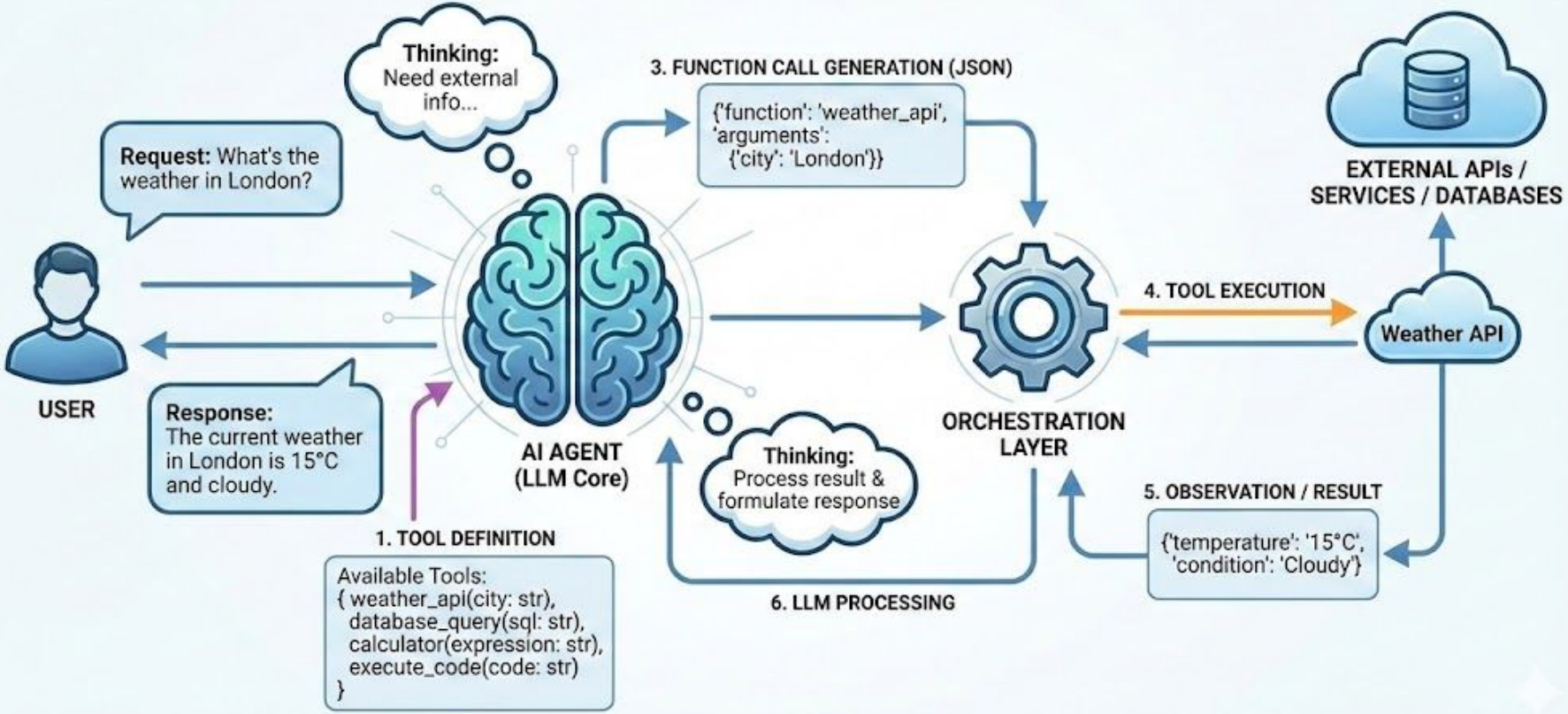
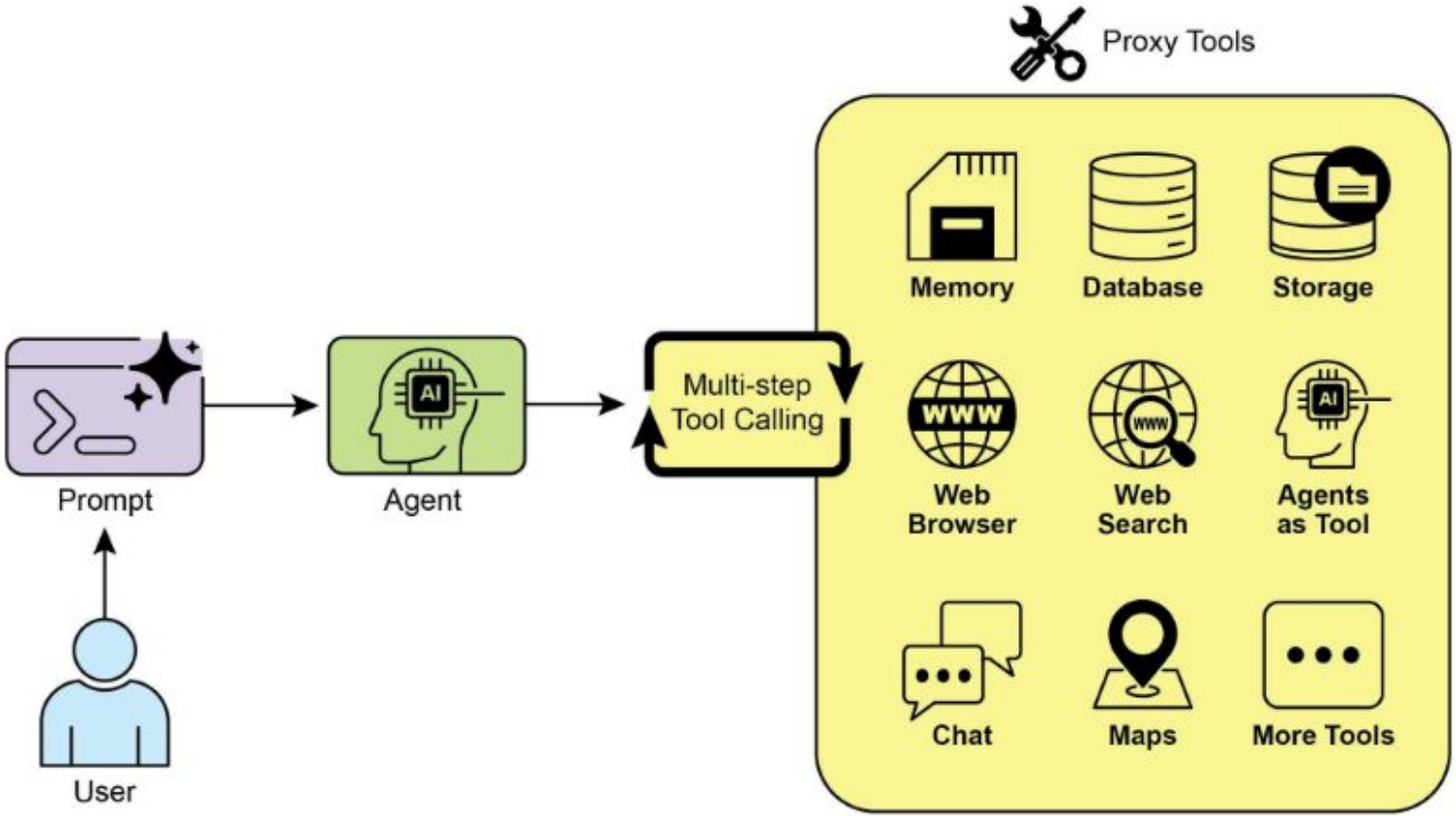
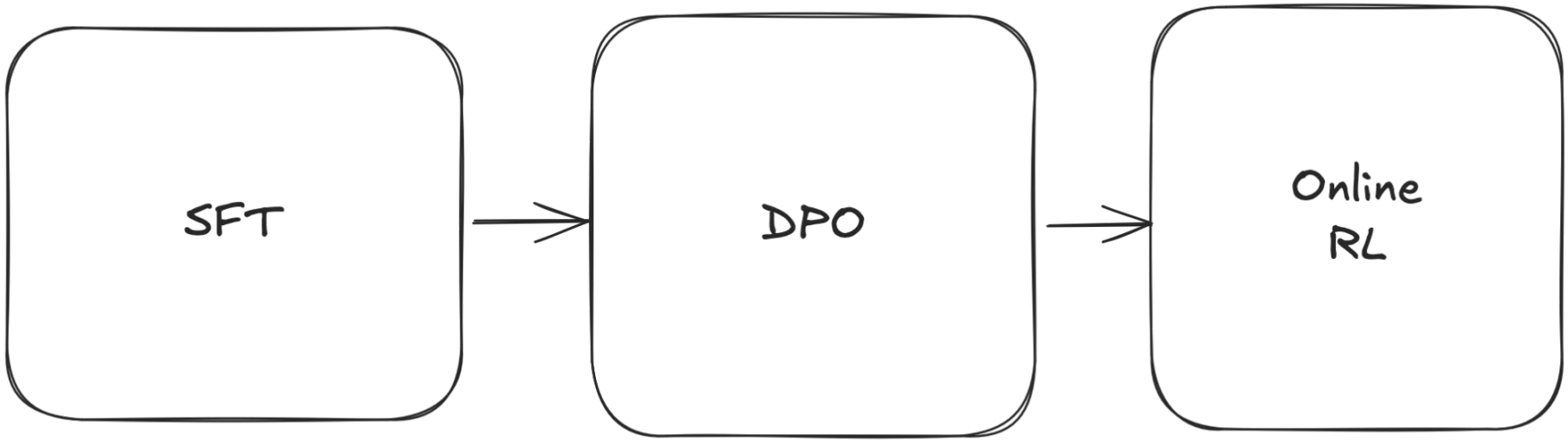
Tool Use, Planning, Multi-Agent

made with ❤️ for “Little ML book club”

Tool Use (Function Calling) Pattern



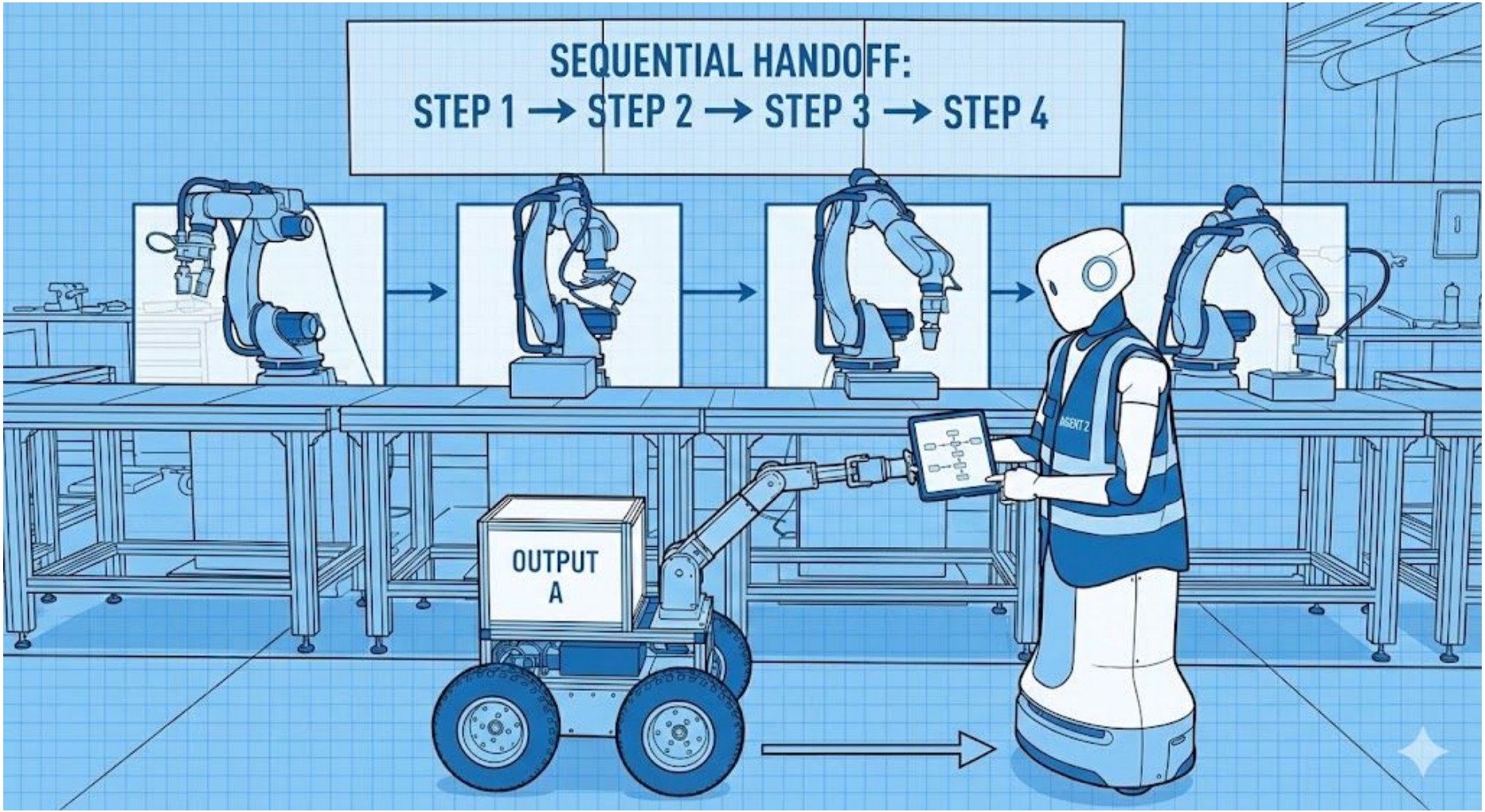

Proxy Tools
Memory
Database
Storage
Multi-step
Tool Calling
Web
Browser
Web
Search
Agents
as Tool
Prompt
Agent
Chat
Maps
More Tools
User



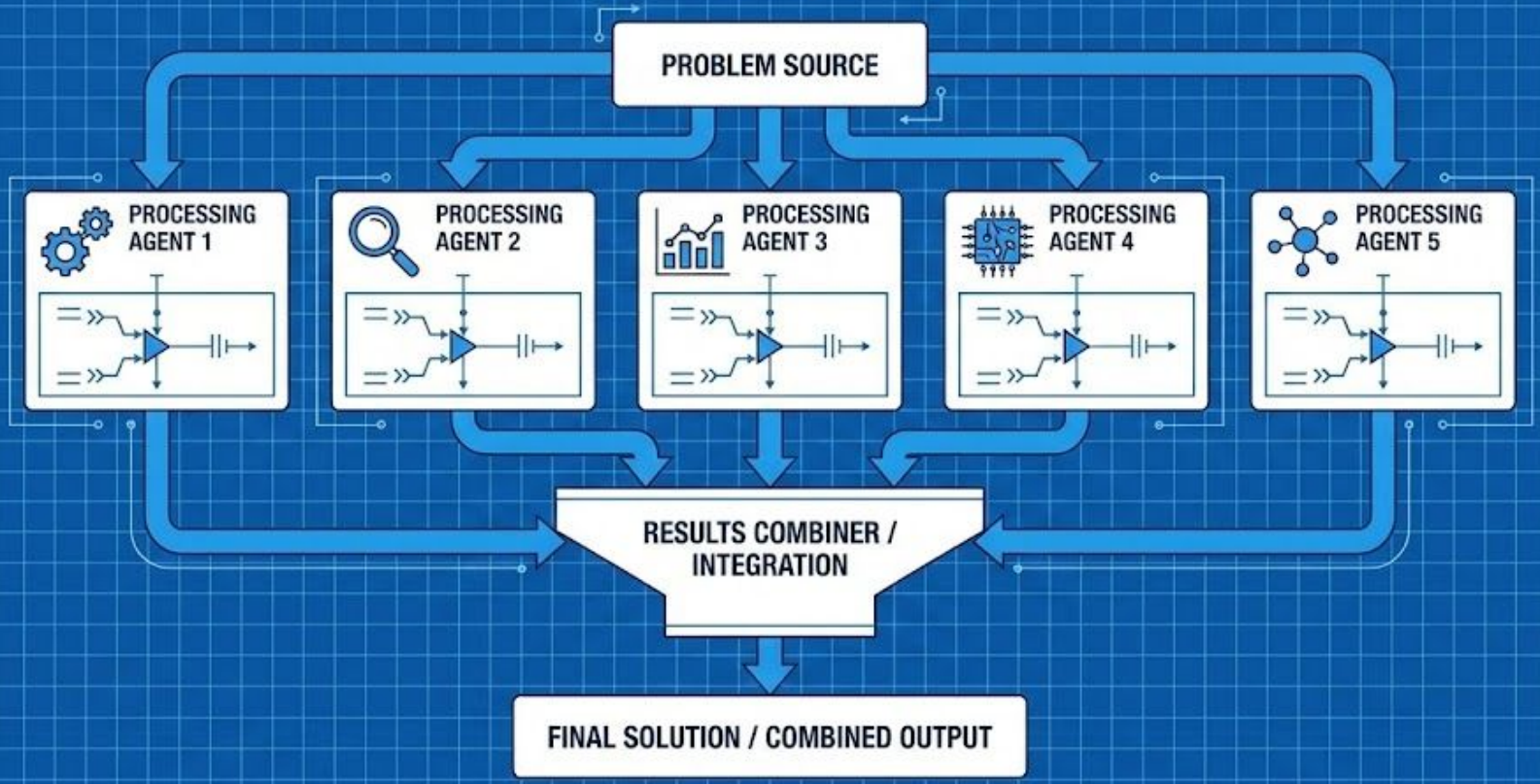
<tool_call>, <tool_result>, </tool_call>

1. **Role + Context** — ground the model
2. **Explicit plan-first instruction** — force the plan before execution
3. **Constraints on the plan format** — so it's actually useful to you

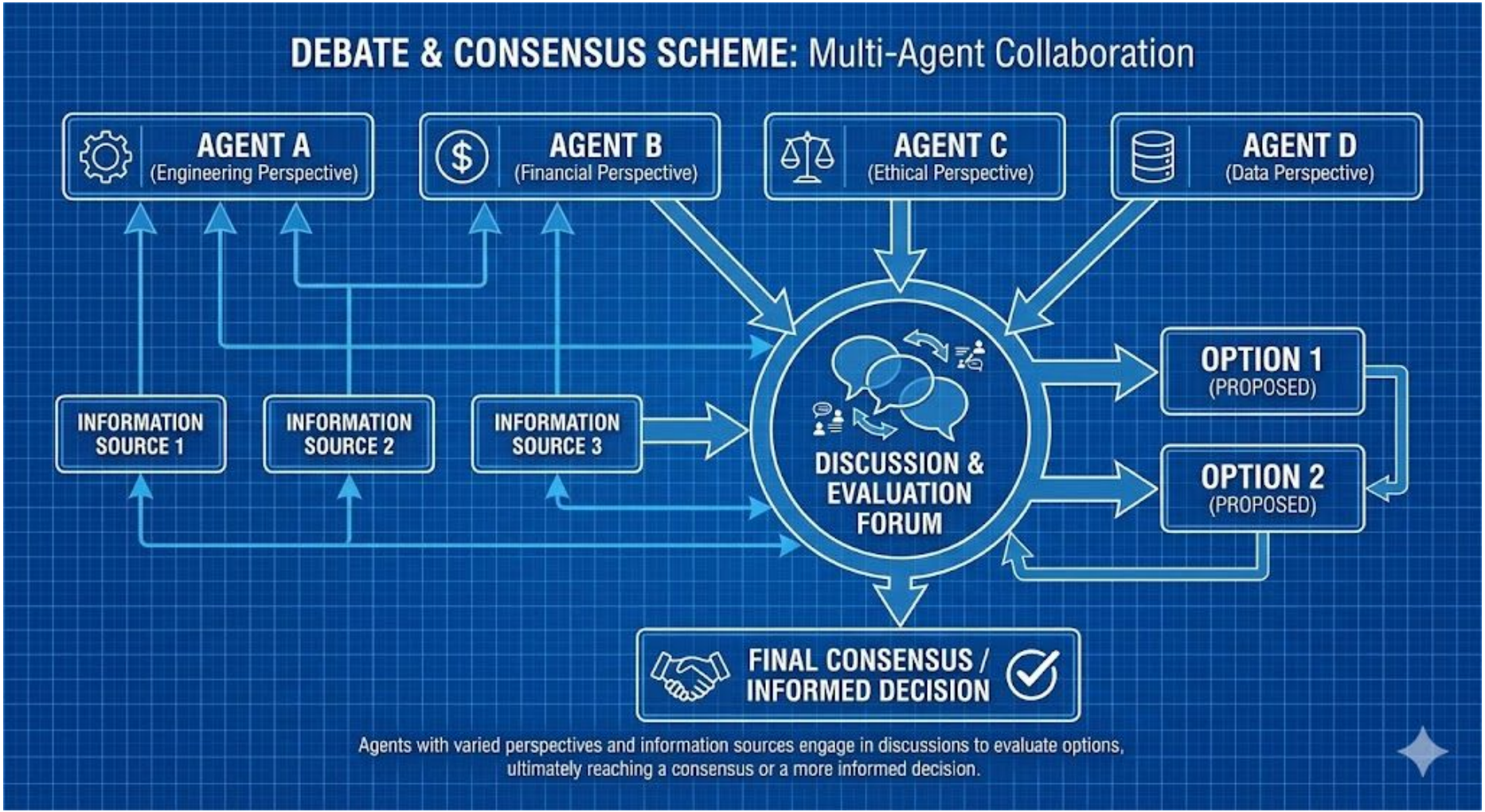
```
You are a senior technical architect. Before writing any code or prose,
you MUST first output a structured plan with the following format:

## Plan
1. **Goal**: Restate the objective in one sentence.
2. **Assumptions**: List anything you're assuming about the environment,
   audience, or constraints.
3. **Steps**: A numbered list of discrete actions you'll take, each with:
   - What you'll produce
   - Why this step is necessary
   - Dependencies on prior steps
4. **Risks**: Anything that could go wrong or where you're uncertain.
5. **Success Criteria**: How we'll know the output is correct.

Wait for my approval of the plan before proceeding to execution.
```


SEQUENTIAL HANDOFF:
STEP 1 → STEP 2 → STEP 3 → STEP 4
OUTPUT
A

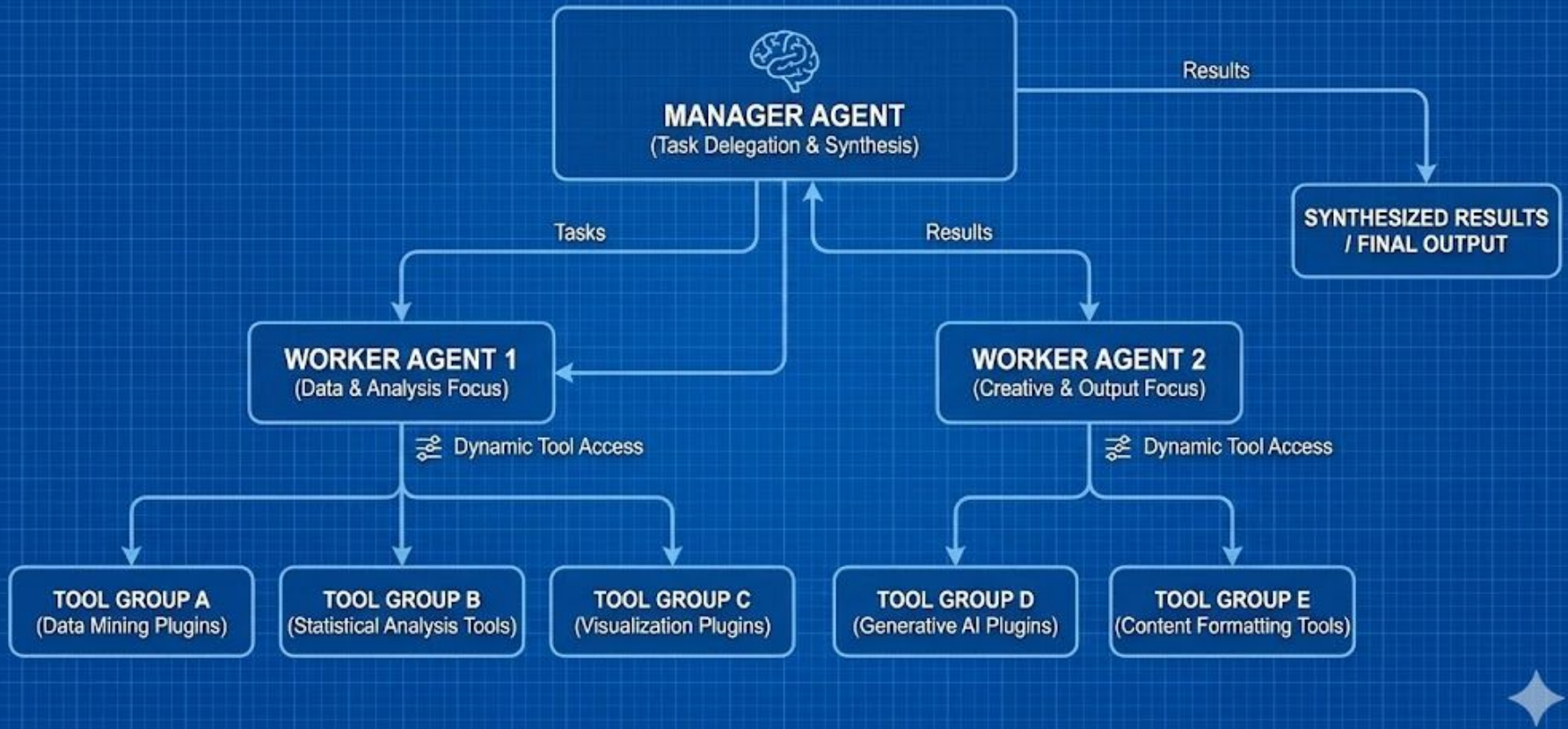
PARALLEL PROCESSING SCHEME

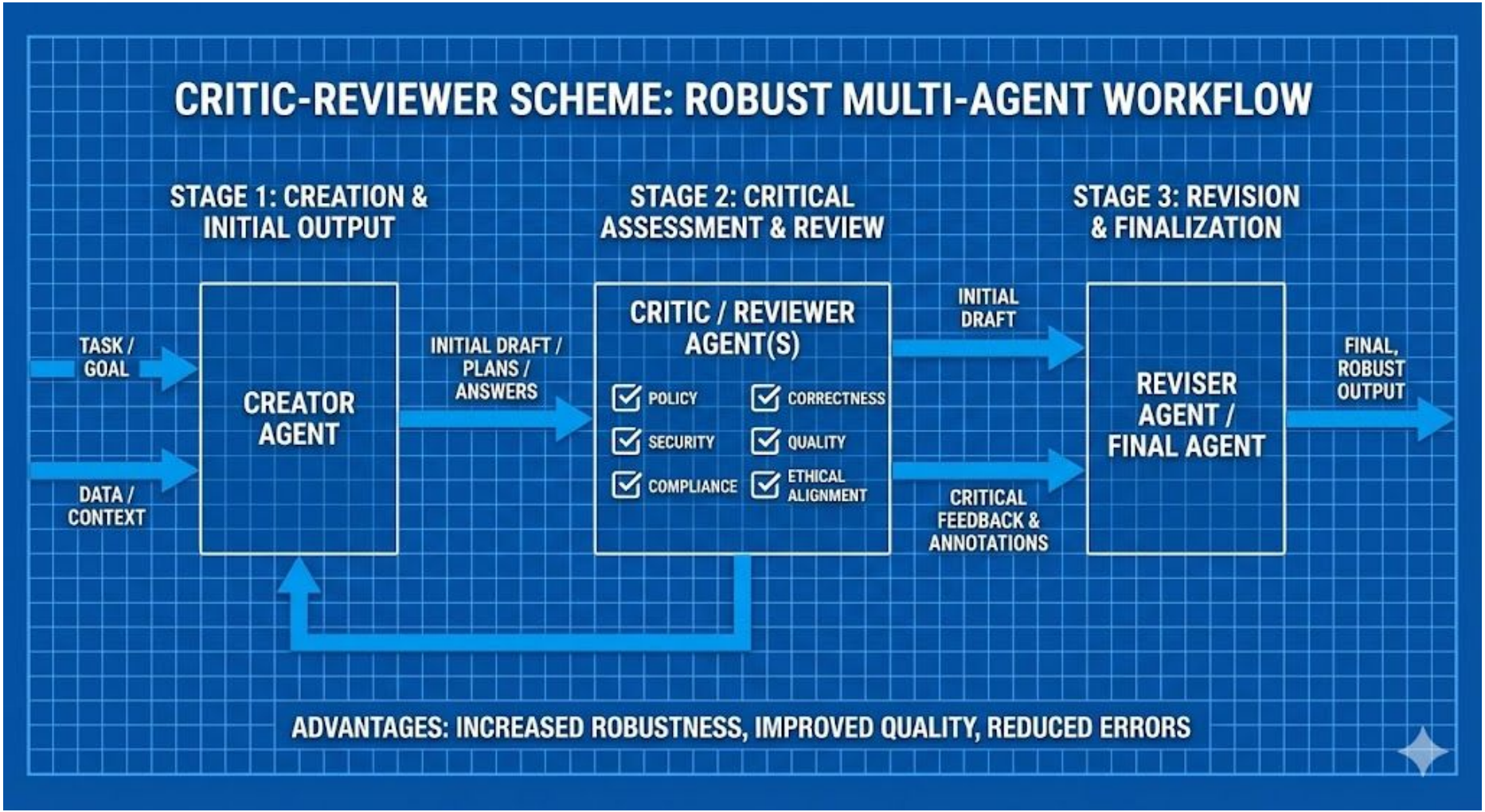


Multiple agents work on different parts of a problem simultaneously, and their results are later combined.


DEBATE & CONSENSUS SCHEME: Multi-Agent Collaboration
AGENT A
(Engineering Perspective)
AGENT B
(Financial Perspective)
AGENT C
(Ethical Perspective)
AGENT D
(Data Perspective)
INFORMATION SOURCE 1
INFORMATION SOURCE 2
INFORMATION SOURCE 3
DISCUSSION & EVALUATION FORUM
OPTION 1
(PROPOSED)
OPTION 2
(PROPOSED)
FINAL CONSENSUS / INFORMED DECISION
Agents with varied perspectives and information sources engage in discussions to evaluate options, ultimately reaching a consensus or a more informed decision.

HIERARCHICAL STRUCTURES & DYNAMIC DELEGATION SCHEME.




CRITIC-REVIEWER SCHEME: ROBUST MULTI-AGENT WORKFLOW
STAGE 1: CREATION & INITIAL OUTPUT
STAGE 2: CRITICAL ASSESSMENT & REVIEW
STAGE 3: REVISION & FINALIZATION
TASK / GOAL
DATA / CONTEXT
CREATOR AGENT
INITIAL DRAFT / PLANS / ANSWERS
CRITIC / REVIEWER AGENT(S)
POLICY
CORRECTNESS
SECURITY
QUALITY
COMPLIANCE
ETHICAL ALIGNMENT
INITIAL DRAFT
CRITICAL FEEDBACK & ANNOTATIONS
REVISER AGENT / FINAL AGENT
FINAL, ROBUST OUTPUT
ADVANTAGES: INCREASED ROBUSTNESS, IMPROVED QUALITY, REDUCED ERRORS

see you next time
for
“Memory Management, Learning and Adaptation, MCP”