

Orchestrating Complex AI Agent-based workflows

...

Anand Ranganathan
anand.ranganathan@gmail.com

All opinions are my own ...



Today's Agenda

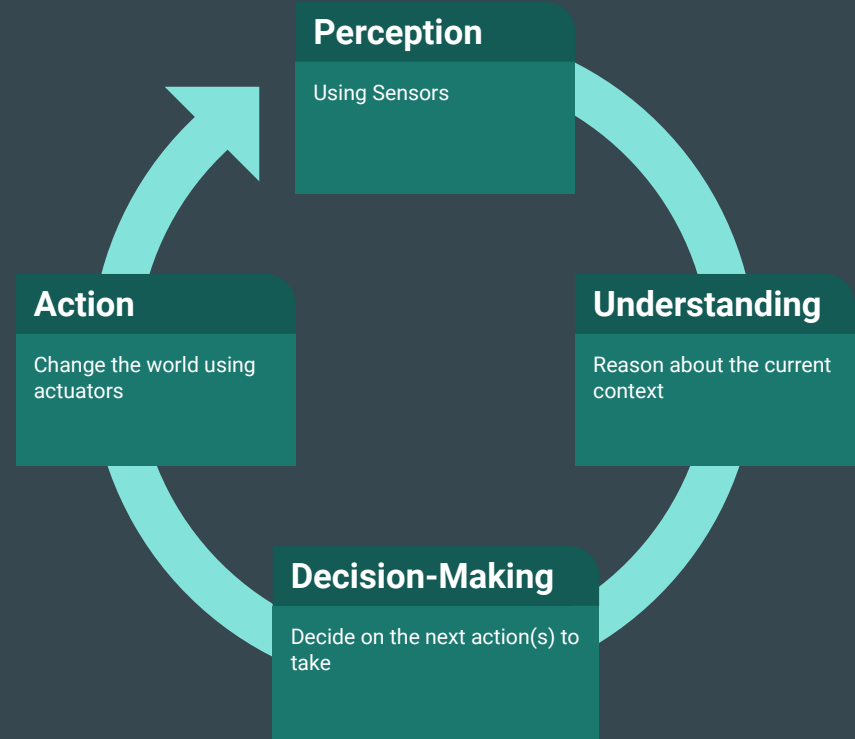
- What are AI Agents?
- AI Agents in the wild
- Key Principles and Design Patterns
- Building AI Agents
- Looking forward ...



What are AI Agents?

AI Agents

- An AI agent is an artificial entity that is able to perceive its surroundings using sensors, understand the current situation, make decisions, and take actions using actuators.
- They can potentially repeat these steps in a cycle to achieve a goal



SAE Levels of Autonomous Driving

Level	Description
0	No driving automation, but can give warnings
1	Driver assistance, such as adaptive cruise control or lane keep assist
2	Partial driving automation, such as lane keep assist and adaptive cruise control
3	Conditional driving automation, where the driver is not required to drive in certain conditions, but needs to take over in other conditions
4	High driving automation, which is considered true driverless territory
5	Full driving automation, where the vehicle can drive itself in all conditions and locations



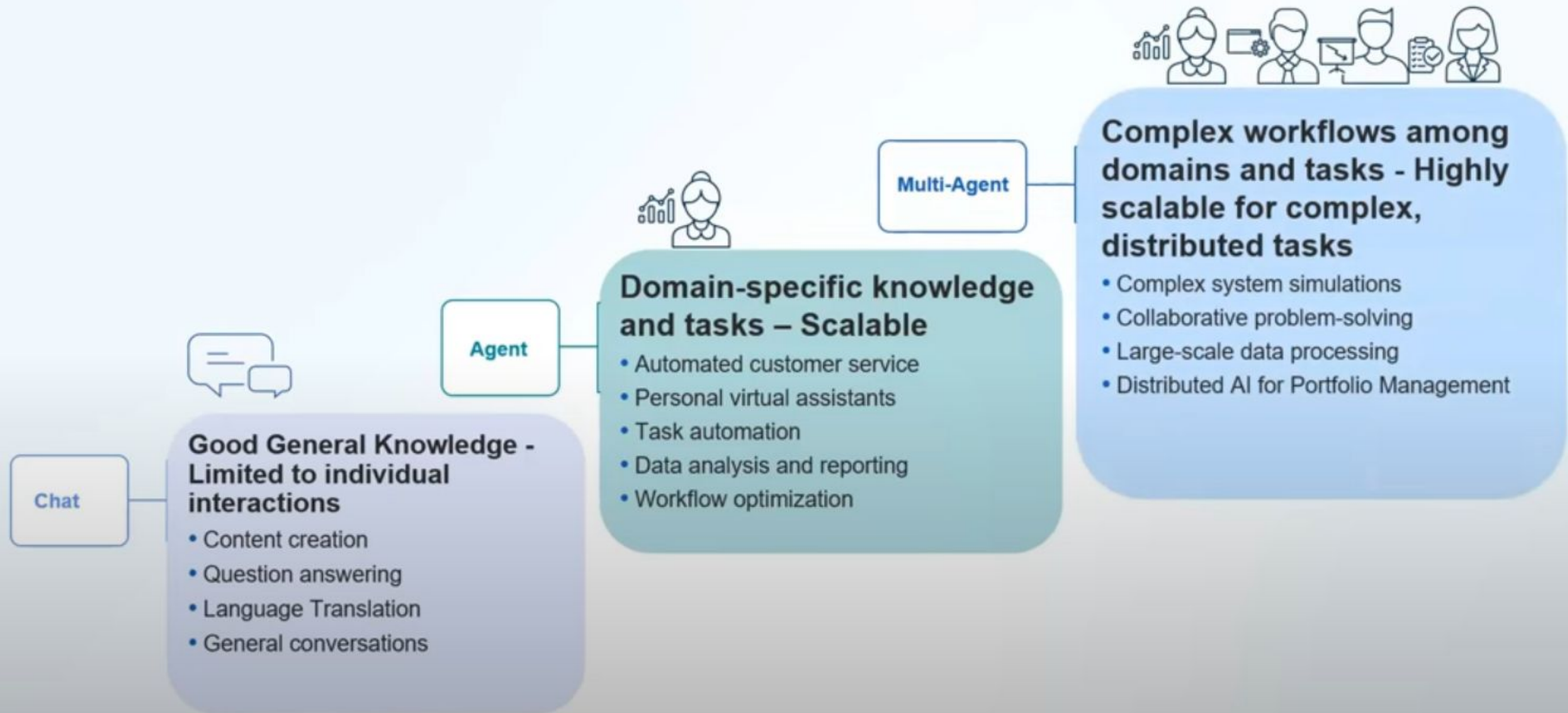
AI Agents in the Real World



- Intelligent personal assistants help users with tasks (Siri, Alexa).
- Autonomous robots operate independently in the physical world (Roomba).
- Gaming agents play games against humans or other agents.
- Fraud detection agents analyze behavior to identify suspicious activity.
- Customer Service Agents behind numerous chatbots

AI Agents in the wild

Clearwater's Gen AI Progression



*From Talk by Daniel Cherry, DE at Clearwater Analytics



Nikki

NAIC Policy Expert

Username: nikki

Regulatory policy expert at a leading financial technology company, adept at explaining regulatory requirements and industry standards. Skilled at helping clients interpret the regulations as it applies to their portfolio of securities, and fostering a culture of integrity.



Carlos

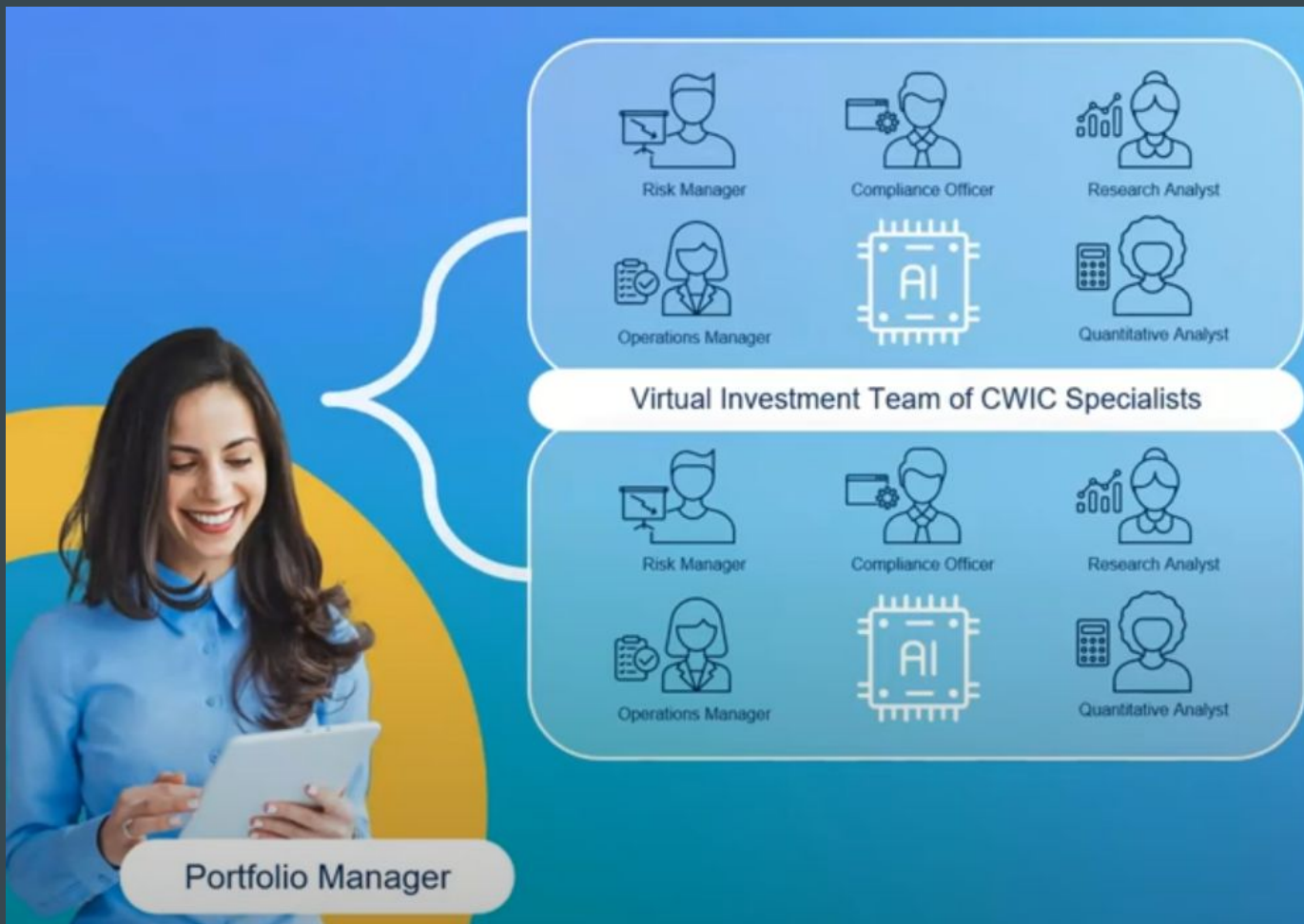
Compliance Analyst

Username: carlos

Experienced compliance analyst at a leading financial technology company, adept at monitoring and ensuring adherence to regulatory requirements and industry standards. Skilled at conducting risk assessments, implementing compliance policies, and fostering a culture of integrity, contributing to the company's commitment to compliance excellence.

Multiple agents with different roles performing different tasks

- Often using fine-tuned SLMs
- Can be personalized
- Can collaborate in autonomous workflows



*From Talk by Daniel Cherry, DE at Clearwater Analytics

ServiceNow

The first ServiceNow AI Agents, which the company says will be available in November, will be customer service management (CSM) AI agents and **IT service management (ITSM)** AI agents. These AI agents will use advanced reasoning, supported by cross-enterprise data from the Now Platform, to provide “deep contextual comprehension,” reducing mean-time-to resolution.

ServiceNow said its first use cases, CSM AI agents and ITSM AI agents, will deliver a boost to live agent productivity, helping them solve employee and customer issues by comprehending context, creating a step-by-step process for resolution, and executing on that plan with approvals from live agents where needed.

*<https://www.cio.com/article/3511490/servicenow-xanadu-brings-ai-agents-to-now-platform.html>

ServiceNow AI Agents

The screenshot displays the ServiceNow user interface. In the background, a case titled "Approval required" is visible, with a description: "A customer's modem has failed a...". The case details include fields for Status, Opened, Caller, and Severity. Below the details, there are "Related Resources" including a KB article (KB0003849) and two articles: "The Customer Retention Case for Approvals" and "Exploring the Top 10 Most Requested Modems".

In the foreground, a "Now Assist" pop-up window is open. It features a green star icon and the text "Now Assist". The main message reads: "Hi, Audrie. Here are the steps that have been taken by the AI agents working on this case." Below this, a section titled "Steps taken by AI agents" lists four steps, each with a green checkmark icon:

- Conducted a network review in the customer's area and confirmed full functionality.
- Verified network stability to ensure no general issues could affect Alectri service.
- Analyzed similar cases and identified the modem as a potential common issue.
- Contacted the customer for details about their router.

The background interface also shows a "Now Assist" section with a list of steps that have been taken by the AI agents, including "In the customer's area and", "ensure no general issues could", "identified the modem as a", and "details about their router.".

What is an Agentforce Agent?

An Agentforce Agent is a proactive, autonomous application that provides specialized, always-on support to employees or customers. They're equipped with the necessary business knowledge to execute tasks according to their specific role.



Role

An agent's purpose on your team



Trusted Data

The context an agent needs to work



Actions

The goals an agent can fulfill



Guardrails

The guidelines an agent can operate under



Channels

Web, mobile, WhatsApp, Slack



What is an agent's role?

The role is the agent's purpose. It defines the job to be done and the broader goals the agent should achieve on your team.



Amori - Agents that give Dating Advice

Amori's coaches had their own personalities, together forming a gang of confidants that could help me analyze my dating miscues. There was Christie the Blunt Bestie, who gives "sassy, frank advice that's straight to the point." Ethan the Wingman, who will give "spot-on dating tips and make it all a good time." Tabitha the Wise Aunt, whose wisdom "feels like learning and getting a hug at once." And Sonya the Love Scholar, who has a "Ph.D. in the science of dating."



Categorization of AI Agents

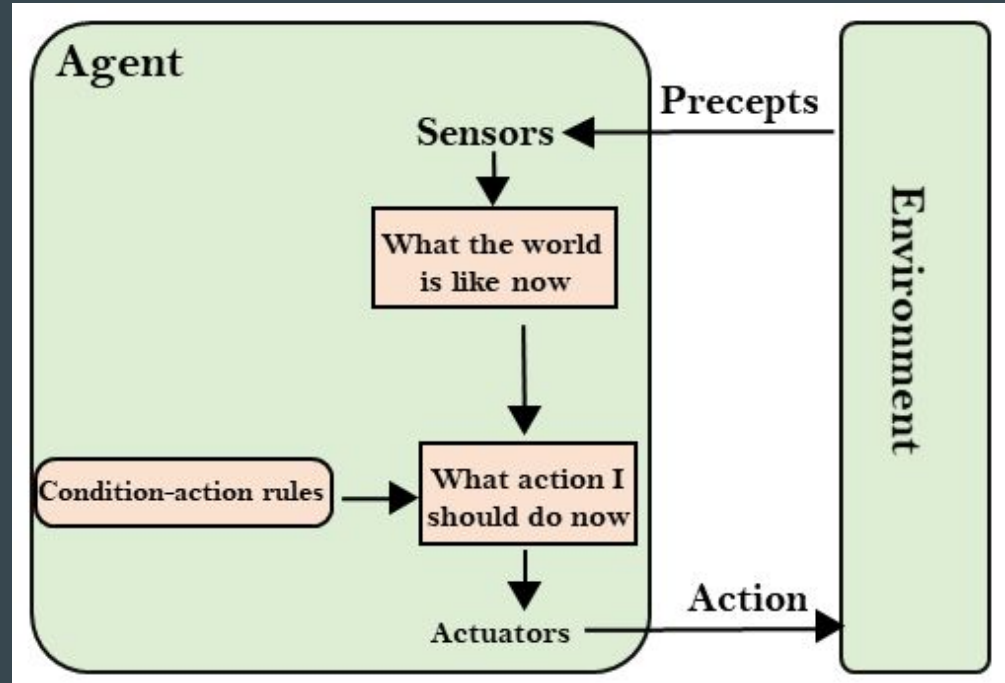
- Simple Reflex Agents
 - Select actions based on current percepts, ignoring history.
- Model-Based Reflex Agents
 - Maintain an internal state to track the world.
- Goal-Based Agents
 - Choose actions to achieve a specific goal.
- Utility-Based Agents
 - Maximize a utility function to choose optimal actions.
- Learning Agents
 - Improve performance through experience.
- Multi-Agent Systems
 - Multiple agents interacting in a shared environment.

Simple Reflex Agent



Rule:

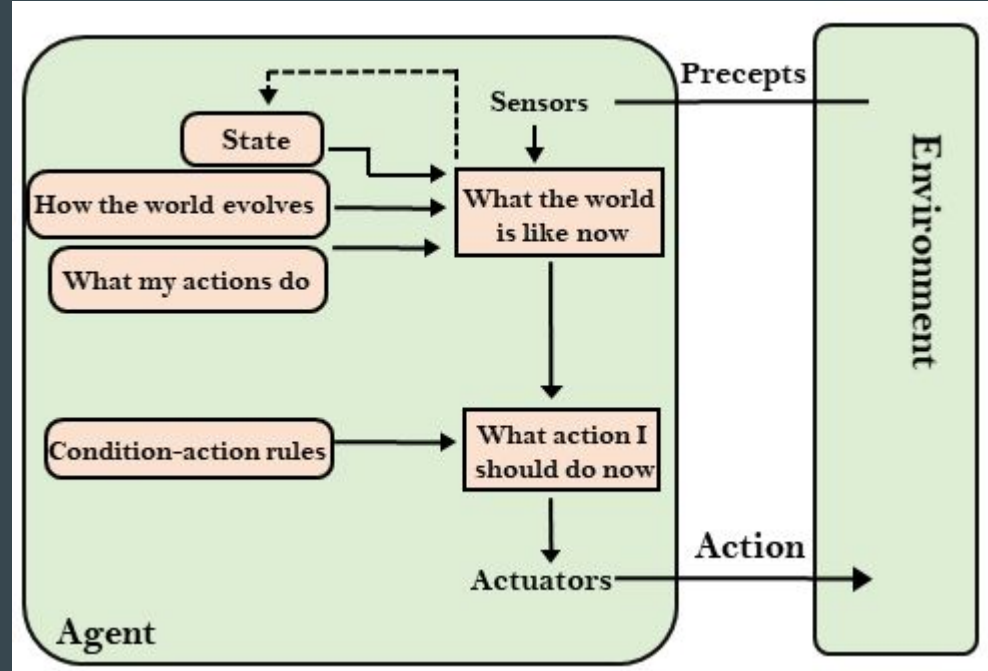
If obstacle detected, move left or right at random



Model-based Reflex Agent



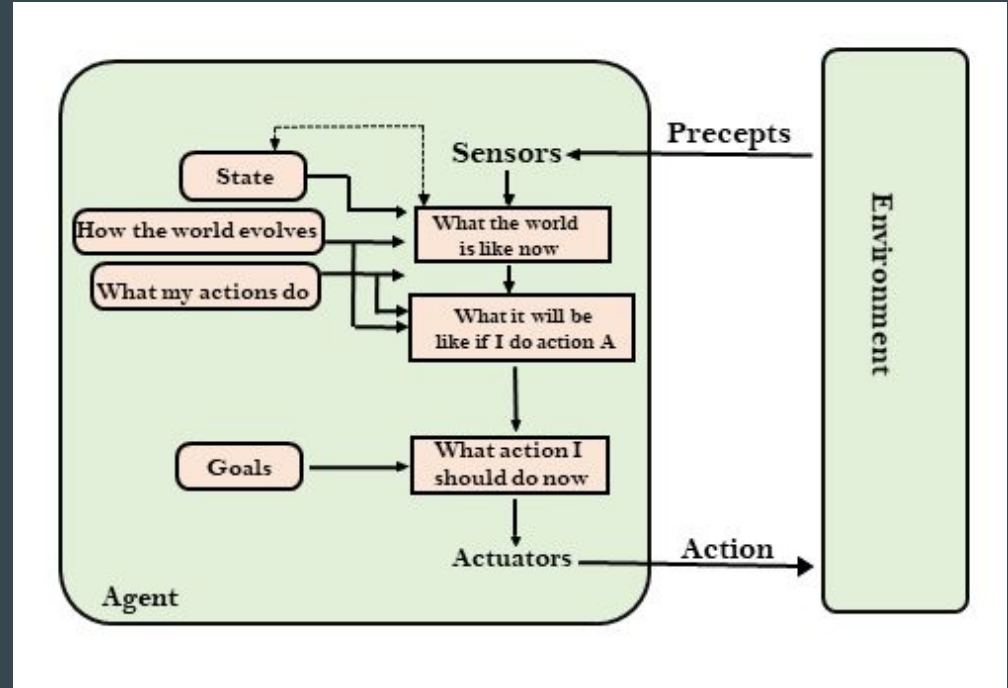
- Build model of walls & obstacles as it goes around
- Prefer going to newer paths that have not been explored before, while avoiding obstacles



Goal-based Agent



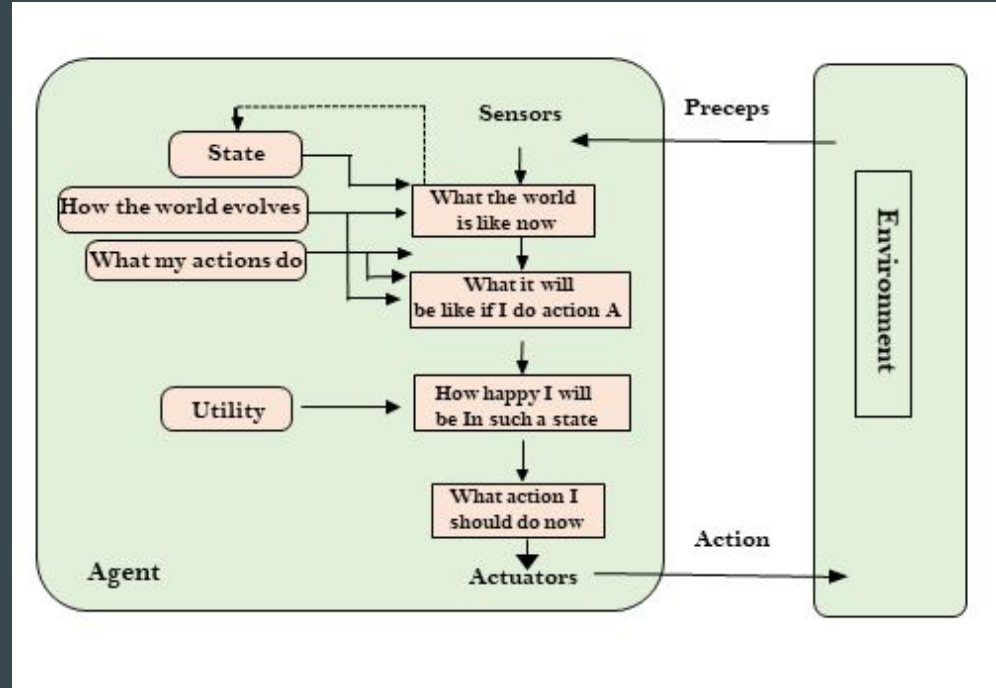
- Goal : Cover all the accessible floor areas



Utility-based Agent



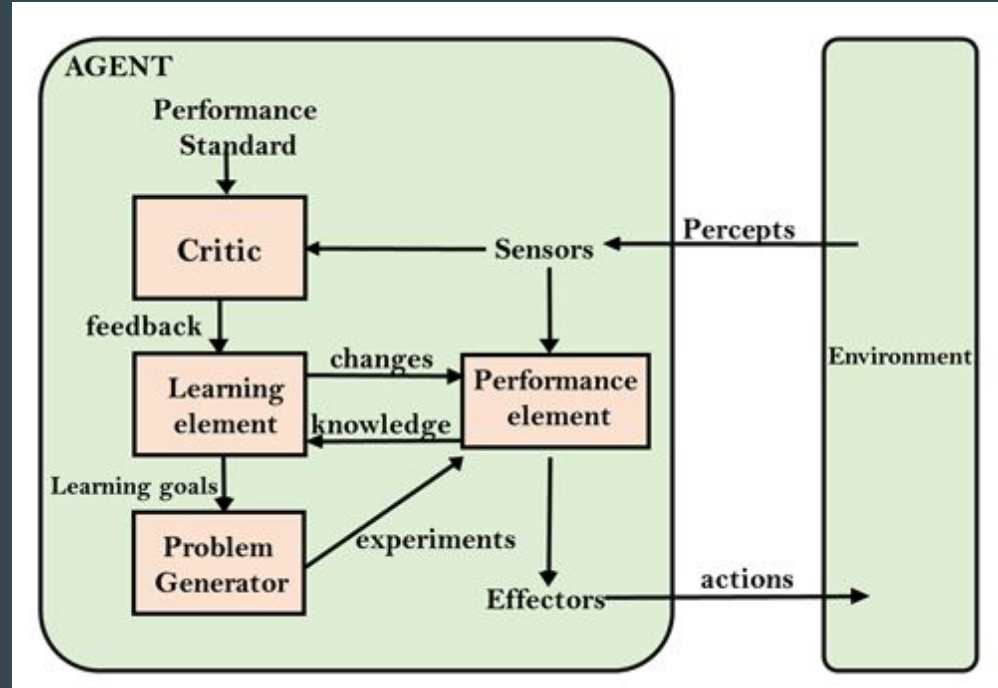
- Goal : Cover all the accessible floor areas
- Utility : Minimize time spent / distance covered



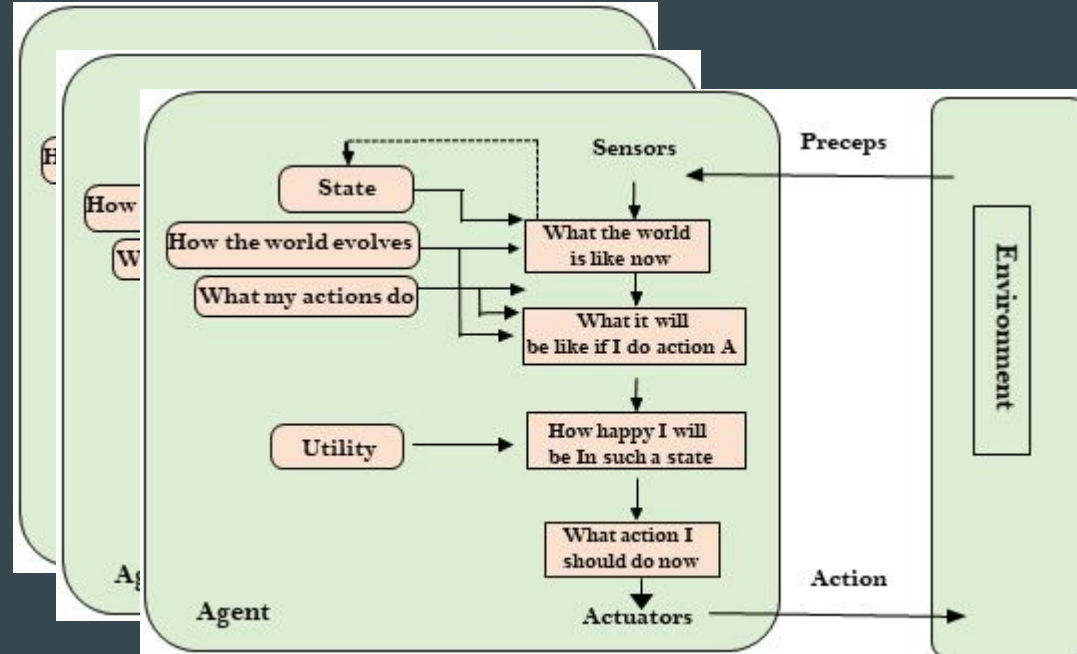
Learning Agent



- Explore new paths
- Learn which paths might take less time



Multi-Agent Systems

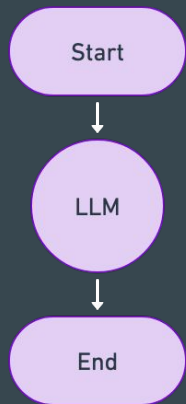


- Agents can communicate with one another and divide the tasks
- Learning and Goal-following can take place in a centralized / distributed / hierarchical manner

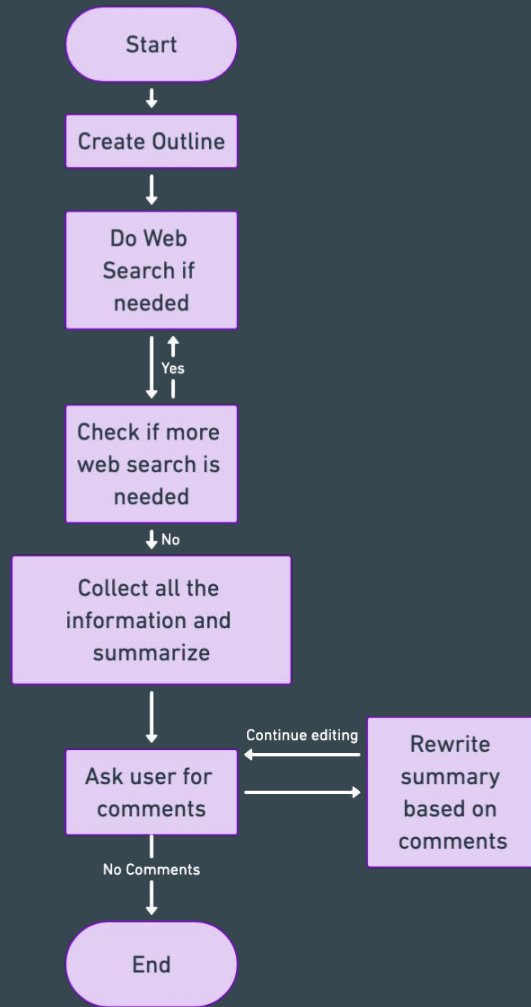
Agents in the context of LLMs

LLMs & Agents

Most LLM Interactions today tend to be zero-shot, single prompt interactions



An agent-based interaction could be multiple steps, reflect on answers, use “tools”, and involve humans



Example from GPT-4o

Zero-shot

Write a 2 paragraph summary on the impact of Hurricane Helene on the alligator population



Hurricane Helene, like other significant storms, had a notable impact on alligator populations, particularly in coastal and wetland areas. Alligators are resilient creatures and have evolved to survive extreme weather conditions, but the intensity of hurricanes can disrupt their habitats. Flooding caused by heavy rains and storm surges can alter the alligator's ecosystem by displacing them from their nests, disrupting their food sources, and changing the salinity of freshwater environments. These changes can lead to a temporary reduction in alligator populations, especially for young or smaller alligators, which are more vulnerable to predation or being swept away by floodwaters.

However, in the long term, alligator populations often recover after such events due to their adaptability. Hurricanes can sometimes create new habitats by increasing the size of wetlands or forming new ponds, giving alligators additional areas to hunt and live. Alligators also use their burrowing skills to create dens or "gator holes" to shelter from the storm, which can protect them during extreme weather. Despite short-term disruptions, alligators' evolutionary traits allow them to survive and eventually thrive again, making them one of the more resilient species in regions prone to hurricanes like Helene.

Agent-based

Based on the outline and all the information extracted from searching the web, create a 2 paragraph essay on the impact of Hurricane Helene on the alligator population



Hurricane Helene had a significant but temporary impact on alligator populations, especially in areas like Florida where flooding was widespread. As the storm brought severe flooding and storm surges, many alligators were displaced from their habitats, with reports of alligators swimming through the flooded streets of Sarasota(Newsweek)(Newsweek). Alligators often seek refuge in deeper wetlands, river channels, or forested areas during storms, avoiding the most dangerous floodwaters(BioMed Central)(Newsweek). The immediate effect on their habitats, particularly on nesting sites, can be severe as storm surges and rising water levels flood their nests, disrupting reproduction cycles and displacing hatchlings. However, research from past hurricanes indicates that while some nests are lost, adult alligators tend to return to their territories once floodwaters recede, mitigating long-term population decline(SEAFWA).

Despite the short-term disruptions caused by Hurricane Helene, alligator populations are resilient and tend to recover quickly. Post-hurricane conditions often create new water bodies, like ponds and wetlands, which provide fresh habitats for alligators. Studies of alligator populations in other areas affected by hurricanes, such as Orange Lake and Lake Woodruff, show that while hurricanes disrupt nesting and feeding patterns, long-term survival is generally unaffected as alligators adapt to new environmental conditions(Thicket of Diversity)(SEAFWA). Alligator resilience is supported by their ability to seek safe refuges during storms and rebuild nesting areas after floods, ensuring that population levels remain stable even after major storms like Helene.

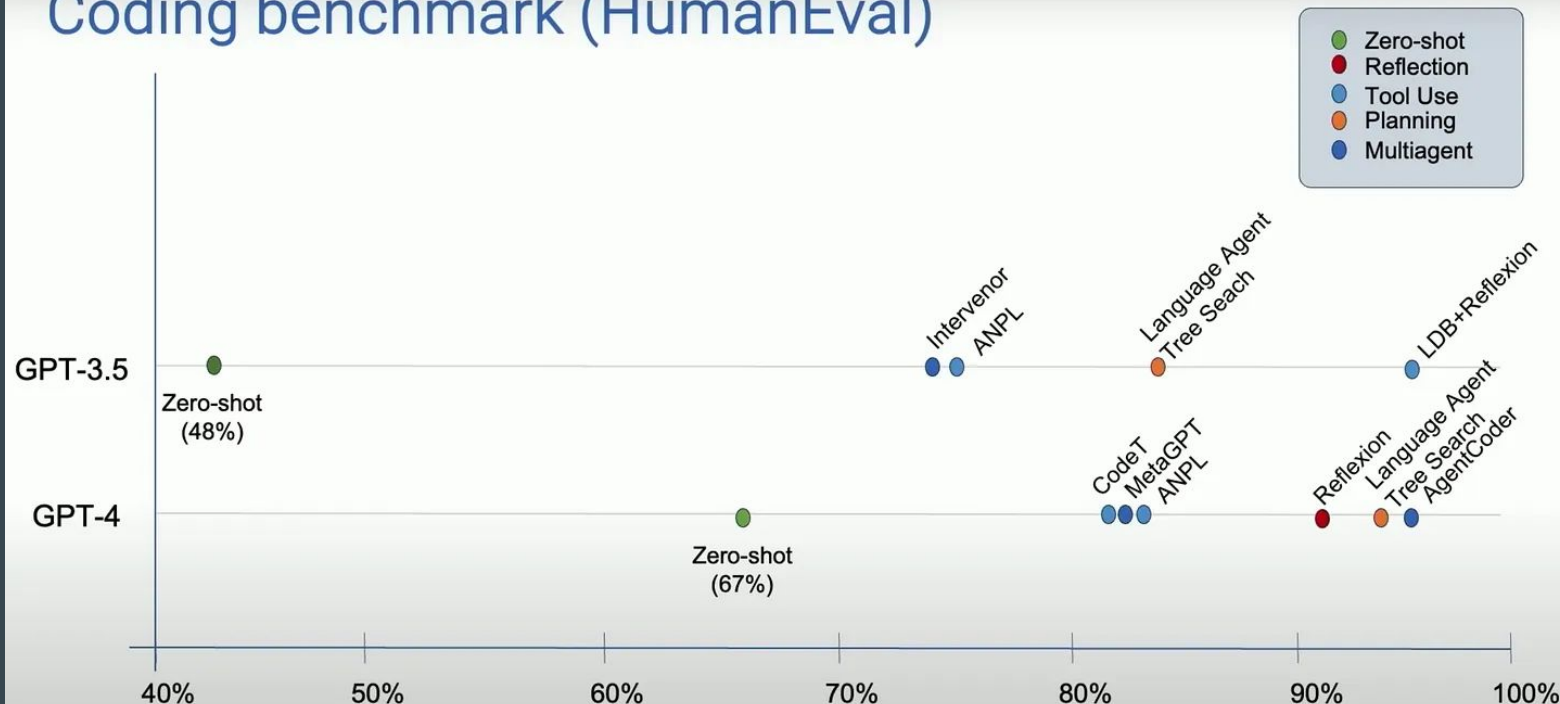
****HumanEval: Coding Benchmark****

- HumanEval: a benchmark for evaluating code generation models.
- Contains 164 hand-written Python programming problems.
- Problems include function descriptions, docstrings, and unit tests.
- Models must generate code that passes all unit tests.
- Example: Write a function to find the first non-repeating character in a string.

```
def first_non_repeating_character(string):  
    """  
    Finds the first non-repeating character in a  
    string.  
  
    Args:  
        string: The input string.  
  
    Returns:  
        The first non-repeating character, or None  
        if none exists.  
    """  
    char_count = {}  
    for char in string:  
        char_count[char] = char_count.get(char, 0) + 1  
  
    for char in string:  
        if char_count[char] == 1:  
            return char  
  
    return None
```

Coding Benchmark

Coding benchmark (HumanEval)



Key Principles & Design Patterns for AI Agents

Reflection



"What is the number of r's in strawberry"

"The word "strawberry" contains two "r's."



Reflection Step



- **Meta-question:** *Think carefully about your answer, break down any complex words into smaller words if needed and fix your answer if needed*

Through reflection, the AI identifies possible additional dimensions of the problem or additional ways of solving it.

"Let's break down the word "strawberry" carefully as you requested: "straw" + "berry"

Now, let's count the "r's" in each part: "straw" has 1 "r." , "berry" has 2 "r's."

So, when we combine them, "strawberry" has a total of 3 "r's."



Tools (Sensors, Reasoning or Actuators)

Web Search

Should we do a web search to get more information for this topic?



Searched 5 sites ^

Q "Hurricane Helene impact on alligator population"
bing.com

N Newsweek — Alligators Swim Through Streets as Hurricane Helene Hits Florida - Newsweek
newsweek.com

W Wikipedia — Hurricane Helene - Wikipedia
en.wikipedia.org

N Newsweek — Alligators Swim Through Streets as Hurricane Helene Hits Florida - Newsweek
newsweek.com

W WGCU PBS & NPR for Southwest Florida — Photos show the devastation from Hurricane Helene...
news.wgcu.org

Hurricane Helene had a noticeable impact on alligator populations, especially in Florida, where the storm hit hardest. The hurricane's heavy flooding displaced many alligators, forcing them to move from their usual habitats into urban areas. Reports surfaced of alligators swimming through

Code Execution

Generate code for calculating the sum of numbers in a list and execute the code and show the result. Show all the steps in the execution of the code execution tool



Here's an explanation of each step for calculating the sum of numbers in a list, including code generation and execution:

Step 1: Write the Code

We generate Python code to calculate the sum of numbers in a list:

python

Copy code

Python code to calculate the sum of a list of numbers

```
numbers = [10, 20, 30, 40]
total_sum = sum(numbers)
print(total_sum)
```

Step 2: Execute the Code

Now, I will run this code using the code execution tool.

Execution:

Let's execute the code and show the result.

Step 3: Show the Result

The sum of the numbers in the list `[10, 20, 30, 40]` is 100.

Lots of Tools ...

Search

The following table shows tools that execute online searches in some shape or form:

Tool/Toolkit	Free/Paid	Return Data
Bing Search	Paid	URL, Snippet, Title
Brave Search	Free	URL, Snippet, Title
DuckDuckGoSearch	Free	URL, Snippet, Title
Exa Search	1000 free searches/month	URL, Author, Title, Published Date
Google Search	Paid	URL, Snippet, Title
Google Serper	Free	URL, Snippet, Title, Search Rank, Site Links
Jina Search	1M Response Tokens Free	URL, Snippet, Title, Page Content
Mojeek Search	Paid	URL, Snippet, Title
SearchApi	100 Free Searches on Sign Up	URL, Snippet, Title, Search Rank, Site Links, Authors
SearxNG Search	Free	URL, Snippet, Title, Category
SerpAPI	100 Free Searches/Month	Answer
Tavily Search	1000 free searches/month	URL, Content, Title, Images, Answer
You.com Search	Free for 60 days	URL, Title, Page Content

Code Interpreter

The following table shows tools that can be used as code interpreters:

Tool/Toolkit	Supported Languages	Sandbox Lifetime	Supports File Uploads	Return Types	Supports Self-Hosting
Azure Container Apps dynamic sessions	Python	1 Hour	✓	Text, Images	✗
Bearly Code Interpreter	Python	Resets on Execution	✓	Text	✗
E2B Data Analysis	Python, In beta: JavaScript, R, Java	24 Hours	✓	Text, Images, Videos	✓
Riza Code Interpreter	Python, JavaScript, PHP, Ruby	Resets on Execution	✓	Text	✓

Productivity

The following table shows tools that can be used to automate tasks in productivity tools:

Tool/Toolkit	Pricing
Github Toolkit	Free
Gitlab Toolkit	Free for personal project
Gmail Toolkit	Free, with limit of 250 quota units per user per second
Infobip Tool	Free trial, with variable pricing after
Jira Toolkit	Free, with rate limits
Office365 Toolkit	Free with Office365, includes rate limits
Slack Toolkit	Free
Twilio Tool	Free trial, with pay-as-you-go pricing after

Database

The following table shows tools that can be used to automate tasks in d

Tool/Toolkit	Allowed Operations
Cassandra Database Toolkit	SELECT and schema introspection
SQLDatabase Toolkit	Any SQL operation
Spark SQL Toolkit	Any SQL operation

Planning

Goal

"We want to reduce response times and handle 80% of incoming customer queries without human intervention."



Tools

- **AI Chatbot** (Generative AI): To handle FAQs and common customer inquiries.
 - DialogFlow or OpenAI API
- **Sentiment Analysis Tool**: To assess customer emotions and escalate if necessary.
 - Google Cloud's NLP APIs
- **CRM Integration**: To log all interactions and allow seamless agent handoffs when required.
 - Hubspot or Salesforce APIs
- **Monitoring & Feedback Loop**: A system that learns from past conversations to improve the AI's responses over time.
 - Zapier

Plan

Step 1: Customer Interaction

AI Chatbot (Primary Agent): Handles inquiries using predefined knowledge bases and real-time NLG

Step 2: Query Classification

AI Agent for Query Classification: e.g., billing, tech support, general inquiries) using machine learning.

Step 3: Sentiment Analysis and Escalation

Sentiment Analysis Tool (Secondary Agent): assesses the tone and urgency of the message (positive, neutral, negative).

Step 4: Context Gathering and CRM Logging

CRM Agent: The AI chatbot gathers contextual information from the customer (name, order ID, issue details) and logs it into the CRM system (e.g., Salesforce) for future reference or human handoff.

Step 5: Continuous Learning and Feedback

Monitoring and Feedback Loop: Every interaction is logged and analyzed by a learning agent.

Multi-Agent Collaboration



- Virtual Software Company
- Multiple agents with distinct personalities, roles and tasks
 - CEO, CPO, CTO, Programmers, Reviewers, Testers, Art Designers
- United by a mission to "revolutionize the digital world through programming"
- Collaborate by participating in specialized functional seminars, including tasks such as designing, coding, testing and documenting

<https://github.com/OpenBMB/ChatDev/blob/main/CompanyConfig/Default/RoleConfig.json>

How do you build AI Agents

Common AI Agent Frameworks



- LangChain + LangGraph: Popular framework for developing applications powered by language models.
- Crew AI: Multi-agent collaboration
- Auto-GPT: An open-source application showcasing the capabilities of the GPT-4 language model.
- BabyAGI: Python script that uses OpenAI and Pinecone to create and manage tasks autonomously.
- Microsoft JARVIS: Framework for building AI Agents using Azure services.
- OpenAI Swarm
- Dify.ai : Graphical tool for building agents

We're going to look a bit deeper into LangGraph

- LangGraph's API supports diverse control flows – single agent, multi-agent, hierarchical, sequential
- Supports Human-in-the-loop
- Has a nice balance of control with AI-driven automation
- Ensure reliability with easy-to-add moderation and quality loops that prevent agents from veering off course.

Supports Fixed Control Flows

- Deterministic sequence of actions



Made with  Whimsical

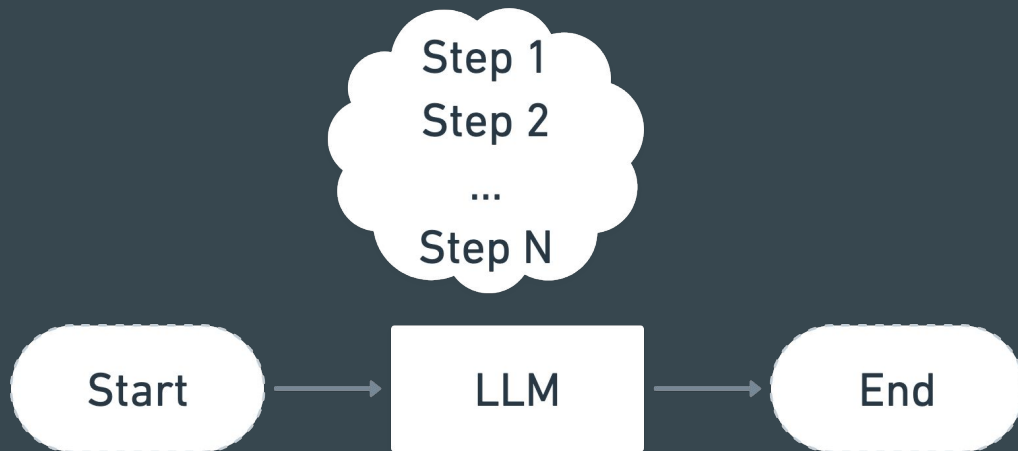
Supports LLM-decided Flow Paths

- LLM acts as a router / orchestrator



Supports Fully Autonomous Flows

- LLM acts as a planner that can invoke multiple steps in any order any number of times



CrewAI

- Multi-Agent Collaboration
- Much more autonomous
- No need to define workflows
- Heavy use of Reflection and React pattern to decide steps to take

Looking Forward ...

Summarizing ...

- Move from monolithic LLM calls to compound AI systems
- Individual Models
 - Limited by the data and tasks they were trained on
 - Relatively difficult to adapt/fine-tune
- Compound AI Systems
 - Expand the scope of what's possible with tools
 - Incorporate Memory, Reflection, Reasoning and Planning
 - Embrace diversity with multi-agent systems
 - Work with humans to be more accurate and controllable

“Every serious thing we do is an effort to automate our intelligence, to make our human experience easier and richer, and AI is the extension of that ambition.”

– Sherry Turkle