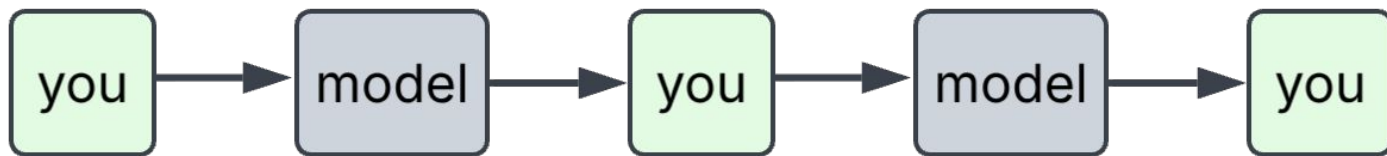


Week 2

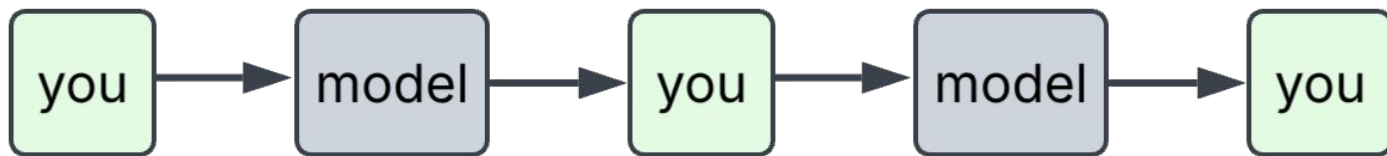
Foundations of Data Warehousing

August 31, 2026

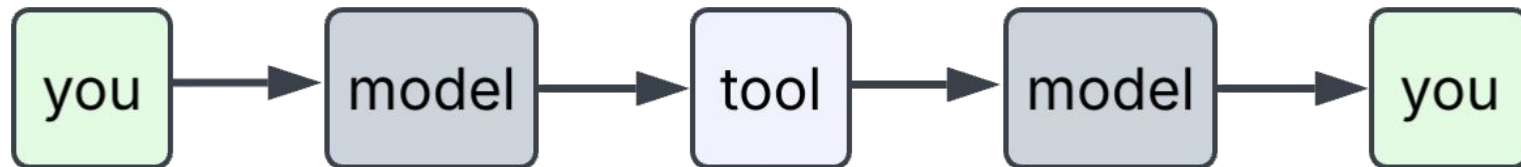
It started with simple chatbots



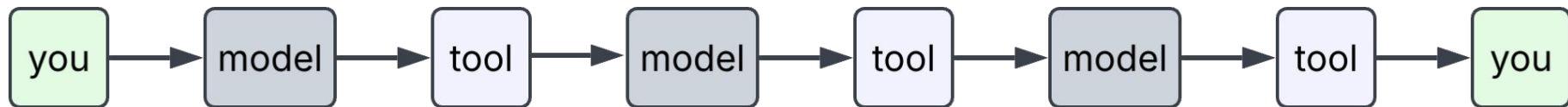
It started with simple chatbots



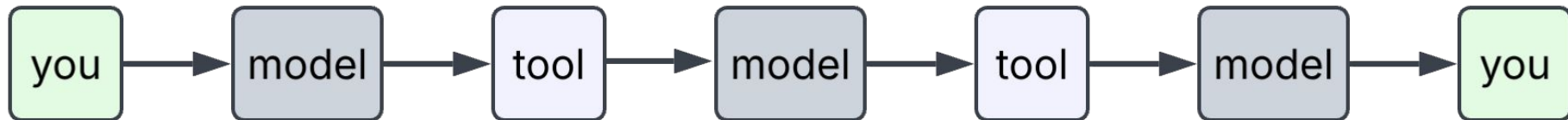
We then got tool calling



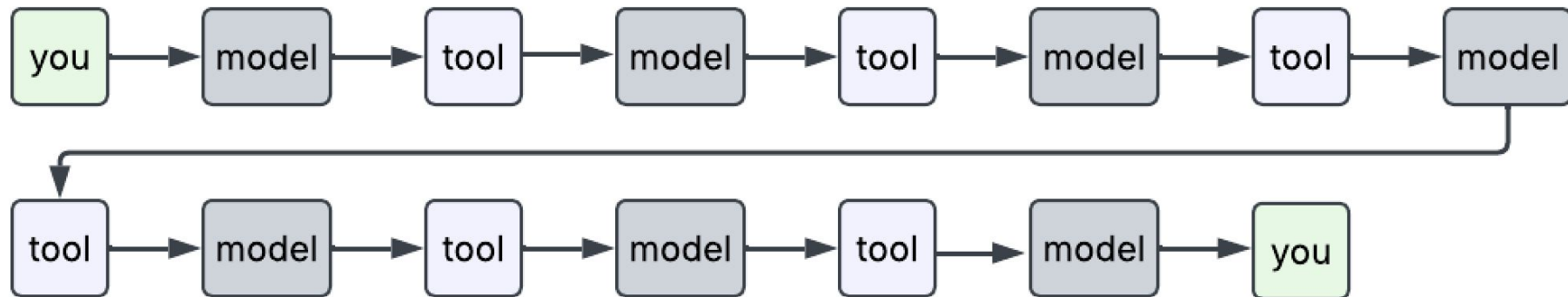
We slowly increased the number of tool calls



We slowly increased the number of tool calls



And added even more tool calls



And this became known as the agent loop or agentic loop

What is a context window?

- Set of tokens the model can see when predicting the next token
- Finite space to do customizations, about 1 million tokens
- Has not changed much in past two years

What does a tool call look like?

Here's a simple tool definition

```
1  {  
2    "name": "lookup_order",  
3    "description": "Look up an order by its order ID...",  
4    "input_schema": {  
5      "type": "object",  
6      "properties": { "order_id": { "type": "string" } },  
7      "required": ["order_id"]  
8    }  
9  }
```

Here's a better one

```
1  {
2    "name": "lookup_order",
3    "description":
4      "Look up an order by its order ID. Use this tool when creating a customer
       support ticket. Use it only after you have confirmed the customer's identity
       and collected the issue description. Do not call this to log internal notes;
       use `add_internal_note` for that. Example: user reports a broken checkout
       flow, you call this with order_id='A7B294X01' ",
5    "input_schema": {
6      "type": "object",
7      "properties": { "order_id": { "type": "string",
8                                   "description": "Customer's order number. Always 9 characters
9                                   long, alphanumeric." },
10                      "minLength": 9,
11                      "maxLength": 9 },
12    "required": ["order_id"]
13  }
```

Here's a tool use request

```
1  {
2    "type": "tool_use",
3    "id": "toolu_01A9F...",
4    "name": "lookup_order",
5    "input": {
6      "order_id": "B0V3KAY02"
7    }
8  }
```

Here's a tool result response

```
1  {
2    "type": "tool_result",
3    "tool_use_id": "toolu_01A9F...",
4    "content": "Order B0V3KAY02\n customer kaib9876\n Status: shipped on
2026-08-31 via UPS (1Z999AA10123456784)\n Placed: 2026-08-29\n Total: $203.
63\n Items: The North Face McMurdo Parka - Men's x 1 (KB-6100-BLK), 2x Free
Returns + Package Protection x 1 (CB-USBC-2M)"
5  }
```

What the request body looks like

```
2  {
3    "model": "claude-opus-5",
4    "max_tokens": 1024,
5    "temperature": 0.2,
6    "system": [
7      {
8        "type": "text",
9        "text": "You are a customer support assistant for Geartrade. Confirm the customer's identity and collect an issue description before looking up any order. Never reveal payment details in full; refer to the last four digits only. If a lookup fails, apologize and offer to escalate to a human agent.",
10       "cache_control": { "type": "ephemeral" }
11     ]
12   ],
13   "tools": [ { "name": "lookup_order", "description": "...", "input_schema": { ... } } ],
14   "messages": [
15     { "role": "user", "content": "Can you check on order B0V3KAY02?" },
16     { "role": "assistant", "content": [ { "type": "tool_use", "id": "toolu_01A9F...", ... } ] },
17     { "role": "user", "content": [ { "type": "tool_result", "tool_use_id": "toolu_01A9F...",
18       ..., ... } ] },
19     { "role": "assistant", "content": "That order shipped on August 31st via UPS..." }
20   ]
21 }
```

What are skills?

SKILL.md

```
1  ---
2  name: ticket-triage
3  description: Creates and routes customer support tickets for Geartrade. Covers identity
  verification, order lookup, severity assignment, and escalation paths. Use when a customer
  reports a problem with an order, requests a refund or replacement, or asks to speak with a
  human agent.
4  ---
5
6  # Ticket Triage
7
8  ## Workflow
9
10  1. Confirm the customer's identity (name plus email or account ID).
11  2. Collect a one-sentence description of the issue in their words.
12  3. Validate the order ID before calling `lookup_order`  run
13  | `scripts/validate_order_id.py <id>`. Malformed IDs are the most
14  | common cause of failed lookups.
15  4. Call `lookup_order` with the validated ID.
16  5. Assign a severity. See SEVERITY.md for the rubric.
17  6. Summarize the ticket back to the customer before filing.
18
19  ## Rules
20
21  - Never state a delivery date the carrier has not confirmed.
```

What the system prompt becomes

```
1  You are a customer support assistant for Geartrade. Confirm the
2  customer's identity and collect an issue description before looking up
3  any order. Never reveal payment details in full; refer to the last four
4  digits only. If a lookup fails, apologize and offer to escalate to a
5  human agent.
6
7  # Available skills
8
9  - ticket-triage: Creates and routes customer support tickets for
10 Geartrade. Covers identity verification, order lookup, severity
11 assignment, and escalation paths. Use when a customer reports a
12 problem with an order, requests a refund or replacement, or asks to
13 speak with a human agent.
```

Model emits a
server tool use
request

```
1  {
2    "role": "assistant",
3    "content": [
4      { "type": "text", "text": "Let me pull up our triage process and that order." },
5      {
6        "type": "server_tool_use",
7        "id": "srvtoolu_01X..",
8        "name": "code_execution",
9        "input": { "command": "cat /mnt/skills/ticket-triage/SKILL.md" }
10     }
11   ]
12 }
```

API responds
with code
execution tool
result

```
1  {
2    "role": "user",
3    "content": [
4      {
5        "type": "code_execution_tool_result",
6        "tool_use_id": "srvtoolu_01X...",
7        "content": {
8          "type": "code_execution_result",
9          "stdout": "# Ticket Triage\n\n## Workflow\n\n1. Confirm the customer's identity...\n",
10         "stderr": "",
11         "return_code": 0
12       }
13     ]
14   }
15 }
```

What competes for space in the context window?

- CLAUDE.md (instructions file Claude reads every session)
- System and user prompt
- Tools, skills
- MCP servers
- Files you've attached
- Conversation history

What **doesn't** compete for space in the context window?

- Hooks
- Settings and permissions
- The filesystem
- Subagents
- Dynamic workflows

```
1  {
2    "hooks": {
3      "PostToolUse": [
4        {
5          "matcher": "Edit|Write",
6          "hooks": [
7            {
8              "type": "command",
9              "command": "echo \"file changed\" >> ~/claude-edits.log"
10           }
11         ]
12       }
13     ]
14   }
15 }
```

<https://claude.com/blog/steering-claude-code-skills-hooks-rules-subagents-and-more>

Term Projects: where we landed

