

# The Beginner's Guide to Building AI Agents

# Why learn AI Agent ?

- **Go Beyond Chatbots:** Agents set goals, use tools, and act autonomously
- **Connect AI to the Real World:** Automate tasks, search the web, analyze data
- **In-Demand Skill:** AI agents what many industries are eyeing and potentially participating in
- **Smarter Than Apps:** They reason, plan, and adapt
- **Empower Yourself:** Build tools that think and act for you

# What is an AI agent?

A digital worker that can understand instructions  
and execute tasks accordingly

# What is an AI agent?

A digital process that starts to feel like a real teammate doing the work for us. It has:

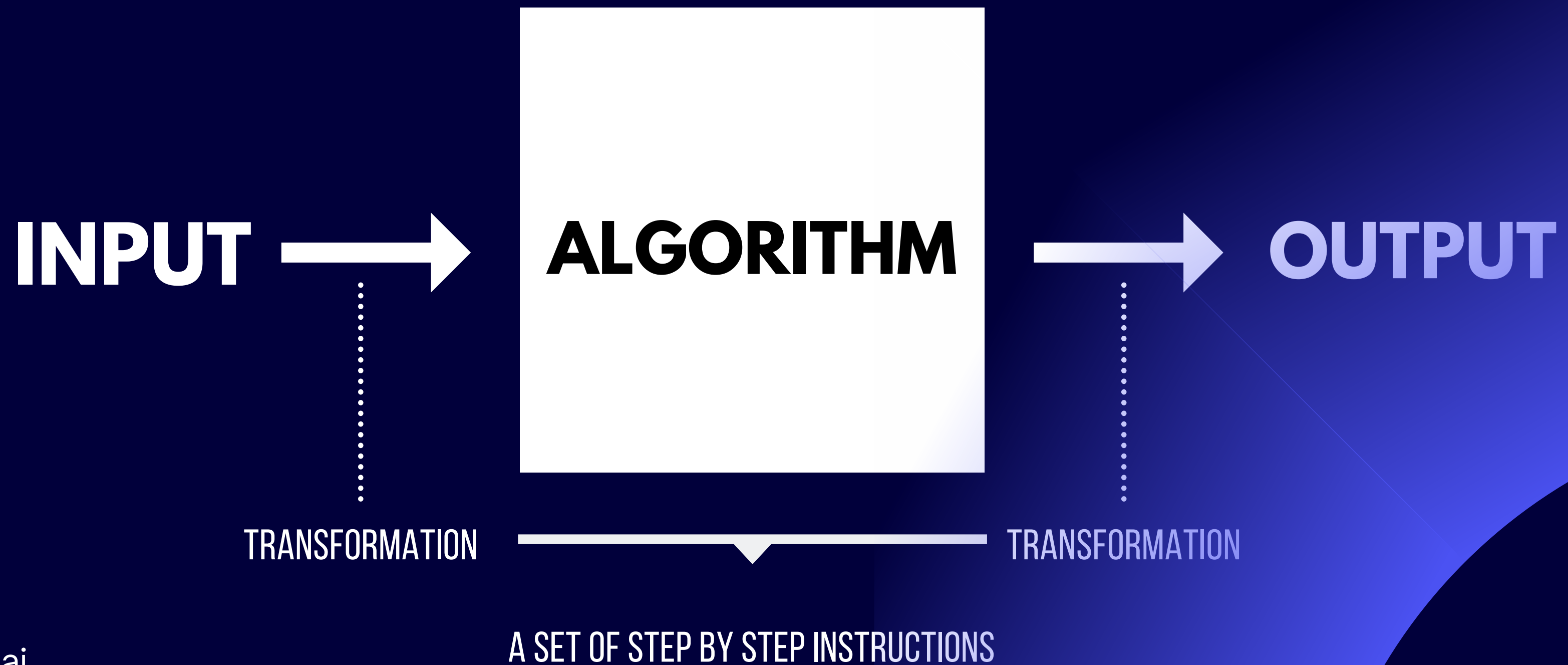
- Reasoning skill: can take a goal and then reason on how to achieve that goal
- Tool access: it can actually do things like move money around, email someone or order something for you
- Memory: it can maintain context throughout a task and even multiple tasks, so it learns from past mistakes just like us

The more you know about them, the more they can help and support you in your own work and life

# How does AI Agent work?



# How does AI Agent work?



# Chatbot vs. AI Agent

Chatbots usually just recite from a ready-made script

AI agents are different. They can receive request, check information and execute tasks.

*This ability to take action is what makes AI agent powerful and not just a glorified chatbot*



# What does it mean to have an AI Agent as a copilot

Having a new employee or colleague:

- Explain the roles, and responsibilities and rules of business
- Give access to the systems (potential risk)
- Trust them to handle tasks



# Challenges and Limitations of AI Agents

## *Technical Challenges of AI Agents*

- Limited memory — forgets context without custom memory systems
- Inconsistent performance — varies output with minor prompt changes
- Tool integration is fragile — errors in APIs or chaining tools
- Context length limits — struggles with long documents or history
- Hidden costs — frequent tool/API calls can be expensive
- Debugging is hard — difficult to trace logic or fix errors

# Challenges and Limitations of AI Agents

## *Ethical and Practical Risks*

- Hallucinations — generates false or misleading information
- Data privacy risks — sensitive input sent to external APIs
- Lack of transparency — hard to audit or explain decisions
- Overreliance — risks in trusting agents for high-stakes tasks
- Robotic or impersonal behavior — lacks emotional intelligence
- Bias and fairness issues — reflects and amplifies LLM training data

# Anatomy of AI agents

**Prompting (Instructions):** How you program the brain

- Defines the agent's role, tone, and behavior
- Includes goals, constraints, and examples

# Anatomy of AI agents

## **Brain — LLM (Large Language Model):**

Thinks, reasons, responds

- Handles natural language
- Makes decisions based on prompts
- Powers goal-directed behavior

# Anatomy of AI agents

## **Memory — Short-term & Long-term:**

Remembers what just happened, or what happened long ago

- Short-term: Keeps recent conversation context
- Long-term: Stores facts, goals, user preferences
- Powered by in-memory context or vector databases



# Anatomy of AI agents

**External Knowledge:** Gives context and depth (optional)

- Ingests PDFs, spreadsheets, databases
- Accesses internal documentation and FAQs
- Makes the agent domain-aware and informed

# Anatomy of AI agents

**Tools — External Capabilities:** Acts beyond just language

- Web search, file reading, math, API calls
- Gives the agent power to interact with the world
- Extensible and customizable



# 5 components of an AI agent

**Prompt**

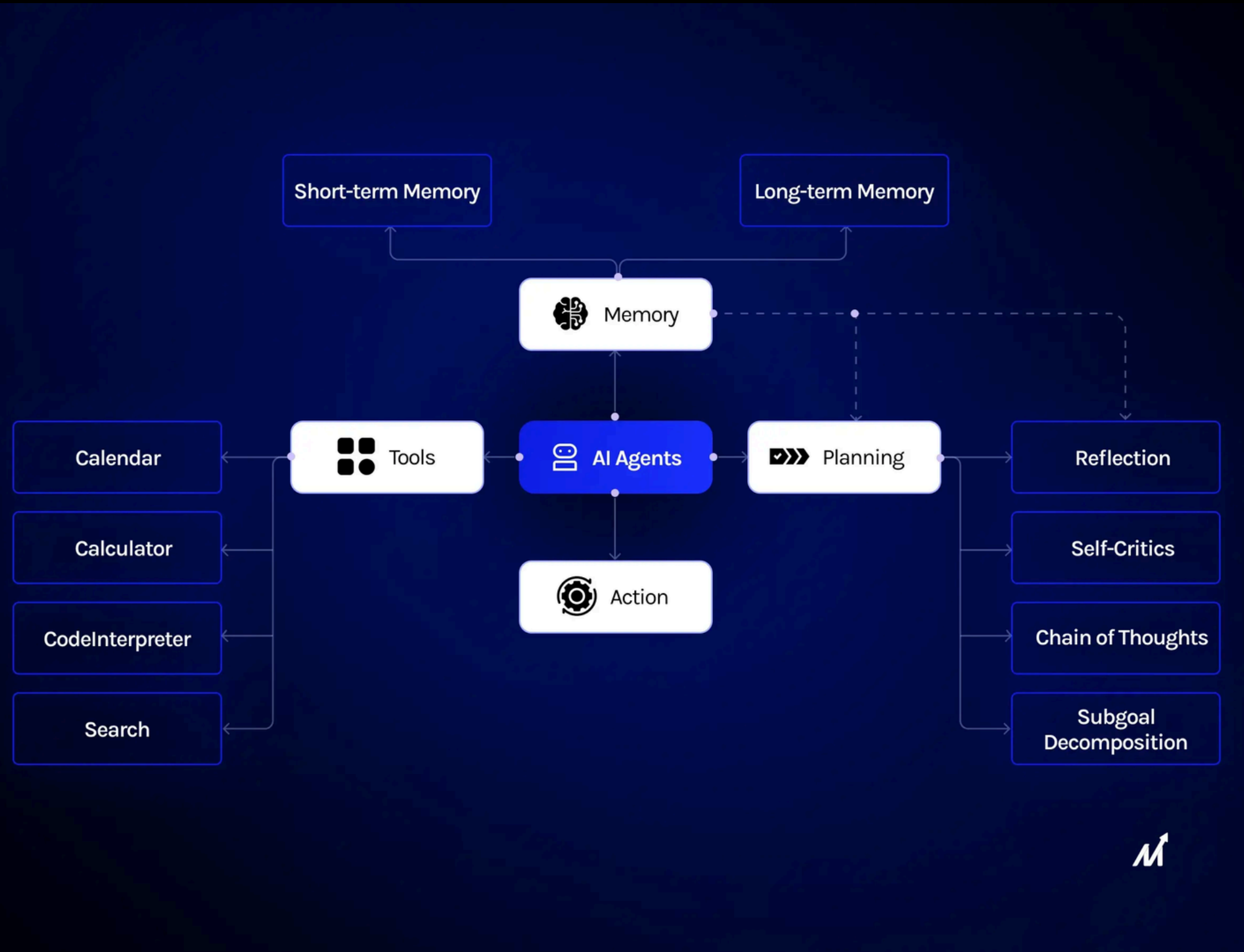
**Brain**

**Memory**

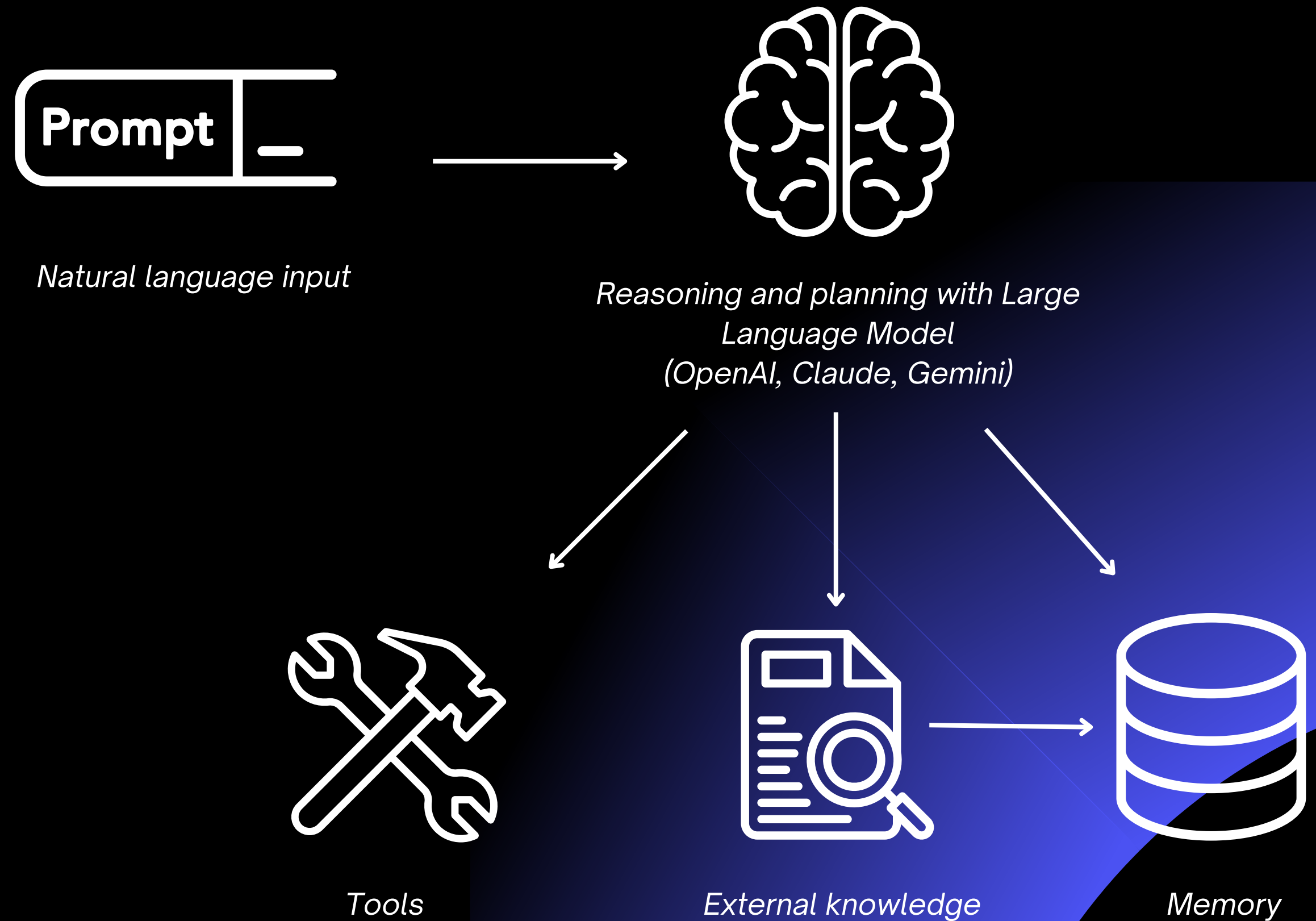
**External Knowledge**

**Tools**

# AI Agent Workflow



# AI Agent Workflow



# 2 types of AI agents

**Conversational Agents:** humans can interact directly

**Automated Agents:** humans don't always need human to interact and work with them. They just need info, working in the background

# What is an API — and Why It Matters for AI Agents?

*API = Application Programming Interface*

An API is how your agent talks to other software or systems — it's like giving your agent access to external tools, data, and actions.

# Why Agents Use APIs?

- *Search APIs – get real-time info from the web*
- *Database APIs – update or query internal systems*
- *Calendar APIs – create meetings, reminders*
- *Email/Chat APIs – send messages or notifications*
- *File APIs – read PDFs, spreadsheets, or upload reports*
- *Payment APIs – process orders or payments (with caution!)*
- *And many more*



# Example of API usage

*An AI agent that sends a daily report to your team uses:*

- *OpenAI API for writing*
- *Google Sheets API to pull data*
- *Gmail API to send the report*



# Popular APIs for Agents

Use Case	API Example
Web search	SerpAPI, Bing API
File management	Dropbox, Google Drive
Messaging	Slack API, Gmail API
Data storage	Notion API, Airtable
Automation	Zapier, Make, IFTTT

*APIs are how your agent reaches into the real or digital world and gets stuff done*

# How to learn AI agent fast and not forget it

## **The Wrong Approach**

- Binge-watch tutorials
- Read tons of docs
- Take notes...
- Then forget everything a week later

# How to learn AI agent fast and not forget it

ds3.ai

## The Right Way: Learn by Doing — With Purpose

### Step 1: Start with a specific goal

Learning without a goal = building without blueprints.

Ask yourself: “What real task can I automate or improve using an AI agent?”

Examples:

- “Build an AI agent that summarises meeting notes and emails them daily to yourself for review”
- “Create a personal assistant that organizes my to-do list”
- “Build a Slack/Teams messenger chatbot that answers internal FAQs using company documents”

The more personal and practical, the better. Your goal gives every line of code meaning.

# How to learn AI agent fast and not forget it

## The Right Way: Learn by Doing — With Purpose

### Step 2: Create a Smart Roadmap

- Don't learn randomly. Learn with direction.
- Do a quick plan:
  - What features will your agent need? (e.g., tools, memory, APIs)
  - What are the technical building blocks? (LLM, prompts, loops, actions)
  - Research what others have built (GitHub, Twitter, YouTube demos)

Use tools like NotebookLM, Notion, or even a spreadsheet to:

- Collect example prompts and agent architectures
- Stay organized with your learning path
- Track API, and AI framework skills you'll need — but only when they become relevant to your agent goal.

# How to learn AI agent fast and not forget it

## The Right Way: Learn by Doing — With Purpose

### Step 3: Build and track Your Progress

- Build something every day — no matter how small.
- Log your daily progress: what you built, what failed, what clicked
- Save useful prompts, links, and snippets
- Use a streak tracker, Kanban board, or checklist to stay motivated
- See your agent evolve over time: from one feature to many



# How to learn AI agent fast and not forget it

## The Right Way: Learn by Doing — With Purpose

### Step 4: Challenge Yourself, Every Day

- Real learning happens when you get stuck and get through it.
- Use ChatGPT or Claude to generate challenges: “Create a memory system for your agent”, “add a weather API integration”
- Test your agent on real tasks: “Can it answer this question correctly?”
- Don’t fear errors — each one rewires your brain

# How to learn AI agent fast and not forget it

## The Right Way: Learn by Doing — With Purpose

### Step 5: Reinforce the cycle of Learn → Practice → Apply → Review

- Don't just read — connect, create, and reflect.
- Take time to ask: “How does this new idea relate to what I already built?”
- Build a personal knowledge map of concepts (LLMs, tools, APIs, memory)
- Write a weekly review or blog post on your progress
- Teach others — or just explain your project to a friend



Build > Watch

Watching tutorials  $\neq$  building an agent

Start building now

Google & ChatGPT when stuck  
Ask better questions as you go.

# Thank You