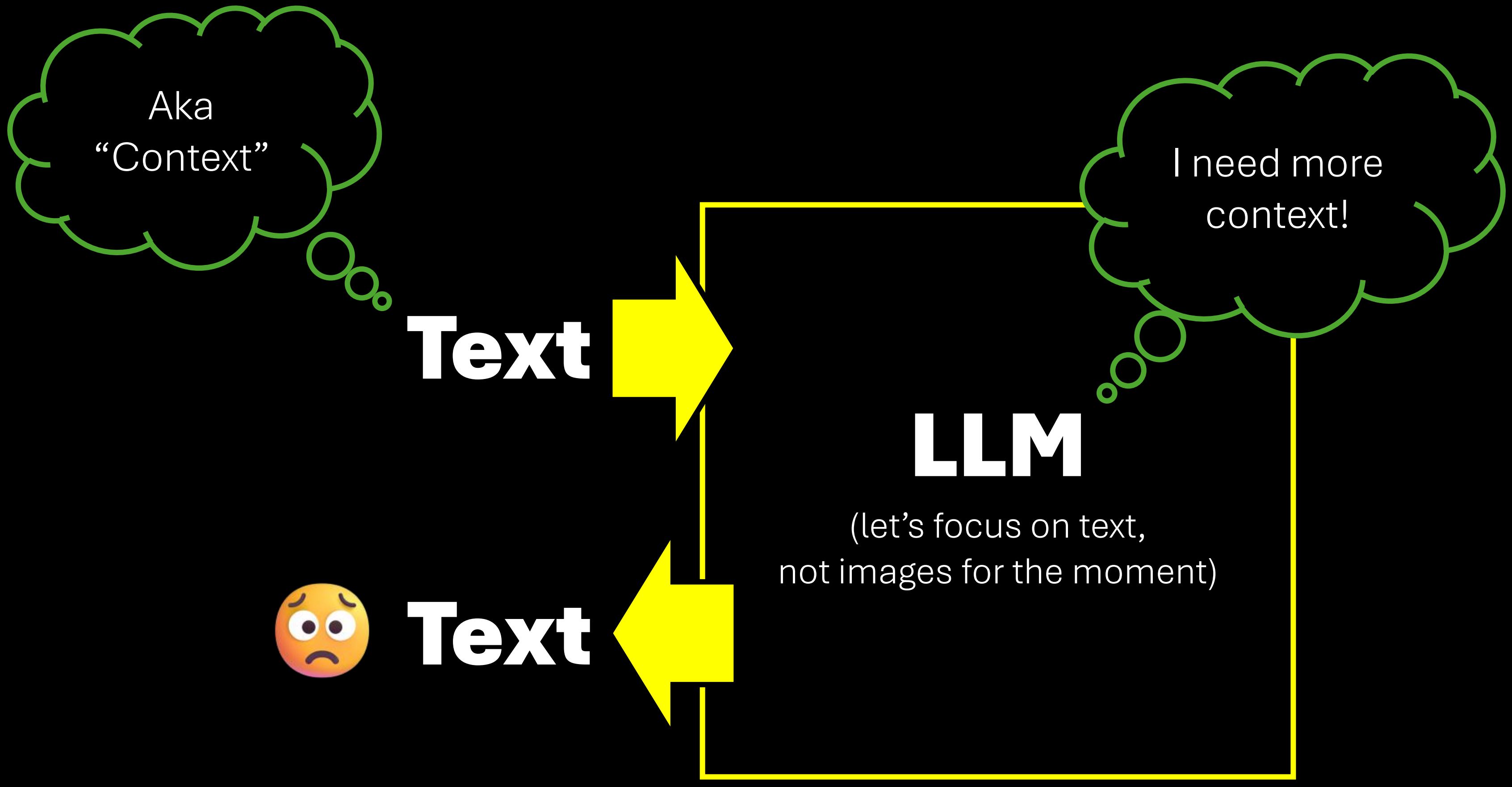


Aka
“Context”

Text

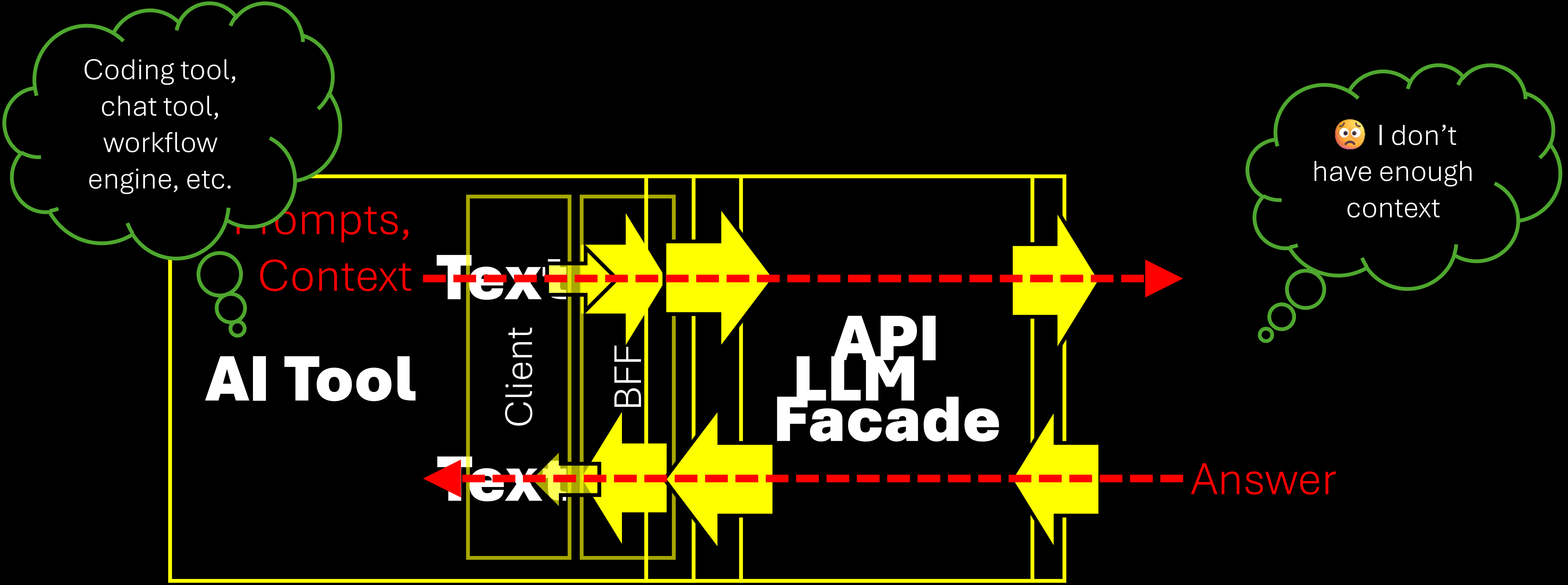
I need more
context!

LLM

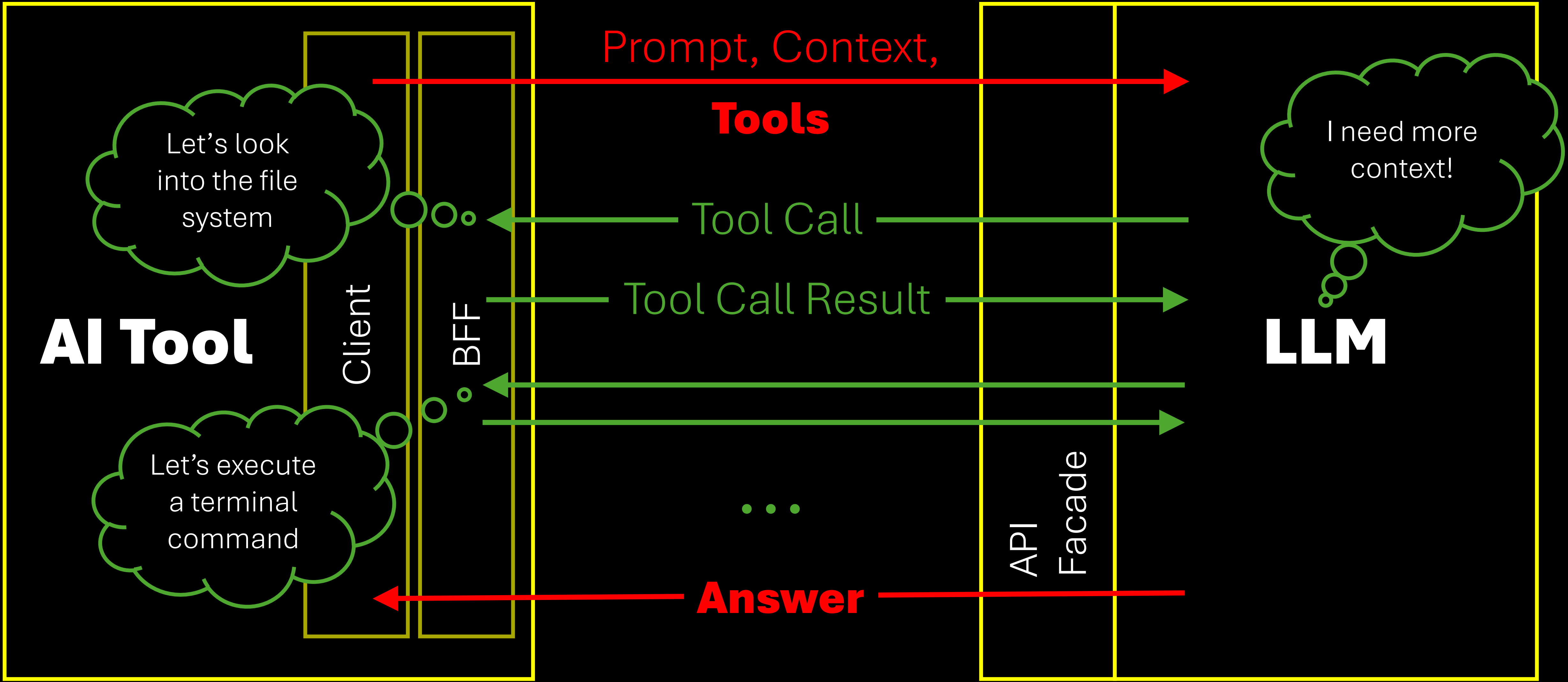
(let’s focus on text,
not images for the moment)

🥺 Text

🚫 **Files, Web, Terminal, IDE, etc.**


Coding tool,
chat tool,
workflow
engine, etc.
Prompts,
Context
Text
AI Tool
Client
BFF
API
LLM
Facade
Text
Answer
😟 I don't
have enough
context

🪄 Enter: Tools



AI Tool

Client

BFF

Let's look into the file system

Let's execute a terminal command

Prompt, Context,

Tools

Tool Call

Tool Call Result

. . .

Answer

API Facade

LLM

I need more context!

There are so many AI software products

For developers, for power users, for end users

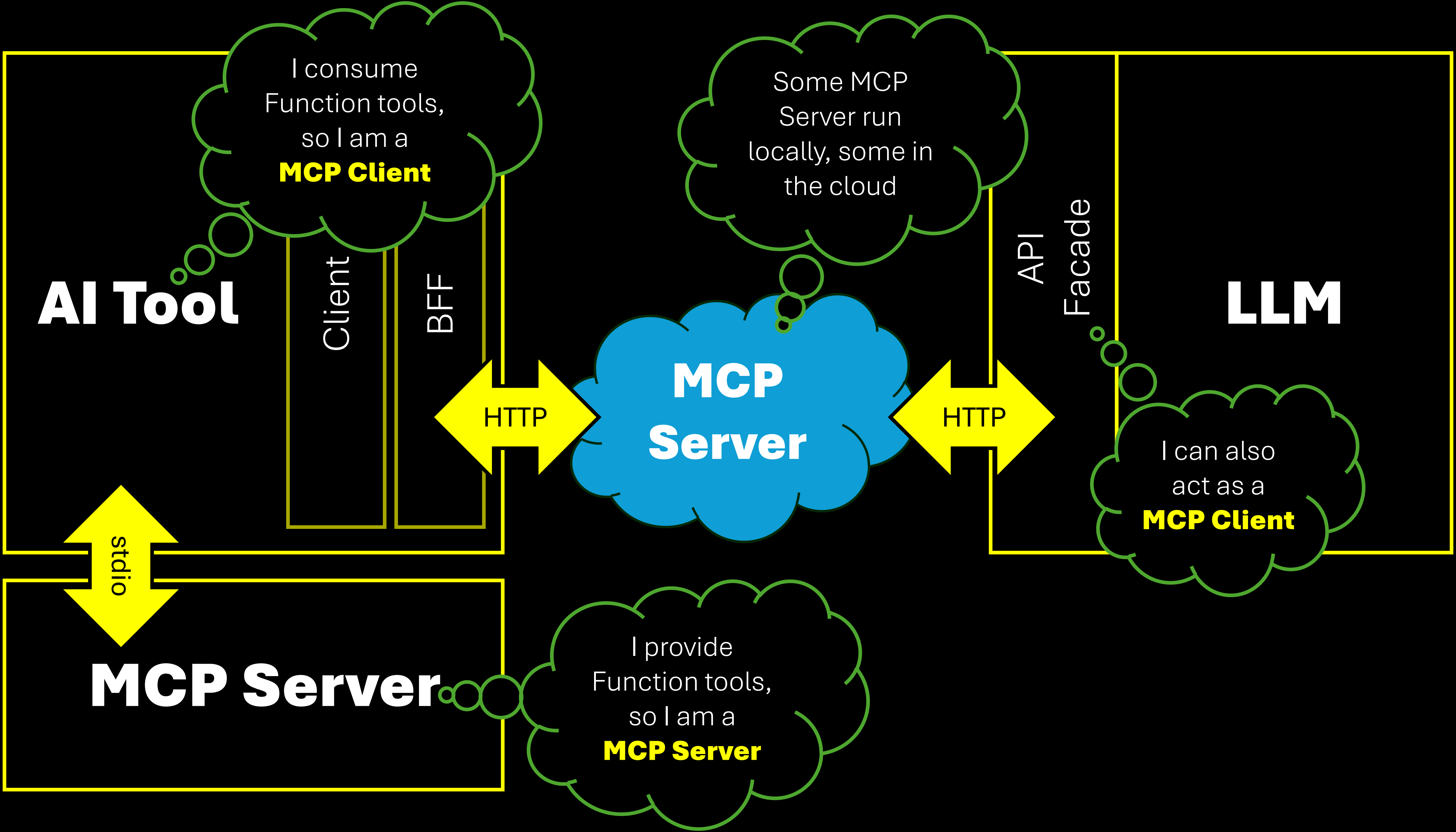
Many *Function Tools* would be useful for all of them

AI tool-specific SDKs would be frustrating

We need a standard!

Enter: **Model Context Protocol**

A standardized protocol to provide Function Tools *to AI software*



AI Tool

I consume Function tools, so I am a **MCP Client**

Client

BFF

HTTP

MCP Server

Some MCP Server run locally, some in the cloud

HTTP

API Facade

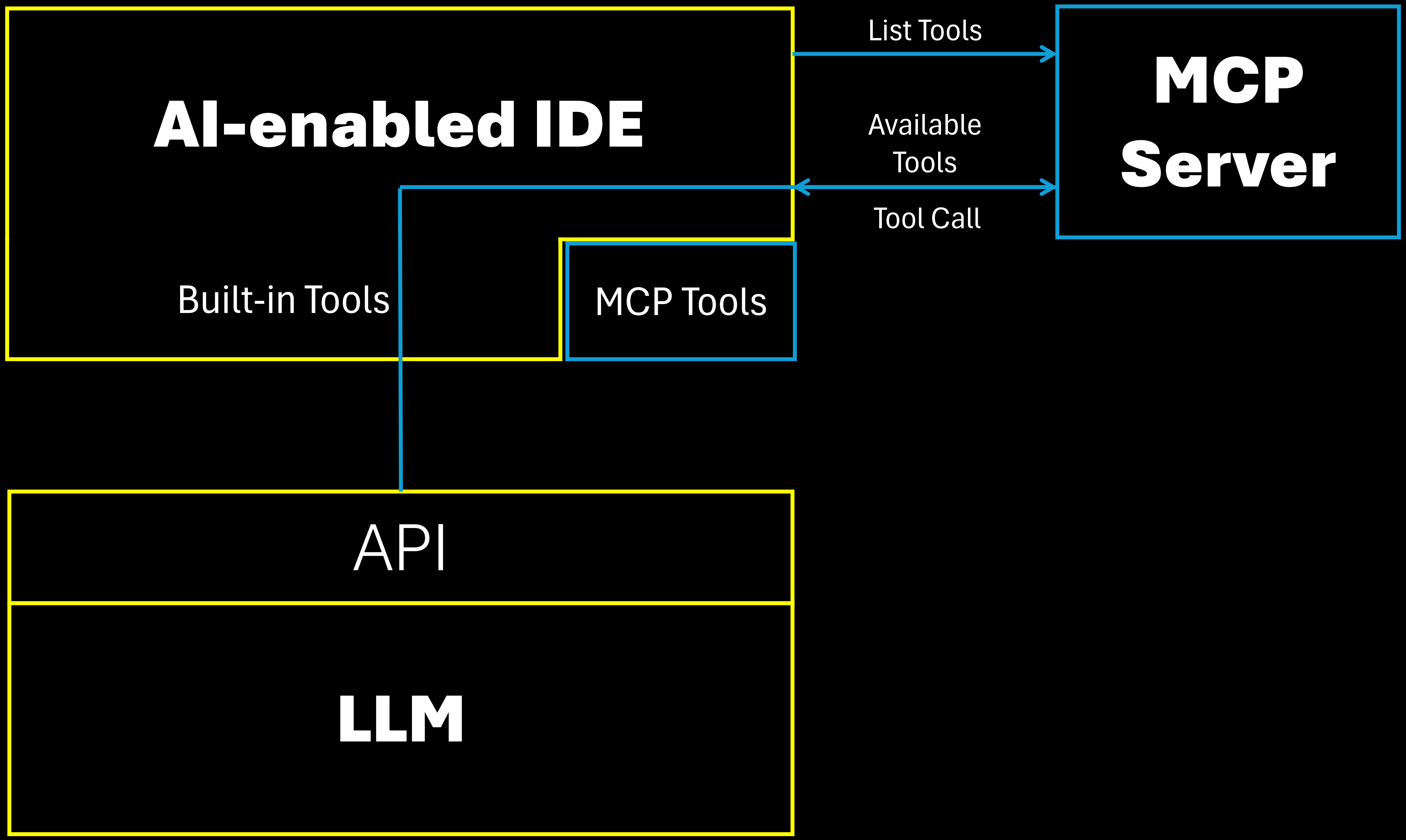
LLM

I can also act as a **MCP Client**

stdio

MCP Server

I provide Function tools, so I am a **MCP Server**

AI-enabled IDE
Built-in Tools
MCP Tools
List Tools
Available Tools
Tool Call
MCP Server
API
LLM

MCP is More Than Just Tools

Resources

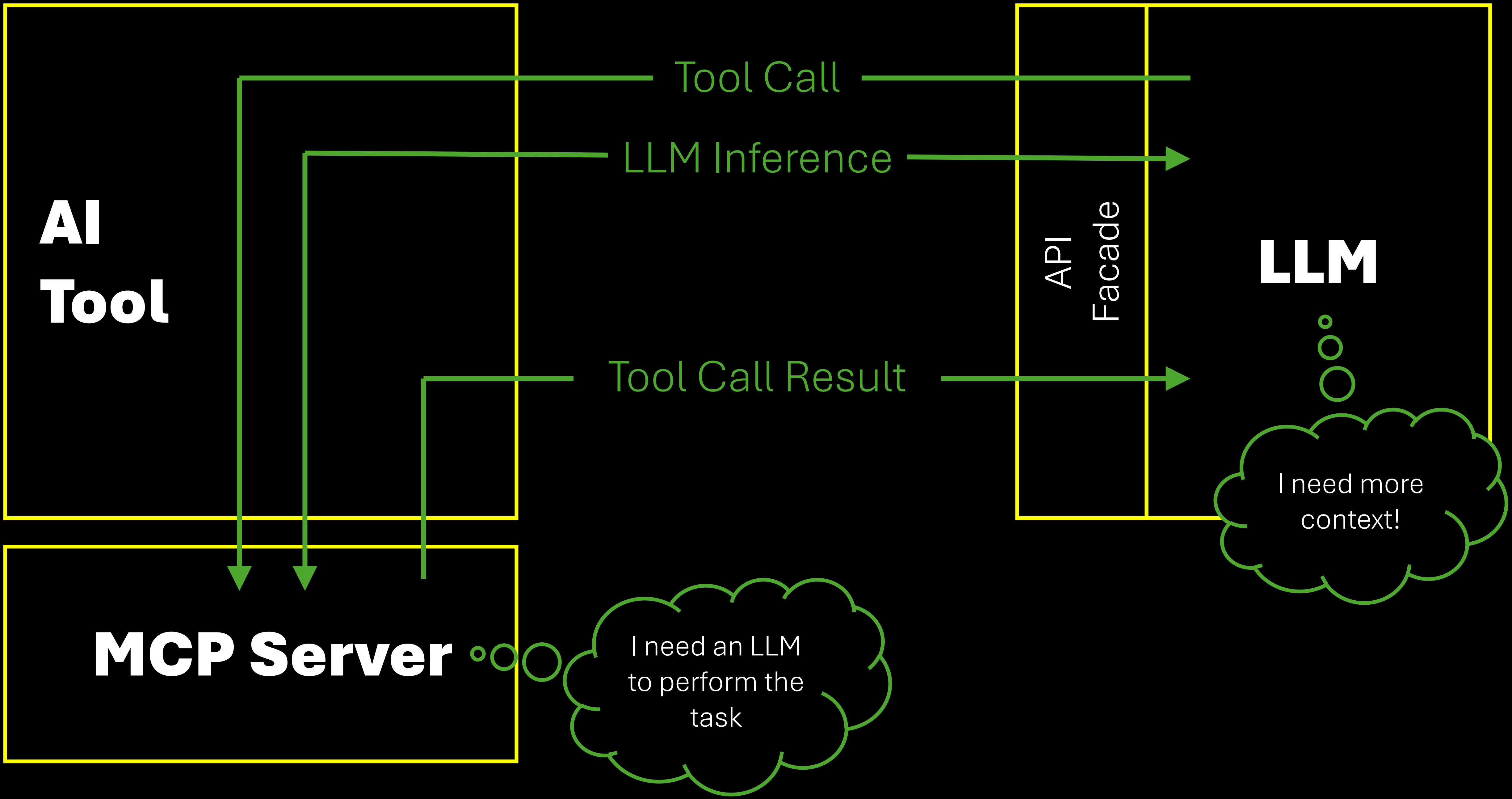
Retrieve resources like files, database content; like read operations in a REST API

Prompts

Structured prompt template for common tasks

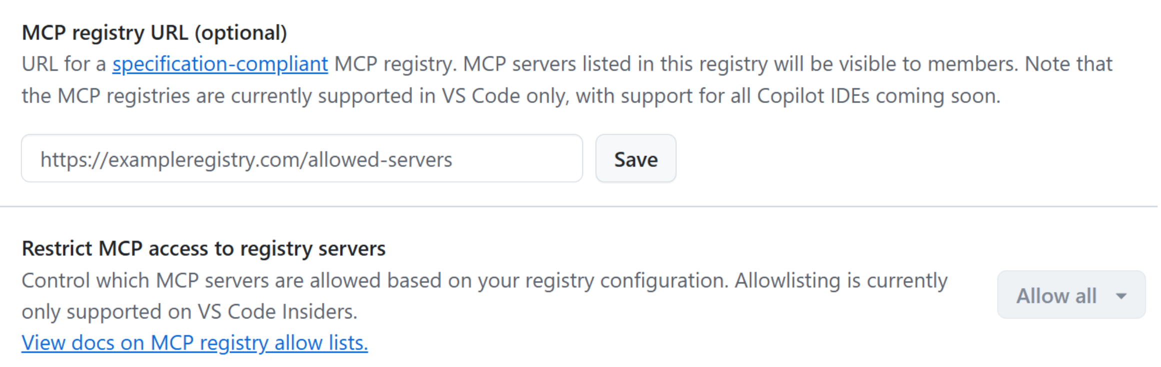
Sampling

MCP can access LLM through the MCP Client


AI Tool
Tool Call
LLM Inference
Tool Call Result
API Facade
LLM
I need more context!
MCP Server
I need an LLM to perform the task

Any Problems?

- Bleading edge 🩸
  - *Not a stable standard yet*
  - *SDKs are under heavy development*
- MCP Server must be trusted
  - *We give them access tokens to act on our behalf* 🔐
  - *Some even run locally* 😱
- Function Tool results are in the conversation history
  - *Processed and potentially stored by LLM providers*
  - *Fill up the context window* 💵



MCP registry URL (optional)

URL for a specification-compliant MCP registry. MCP servers listed in this registry will be visible to members. Note that the MCP registries are currently supported in VS Code only, with support for all Copilot IDEs coming soon.

https://exampleregistry.com/allowed-servers

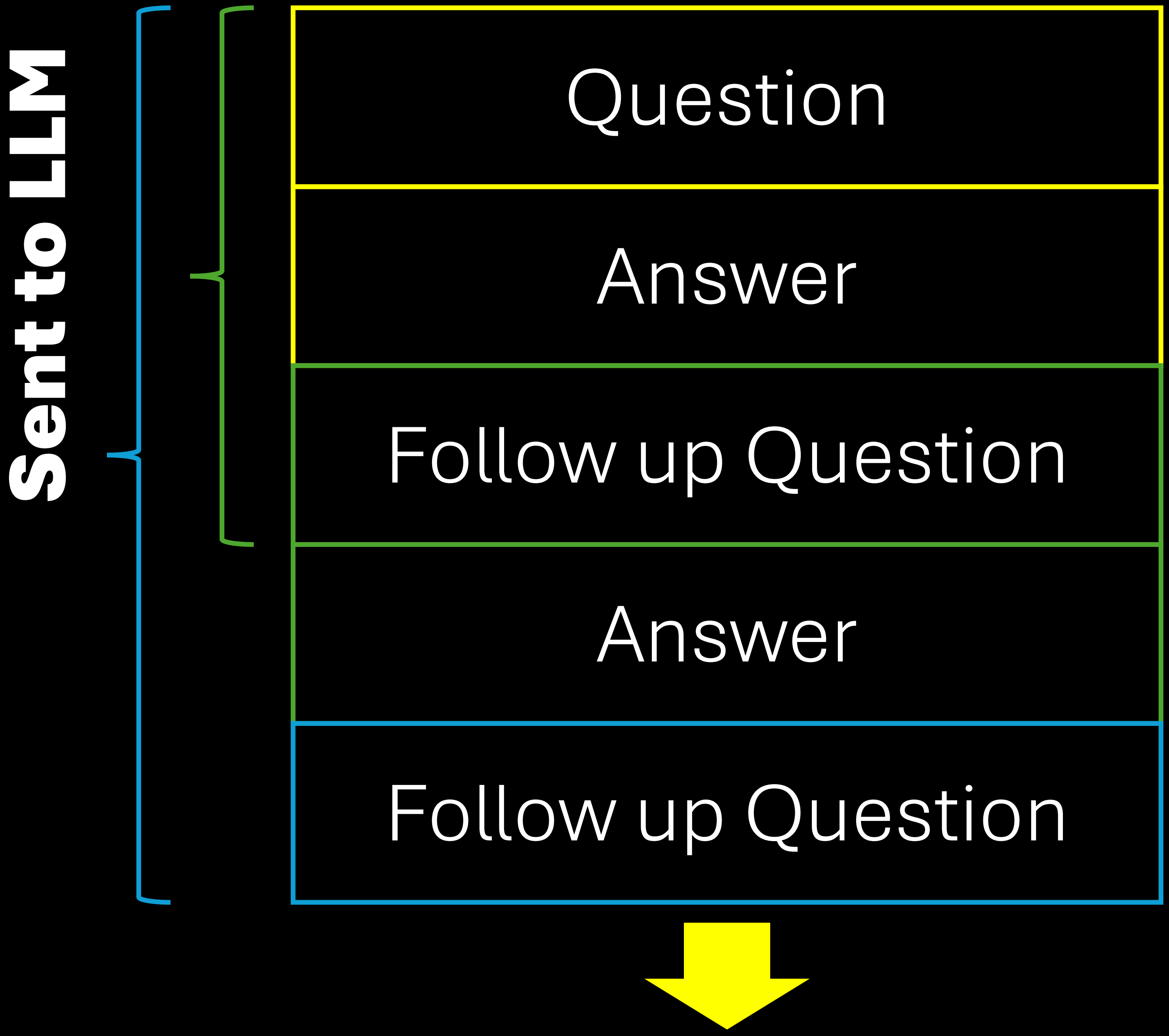
Restrict MCP access to registry servers

Control which MCP servers are allowed based on your registry configuration. Allowlisting is currently only supported on VS Code Insiders.

View docs on MCP registry allow lists.

Allow all

https://github.com/modelcontextprotocol/registry



Sent to LLM

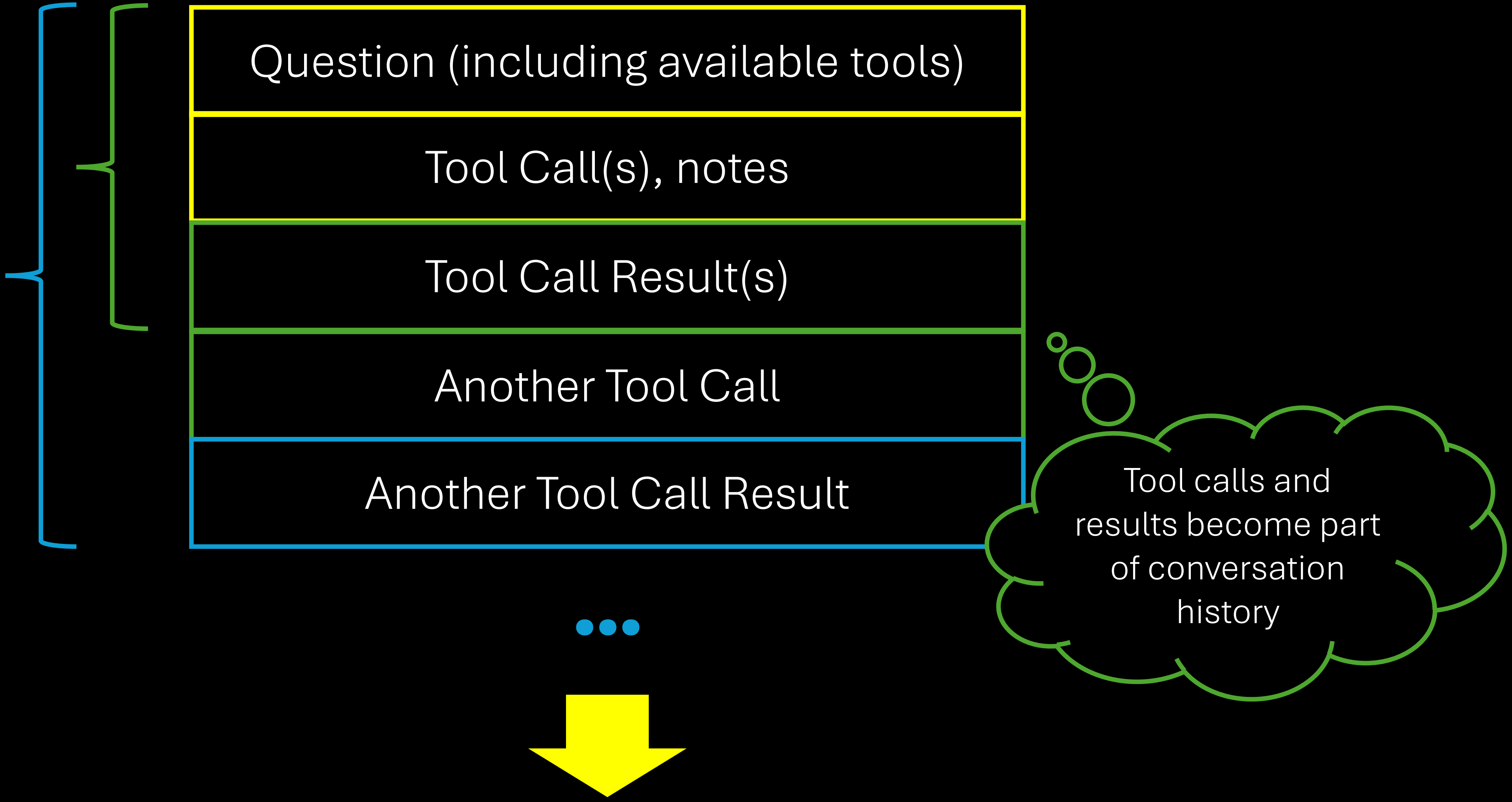
Question

Answer

Follow up Question

Answer

Follow up Question



Question (including available tools)

Tool Call(s), notes

Tool Call Result(s)

Another Tool Call

Another Tool Call Result

Tool calls and results become part of conversation history

Any Problems?

Bleading edge 🩸

Not a stable standard yet

SDKs are under heavy development

MCP Server must be trusted

We give them access tokens to act on our behalf 🔐

Some even run locally 😱

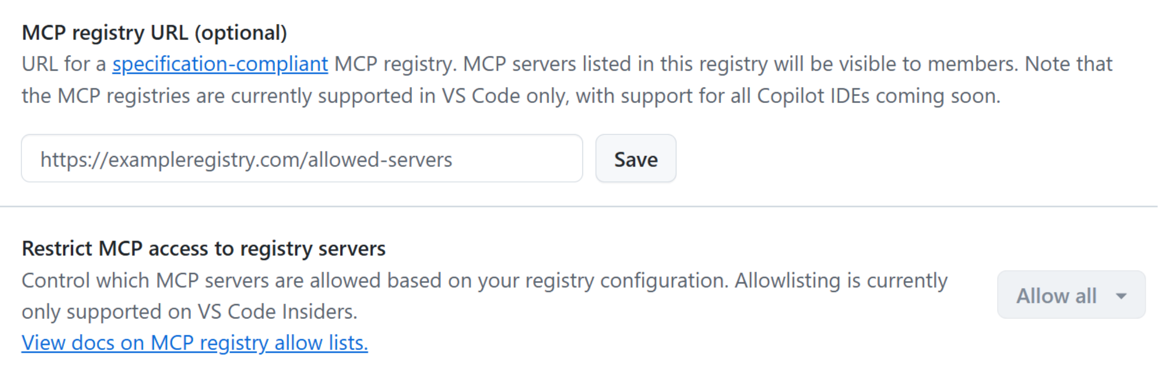
Function Tool results are in the conversation history

Processed and potentially stored by LLM providers

Fill up the context window 💵

Authentication is difficult

OAuth2 is required, DCR is recommended



MCP registry URL (optional)

URL for a specification-compliant MCP registry. MCP servers listed in this registry will be visible to members. Note that the MCP registries are currently supported in VS Code only, with support for all Copilot IDEs coming soon.

https://exampleregistry.com/allowed-servers

Restrict MCP access to registry servers

Control which MCP servers are allowed based on your registry configuration. Allowlisting is currently only supported on VS Code Insiders.

View docs on MCP registry allow lists.

https://github.com/modelcontextprotocol/registry

🪄 LLMs are amazing when it comes to *Tool Calling*

They combine independent tools to achieve a goal

⚒️ Today: Primarily useful for devs and power users

Most leading MCP Servers deal with dev-related stuff

✨ In the future? MCP Servers for everything?

No UIs anymore, no Web APIs?

🔮 Probably not for everything, but for many things

Custom UIs and APIs for special cases