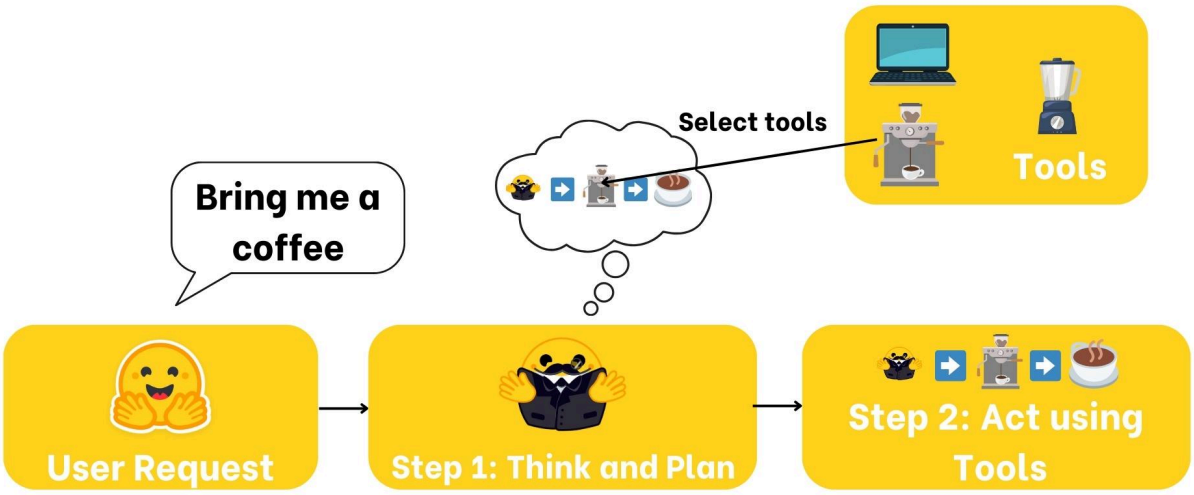
What is an Agent?

::AI model capable of reasoning, planning, and interacting with its environment.



6

More Theoretically:

An Agent is a system that leverages an AI model to interact with its environment in order to achieve a user-defined objective. It combines reasoning, planning, and the execution of actions (often via external tools) to fulfill tasks.

Think of the Agent as having two main parts:

1. The Brain (AI Model)

This is where all the thinking happens. The AI model handles reasoning and planning. It decides which Actions to take based on the situation.

2. The Body (Capabilities and Tools)

This part represents everything the Agent is equipped to do.

The scope of possible actions depends on what the agent has been equipped with. For example, because humans lack wings, they can't perform the "fly" Action, but they can execute Actions like "walk", "run" ,"jump", "grab", and so on.

What type of AI Models do we use for Agents?

The most common AI model found in Agents is an LLM (Large Language Model), which takes Text as an input and outputs Text as well.Well known examples are GPT4 from OpenAI, LLama from Meta, Gemini from Google, etc. These models have been trained on a vast amount of text and are able to generalize well

How does an AI take action on its environment?

LLMs are amazing models, but they can only generate text.

However, if you ask a well-known chat application like HuggingChat or ChatGPT to generate an image, they can! How is that possible?

The answer is that the developers of HuggingChat, ChatGPT and similar apps implemented additional functionality (called Tools), that the LLM can use to create images.

What type of tasks can an Agent do?

An Agent can perform any task we implement via Tools to complete Actions.

For example, if I write an Agent to act as my personal assistant (like Siri) on my computer, and I ask it to "send an email to my Manager asking to delay today's meeting", I can give it some code to send emails. This will be a new Tool the Agent can use whenever it needs to send an email. We can write it in Python:

Copied

```
def send_message_to(recipient, message):

    """Useful to send an e-mail message to a recipient"""
```

The LLM, as we'll see, will generate code to run the tool when it needs to, and thus fulfill the desired task.

Copied

```
send_message_to("Manager", "Can we postpone today's meeting?")
```

The design of the Tools is very important and has a great impact on the quality of your Agent. Some tasks will require very specific Tools to be crafted, while others may be solved with general purpose tools like "web_search".

Note that Actions are not the same as Tools. An Action, for instance, can involve the use of multiple Tools to complete.

Allowing an agent to interact with its environment allows real-life usage for companies and individuals.

Example Of Agent :

1: Personal Virtual Assistants

2: Customer Service Chatbots

3: AI Non-Playable Character in a video game

To summarize, an Agent is a system that uses an AI Model (typically an LLM) as its core reasoning engine, to:

- Understand natural language: Interpret and respond to human instructions in a meaningful way.
- Reason and plan: Analyze information, make decisions, and devise strategies to solve problems.
- Interact with its environment: Gather information, take actions, and observe the results of those actions.