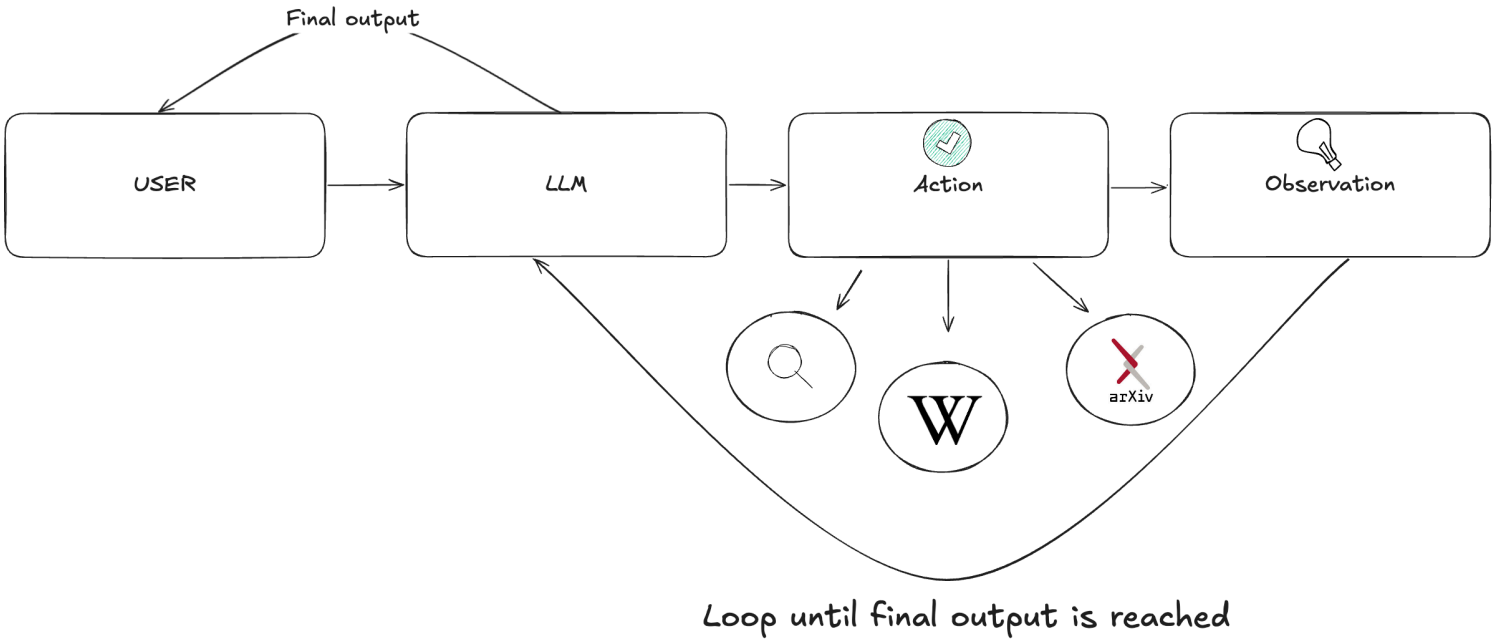
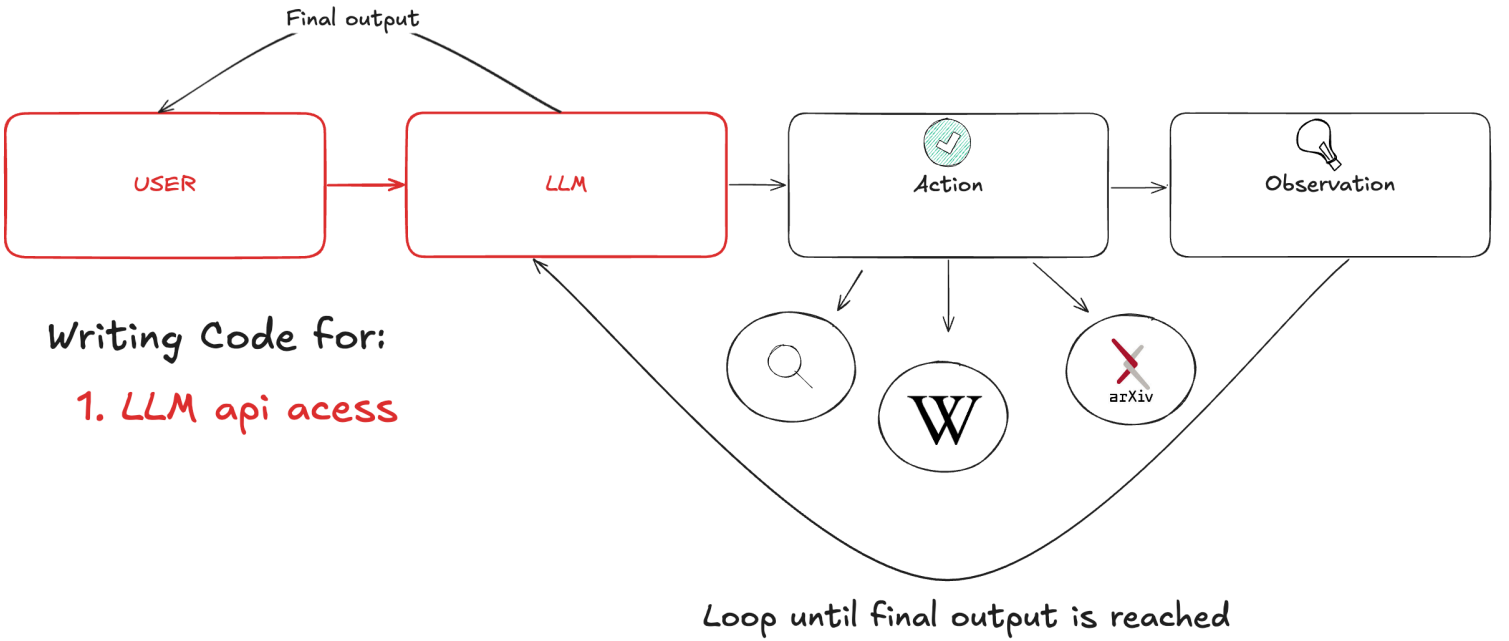
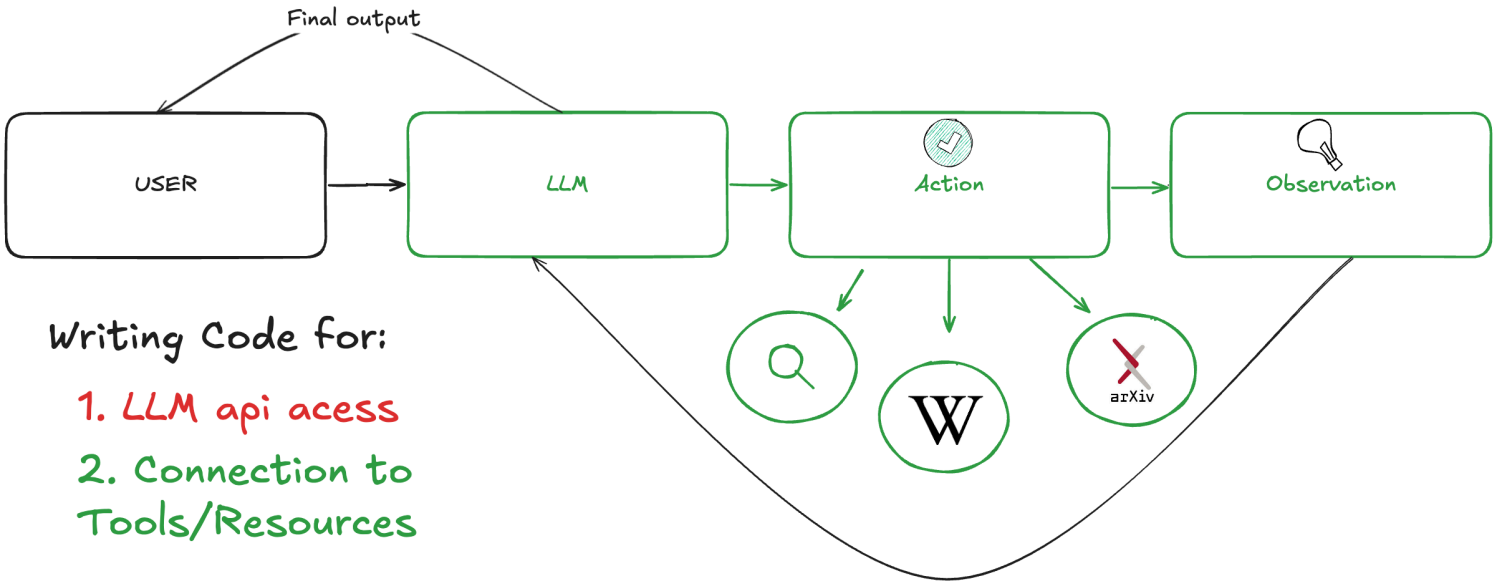
Building Agents with MCP

The HTTP Moment of AI?

Building an Agent in 2025

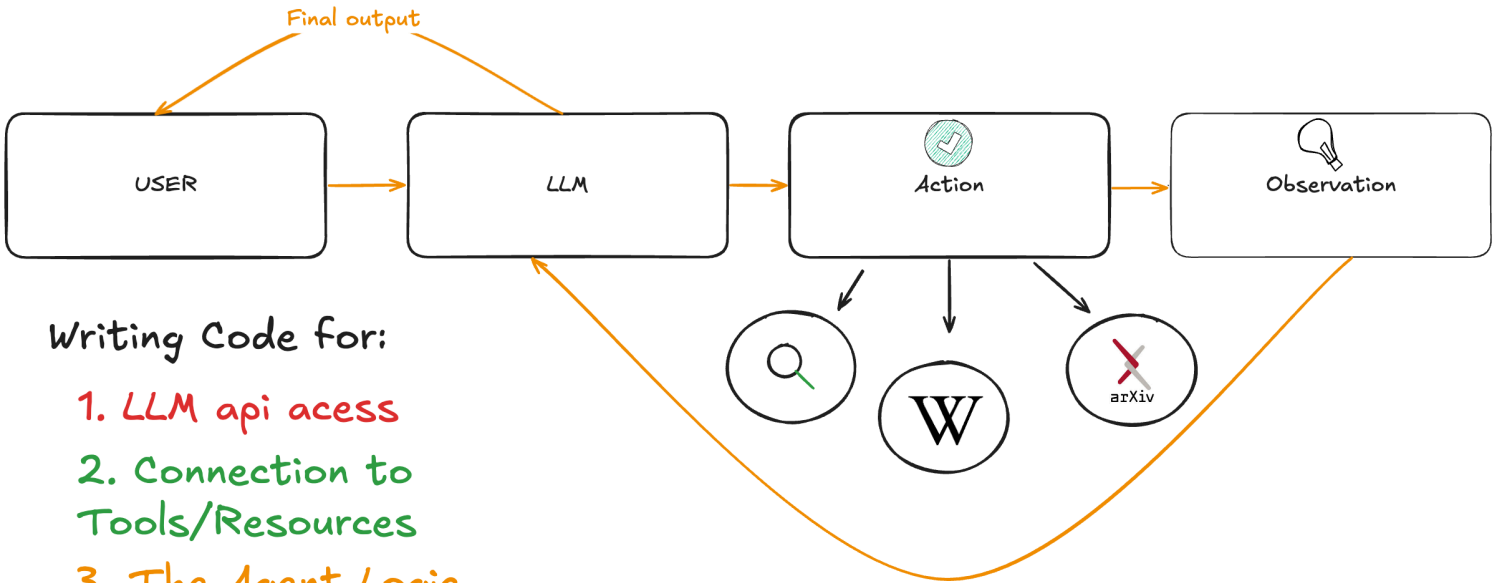

Final output
USER
LLM
Action
Observation
arXiv
Loop until final output is reached


Final output
USER
LLM
Action
Observation
arXiv
Writing Code for:
1. LLM api acess
Loop until final output is reached

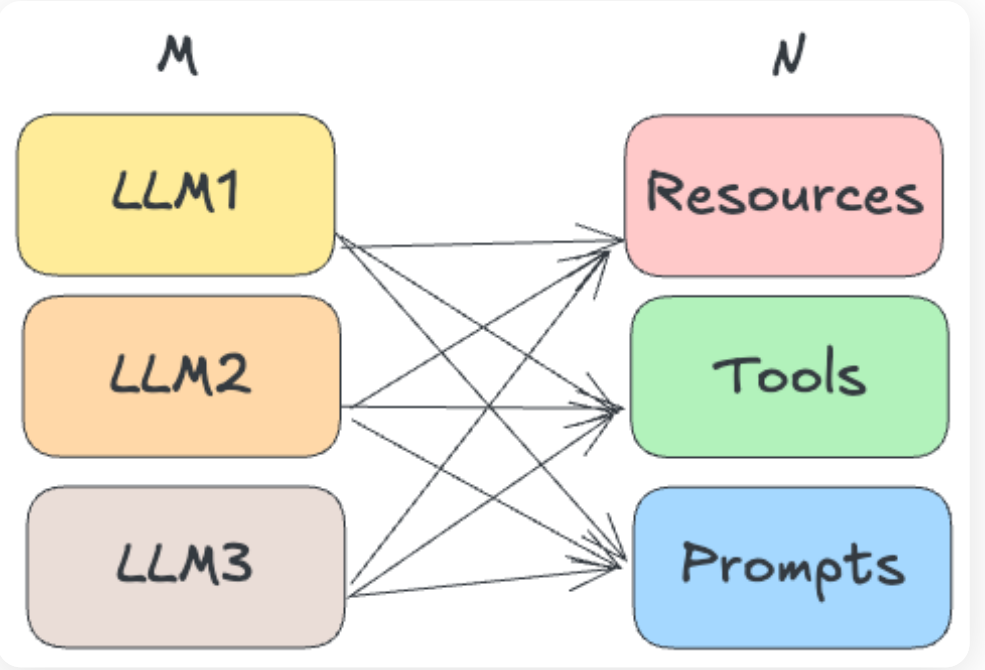


Writing Code for:

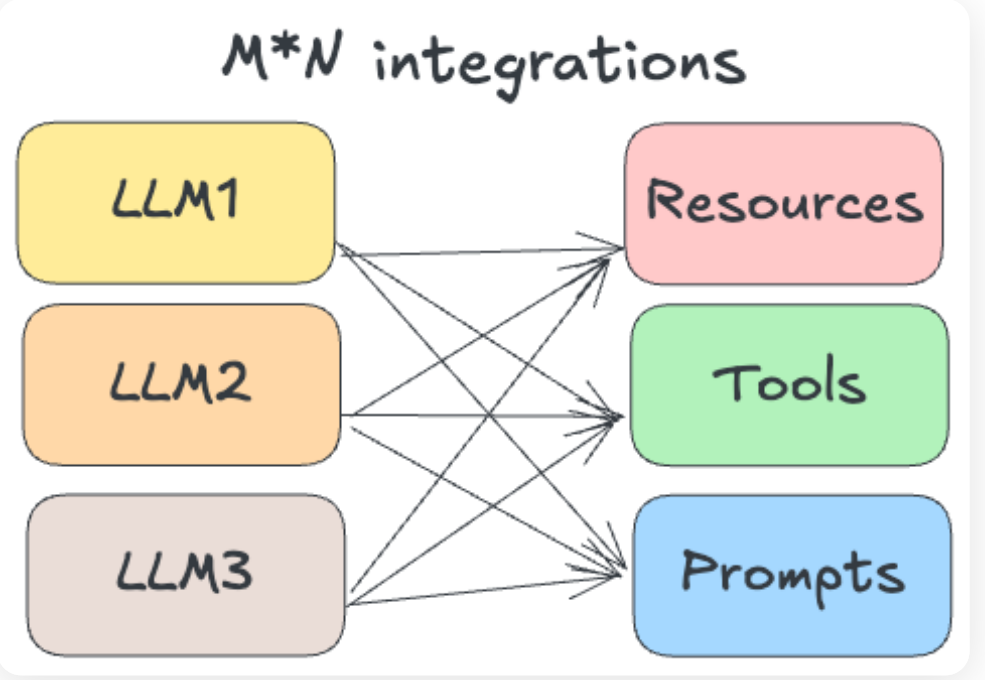
1. LLM api acess
2. Connection to Tools/Resources


Final output
USER
LLM
Action
Observation
arXiv
Writing Code for:
1. LLM api acess
2. Connection to Tools/Resources
3. The Agent Logic
Loop until final output is reached

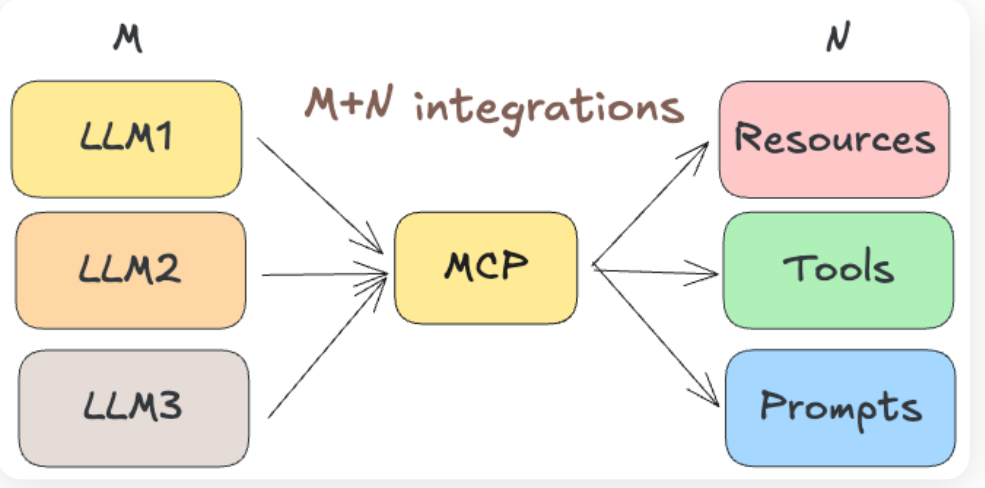
The MN Integration Problem: Multiple LLMs



The MN Integration Problem: Multiple LLMs

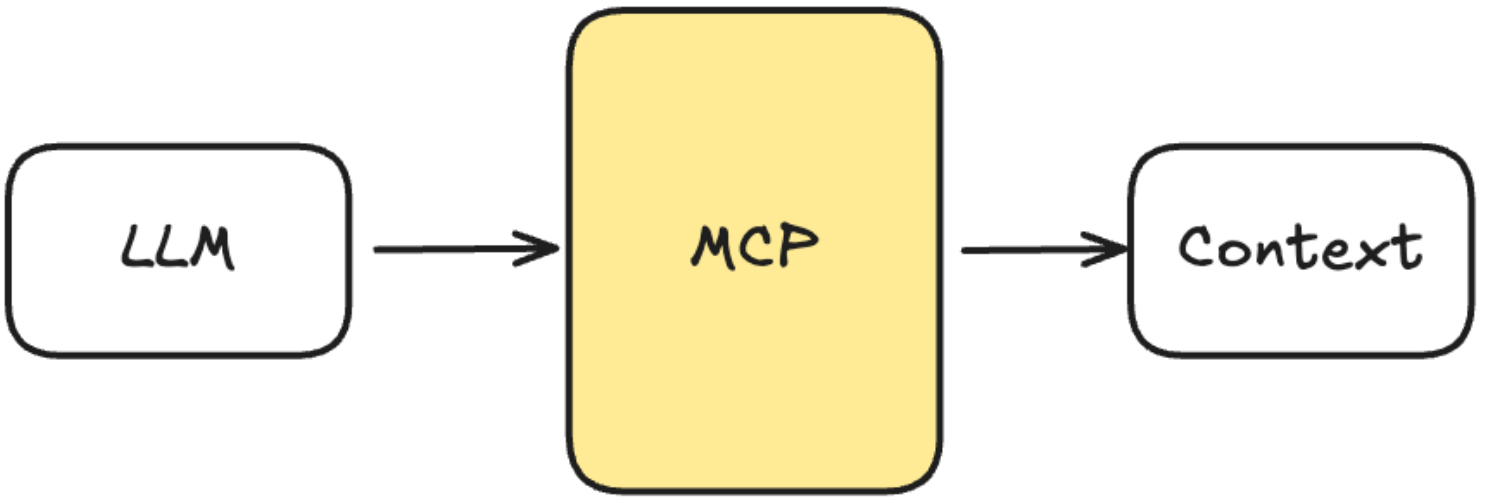


The MN Integration Problem: Multiple LLMs



What is MCP?

Open Protocol to standardize connections between LLMs and Context

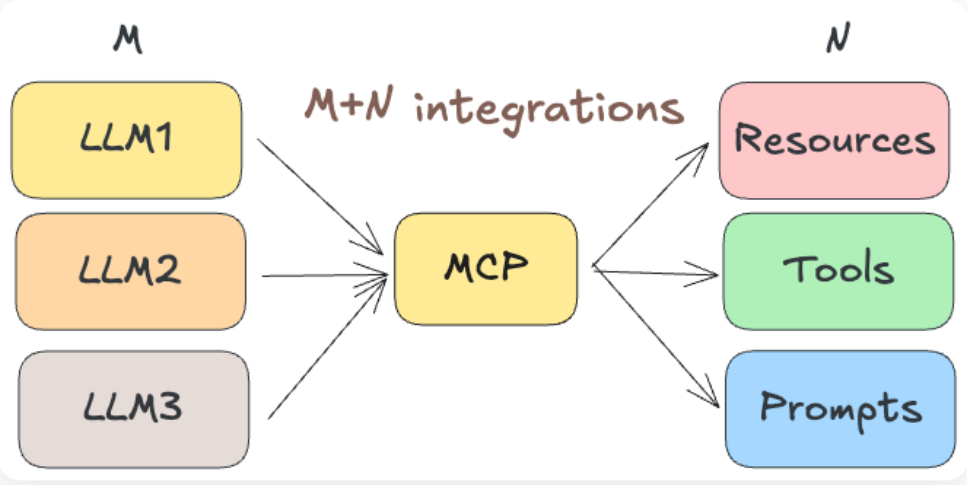


MCP is what makes AI actually useful for real apps

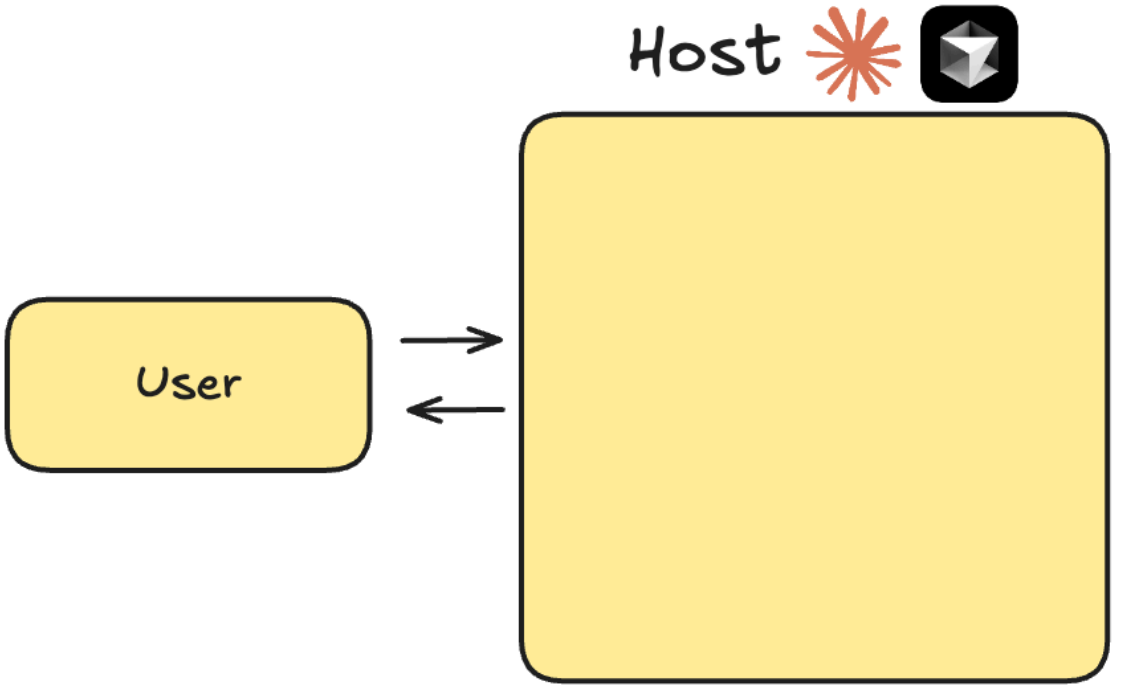
MCP is what makes AI actually useful for real apps

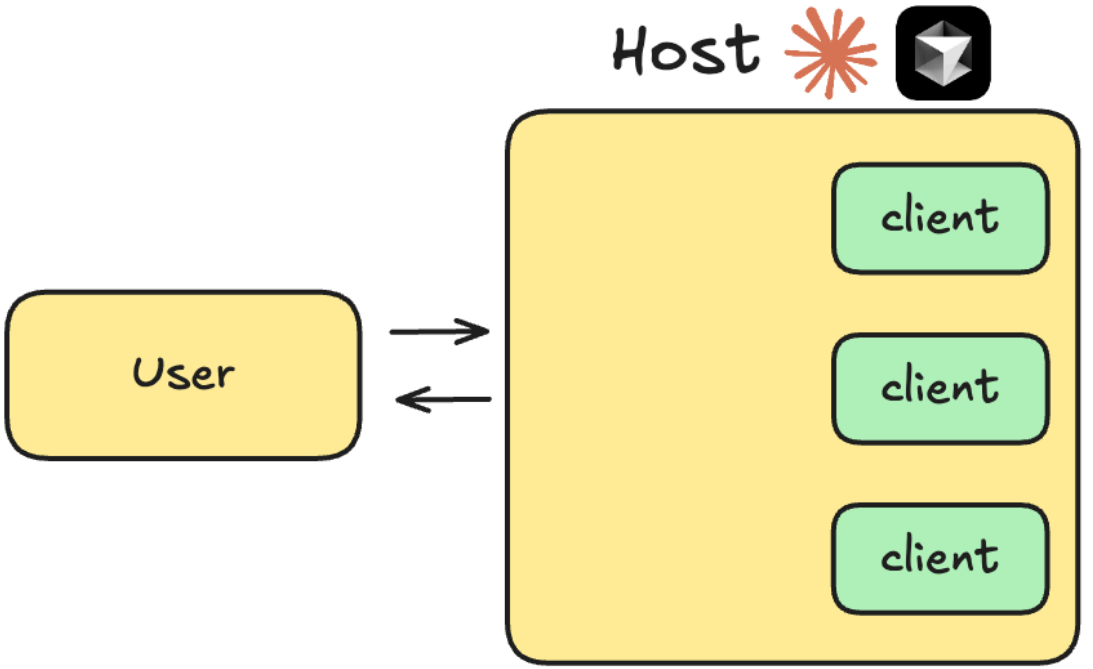
And for building agents!

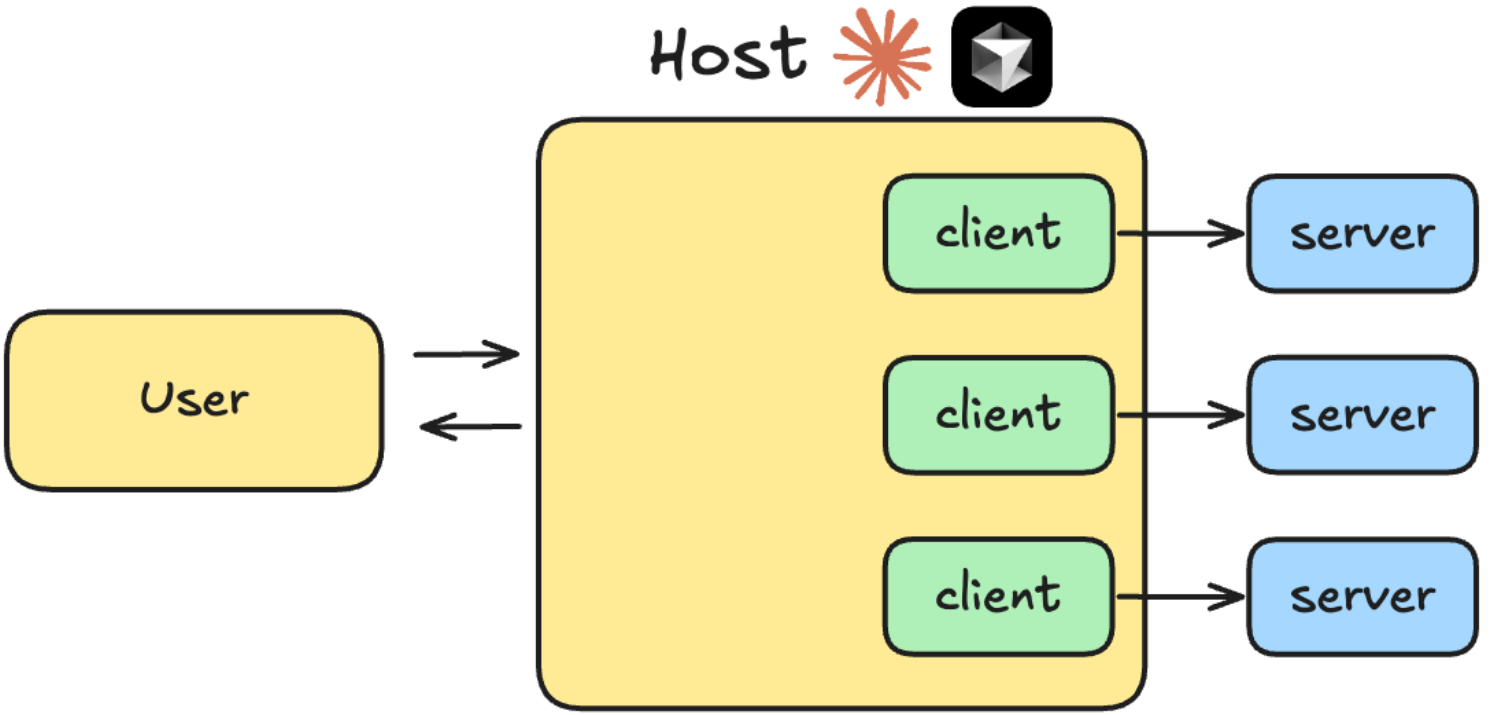
MCP Simplifies the Integration of Problem for Agent Development

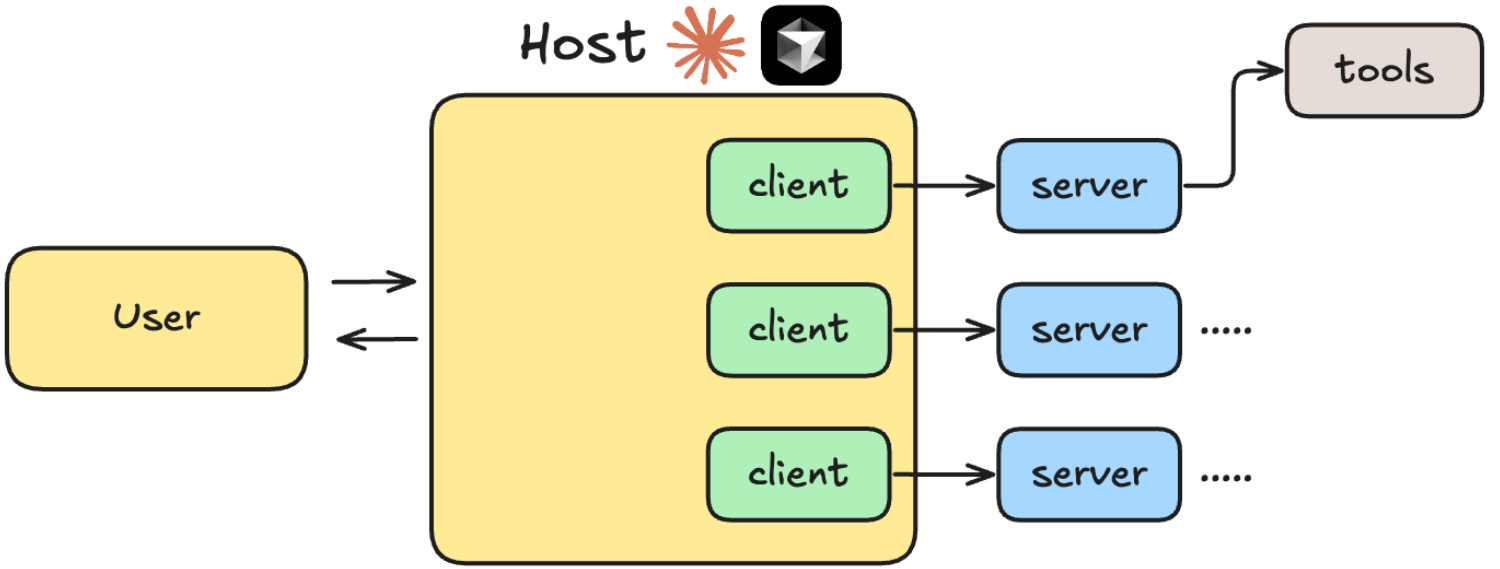


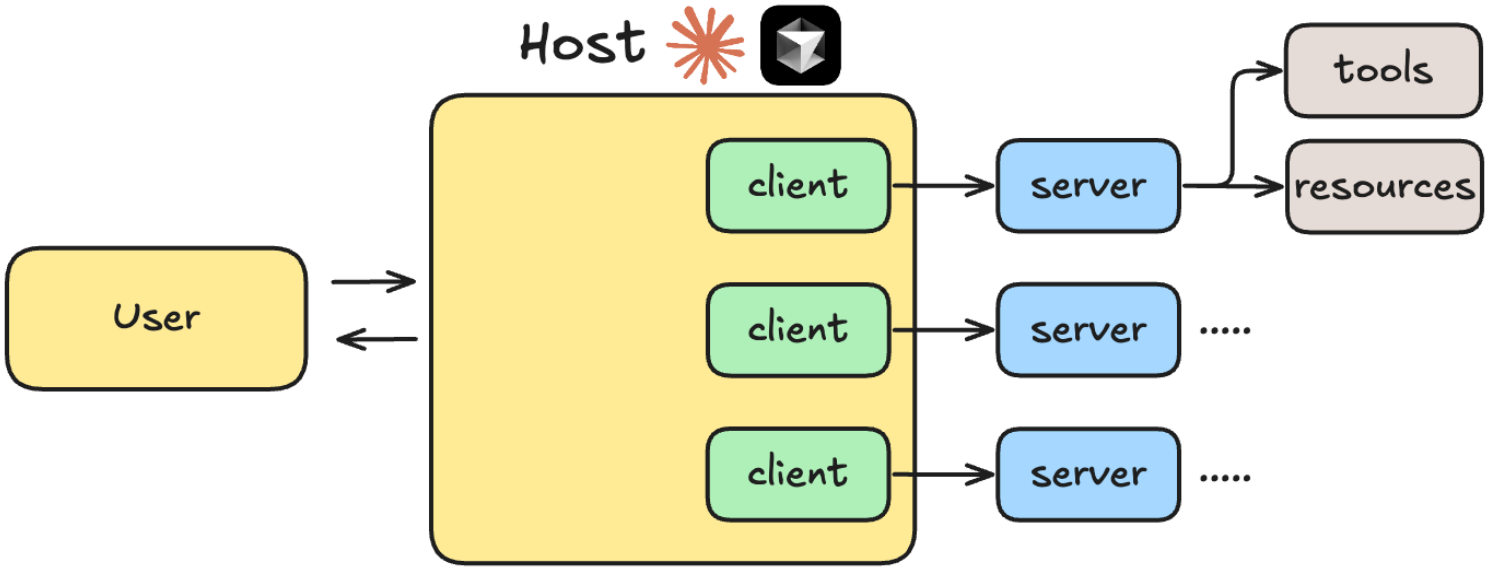
MCP Core Components

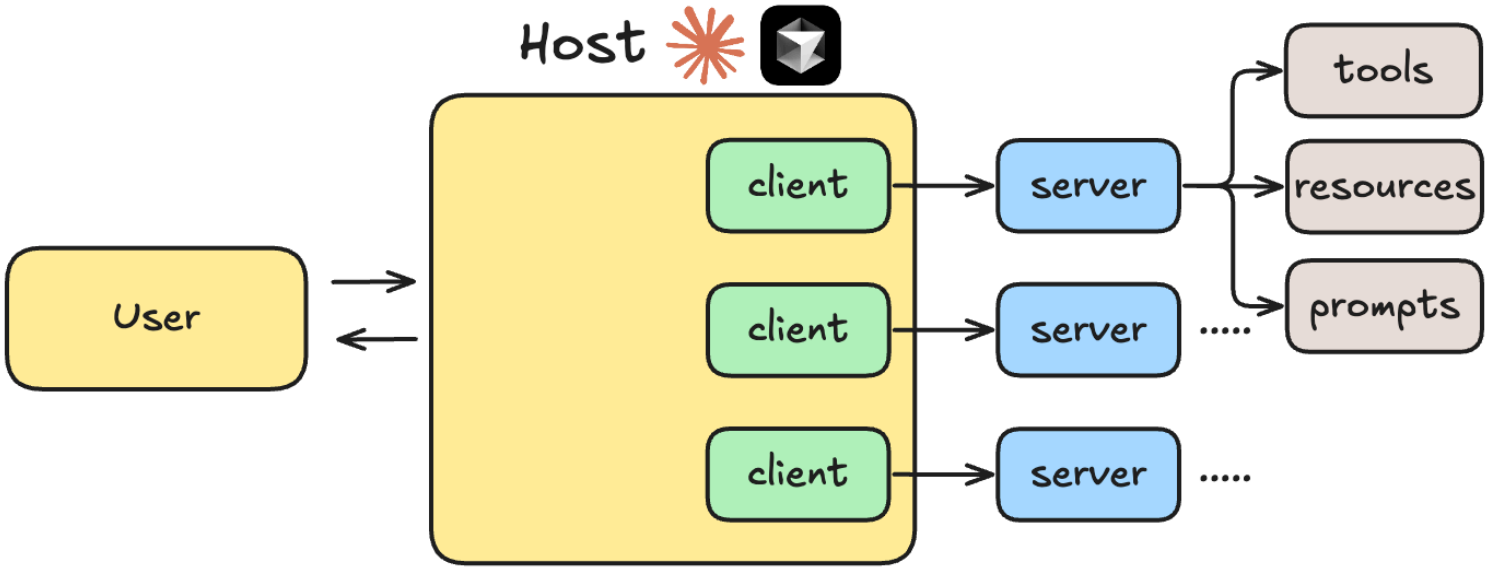

Host
User


Host
client
client
client
User

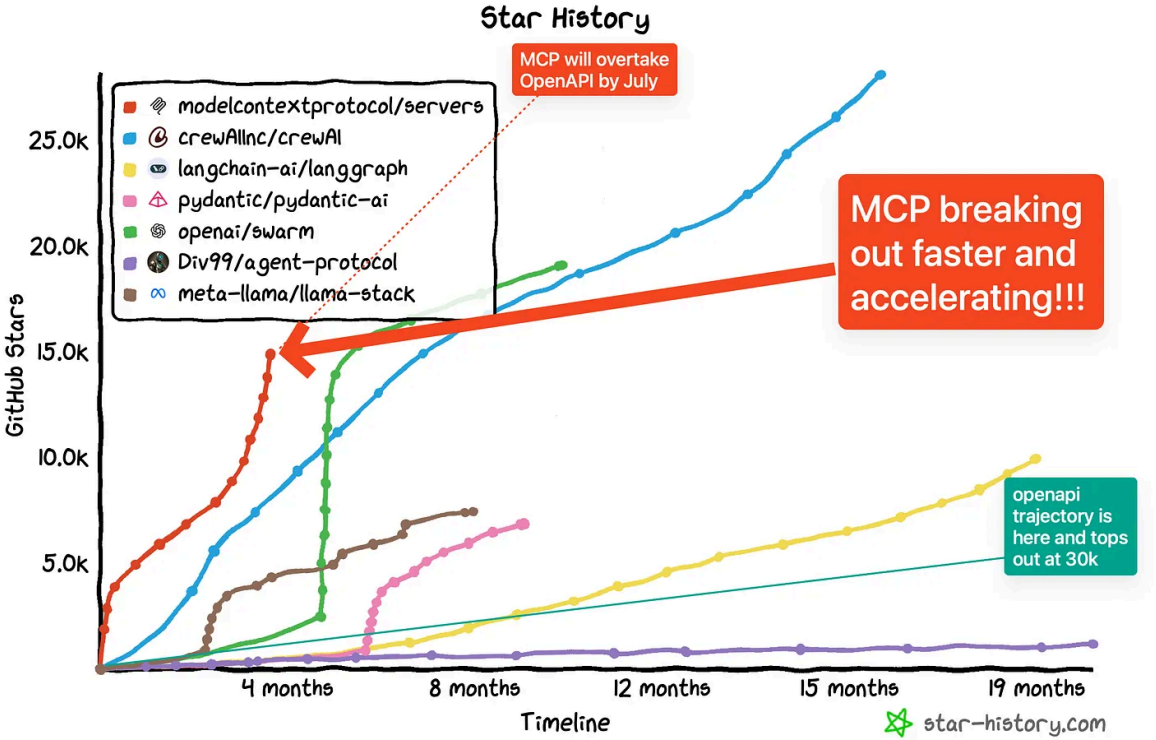

Host
User
client
client
client
server
server
server


Host
User
client
client
client
server
server
server
tools
.....
.....


Host
User
client
client
client
server
server
server
tools
resources


Host
User
client
client
client
server
server
server
tools
resources
prompts

MCP is Growing Super Fast



Big Players Are Moving Fast

- **Early Pioneers**

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard
  - Seamless workflows across multiple applications

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard
  - Seamless workflows across multiple applications
- **Enterprise Adoption is Accelerating**

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard
  - Seamless workflows across multiple applications
- **Enterprise Adoption is Accelerating**
  - **Block:** Automating workflows with MCP integration

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard
  - Seamless workflows across multiple applications
- **Enterprise Adoption is Accelerating**
  - **Block:** Automating workflows with MCP integration
  - **Snowflake:** Connecting enterprise data seamlessly

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard
  - Seamless workflows across multiple applications
- **Enterprise Adoption is Accelerating**
  - **Block:** Automating workflows with MCP integration
  - **Snowflake:** Connecting enterprise data seamlessly
  - **MinIO:** Enabling AI access to storage systems

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard
  - Seamless workflows across multiple applications
- **Enterprise Adoption is Accelerating**
  - **Block:** Automating workflows with MCP integration
  - **Snowflake:** Connecting enterprise data seamlessly
  - **MinIO:** Enabling AI access to storage systems
  - **Cloudflare:** Just launched remote MCP services

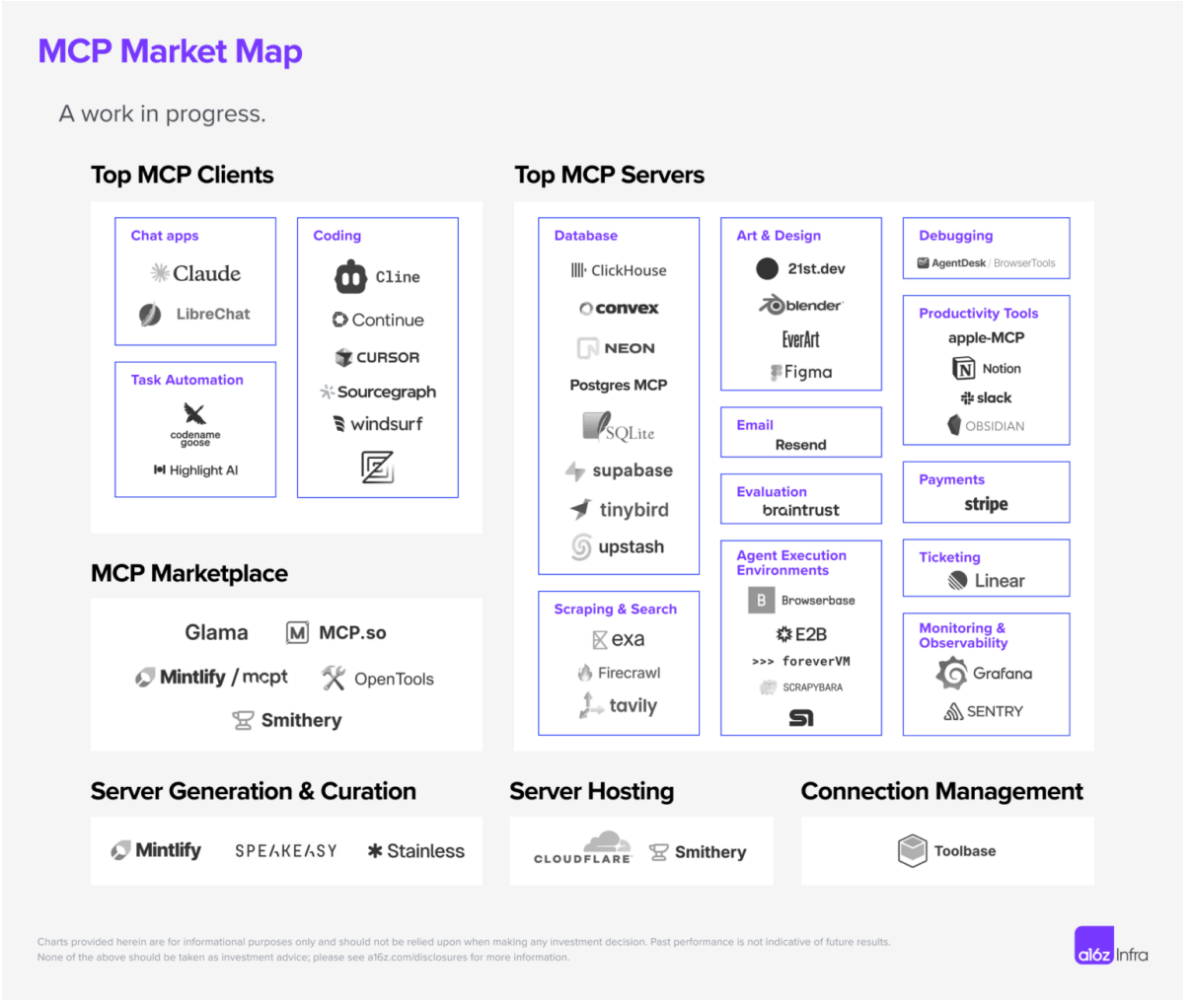
Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard
  - Seamless workflows across multiple applications
- **Enterprise Adoption is Accelerating**
  - **Block:** Automating workflows with MCP integration
  - **Snowflake:** Connecting enterprise data seamlessly
  - **MinIO:** Enabling AI access to storage systems
  - **Cloudflare:** Just launched remote MCP services
- Easy cross-app integrations for users

Big Players Are Moving Fast

- **Early Pioneers**
  - Claude Desktop, Cursor & Microsoft
  - First Movers Setting the Standard
  - Seamless workflows across multiple applications
- **Enterprise Adoption is Accelerating**
  - **Block:** Automating workflows with MCP integration
  - **Snowflake:** Connecting enterprise data seamlessly
  - **MinIO:** Enabling AI access to storage systems
  - **Cloudflare:** Just launched remote MCP services
- Easy cross-app integrations for users
- Platforms like **Agent.ai with Cursor** - The HubSpot moment for AI development

The Growing MCP Ecosystem



Workflow Automation Revolution

Workflow Automation Revolution

- Pro tip: use MCP in an app like Claude or Cursor to feel the power of MCP

Workflow Automation Revolution

- Pro tip: use MCP in an app like Claude or Cursor to feel the power of MCP
- Customer support agents with instant CRM integration

Workflow Automation Revolution

- Pro tip: use MCP in an app like Claude or Cursor to feel the power of MCP
- Customer support agents with instant CRM integration
- Data analysis across multiple systems without custom code

Workflow Automation Revolution

- Pro tip: use MCP in an app like Claude or Cursor to feel the power of MCP
- Customer support agents with instant CRM integration
- Data analysis across multiple systems without custom code
- Automated reporting and insights

Workflow Automation Revolution

- Pro tip: use MCP in an app like Claude or Cursor to feel the power of MCP
- Customer support agents with instant CRM integration
- Data analysis across multiple systems without custom code
- Automated reporting and insights
- Context-Aware Applications that can communicate with context and other apps easily

Workflow Automation Revolution

- Pro tip: use MCP in an app like Claude or Cursor to feel the power of MCP
- Customer support agents with instant CRM integration
- Data analysis across multiple systems without custom code
- Automated reporting and insights
- Context-Aware Applications that can communicate with context and other apps easily
- Personal assistants with deep system access (Claude Desktop)

Workflow Automation Revolution

- Pro tip: use MCP in an app like Claude or Cursor to feel the power of MCP
- Customer support agents with instant CRM integration
- Data analysis across multiple systems without custom code
- Automated reporting and insights
- Context-Aware Applications that can communicate with context and other apps easily
- Personal assistants with deep system access (Claude Desktop)
- Development environments with intelligent tooling (Claude-Code, Cursor)

Workflow Automation Revolution

- Pro tip: use MCP in an app like Claude or Cursor to feel the power of MCP
- Customer support agents with instant CRM integration
- Data analysis across multiple systems without custom code
- Automated reporting and insights
- Context-Aware Applications that can communicate with context and other apps easily
- Personal assistants with deep system access (Claude Desktop)
- Development environments with intelligent tooling (Claude-Code, Cursor)
- Multi-Language Support (Python, TypeScript, Swift, Kotlin, Java, Go)

Business Impact: Enterprise ROI

- **Cost Revolution**

Business Impact: Enterprise ROI

- **Cost Revolution**
  - Eliminates redundant integration development

Business Impact: Enterprise ROI

- **Cost Revolution**
  - Eliminates redundant integration development
  - Reduces maintenance overhead by 90%+

Business Impact: Enterprise ROI

- **Cost Revolution**
  - Eliminates redundant integration development
  - Reduces maintenance overhead by 90%+
- **Speed to Market**

Business Impact: Enterprise ROI

- **Cost Revolution**
  - Eliminates redundant integration development
  - Reduces maintenance overhead by 90%+
- **Speed to Market**
  - Standard tools work across all AI applications

Business Impact: Enterprise ROI

- **Cost Revolution**
  - Eliminates redundant integration development
  - Reduces maintenance overhead by 90%+
- **Speed to Market**
  - Standard tools work across all AI applications
  - Days instead of months for new AI features

Business Impact: Enterprise ROI

- **Cost Revolution**
  - Eliminates redundant integration development
  - Reduces maintenance overhead by 90%+
- **Speed to Market**
  - Standard tools work across all AI applications
  - Days instead of months for new AI features
- **The New Economics**

Business Impact: Enterprise ROI

- **Cost Revolution**
  - Eliminates redundant integration development
  - Reduces maintenance overhead by 90%+
- **Speed to Market**
  - Standard tools work across all AI applications
  - Days instead of months for new AI features
- **The New Economics**
  - Solo founders competing with enterprise teams

Business Impact: Enterprise ROI

- **Cost Revolution**
  - Eliminates redundant integration development
  - Reduces maintenance overhead by 90%+
- **Speed to Market**
  - Standard tools work across all AI applications
  - Days instead of months for new AI features
- **The New Economics**
  - Solo founders competing with enterprise teams
  - Lower barriers, higher innovation velocity

⚠️ Security Risks: MCP Vulnerabilities

- **Critical "Tool Poisoning Attacks" Discovered**

⚠️ Security Risks: MCP Vulnerabilities

- **Critical "Tool Poisoning Attacks" Discovered**
- Malicious instructions embedded in MCP tool descriptions

⚠️ Security Risks: MCP Vulnerabilities

- **Critical "Tool Poisoning Attacks" Discovered**
- Malicious instructions embedded in MCP tool descriptions
- Instructions invisible to users but visible to LLMs

⚠️ Security Risks: MCP Vulnerabilities

- **Critical "Tool Poisoning Attacks" Discovered**
- Malicious instructions embedded in MCP tool descriptions
- Instructions invisible to users but visible to LLMs
- **Potential Damage:** Data exfiltration, hijacked agent behavior

⚠️ Security Risks: MCP Vulnerabilities

- **Critical "Tool Poisoning Attacks" Discovered**
- Malicious instructions embedded in MCP tool descriptions
- Instructions invisible to users but visible to LLMs
- **Potential Damage:** Data exfiltration, hijacked agent behavior
- **Mitigation Strategies:** Tool pinning, clear UI patterns, cross-server protection

⚠️ Security Risks: MCP Vulnerabilities

- **Critical "Tool Poisoning Attacks" Discovered**
- Malicious instructions embedded in MCP tool descriptions
- Instructions invisible to users but visible to LLMs
- **Potential Damage:** Data exfiltration, hijacked agent behavior
- **Mitigation Strategies:** Tool pinning, clear UI patterns, cross-server protection
- **Reference:** Invariant Security Research

⚠️ Security Risks: MCP Vulnerabilities

- **Critical "Tool Poisoning Attacks" Discovered**
- Malicious instructions embedded in MCP tool descriptions
- Instructions invisible to users but visible to LLMs
- **Potential Damage:** Data exfiltration, hijacked agent behavior
- **Mitigation Strategies:** Tool pinning, clear UI patterns, cross-server protection
- **Reference:** Invariant Security Research

Key Takeaway: Extensive guardrailing needed for production deployments

The Protocol "Wars"

The Protocol "Wars"

MCP vs A2A vs ACP

Three Major Players Competing/Complimenting? for Standardization:

The Protocol "Wars"

MCP vs A2A vs ACP

Three Major Players Competing/Complimenting? for Standardization:

MCP (Anthropic): AI-to-tool communication and data access

The Protocol "Wars"

MCP vs A2A vs ACP

Three Major Players Competing/Complimenting? for Standardization:

MCP (Anthropic): AI-to-tool communication and data access

A2A (Google): Agent-to-agent system communication, secure collaboration

The Protocol "Wars"

MCP vs A2A vs ACP

Three Major Players Competing/Complimenting? for Standardization:

MCP (Anthropic): AI-to-tool communication and data access

A2A (Google): Agent-to-agent system communication, secure collaboration

ACP (IBM Research): Agent Communication Protocol, focuses on practical adoption first

The Protocol "Wars"

MCP vs A2A vs ACP

Three Major Players Competing/Complimenting? for Standardization:

MCP (Anthropic): AI-to-tool communication and data access

A2A (Google): Agent-to-agent system communication, secure collaboration

ACP (IBM Research): Agent Communication Protocol, focuses on practical adoption first

The Stakes: Who becomes the "HTTP" of AI agent communication?

The Protocol "Wars"

MCP vs A2A vs ACP

Three Major Players Competing/Complimenting? for Standardization:

MCP (Anthropic): AI-to-tool communication and data access

A2A (Google): Agent-to-agent system communication, secure collaboration

ACP (IBM Research): Agent Communication Protocol, focuses on practical adoption first

The Stakes: Who becomes the "HTTP" of AI agent communication?

Current Reality: Fragmentation risk vs innovation through competition

Connect With Me

 Blog

 LinkedIn

 Twitter/X

 YouTube

 Email: lucasenkrateia@gmail.com