩充而不是组件的替换
- ✓ 是能力的升级和资源的进一步整合
- ✓ “降本增效” 效应更加明显



面向未来：LLMOps 的未来发展

发展历程

参考云平台的发展

- 各搞各的
- 互相学习形成行业最佳实践



终局

- 专门的公司提供“相互之间差不多”的“最好的服务”
- 其它人不关注细节，只关注服务



面向未来：大模型驱动 AI 应用

扩展了人机交互的形式，新的流量入口

智慧城市



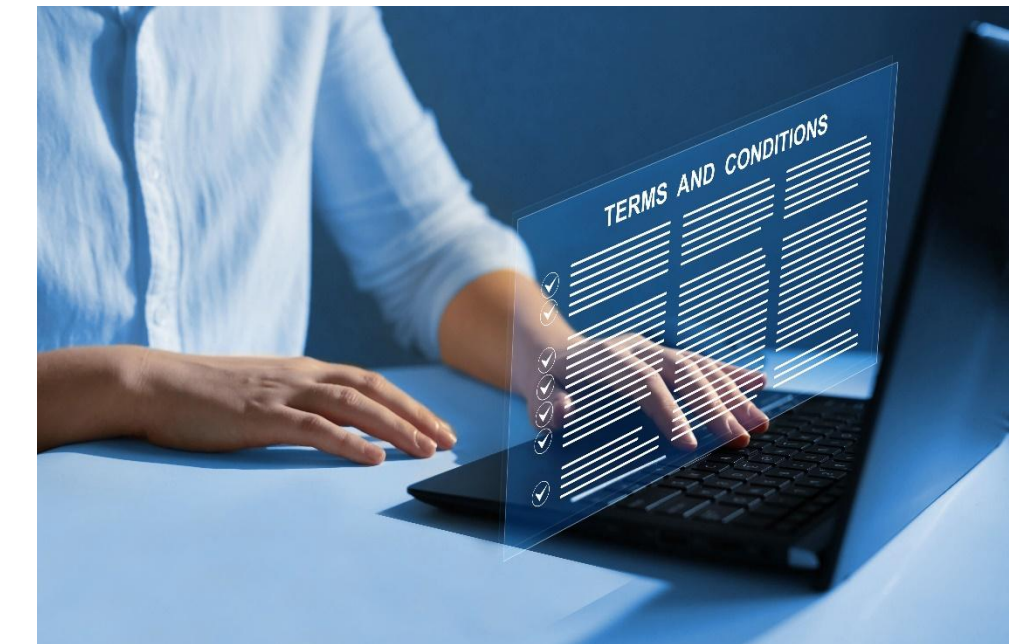
智慧医疗



行政文案



法律法规



THANKS



软件正在重新定义世界

Software Is Redefining The World