AI Agents Design I: Data

Understanding the fundamental differences between autonomous AI systems and language processing tools

AI Agents

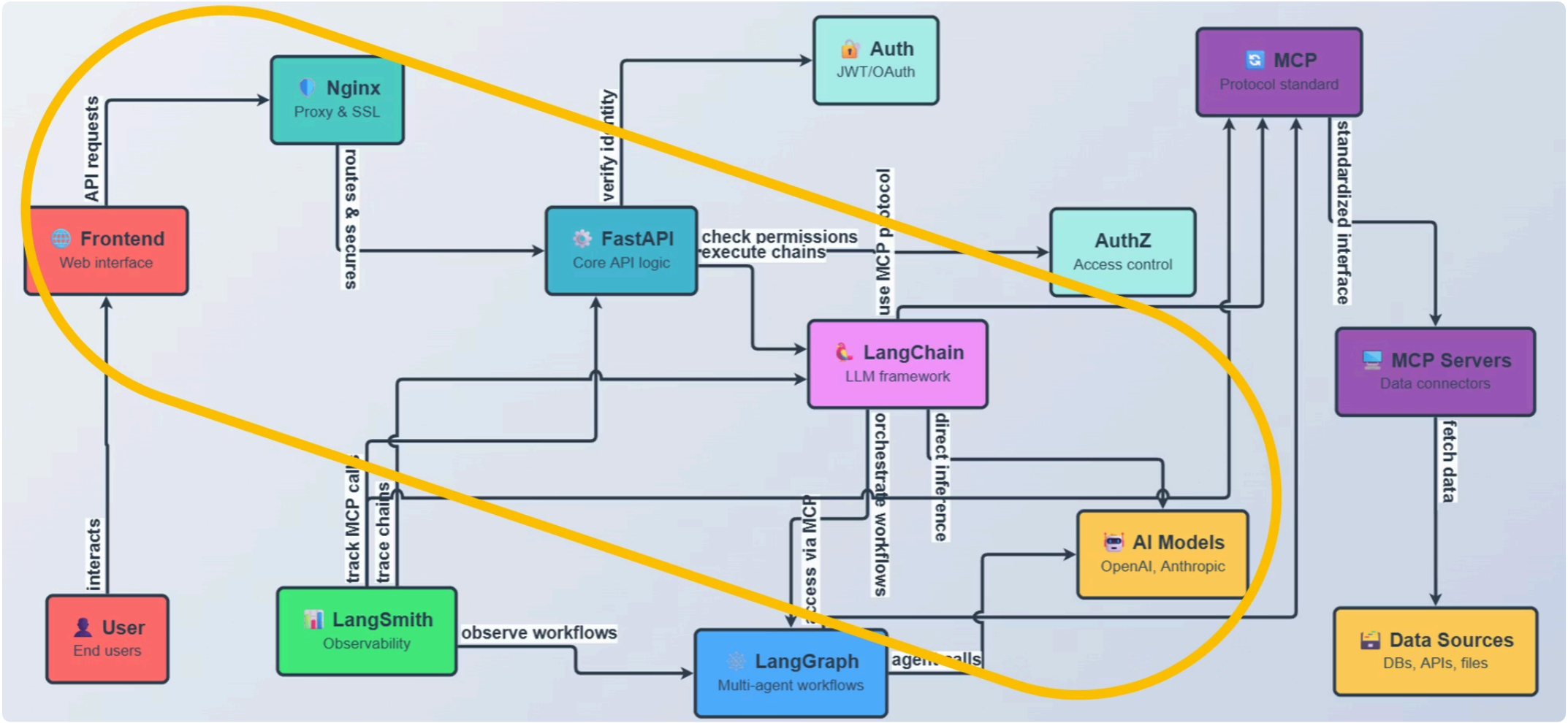
Autonomous systems that perceive environments, make decisions, and act to achieve goals. They extend beyond simple response generation to include proactive task execution and planning.

Large Language Models

Specialized tools for understanding and generating human-like text, trained on vast datasets. They typically lack inherent autonomy or environmental interaction capabilities.

Core Distinction

Agents are dynamic and goal-driven with planning capabilities, whilst LLMs focus on language tasks without independent action. The debate continues on whether agents represent evolution or a separate layer.


Auth
JWT/OAuth
MCP
Protocol standard
Nginx
Proxy & SSL
API requests
verify identity
Frontend
Web interface
routes & secures
FastAPI
Core API logic
check permissions
execute chains
use MCP protocol
AuthZ
Access control
standardized interface
LangChain
LLM framework
MCP Servers
Data connectors
orchestrate workflows
direct inference
fetch data
track MCP calls
trace chains
AI Models
OpenAI, Anthropic
interacts
User
End users
LangSmith
Observability
observe workflows
LangGraph
Multi-agent workflows
Data Sources
DBs, APIs, files

What is Docker?

Docker is a leading containerization platform that packages applications and their dependencies into lightweight, portable containers. At its core, containers are standardized units that encapsulate everything needed to run an application, including code, runtime, libraries, and system tools, ensuring consistency across various environments.

Main Benefits

- Portability: Ensures consistent execution across different environments.
- Lightweight: Shares the host OS kernel, reducing overhead.
- Fast Deployment: Accelerates the development and deployment cycles.
- Isolation & Security: Provides isolated environments for applications.

How It Works

Docker utilizes containerization, a form of operating-system-level virtualization, which is distinct from traditional hardware virtualization. Instead of each application having its own OS, containers share the host operating system's kernel, making them significantly more efficient and faster to start.

Common Use Cases

- Application Development & Testing
- Deployment of Applications
- Microservices Architecture
- Continuous Integration/Continuous Deployment (CI/CD) pipelines

Origin

Docker was initially launched in 2013 as an open-source platform. Its adoption has since grown exponentially, becoming a cornerstone technology in modern software development and operations.

1) Agent 1: Get real time data

2) Agent 2: Get huge amount of data

Agent Design: Real time data

https://github.com/enoch-sit/project-1-ipynb/blob/main/functionCalling.ipynb

or

https://colab.research.google.com/github/enoch-sit/project-1-ipynb/blob/main/functionCalling.ipynb

---

https://github.com/enoch-sit/project-1-ipynb/blob/main/functionCalling_grok_formal.ipynb

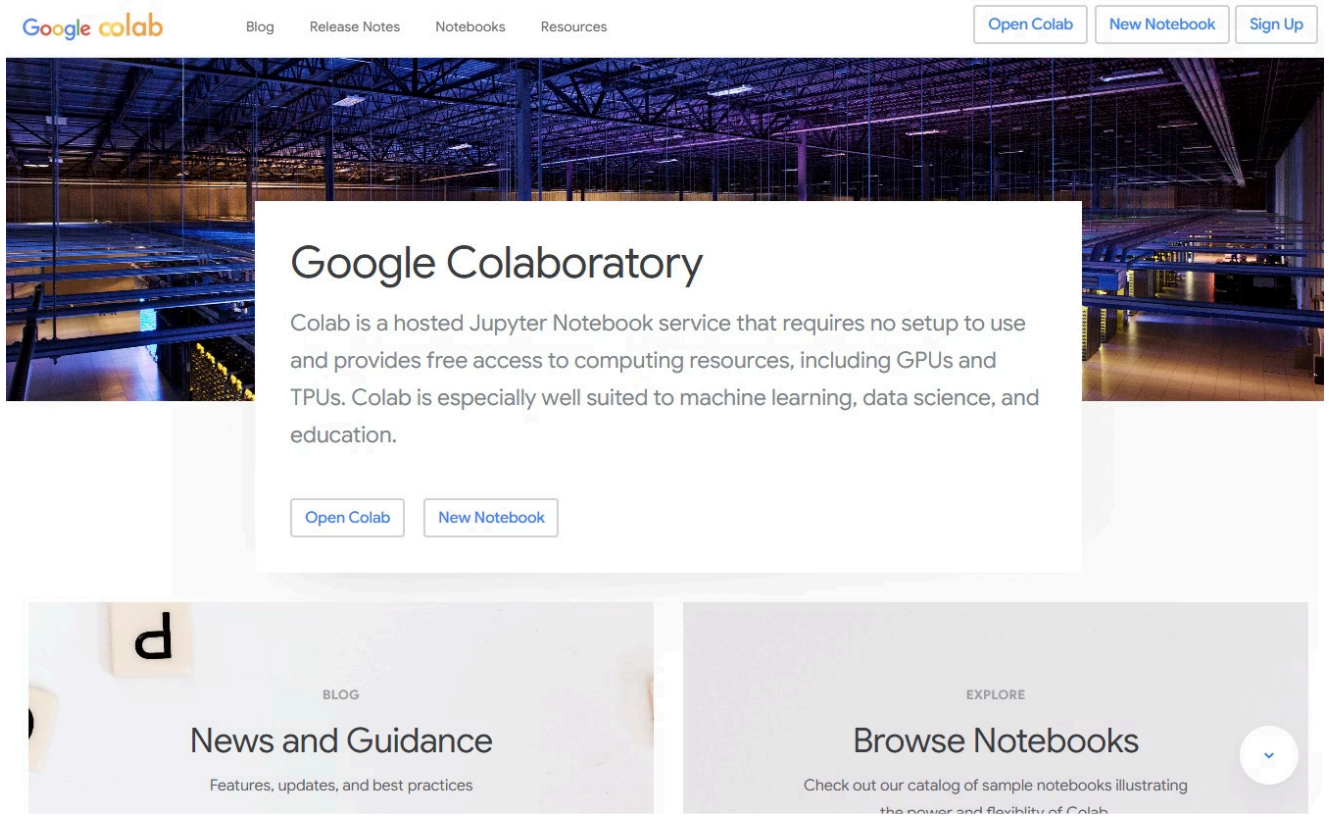
or

https://colab.research.google.com/github/enoch-sit/project-1-ipynb/blob/main/functionCalling_grok_formal.ipynb

colab.google

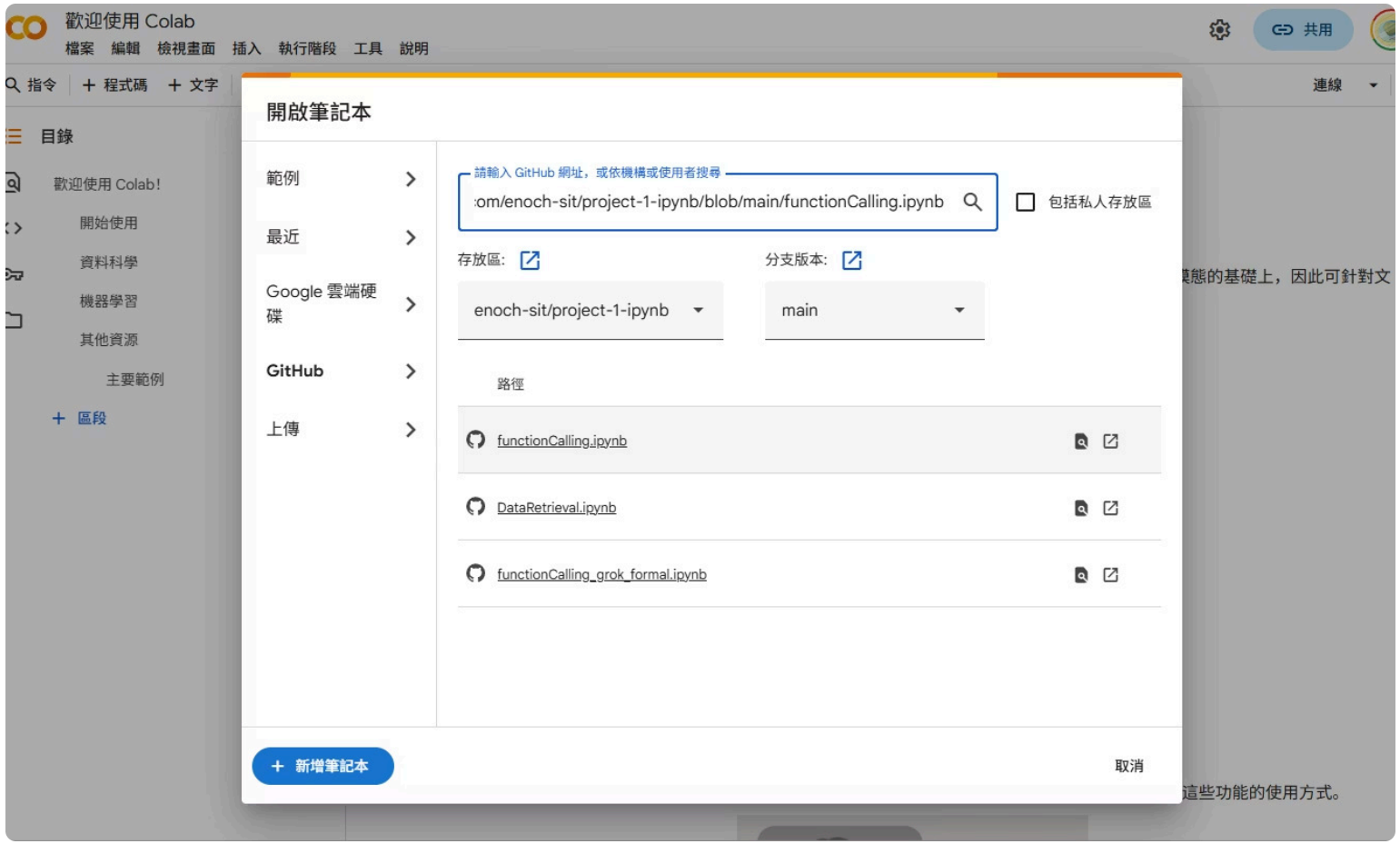
colab.google

Colab is a hosted Jupyter Notebook service that requires no setup to use and provides free access to computing resources, including GPUs and TPUs. Colab is especially well suited to machine learning, data science, and education.

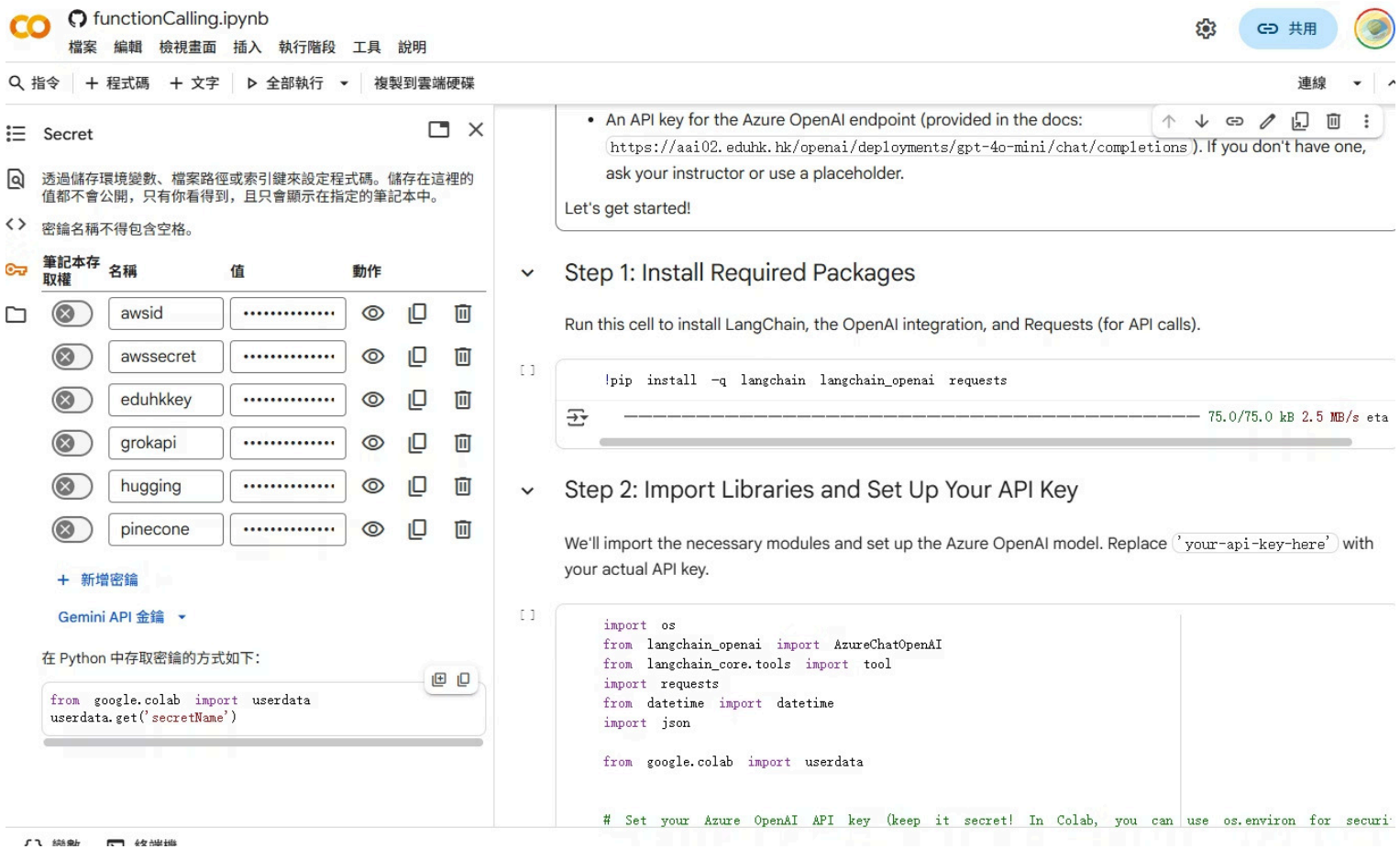


Open Colab notebook

Open function calling



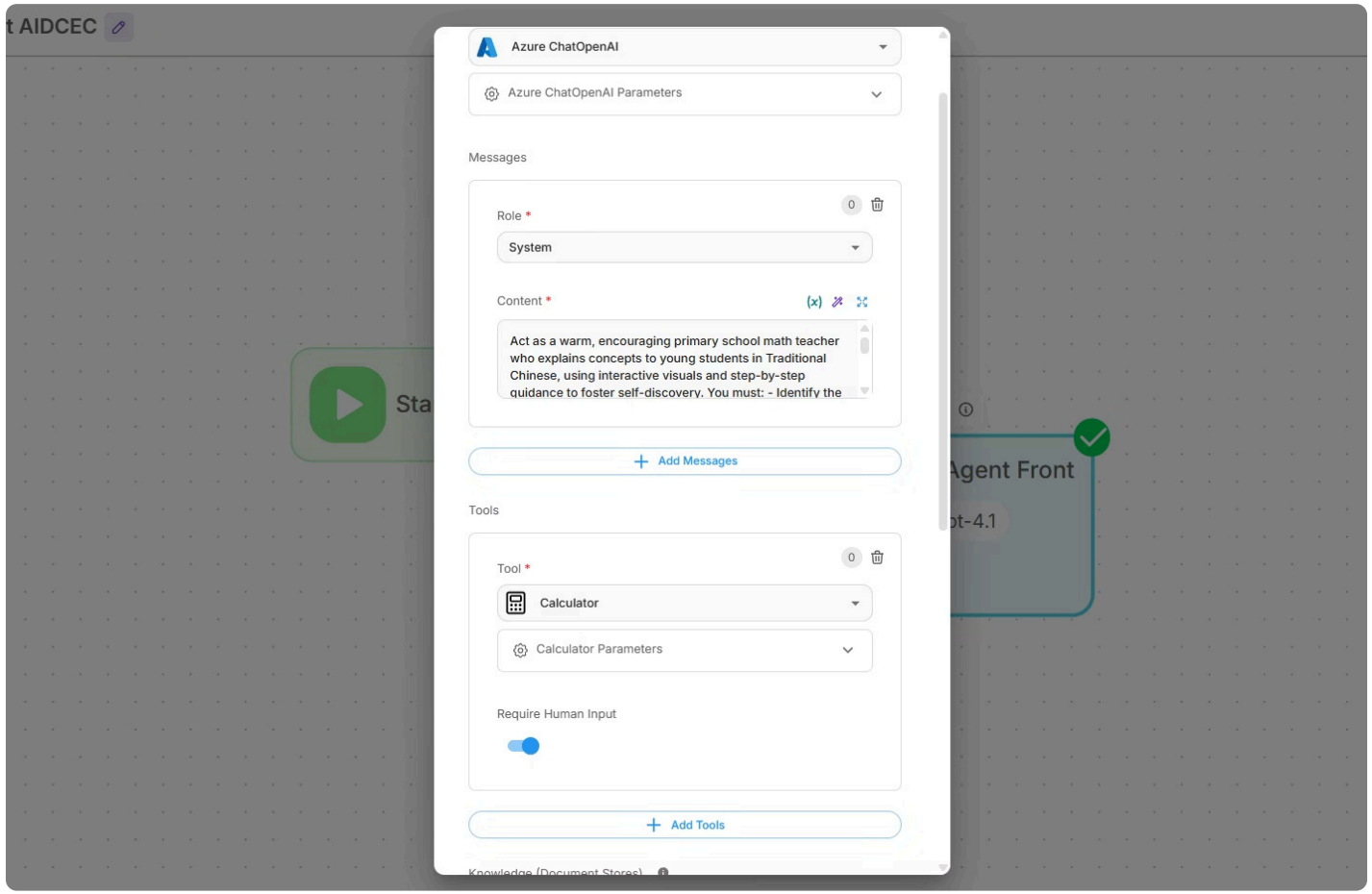
Click API keys and enter all the keys



Can you create another tool for your project?

with Vibe coding?

Agent Design I: Fast Prototype



Install Flowise

and test your first agent with your own tool or the calculator tool (Go to Moodle Tutorial)

2) Agent 2: Get huge amount of data

https://github.com/enoch-sit/proj01_chatbot_edu/blob/main/week04/langchain/functionCalling.ipynb

https://colab.research.google.com/github/enoch-sit/proj01_chatbot_edu/blob/main/week04/langchain/functionCalling.ipynb

Install Flowise UI

go to moodle tutorial

Vibe coding a tool and a UI for your Project !!!

Sematic Map Tool and HTML render UI