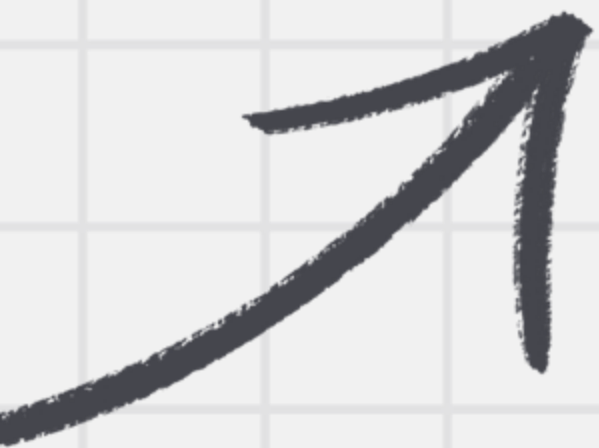


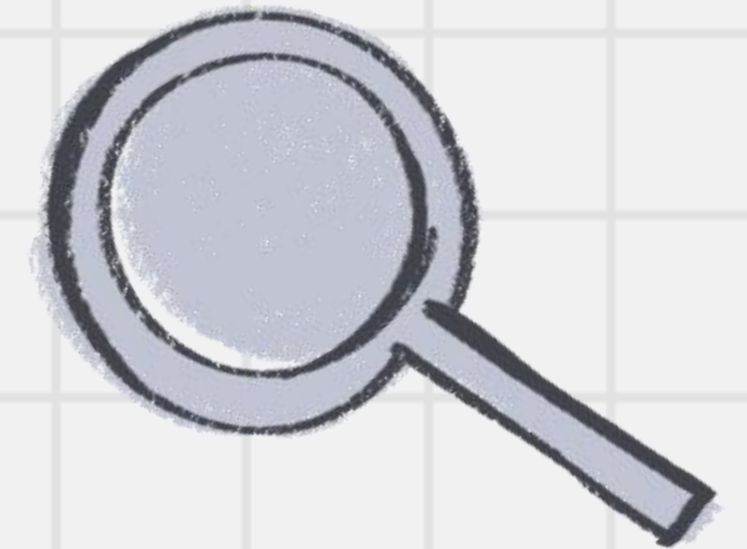


Group 1

R3 外部工具Tool



團隊成員



DS 吳曉瑛



CI 洪渝詠



DS 王旭龍

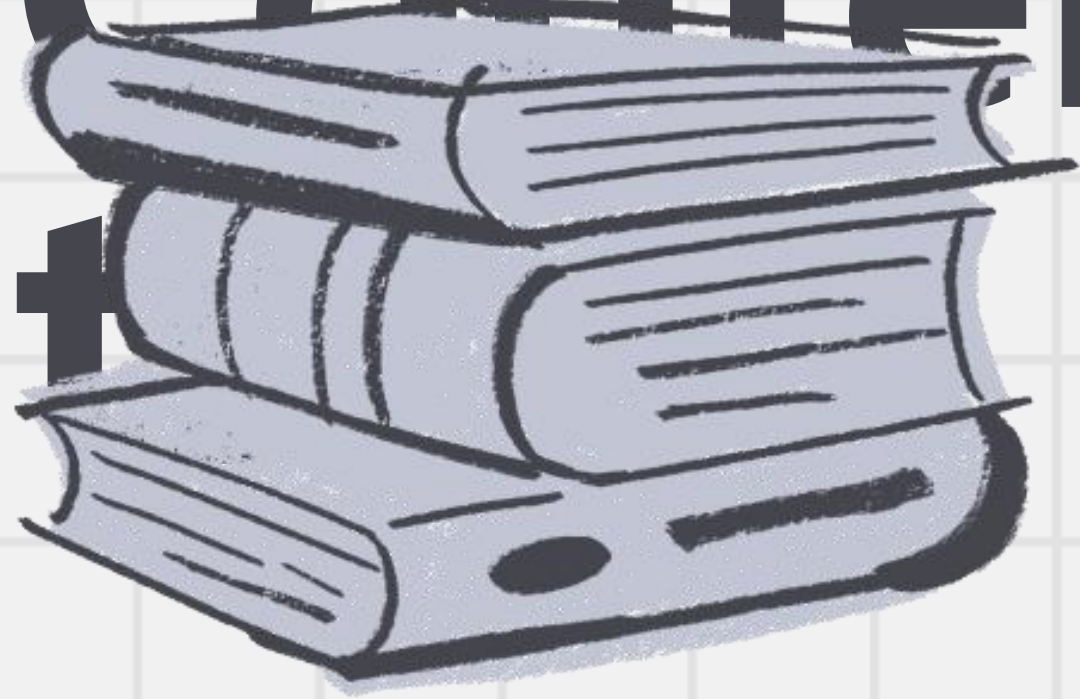


CT 謝博丞



CI 翁瑄佑

Table of Content



1

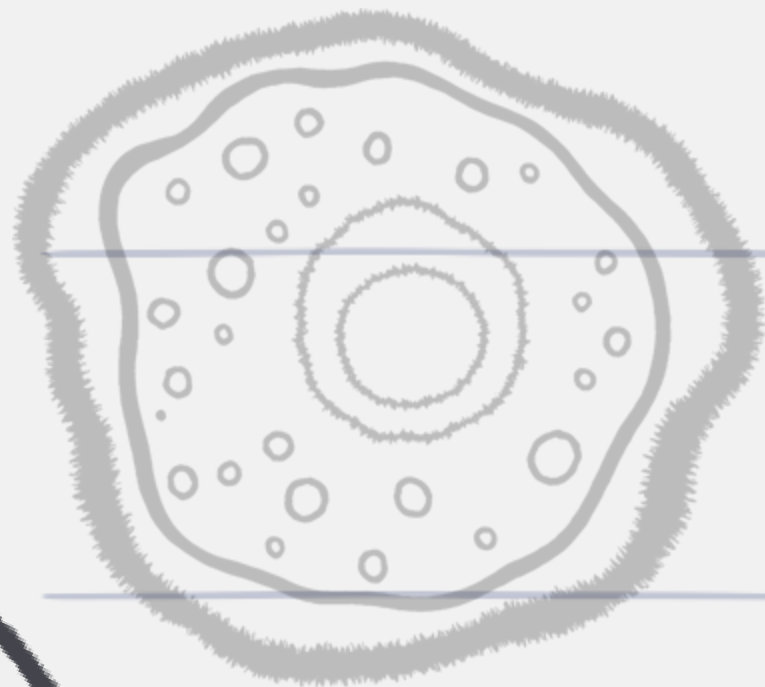
Tool & Function

2

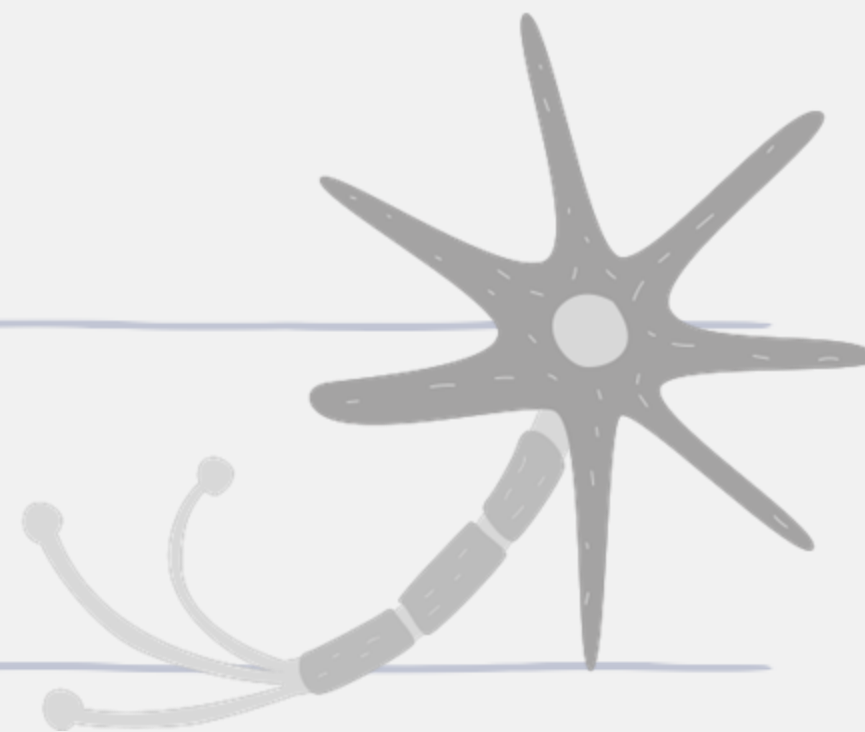
MCP概念與運作流程

3

MCP實作



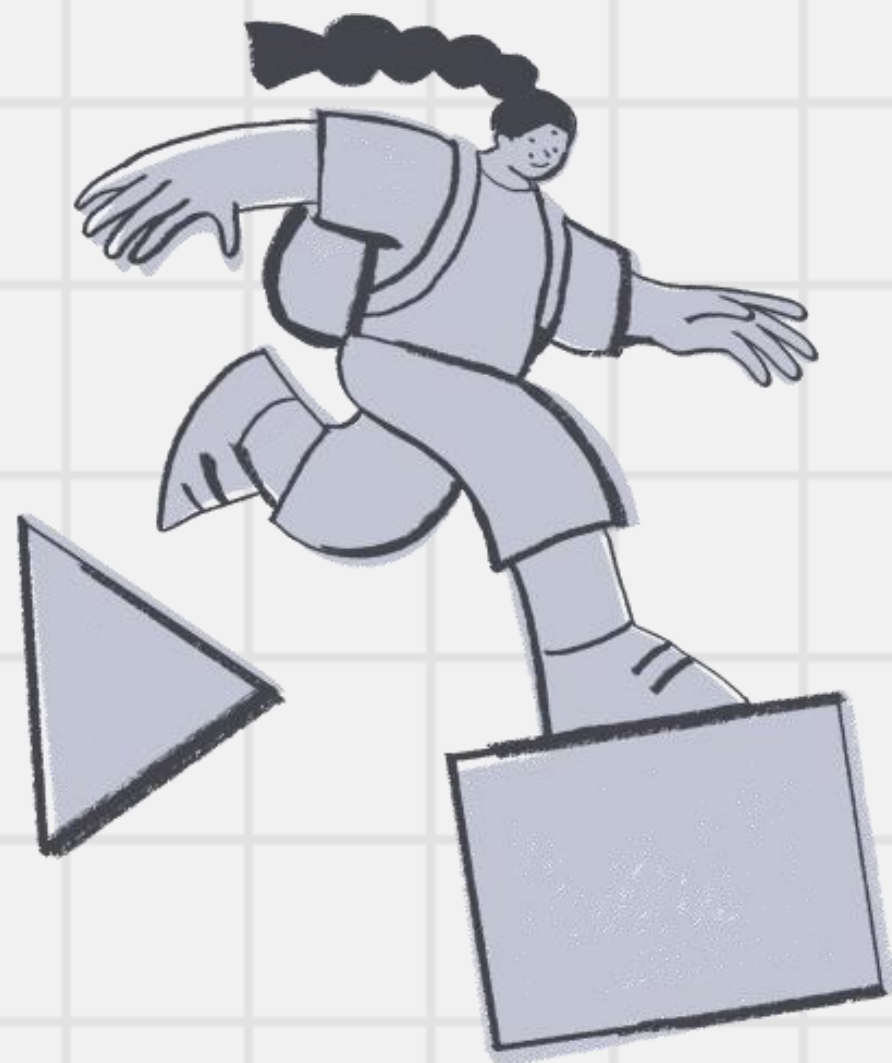
01



Tool & Function

AI 需要「Tools」走進現實世界

AI vs. Tools



AI 模型 (e.g., ChatGPT, LLM...) 會講話、懂道理，是一位很聰明的顧問

會講話



上網查資料

e.g., 叫 Uber、查詢天氣

告訴電腦「怎麼做某事」

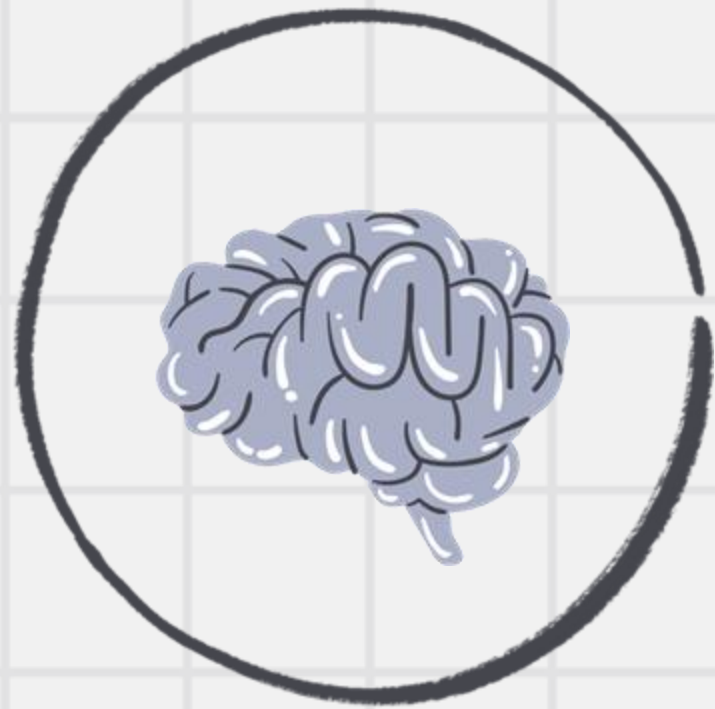
e.g., 預約餐廳、啟動智能家電

提供最新參考資訊

e.g., 公司內部手冊回答問題

會做事

LLM->AI Agent



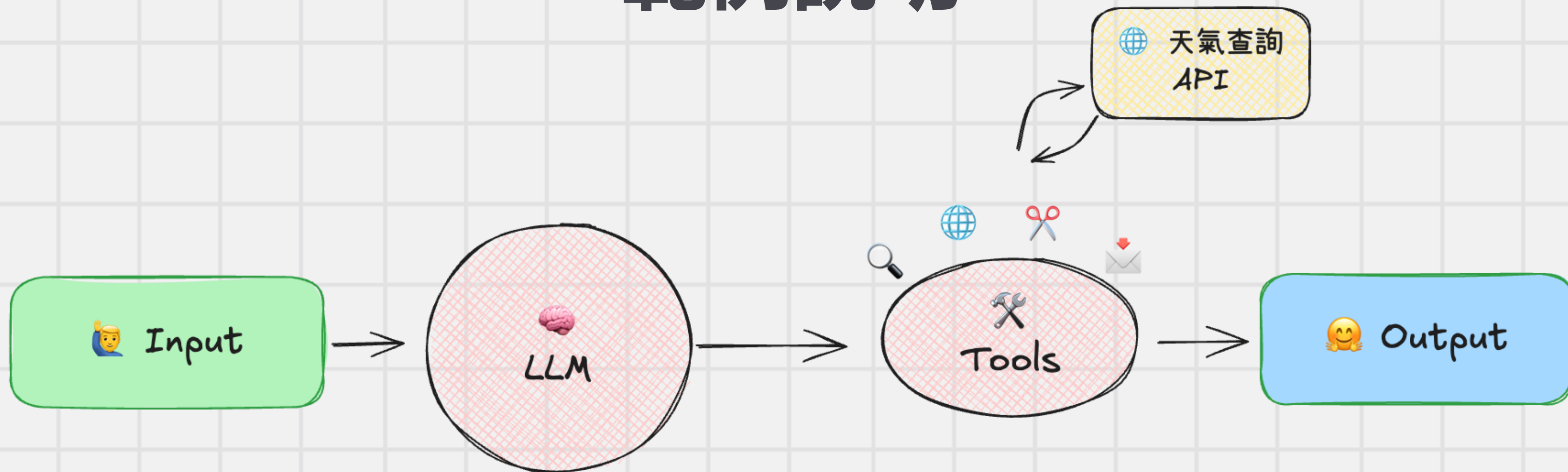
小房間的天才



缺乏即時資訊

讓 LLM 透過工具，由外部系統協助執行，與**真實世界產生連結**

範例說明



Q: 我想知道現在
「台北」的天氣如何

思考與執行

可以用工具來查詢現在的天氣，
`get_current_weather(place)`

`get_current_weather(台北)`
得知台北現在的天氣

思考與執行

我無法與真實世界互動，但我可以
透過工具查詢結果

`get_current_weather(台北)`
= 雨天

思考與執行

透過工具與參數設定，得到結果

A: 台北現在的天氣為雨天

思考與執行

將結果由外部系統輸出

工具的最佳實踐

名稱、參數、指令明確

功能要直觀、避免無效呼叫

最小意外原則

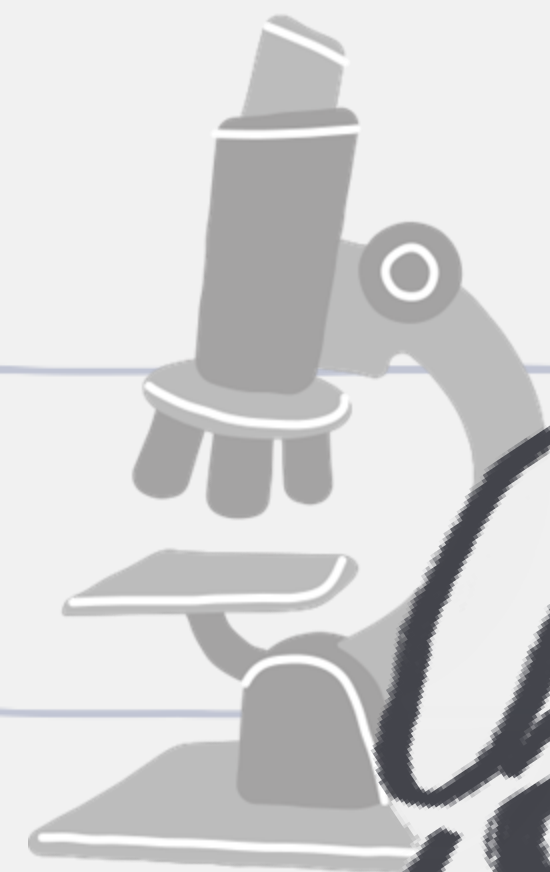


各函數相同參數不要重複設定

避免過多函數(<20)



02



MCP概念與運作流程

統一LLM與外部世界的接口/協定， 就像TYPE C，隨插即用



✓ 快速擴展

- MCP 採用統一的 metadata 與 API 格式
- AI 系統可以像模組化支援多元業務場景。

✓ 任務共享

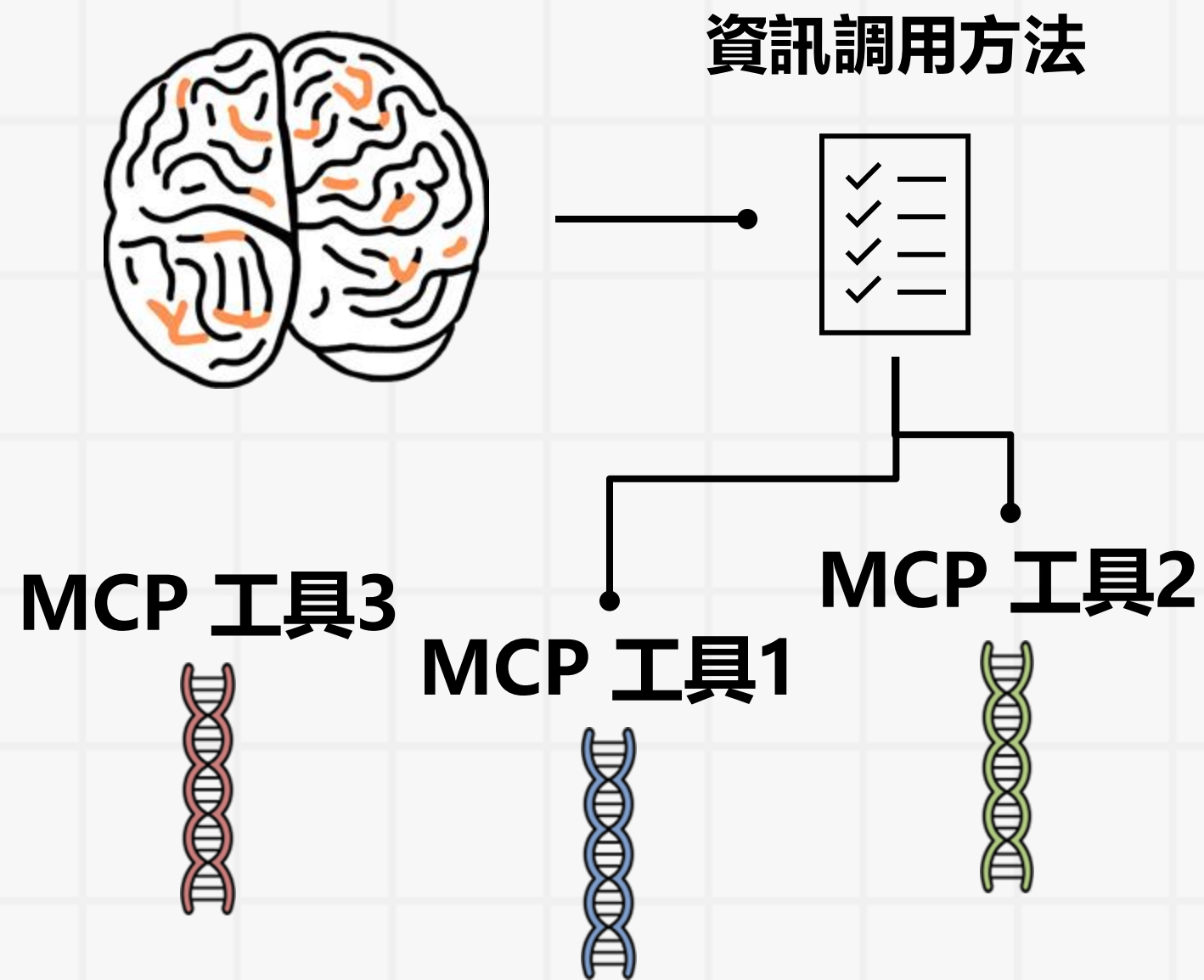
- MCP 支援模型與模型之間**共享上下文與任務歷程**，讓多個 Agent 能在同一語意框架下協作完成複雜任務。
- 提升處理效率，邁向智慧決策與多步推理。

✓ 彈性調用

- 透過**標準化的 context 與能力描述 (capabilities)**，主模型能根據任務內容動態選擇最適合的 Agent 執行。
- 不論是分析、預測、翻譯還是查詢工具，皆能用相同邏輯調用，實現極高的適應彈性與可組合性。

大腦+基因 = 大腦佈達需求給各基因發揮

主控LLM (AI app)



功能要有metadata描述檔：明確宣告各功能的能力、輸入格式、API 路徑等資訊

Step 1 初始化 🔍 使用者發問透過 LLM Desktop 輸入：
「請分析這份財報並翻譯為繁體中文」

Step 2 🧠 模型判斷此任務需要特定 MCP 工具
(財報分析 → 翻譯)

Step 3 📢 廣播 context 與任務描述給註冊中的 MCP 功能

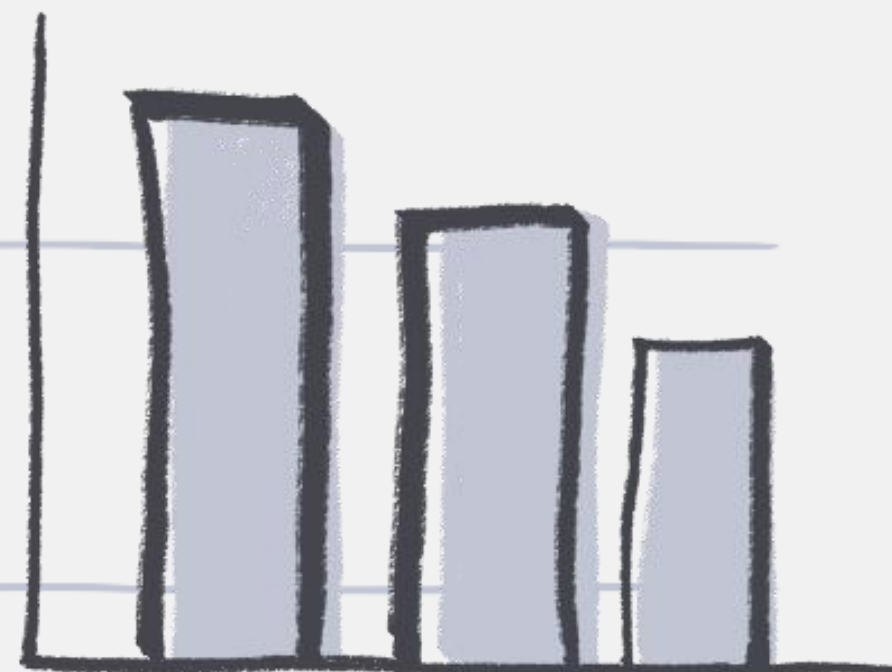
Step 4 🤖 各功能自主回應，財經功能回應：
「我能處理財報分析」→ 提供摘要結果

Step 5 🔄 功能協作，LLM將摘要傳給翻譯功能，翻譯為繁中

Step 6 📧 回傳整合結果LLM將所有步驟整合，產生回應：
「以下是繁體中文財報摘要...」 返回使用者



03



MCP實作



A hand-drawn sign on a grid background. The sign is a rectangle with a thick black border and a smaller inner rectangle. The text "THANK YOU" is written in a bold, black, hand-drawn font. "THANK" is on the top line and "YOU" is on the bottom line. A light blue oval highlights the word "THANK", and a light blue horizontal brushstroke is under the word "YOU".

THANK
YOU