温有鹏

男 | 28 岁 | 15531511630 | 2573852828@qq.com

7 年工作经验 | 求职意向：Agent 开发工程师 / AI 应用开发 | 期望城市：北京

个人作品集 / 交互简历：http://39.105.127.172:6758/

个人优势

- **生产级 Agent 与安全隔离落地**：主导央企内部 AI 平台核心研发，具备从 **MCP 工具协议封装、ReAct 循环编排与预算熔断、研发数字员工三层隔离（独立角色密钥 + Git Worktree + Docker 容器沙箱）到人工协同复核（HITL）**的完整自研落地经验。
- **大规模受控 RAG 与知识治理**：具备 **10 万量级文档（含历史版本）**的多租户知识治理实践；打通“审核入 Git 源库 → 增量索引同步 → Milvus 稠密+双稀疏三路混合检索与重排 → FTS5 容灾降级”闭环，基于 Promptfoo 构建与生产同构的评测体系。
- **7 年微服务与企业级后端底座**：兼具 Python 异步 AI 应用研发与 5 年+ .NET Core 微服务开发经验，具备**核心业务数据库设计、千万级订单分库分表与冷热数据分离、数据库查询调优**、细粒度 RBAC 数据权限及容器化交付能力。

专业技能

- **Agent 工程与运行时**：Python、Starlette、MCP 协议、Function Calling（ReAct）、独立身份与密钥管控、Git Worktree 并发工作区隔离、Docker 沙箱执行、会话级工具鉴权、预算熔断、人工复核（HITL）
- **知识库与混合检索**：Milvus（稠密向量 + 正文稀疏 + 标识符稀疏三路召回）、RRF 融合与精排阈值解耦、SQLite FTS5 降级、多租户隔离、Git 审核准入与增量索引同步
- **评测与平台治理**：Promptfoo 端到端回归评测、引用溯源校验、可回答性判定与置信度评估、Skills 技能管理、Prompt 广场、模型配置与全链路调用记录
- **微服务与数据工程**：C# / .NET Core 微服务、ASP.NET Core Web API、数据库表结构设计、分库分表与冷热数据分离、SQL Server / MySQL 查询调优、SqlSugar、Redis、RabbitMQ、Quartz、Jenkins、Docker

工作经历

中国旅游集团有限公司 **Agent 开发工程师** 2026.03 - 至今

- 负责集团内部 **DevPilot 企业 AI 应用平台**整体方案设计与核心开发，统筹建设“多租户受控企业知识库”与“自动化研发数字员工（Coding Agent）”两大核心模块。
- 主导约 **10 万量级文档（含历史版本）**的多租户权限隔离、审核发布流、增量索引任务同步及基于 Milvus 的三路混合检索问答能力研发。
- 落地可切换 Function Calling（ReAct）受控循环，以及基于独立角色密钥、Git Worktree 与 Docker 隔离的自动改码验证闭环；基于 Promptfoo 按生产检索参数建立持续评测体系。

计世在线网络技术（北京）有限公司 **.NET 开发工程师** 2021.01 - 2026.03

- 参与西门子**千万级订单规模**履约平台后端微服务开发（覆盖 PC 管理端与微信小程序），负责订单、委托订单、信用额度、物流跟踪及客户服务等业务服务模块设计与实现。
- 参与核心业务数据库表结构设计；针对千万级订单增长落地**冷热数据分离与分库分表**，配合日常数据库查询调优、Redis 热点缓存及 Quartz 定时任务保障系统稳定运行。
- 参与权限与运营后台建设，按组织角色控制可访问的数据范围；基于 Jenkins + Docker 完成微服务构建发布，跟进线上问题排查与修复。

北京鼎创恒达智能科技有限公司 **自动化工程师（项目组长）** 2019.06 - 2021.01

- 担任项目组长带领团队研发交付公安危险品智能仓库系统，统筹 Web 网页端、WinForm 桌面上位机与移动端全链路开发及软硬件联调验收。
- 负责上位机对接 RFID 读写器与通道门设备实现自动出入库识别与异常报警；主导研发元数据驱动的内部低代码配置工具，支持动态生成后台页面并实现不停机更新。

项目经历

DevPilot 企业 AI 应用平台　核心开发　2026.03 - 至今

面向集团多子公司场景的企业级 AI 应用平台：知识库侧实现按公司隔离、审核准入、混合检索与可信问答；数字员工侧结合企业私域知识与代码仓库上下文，在隔离环境中自动完成代码修改、编译测试与报错自修复，超限或高危操作协同转人工。

> **技术栈：**Python、Starlette、MCP、Function Calling（ReAct）、Milvus、SQLite（FTS5）、Git / Git Worktree、Docker、Promptfoo

- **多租户隔离与受控准入**：按公司严格隔离知识域；文档经收件箱投递并审核通过后写入 Git 源库（累计纳管约 **10 万量级文档及历史修订版本**），再同步至知识库只读镜像并触发增量索引更新；未审核与未登记路径阻断入库，保障索引构建与检索阶段复用同一套可见性规则。
- **三路混合检索、阈值解耦与容灾降级**：基于 Milvus 实现**稠密语义、正文稀疏、标识符稀疏**三路召回与 RRF 融合，按需衔接精排，底层异常时平滑降级至 SQLite FTS5 全文检索；评测严格对齐生产检索参数，将精排分与 RRF 分阈值独立解耦治理。
- **服务端强鉴权 ReAct 循环与可信输出**：支持标准检索增强生成与 Function Calling（ReAct）循环双模式切换（最小权限仅暴露 `kb_search` 与 `kb_read`）；**租户上下文与工具权限强绑定服务端会话，绝不信任模型生成入参**；内置预算耗尽强制停工具收尾机制，配套落地引用溯源校验、可回答性与置信度评估、日报周报生成，以及 Prompt 广场、Skills、模型配置与调用审计。
- **研发数字员工与三层隔离自修复闭环**：为数字员工配置**独立系统角色与专属密钥**，通过 **Git Worktree** 创建隔离分支工作目录，并在 **Docker 容器隔离环境**中按拆解步骤自动修改代码、执行编译与单元测试；失败时自动捕获错误输出驱动多轮修复，超出重试上限或命中高危操作自动挂起转人工复核。

Siemens Diomis 订单履约系统　后端开发　2021.02 - 2026.03

面向西门子业务的企业级微服务订单履约与运营系统（覆盖 PC 管理端与微信小程序），支撑支付后**千万级订单规模**下的订单查询、委托履约流转、信用额度管理、物流跟踪及客户服务。

> **技术栈：**.NET Core 微服务、ASP.NET Core Web API、SqlSugar、SQL Server、Redis、Quartz、Docker、Jenkins

- **微服务模块与核心业务开发**：基于微服务架构参与订单、委托订单、信用额度、物流跟踪及客户服务等模块的接口与业务逻辑开发，处理跨模块业务流转、额度占扣释放与状态同步。
- **数据库设计与分库分表治理**：参与订单主子表、委托单关联、信用流水等业务数据库表结构设计；针对千万级历史与活跃订单累积带来的单表膨胀问题，落地**分库分表与冷热数据分离**方案，将历史归档数据与在线活跃热表解耦，控制核心单表数据体量。
- **数据库查询调优与缓存应用**：针对多条件组合筛选与关联查询场景开展 SQL 与索引层面的数据库调优，减少慢查询开销；结合 Redis 缓存高频访问的热点数据，使用 Quartz 执行定时归档与业务批处理任务。
- **数据范围权限与容器化交付**：参与角色权限、团队管理与运营后台开发，按角色动态控制可访问的数据范围与操作权限；通过 Jenkins + Docker 完成多服务持续集成部署，跟进联调测试与生产问题排查。

智能仓库与内部低代码配置平台　项目组长　2019.06 - 2021.01

- **软硬一体危险品仓储系统**：覆盖 Web 端、WinForm 桌面上位机与移动端；上位机对接 RFID 硬件实现危险品自动出入库采集与异常报警，手机端支持扫码作业，跨端异步消息基于 RabbitMQ 可靠传输。
- **元数据驱动低代码工具**：设计研发内部低代码配置引擎，通过业务元数据动态渲染标准列表与树形管理页面，显著减少重复性后台开发工作，并支持生产环境不停机热更新。

教育经历

河北农业大学　本科　计算机应用技术