Microsoft

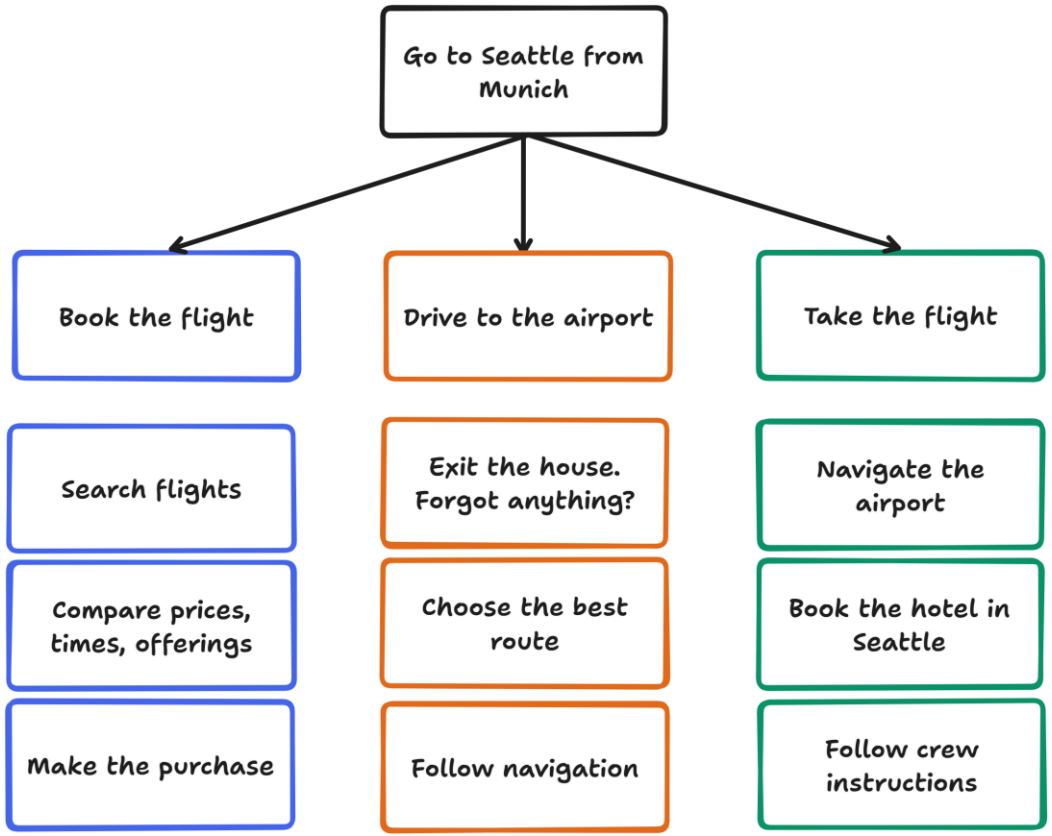
Introduction to Autonomous Agents Workshop

Agenda

Topic	Details	Timing
Autonomous Agents Introduction	• From LLMs to Autonomous Agents • Agent framework overview and capabilities	20 min
AutoGen	• AutoGen overview • Building a multi-agent conversation from scratch • AutoGen Studio Demo • Autonomous Agents Strengths and Limitations	60 min
Business scenarios	• Interactive Image Generation • HR Onboarding Buddy • Service Center Troubleshooting Agent	60 min
Envisioning	• Identification of potential use cases • PoC scope definition	90 min

Improving reasoning capability of LLMs

- Most processes are complex: require many separate, hierarchical actions
- To achieve best logical reasoning in LLMs, we need to **decompose** the problem



Agentic Reasoning Evolution

ChatGPT

Ask a question on a topic.

You get a response in one go.

Q

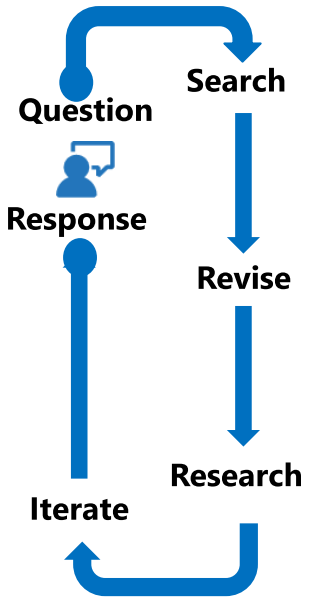
R

Language model as **reasoners**

What If?

Ask a question on a topic

Do web search?
→ First draft response.
Need more research?
→ Do revision on response.
Iterate for more details?
→ Revise, act and respond.



Language model **actionable**

Agentic Reasoning Design

1. Reflection
2. Tool Use

Robust Technology

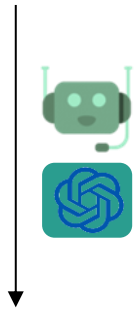
3. Planning
4. Multi-agent collaboration

Emerging Technology

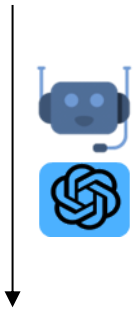
Agentic AI

What is an Agent?

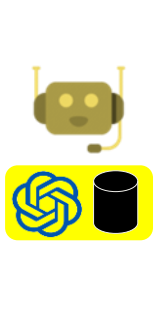
Agent = LM + Planner + Memory + Tools / Skills



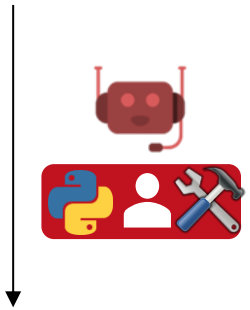
Azure
Open AI



Goals to Subgoals
Chain / Tree of Thoughts
Decomposition of Tasks
Reflect
Refinement for next task



Prompt Engineering
One/Few Shot
Long-/Short-term Memory
Retain and Recall



Bing Search
Wolfram Alpha
Code Interpreter
Calculator
Custom Code
Plugins

When do I use AI agents?

Automate complex or repetitive tasks that requires human intelligence like **data analysis, natural language processing**.

Enhance human capabilities or augment human decision making such as providing **recommendations, feedback or guidance based on data or preference**.

Create engaging and interactive experiences, such as games, simulations or virtual AI assistants that can **adapt to user behavior and preferences**.

Explore and discover new knowledge or solutions, such as finding optimal strategies, **generating novel designs or solving hard problems that are beyond human reach**.

Improve social and environmental outcomes, such as supporting education, health or sustainability initiatives that can benefit from AI agent's **scalability, efficiency or creativity**.

AI Agents Business Use Case Examples

PRIVACY-COMPLIANT DATA COLLECTION
- Legal Agent: Ensures privacy regulations.
- Marketing Agent: Collects customer data.

VENDOR EVALUATION AND COST OPTIMIZATION
- Procurement Agent: Selects suppliers.
- Product Agent: Assesses quality.

EMPLOYEE ONBOARDING
- Onboarding Buddy: Onboards the new hire
- Memory manager: responsible for dynamic memory

CONTRACTOR INVOICE VERIFICATION
- Procurement Agent: Manages contractor payments.
- Invoice Reconciliation Agent: Validates invoices.

SOFTWARE COMPLIANCE MANAGEMENT
- Tech Agent: Ensures licensing compliance.
- Legal Agent: Reviews software contracts.

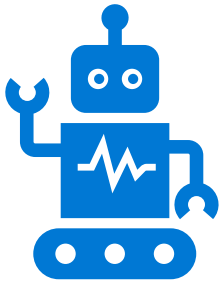
PERSONALIZED PRODUCT RECOMMENDATIONS
- Product Agent: Analyzes customer behavior.
- Marketing Agent: Tailors recommendations for campaigns.

IT SUPPORT AUTOMATION
- HR Agent: Handles technical issues.
- Tech Agent: Resolves support requests.

CUSTOMER SERVICE TROUBLESHOOTING
- Troubleshooter: Analyzes the issue.
- Data Engineer: Retrieves and analyzes data

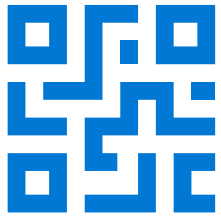
SUPPLY CHAIN OPTIMIZATION
- Tech Agent: Predicts demand, manages inventory.
- Procure Agent: Automates purchasing decisions.

Agentic AI Application Development



Autonomous Agents

capable of planning & executing decisions



Task Execution Tools

identify and execute the right tools for each task

Conversational Workflows

coordinate actions across agents, user, environment

Agentic AI Applications use **autonomous agents to execute tasks on behalf of users**, interacting with their environment or remote services as needed, and **coordinating actions with other agents** for efficiency

Frameworks for Creating AI Agents

Assistants API: A versatile platform for rapidly developing sophisticated, stateful AI assistants. It excels in performing complex computations, data analysis, and safely acting on the user's behalf by integrating and augmenting multiple APIs.

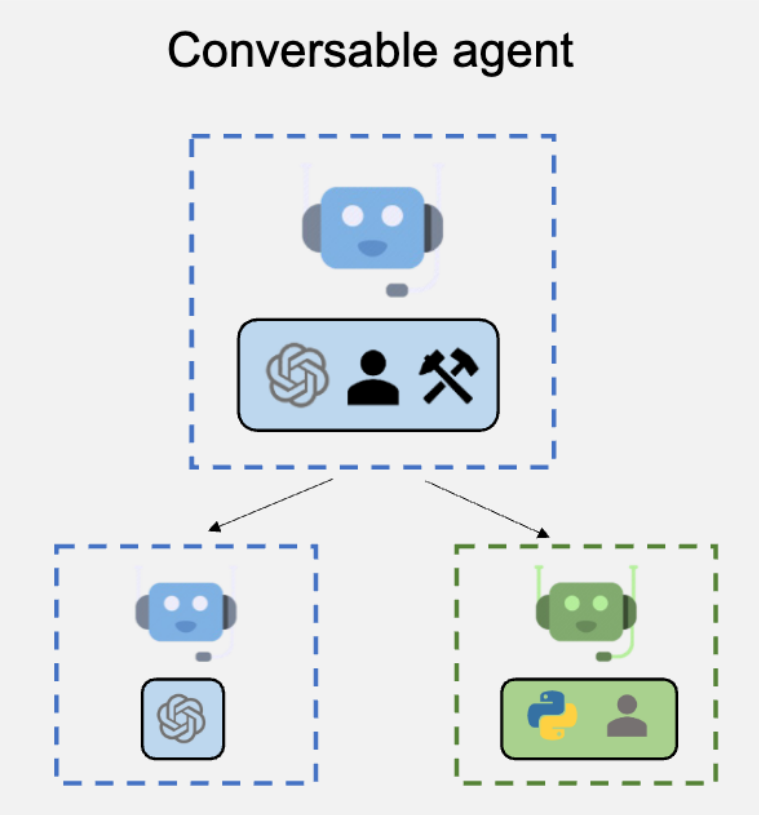
AutoGen: A framework focused on automating the generation of code and scripts for data analysis and business tasks. It's ideal for creating custom agents that handle long-form thinking, research, and planning, enabling advanced automation in various domains.

Semantic Kernel: A modular and extensible framework designed for building AI agents that orchestrate multiple plugins, APIs, and services. It's particularly suited for enterprise-grade applications where complex tasks need to be managed efficiently.

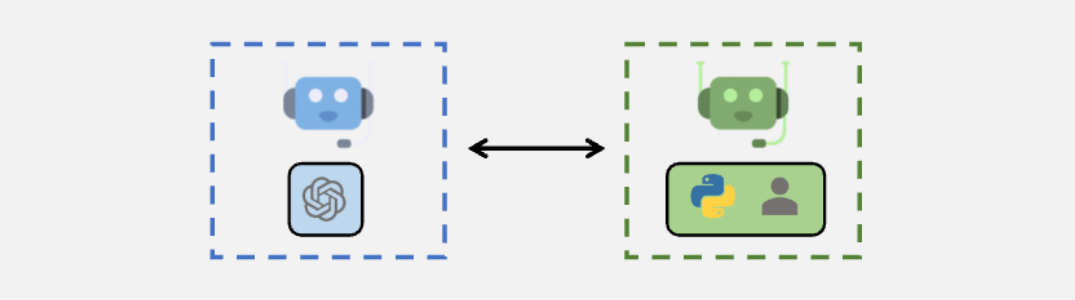
TaskWeaver: A code-first framework tailored for data analytics tasks, which translates user requests into executable code snippets. It efficiently coordinates plugins and manages complex data structures in a stateful environment, ensuring consistent results across sessions.

LangGraph: An advanced orchestration framework that enables the creation of complex, stateful AI agents through graph-defined workflows. It provides detailed control over agent behavior, including the ability to implement loops, conditional branching, and persistent states, making it ideal for sophisticated, production-ready applications.

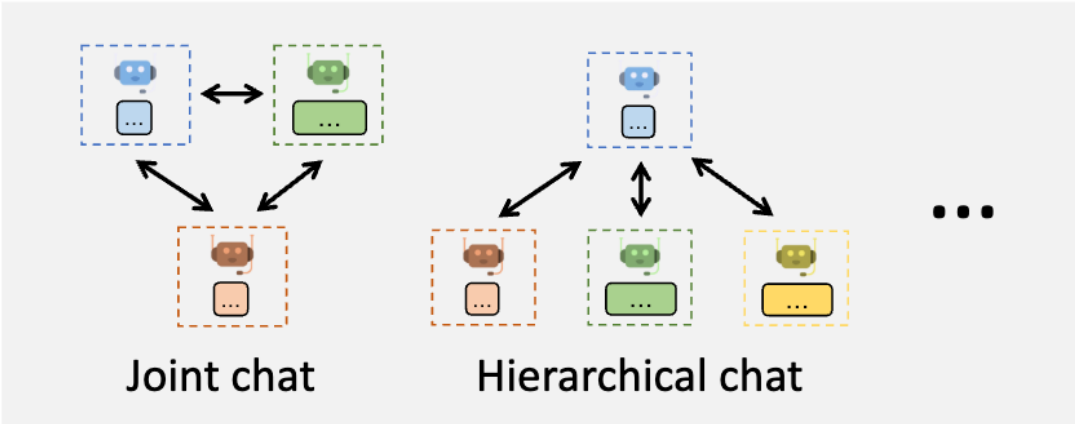
Introducing the AutoGen Framework



Agent Customization



Multi-Agent Conversations



Flexible Conversation Patterns

Open-Source
Framework & Samples

Customizable
Conversable Agents, LLMs

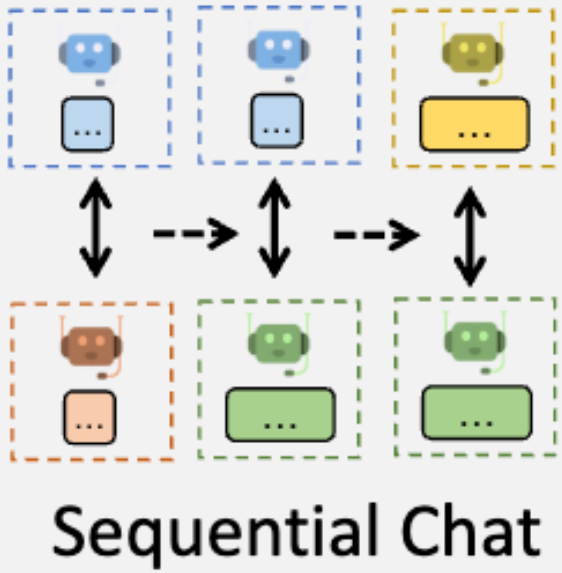
Research-Driven
Tools & Patterns

No-Code and Code-First
Development

Docs: https://aka.ms/autogen/website

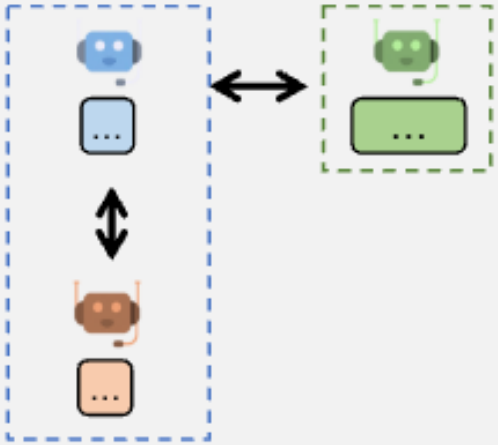
Discord: https://aka.ms/autogen/discord

Conversation Patterns



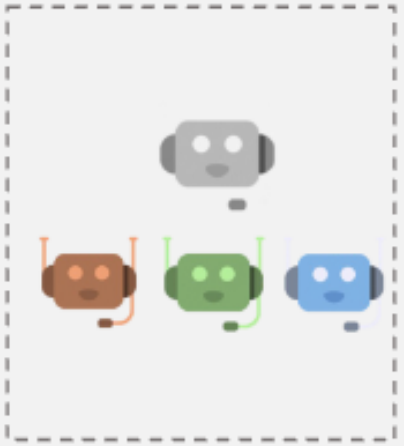
Sequential Chat

- Sequence of chats between two agents, chained together by a carryover mechanism
- useful for complex task that can be broken down into interdependent sub-tasks
- Example: Customer Support Resolution Workflow



Nested Chat

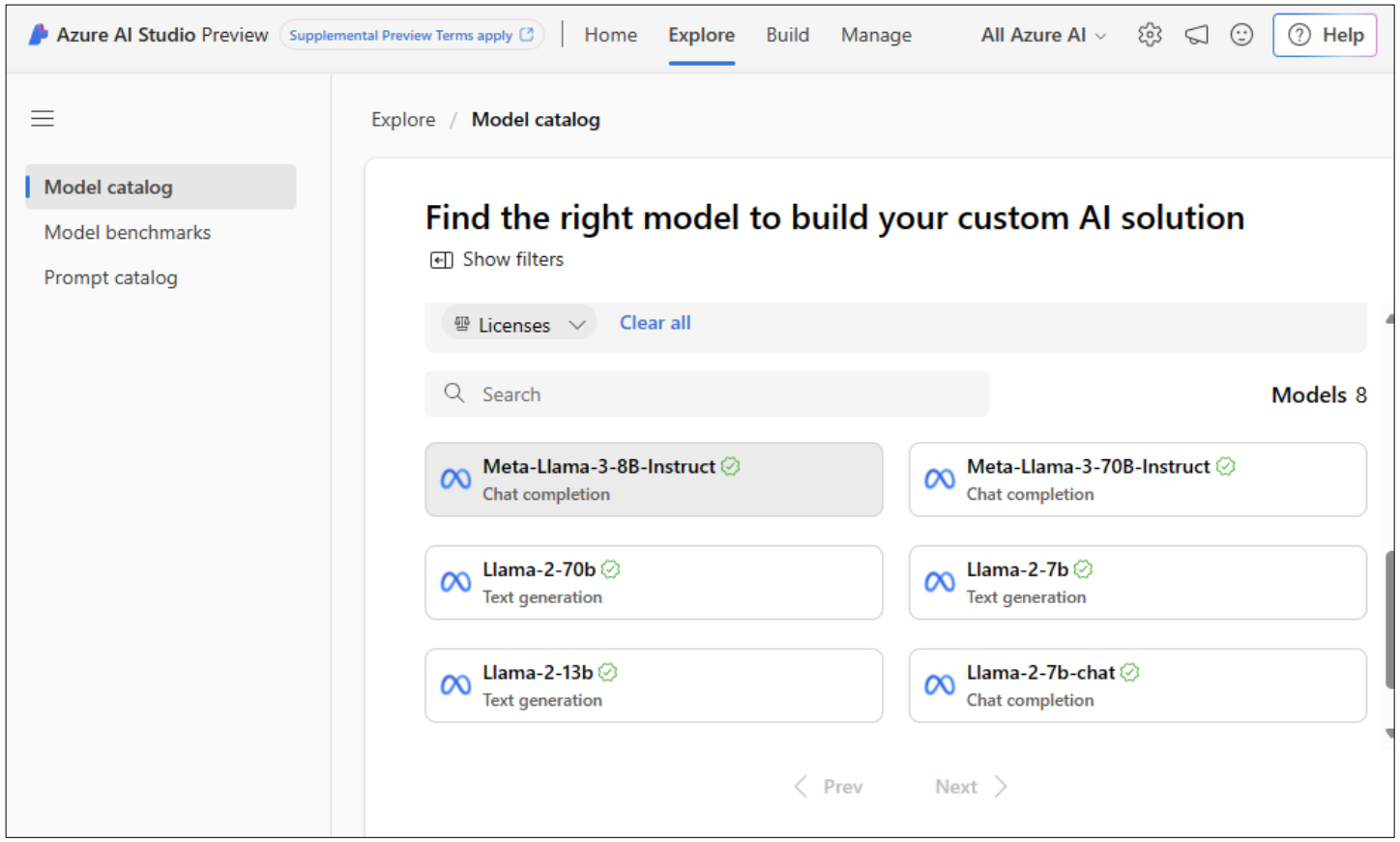
- Package a workflow into a single agent for reuse in a larger workflow
- Orchestrated by the Nested Chat Handler which triggers a series of nested chats when a message is received.
- Example: Complex Decision-Making Assistant



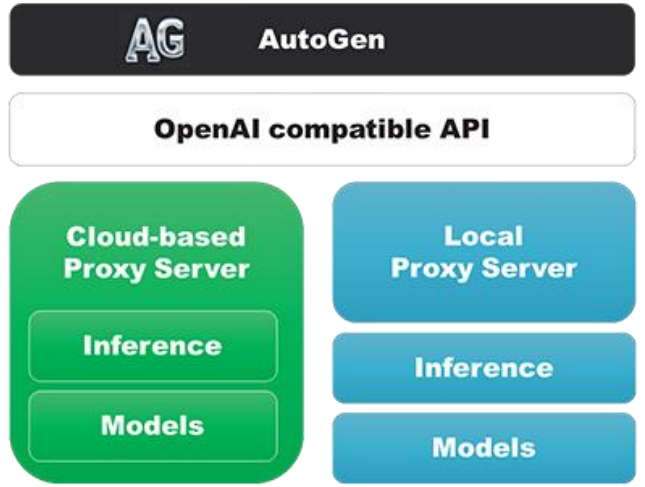
Group Chat

- Agents contribute to a single conversation thread and share the same context.
- Useful for tasks that require collaboration among multiple agents.
- Orchestrated by Group Chat Manager Agent that selects the next agent.
- Example: Collaborative Project Management

AutoGen Language Model Support



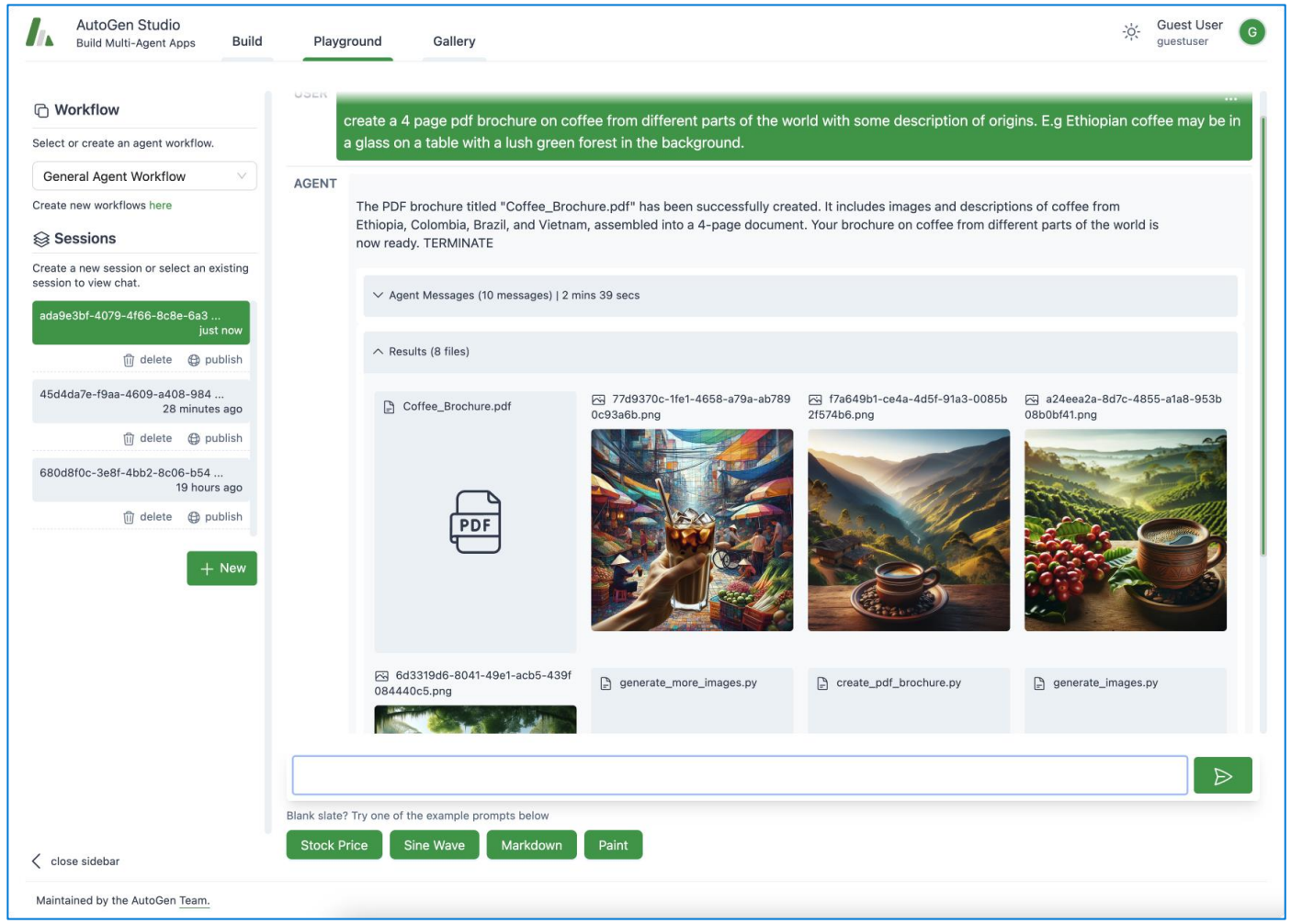
1. OpenAI Compatible API



OpenAI, Anthropic, Together AI, Mistral AI, LiteLLM etc.

2. Custom Model Client Class

AutoGen Studio



Define Skills
Create reusable functions, tools

Define Models
Define & configure required LLMs

Define Agents
Configure LLM, skills, behaviors

Define Workflows
Create agents, multi-agent conversations

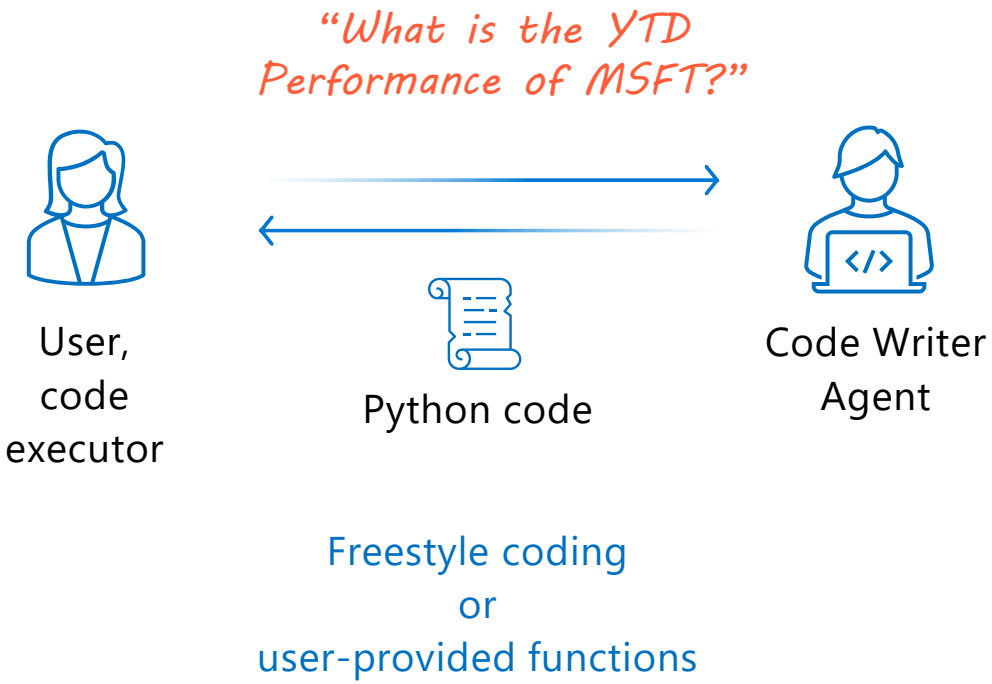
Create Sessions
Test and validate agent workflows

Publish Sessions
Share sessions to a gallery to revisit

Docs: https://microsoft.github.io/autogen/blog/2023/12/01/AutoGenStudio/

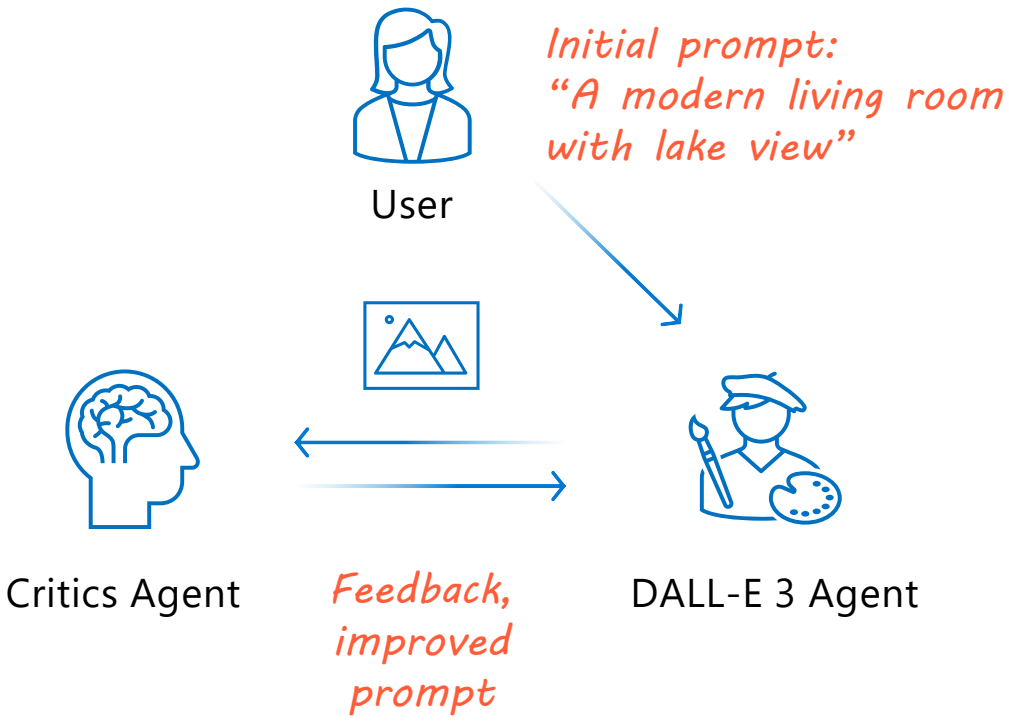
Business Use Case Demos

Code Generation for Financial Analysis



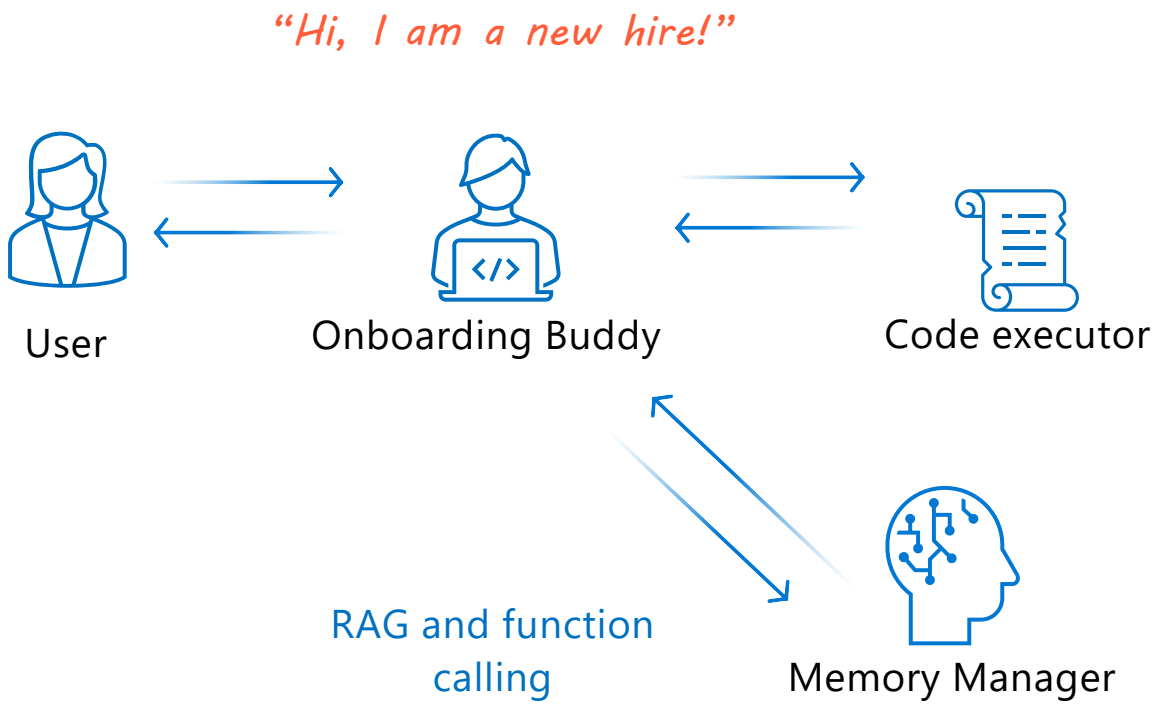
- Basic example of two-agent-interaction for getting latest financial insights
- The required code can be created by the LLM or given as pre-defined Python functions
- User confirms result or asks for adjustments in interactive dialog
- Example uses GPT-4o as LLM
- Code execution can be local or in a Docker container (recommended)

Interactive Architecture and Interior Design



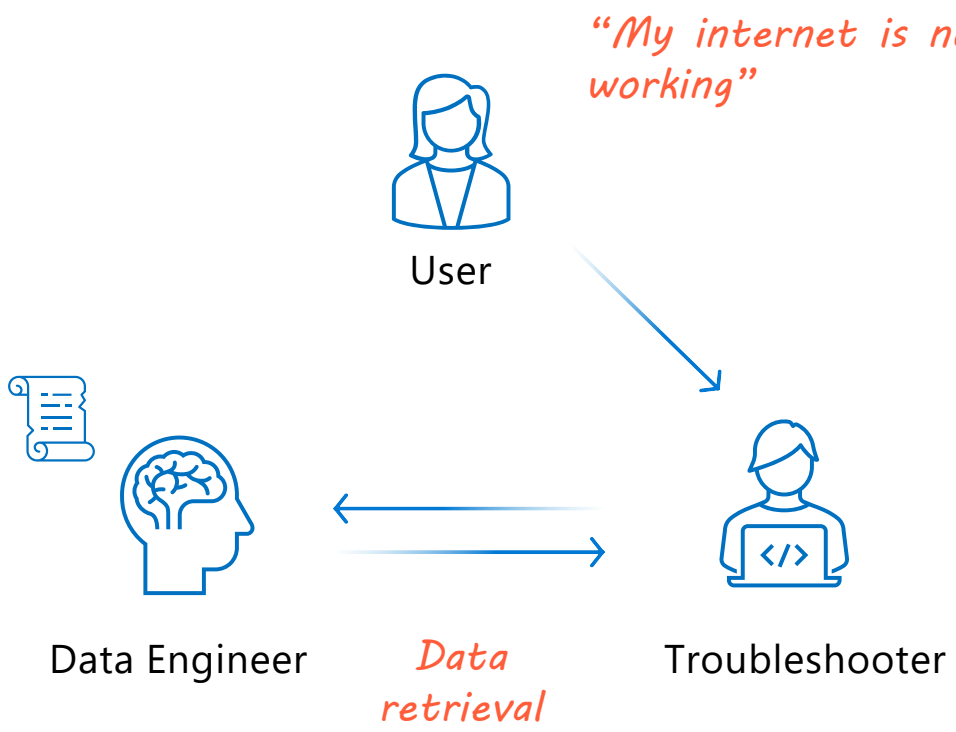
- Multimodal example to iteratively improve a visual concept
- Example uses GPT-4o as LLM incl. visual analysis and DALL-E 3 for image generation
- Note that prebuilt DALL-E 3 prompt rewrite needs to be disabled for optimal results
- The MultimodalConversableAgent is used as Critics because it handles text and image content
- The ConversableAgent with custom logic for image generation is used to create the DALL-E 3 Agent

HR Onboarding Buddy for New Employees



- Example of a RAG-based chat flow with constant user feedback
- Memory Manager acts as an agent responsible for creating and maintaining memories in the database such that the session can resume at any moment
- Function calling for memory management and information retrieval
- Example uses GPT-4o as LLM and CosmosDB as the data source
- Code execution can be local or in a Docker container (recommended)

Service Center Troubleshooting Assistant



- Simplified example of a customer service troubleshooting scenario with pre-defined functions and APIs
- Data engineer acts as a retriever of the information: free style coding can be added if necessary
- Allows for dynamic user feedback
- Can be extended with more agents (e.g. Planner) for complex troubleshooting flows
- Example uses GPT-4o as LLM and CosmosDB as the data source for customer and product information

Autonomous Agents Considerations

Advantages

- Flexible approach for solving complex business problems.
- Easy to get started with frameworks like AutoGen.
- AI agents evolve beyond standalone models, using multi-step workflows can outperform single-step LLM usage significantly.
- Cost-efficient solution to automate repetitive tasks and assisting decision makers.

Limitations

- Variability of results in each workflow step makes overall outcome less predictable.
- Number of back-and-forth interactions between agents might be challenging for debugging and end user communication.
- Human needs to stay in the driver seat
  - Human-provided code instead of free-style coding
  - User confirmation before executing important steps
- Agent-initiated use of APIs / services raise data privacy & security concerns and ethical considerations.

Envisioning Discussion