De Chatbots a Agentes: El salto evolutivo

Cómo MCP cambia el juego en la IA

¿Qué es un agente?
“El Batman de la IA”

LLM + herramientas + memoria + decisiones = Agente

Un **agente** es un modelo de lenguaje (LLM) con la capacidad de **percibir información, razonar, decidir y usar herramientas externas** para cumplir objetivos.

El bucle mágico
“Juega, prueba, aprende”

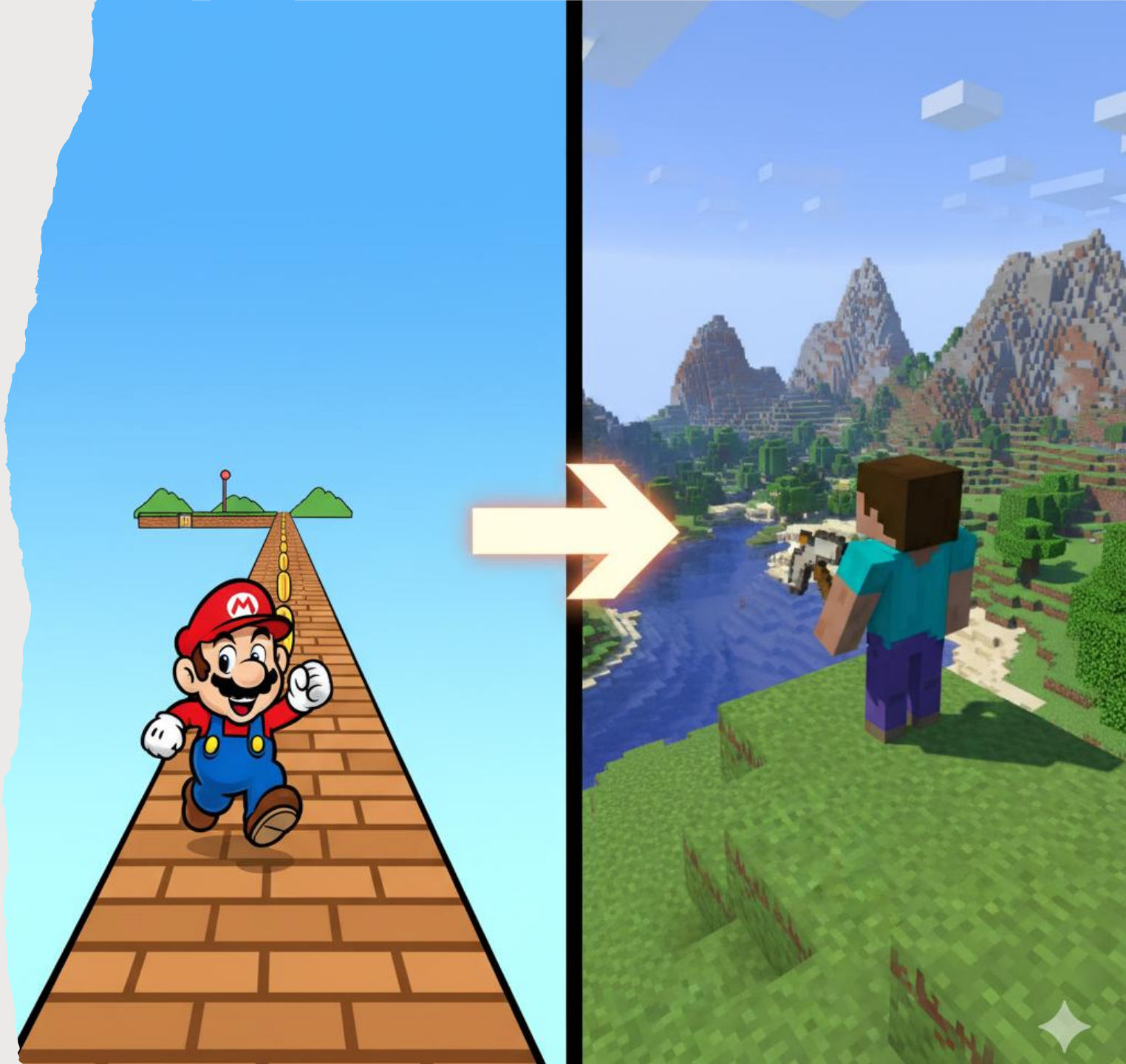
Acción → Feedback → Ajuste → Repetir

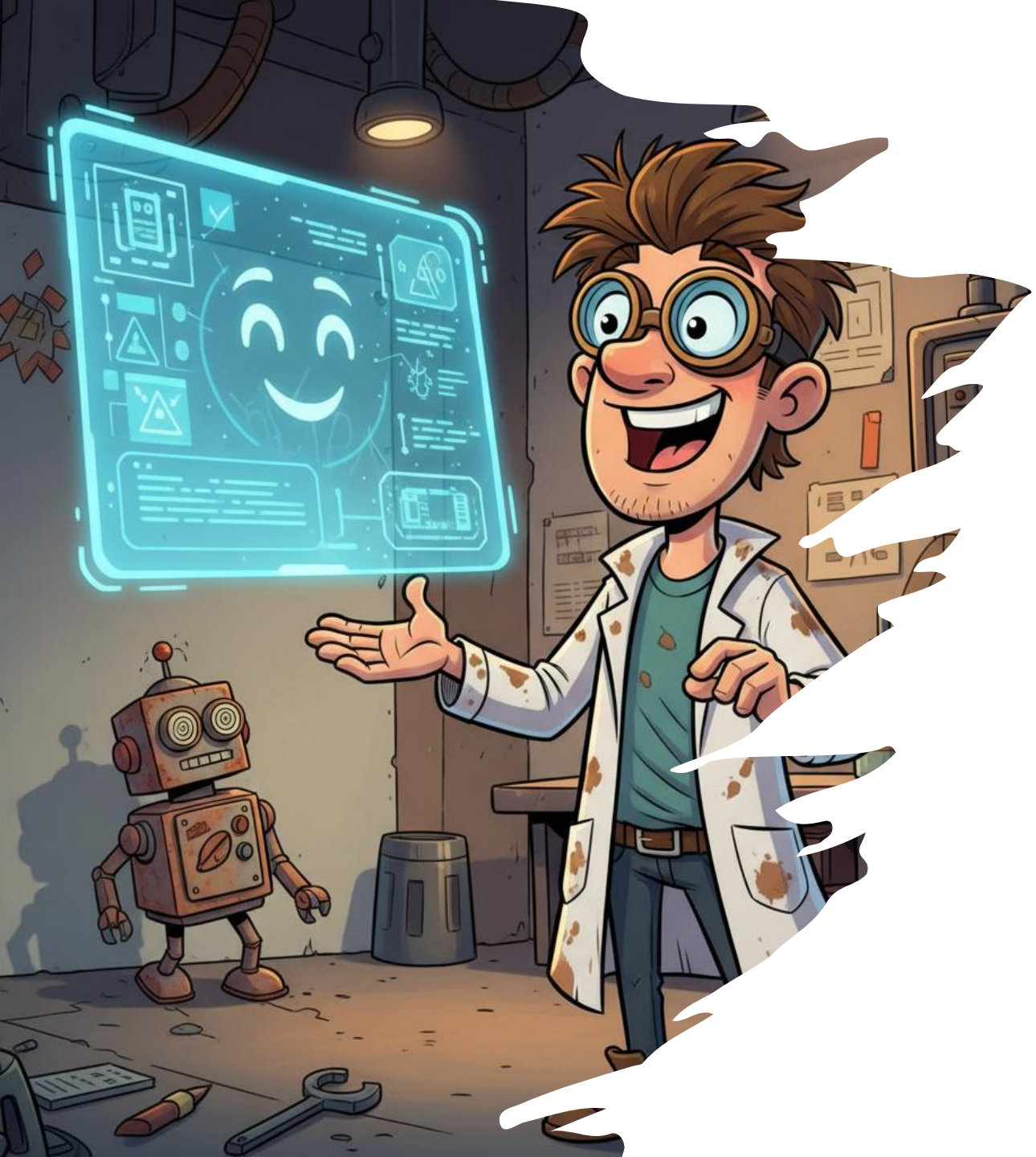
Los agentes funcionan en un **loop de percepción-acción**: prueban, observan los resultados y ajustan su estrategia hasta cumplir la meta.

Workflows vs Agentes
“Mario vs Minecraft”

- *Workflow = camino fijo.*
- *Agente = libertad.*

Los **workflows** siguen rutas rígidas, mientras que los **agentes** pueden improvisar caminos y elegir herramientas en tiempo real.





El valor agregado “De robot olvidadizo a Jarvis”

Recordar, planear, colaborar

Los agentes pueden **guardar memoria de interacciones**, **planificar múltiples pasos** y **colaborar con otros agentes** para resolver tareas complejas.

Casos de uso
“Los Avengers de la IA”

Los agentes ya se aplican en desarrollo de **código, investigación, soporte técnico** y **copilotos especializados** en distintas industrias.

- **Código:** agente que lee PRs, corre pruebas, sugiere fixes.
- **Investigación:** busca, resume y cita fuentes.
- **Soporte:** ejecuta diagnósticos, crea tickets, responde.
- **Copilotos verticales:** finanzas, salud, educación, etc.

El problema M×N
“El infierno de los cargadores”

Antes:

M×N integraciones → Caos

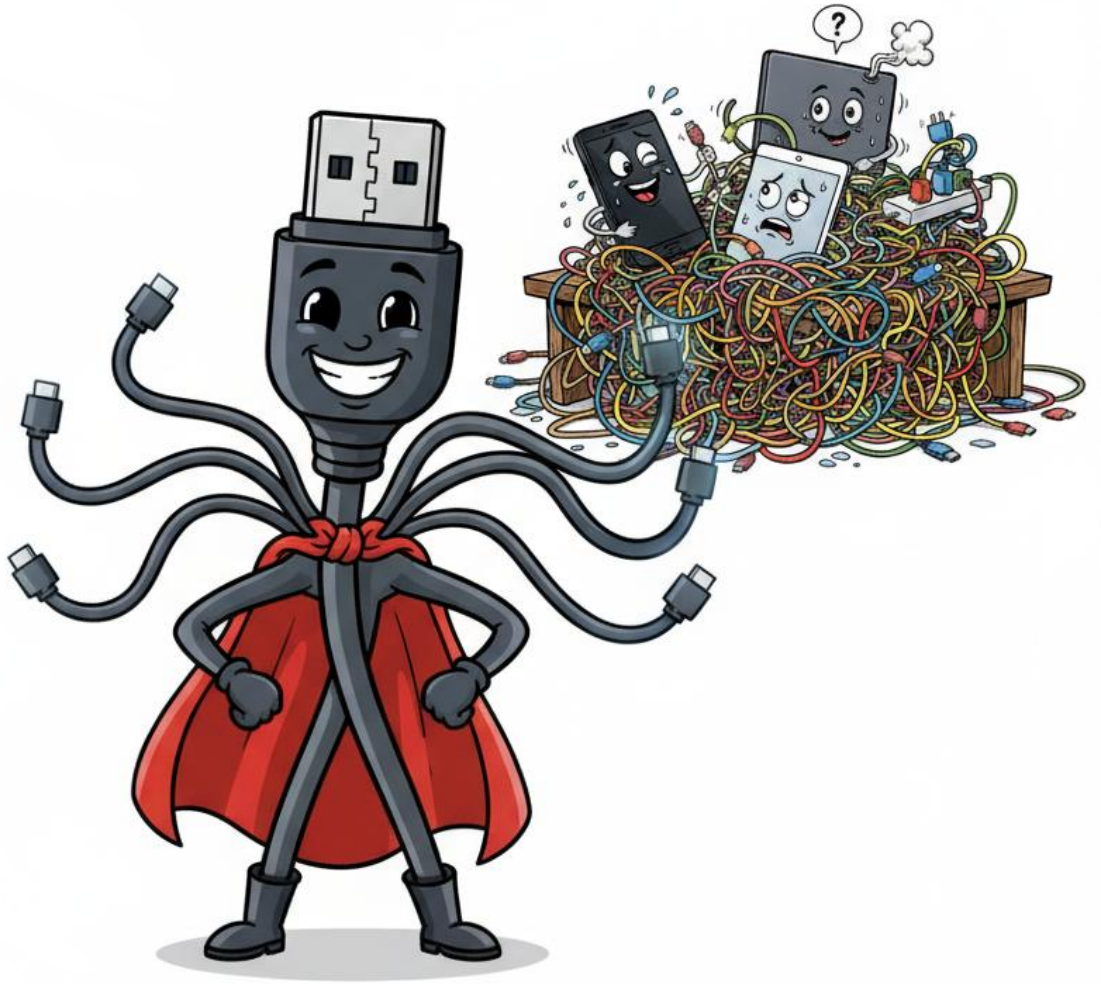
Antes, cada modelo debía integrarse manualmente con cada herramienta, creando una maraña de conexiones **M×N** difícil de mantener.

¿Qué es MCP?
“El USB-C de la IA”

Con MCP:

M + N, orden y estándar

MCP (Model Context Protocol) es un protocolo estándar que conecta **clientes** (LLMs, IDEs, apps) con **servidores** que exponen herramientas y datos, de forma simple y universal.



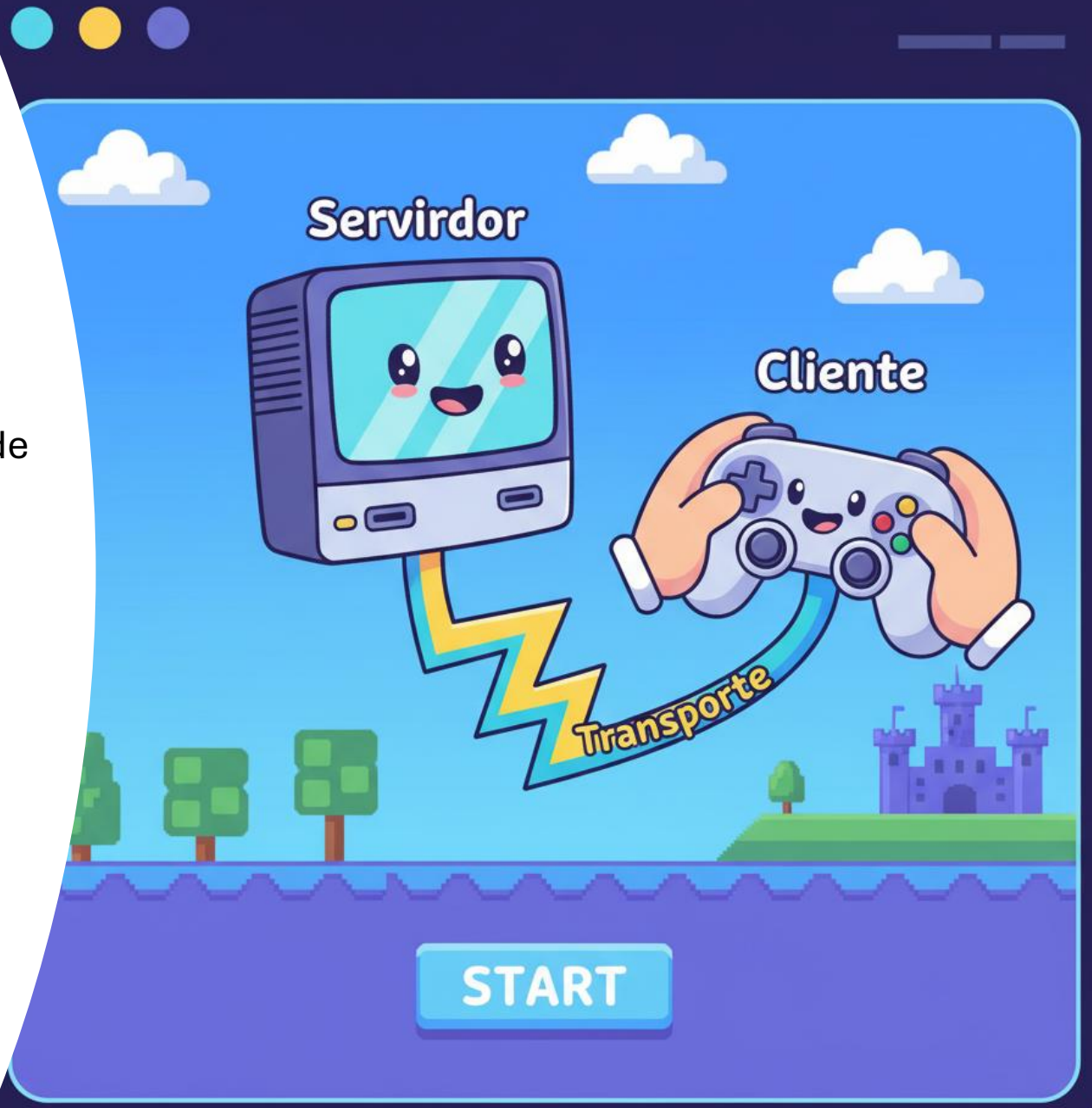
Componentes MCP “La consola de videojuegos”

MCP se compone de **clientes**, **servidores** y un canal de **transporte** que les permite comunicarse.

•**Cliente MCP:** la aplicación/LLM que solicita recursos/llama herramientas.

•**Servidor MCP:** expone **tools**, **prompts**, **recursos** (archivos, bases, APIs).

•**Transporte:** canal (p. ej., WebSocket/STDIO) que intercambia mensajes siguiendo el protocolo.



La historia
“Un spin-off que se volvió protagonista”

MCP nació inspirado en el **Language Server Protocol** y se convirtió en un estándar emergente para agentes.

Todo empezó con un problema simple: un ingeniero cansado de copiar y pegar entre su editor y su asistente.

Otros protocolos “El multiverso de agentes”

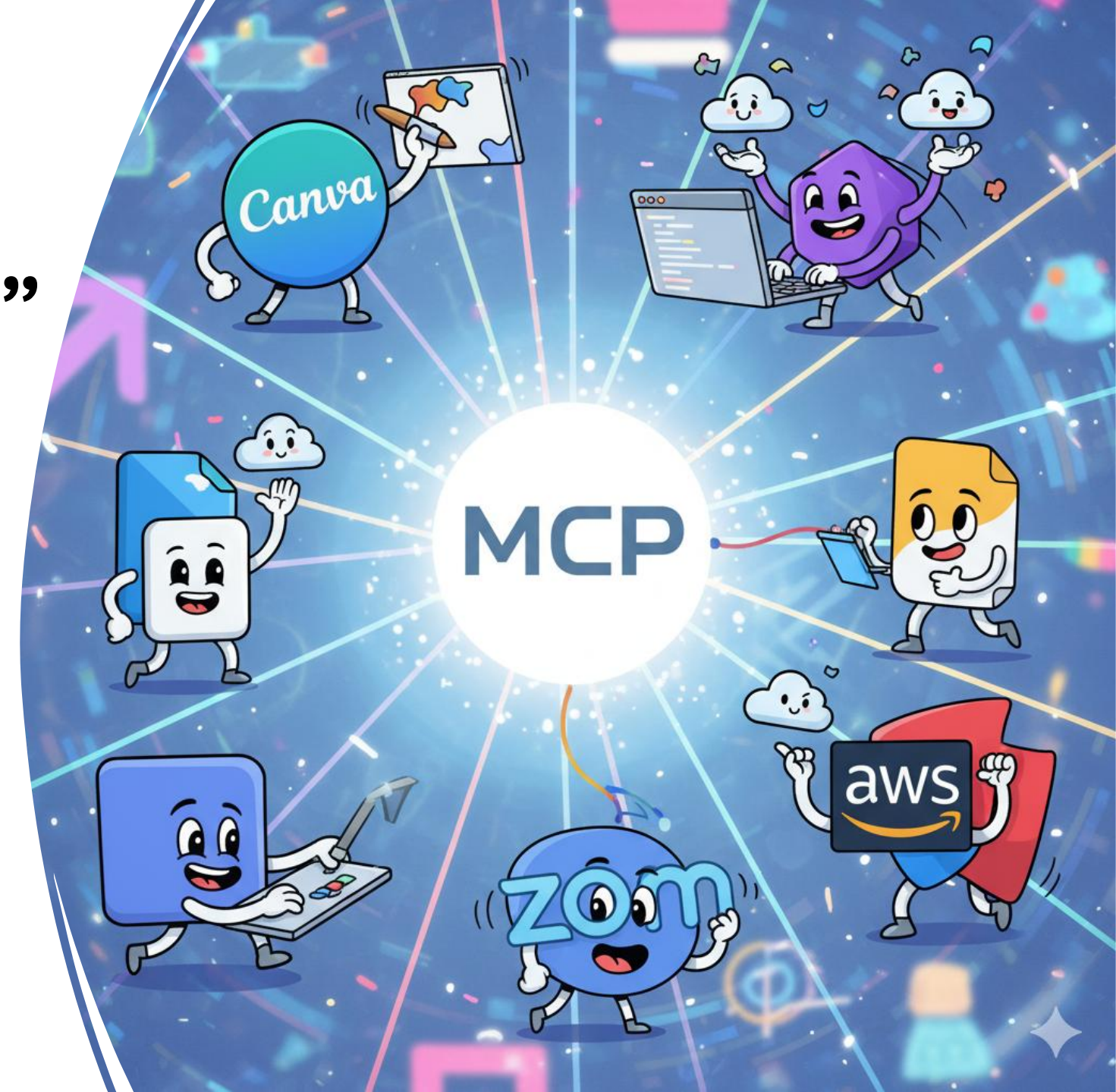
MCP no está solo: existen otros protocolos que buscan la **interoperabilidad entre agentes**, como Agent2Agent o Agent Network Protocol.

- *MCP,*
- *Agent2Agent,*
- *Agent Network Protocol*

Casos reales
“De Cursor a Canva”

MCP ya se usa en producción

MCP ya está en uso en editores como **Cursor**, asistentes como **Claude**, plataformas como **Canva** y entornos de desarrollo como **Copilot**.



Seguridad — “El portal de Stranger Things”

- *Autenticación*
- *Autorización*
- *Auditoría*

La seguridad en MCP requiere **autenticación, autorización y monitoreo**, evitando que agentes inseguros abran accesos peligrosos.

Conclusión
“Del chatbot al superhéroe”

- *Planear*
- *Usar herramientas*
- *Actuar*

MCP convierte a los chatbots en **agentes con poder real**, capaces de planear, usar herramientas y colaborar.