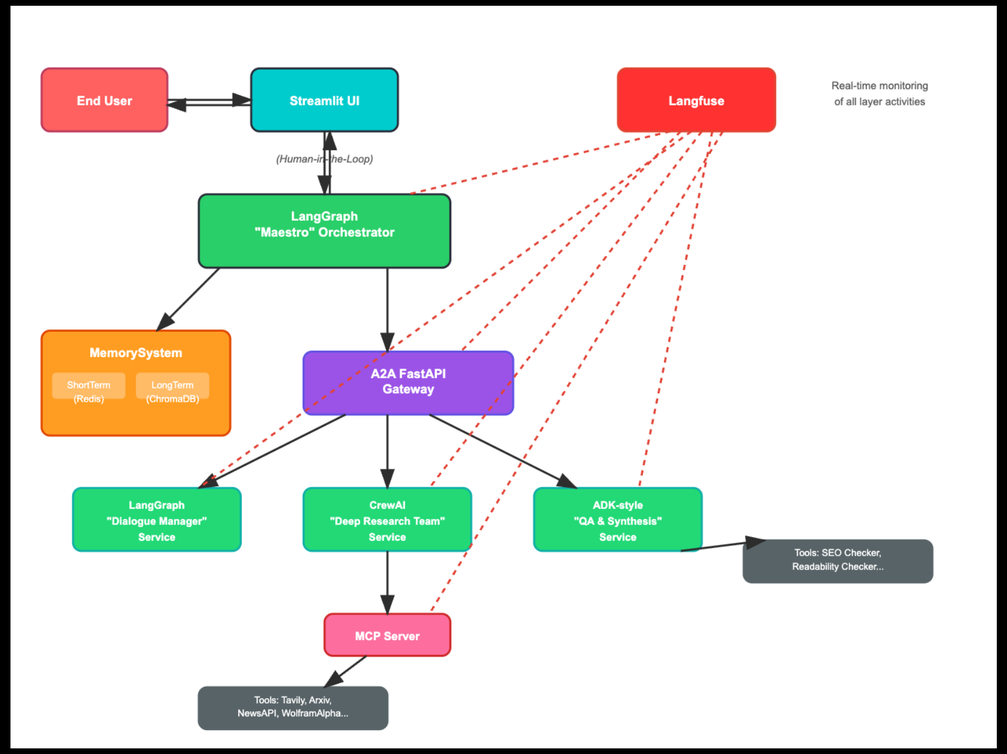
AI Agent 과정

Agent 설계 및 프로젝트

프로젝트 목표

프로젝트 목표

- 심층 분석 보고서 자동 생성 에이전트
  - 단순 정보 검색을 넘어, 여러 관점(기술, 시장, 생태계)을 종합적으로 분석
  - 각 분야의 전문성을 가진 AI 에이전트들의 협업을 통해 결과물의 깊이와 신뢰성 확보
  - 사람이 개입을 최소화한 보고서

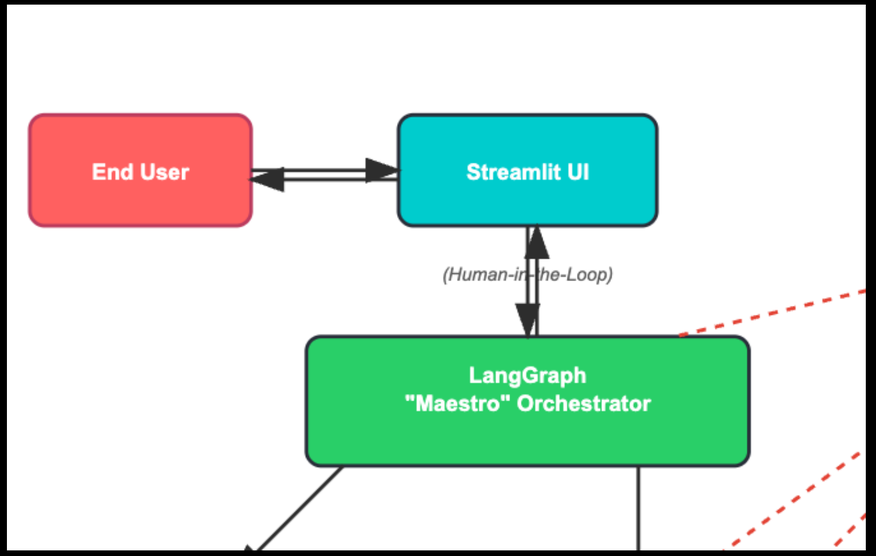


전체 구조 - MAS

- Why MAS?
  - 일 에이전트의 한계 극복
    - 하나의 에이전트가 모든 전문 분야(리서치, 분석, 글쓰기, QA)를 완벽히 수행하기 어려움
    - 단일 에이전트가 순차적으로 처리 시 발생하는 시간적 비효율성
    - 정해진 시나리오를 벗어나는 동적인 문제 해결 능력 부족
  - 현업에서의 'AI 전문가 팀' 구현
    - 각 에이전트가 가장 잘하는 역할(데이터 수집, 분석, 보고서 작성)에 집중
    - 새로운 기능(e.g., 이미지 생성, 코드 분석)이 필요할 때, 새로운 에이전트를 추가하는 방식으로 확장
    - 중앙 오케스트레이터의 지휘 아래, 각 팀이 자율적으로 작업을 수행하며 최적의 결과 도출

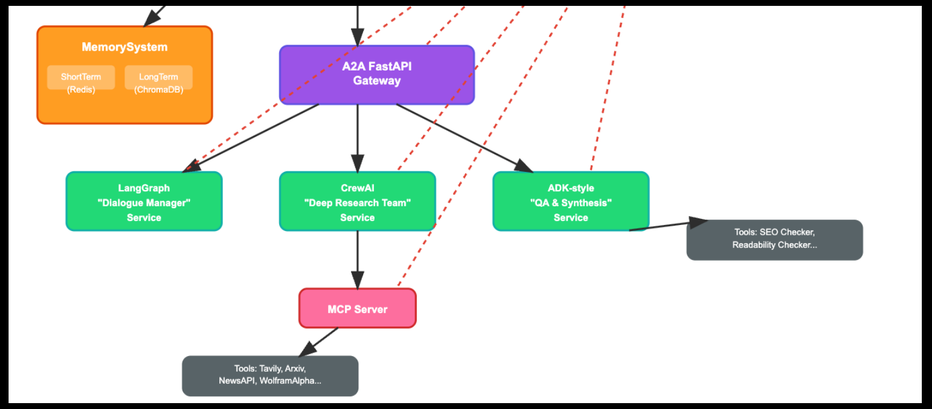
Maestro

- LangGraph 기반 오케스트레이터
  - 사용자와 Streamlit을 통해 소통
  - 목표를 입력받아 전체 작업 계획을 동적으로 수립 & 지휘
  - Plan-and-Execute 추론 패턴
    - 전체 리서치 계획을 수립
    - 각 단계에 가장 적합한 전문가 팀에게 작업을 순차적/병렬적으로 위임



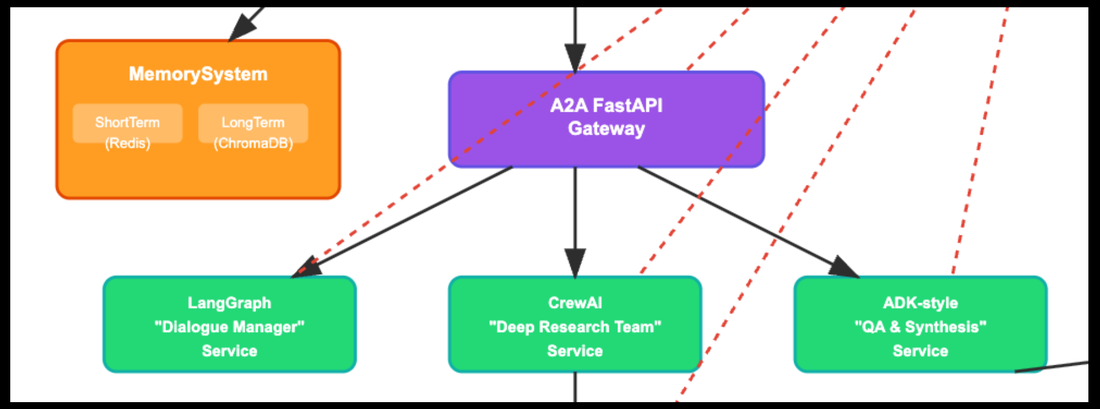
Multi-Agent Team

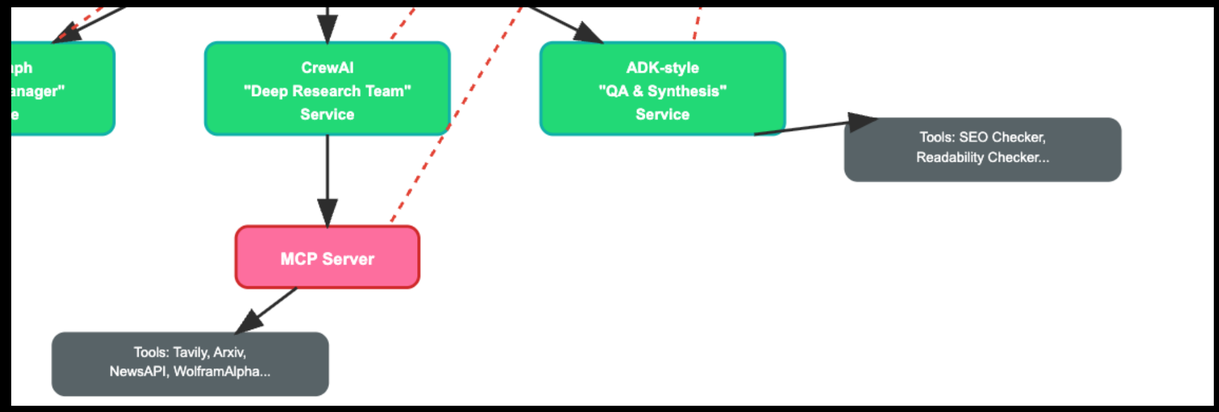
- CrewAI 리서치 팀
  - 특정 주제에 대한 심층 정보 수집 및 분석
  - 웹 검색, 논문 검색 등 다양한 외부 정보 소스
- ADK-style QA
  - Google ADK 기반
  - 리서치 팀이 수집하고 분석한 내용의 품질을 검수



통신 프로토콜

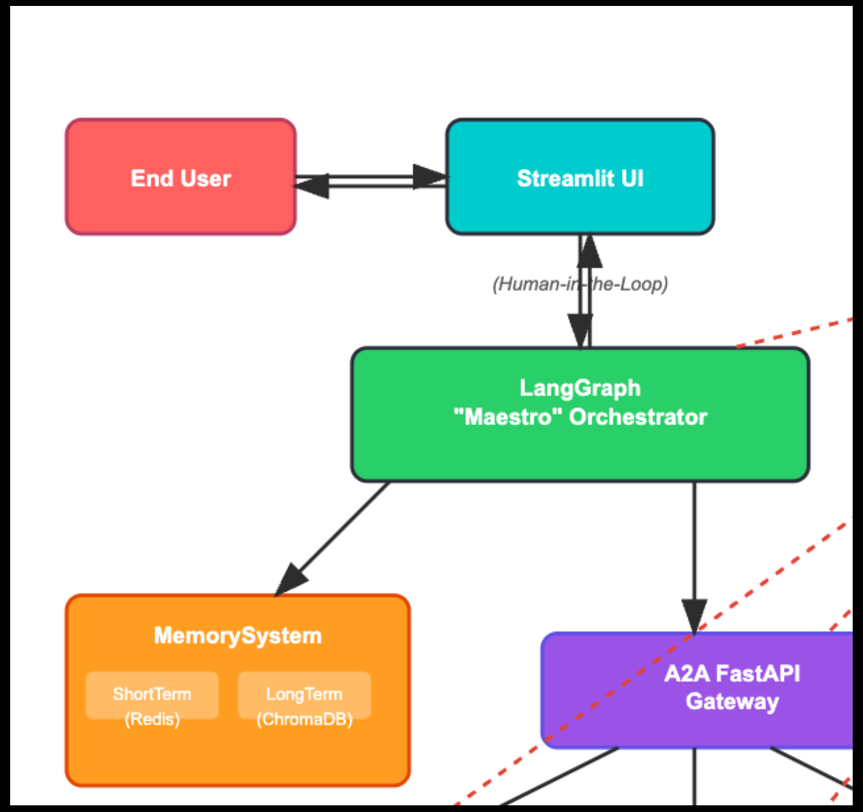
- 내부 팀 간 소통
  - A2A(Agent-to-Agent)Protocol
  - 시스템 내부의 각 전문가 팀(서비스) 작업 결과 공유를 위한 통신 규약
- 외부 도구와의 소통
  - MCP(Model Context Protocol)
    - 내부 에이전트가 외부 세계의 정보를 얻기 위해 사용





메모리 시스템

- 단기 기억 (Short-Term Memory - Redis)
  - 현재 진행 중인 작업의 컨텍스트를 빠르게 저장하고 공유
  - (예: "방금 검색한 웹페이지 내용", "분석 중인 데이터 조각")
  - 에이전트가 동일한 작업에 대한 최신 정보를 실시간으로 공유
- 장기 기억 (Long-Term Memory - ChromaDB)
  - 과거에 수행했던 작업의 성공/실패 경험
  - 중요한 분석 결과 등을 벡터 형태로 저장
  - 시스템의 '경험적 지식' 창고



신뢰성 및 모니터링

- Langfuse
  - 사용자 요청부터 최종 보고서 생성까지, 시스템 내부에서 일어나는 모든 활동을 실시간으로 추적 & 기록
  - LLM 호출, Tool 사용, 중간 결과, 비용, 지연 시간 등
  - 어느 부분에서 오류가 발생했는지 신속하게 파악하고 디버깅
  - 에이전트의 전체 추론 과정을 투명하게 이해