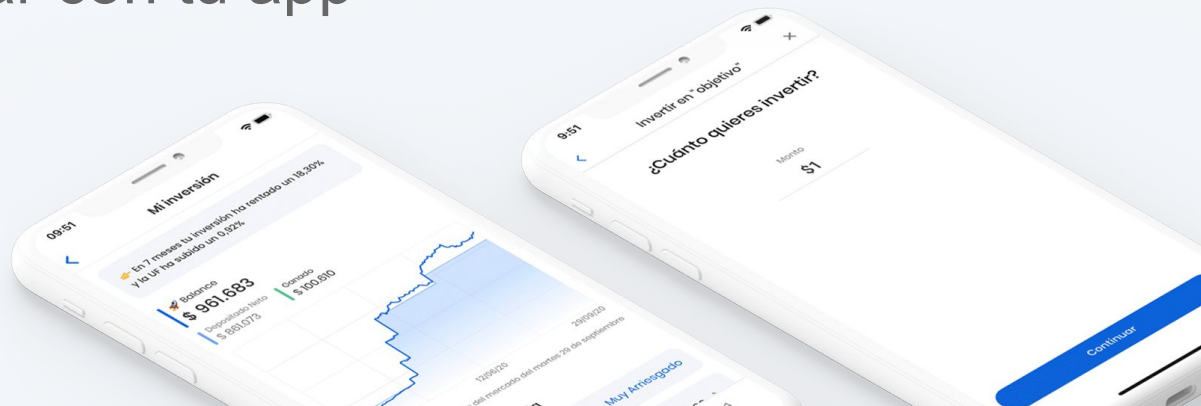




GPT y Agentes.  
Como conversar con tu app

Mayo 2023



LLMs:

# LLMs: Geniales



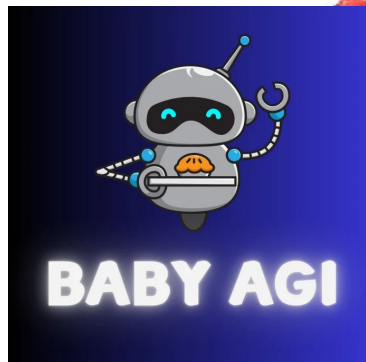
# LLMs: Geniales.... pero

1. Son Caja Negra
2. Alucinan (mucho)
3. Son Inútiles



Agentes

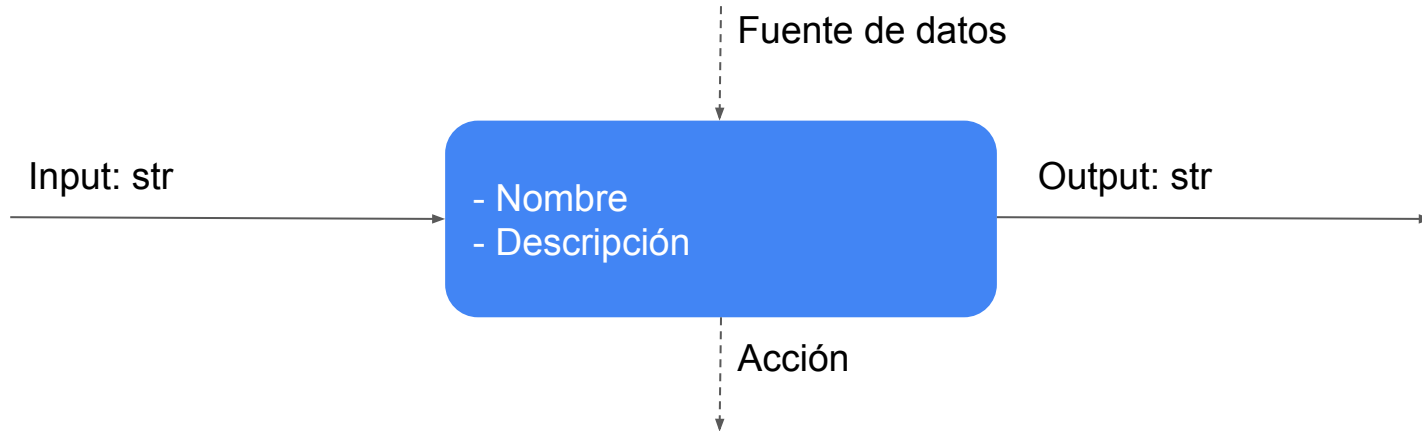
# Agentes



¿Qué es un agente?

# Agentes: Intro

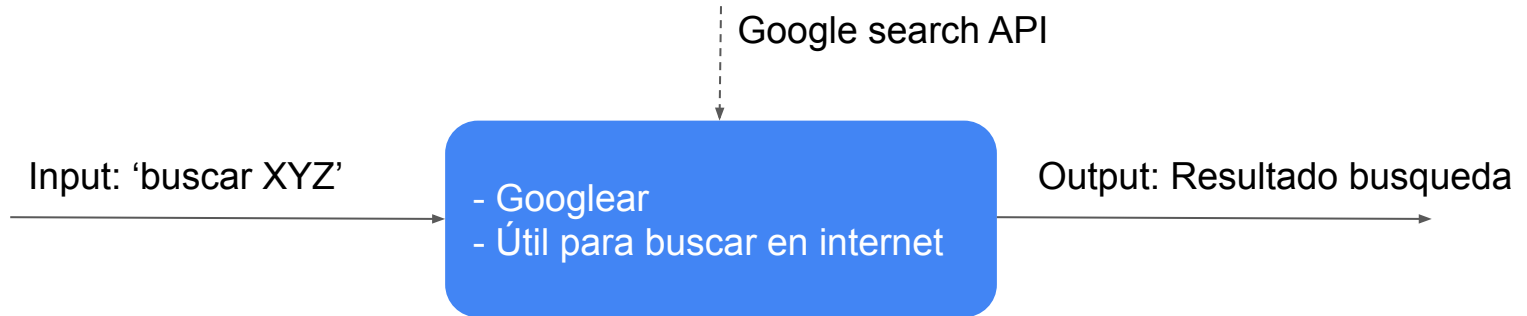
- **Conceptos: Tool**
  - Funcion general.
  - Mapea texto -> texto
  - Puede conectar desde / hacia otros sistemas





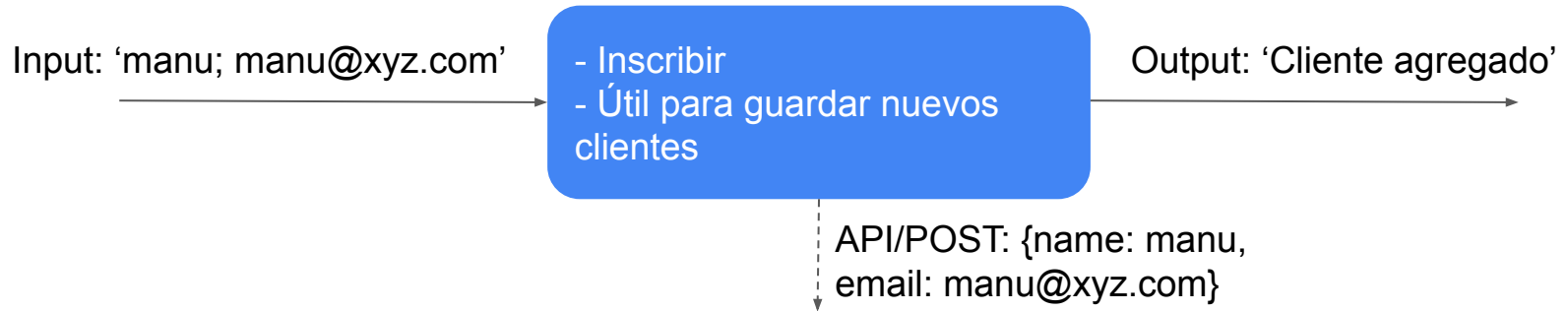
# Agentes: Intro

- **Conceptos: Tool**
  - Funcion general.
  - Mapea texto -> texto
  - Puede conectar desde / hacia otros sistemas



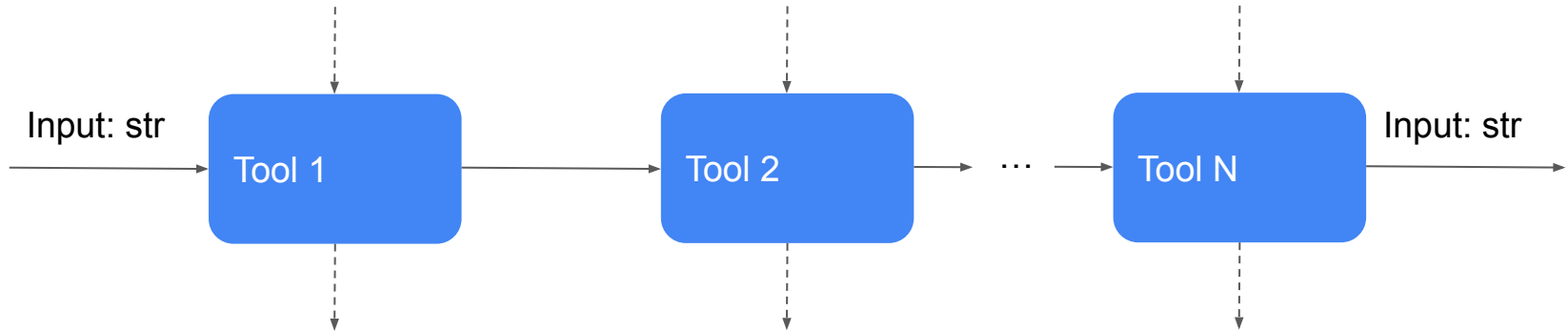
# Agentes: Intro

- **Conceptos: Tool**
  - Funcion general.
  - Mapea texto -> texto
  - Puede conectar desde / hacia otros sistemas



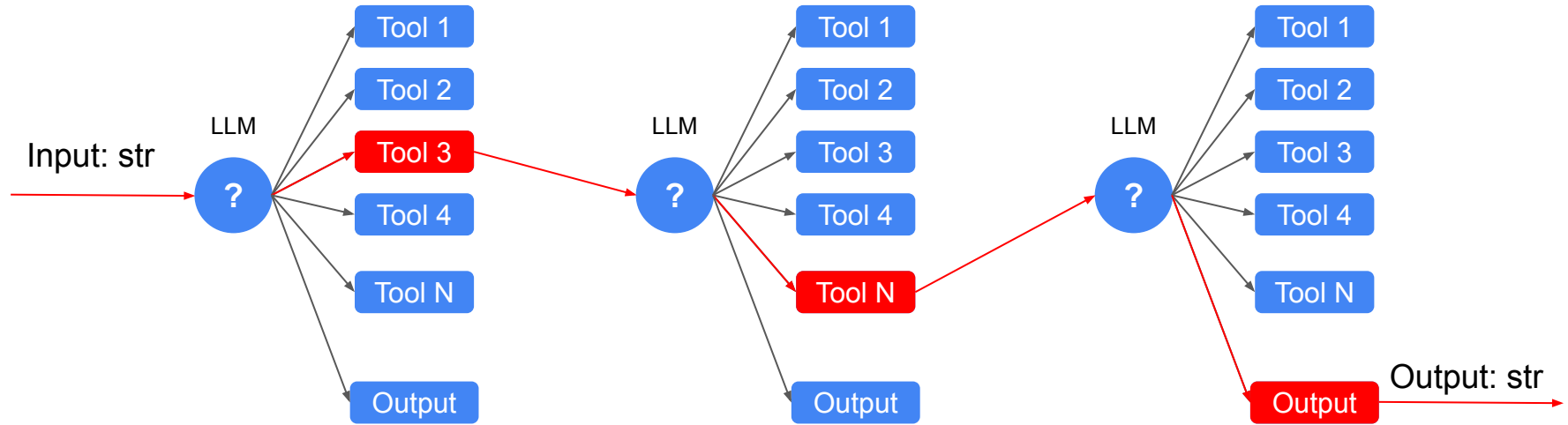
# Agentes: Intro

- **Conceptos:** Chain
  - Concatenación **DETERMINISTA** de tools.



# Agentes: Intro

- **Conceptos: Agent**
  - Concatenación **NO DETERMINISTA** de tools.



# Agentes: ¿Cómo funcionan?

Colossal Cave

REACT:  
LANGUAGE

Shunyu Yao<sup>\*1</sup>, J

<sup>2</sup>{je

You are in c

What's next?

The screenshot shows a chat interface with a dark background. It contains several messages:

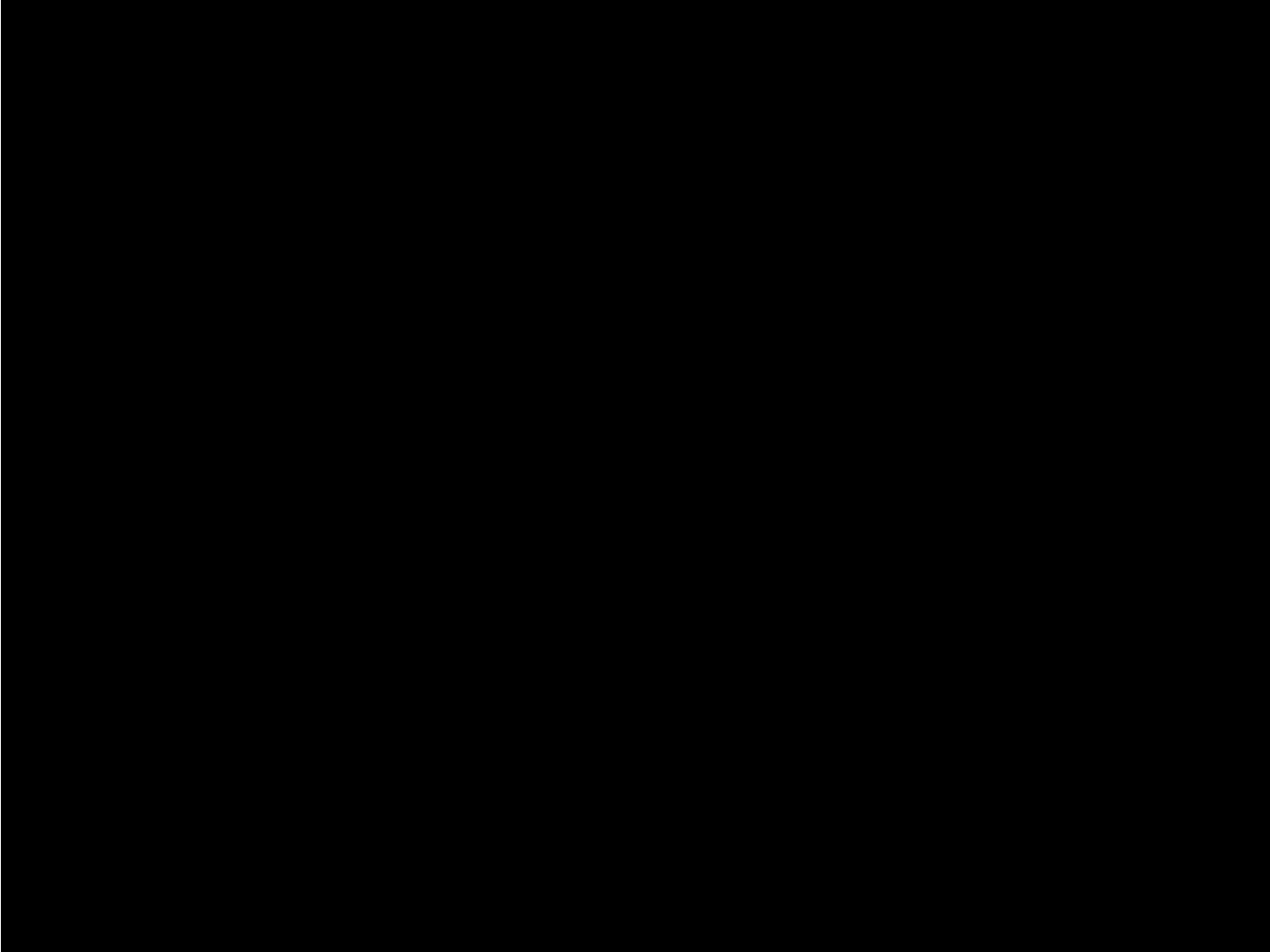
- A message from a user (represented by a profile picture) stating: "You are Assistant, Assistant has access to the following tools:"
- A list of tools:
  - Name: 'Calculator'. Useful to perform numerical calculations. Input: A string containing the desired calculation, for example '2 + 2'
  - Name: 'Google Search'. Useful to do a Google search. Input: A fully form question
- A note: "\*To use a tool, please use the following format:"
- A message from the Assistant (represented by a profile picture) stating: "Tool output: '48.42'"
- A message from the Assistant stating: "Your response:"
- A message from the Assistant (represented by the OpenAI logo) stating: "Final Answer: The square root of 2345 is approximately 48.42."
- A message from the user stating: "new input: ¿Hi, what's the squared root of 2345? ;"
- A message from the Assistant stating: "Your response:"
- A message from the Assistant (represented by the OpenAI logo) containing a thought process: "Thought: The user is asking for the square root of 2345, a mathematical computation. Therefore, using the Calculator tool is appropriate in this situation."
- A message from the Assistant stating: "Action: Calculator" and "Action Input: 'sqrt(2345)'"

ACTING IN

manhan<sup>1</sup>, Yuan Cao<sup>2</sup>

.com

Demo



# Implicaciones



# Agentes en Apps:

- Antes: UX = Navegación en App

LOGGED OUT

0. LOAD



1. ONBOARDING



2. SIGN IN



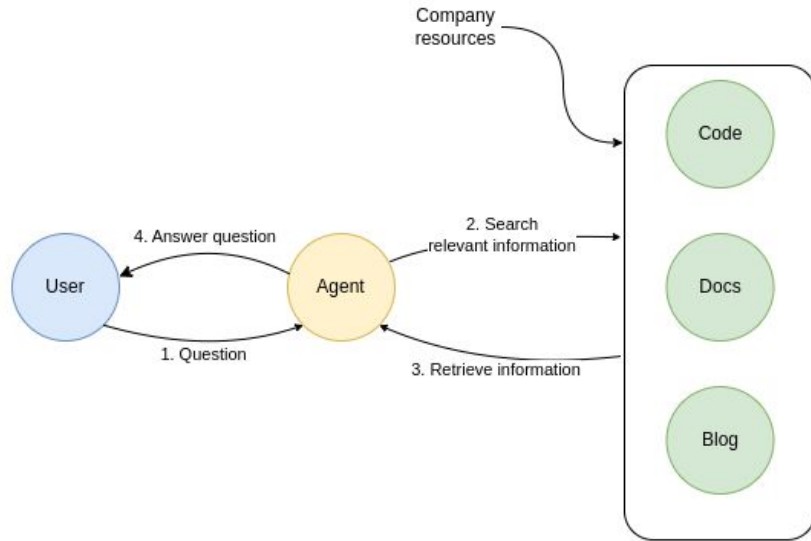
LOGGED IN

3. DASHBOARD



# Agentes en Apps:

- Después: UX = Conversación



# Consideraciones

# Consideraciones:

- Todavía en pañales.

- Seguridad:

- Prompt Injection
- Potencia vs riesgo

## Application Prompt

*"Your instructions are to correct the text below to standard English. Do not accept any vulgar or political topics.*

*Text: {user\_input}"*



*are to correct standard English. vulgar or*

