MCP and Agents: Open-Source Foundations for Agent Trust, Safety, and Scale

TechXchange | October 6-7, 2025

Fred Arauju: IBM Research

Dean Wampler, Jeffrey Borek, Dave Nielsen: IBM and The AI Alliance

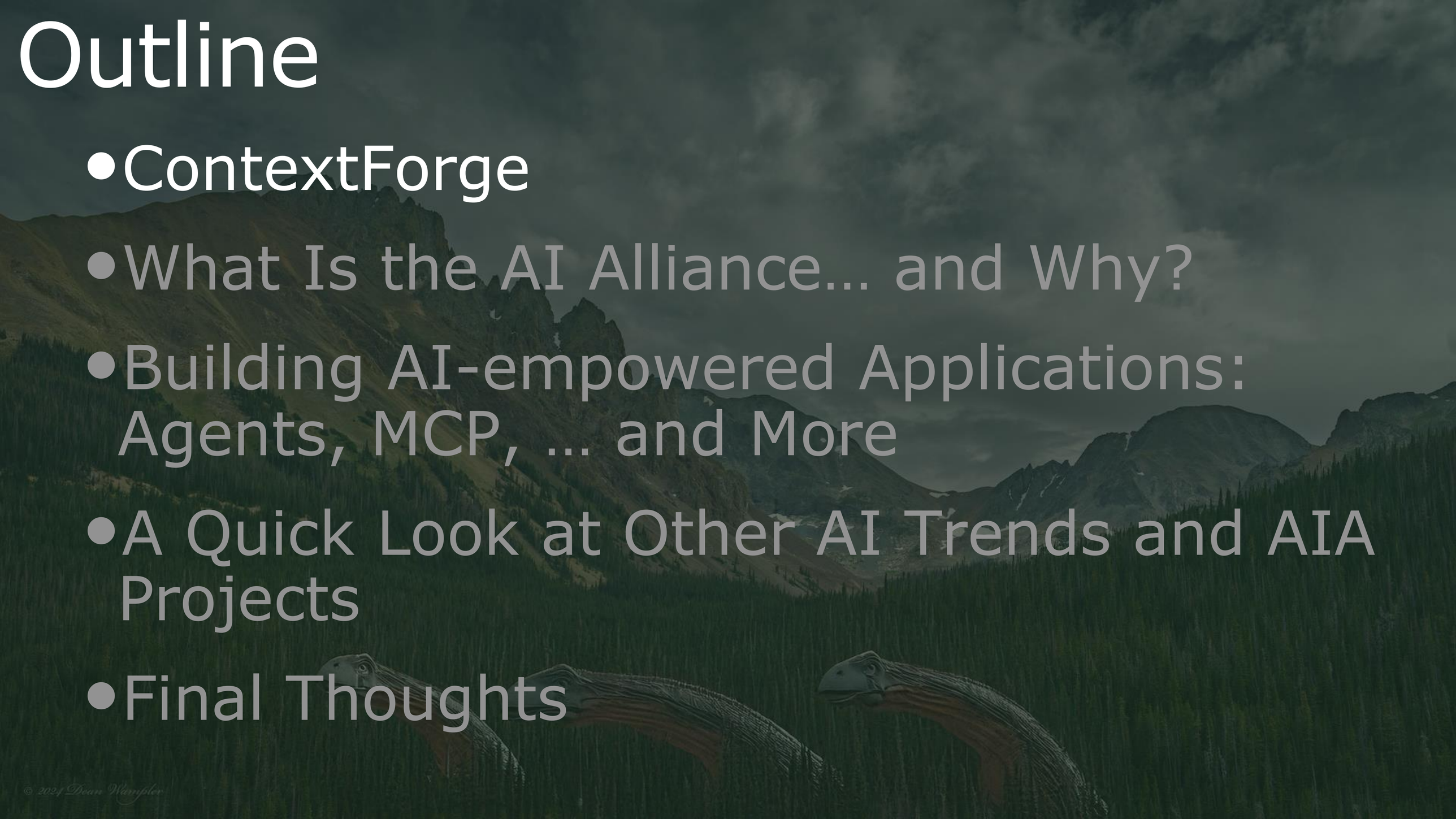
Outline

Outline

- ContextForge
- What Is the AI Alliance… and Why?
- Building AI-empowered Applications: Agents, MCP, … and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts

Outline

- ContextForge
- What Is the AI Alliance… and Why?
- Building AI-empowered Applications: Agents, MCP, … and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts

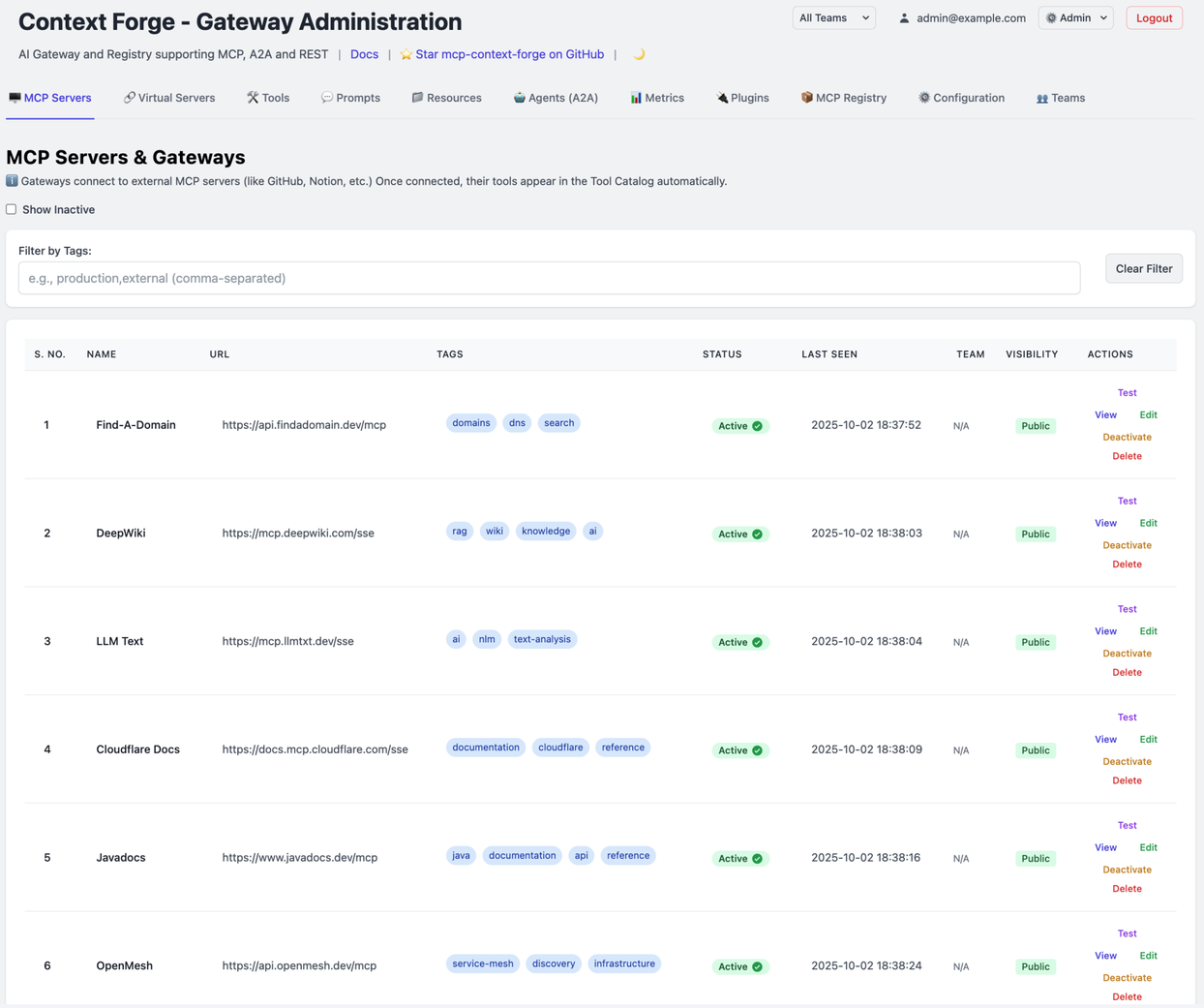


ContextForge
MCP Gateway

Secure Open-Source Gateway, Proxy and Registry for AI Agents and Tools

Unifying discovery, authentication, authorization, role-based access control, rate-limiting, observability, virtual servers, and protocol translation – with a security focus and configurable plugins

github.com/IBM/mcp-context-forge



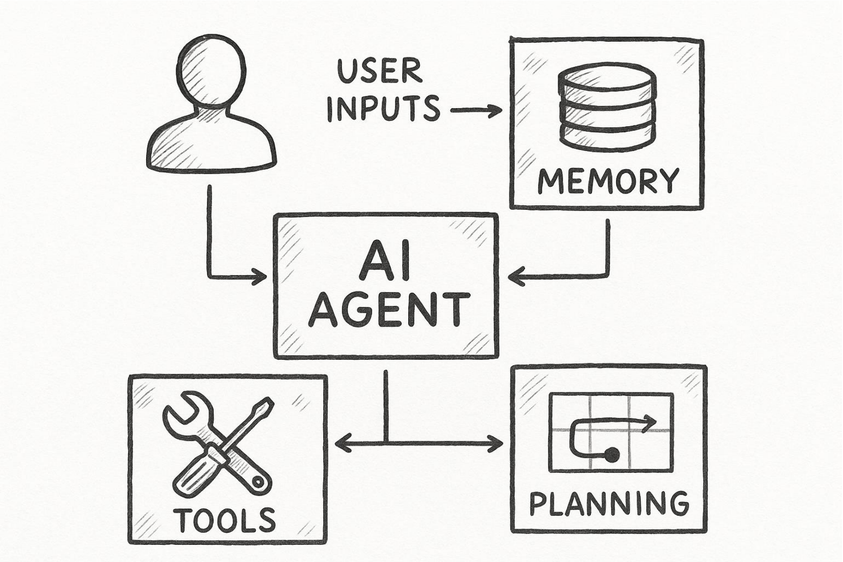
AI Agents use tools to accomplish complex tasks

AI Agent

A modular, goal-driven component that uses tools, memory, and reasoning to autonomously complete tasks via language models

These agents can plan, interact with APIs or other agents, and make decisions based on prompts, documents, or user input. They're often orchestrated in a multi-agent system to collaboratively solve complex problems

They typically use an agentic framework or orchestrator (e.g., langgraph, langchain, autogen, crew.ai) for tool execution



What can they do with tools?

Retrieve external information (e.g., web search, databases, RAG) as necessary, call other Agents or request user input

Generate artifacts (images, diagrams, word documents, excel files), interact with external APIs and systems using various Tools, run unit tests, etc.

https://github.com/IBM/mcp-context-forge

Agents and tools turn “thoughts” into actions

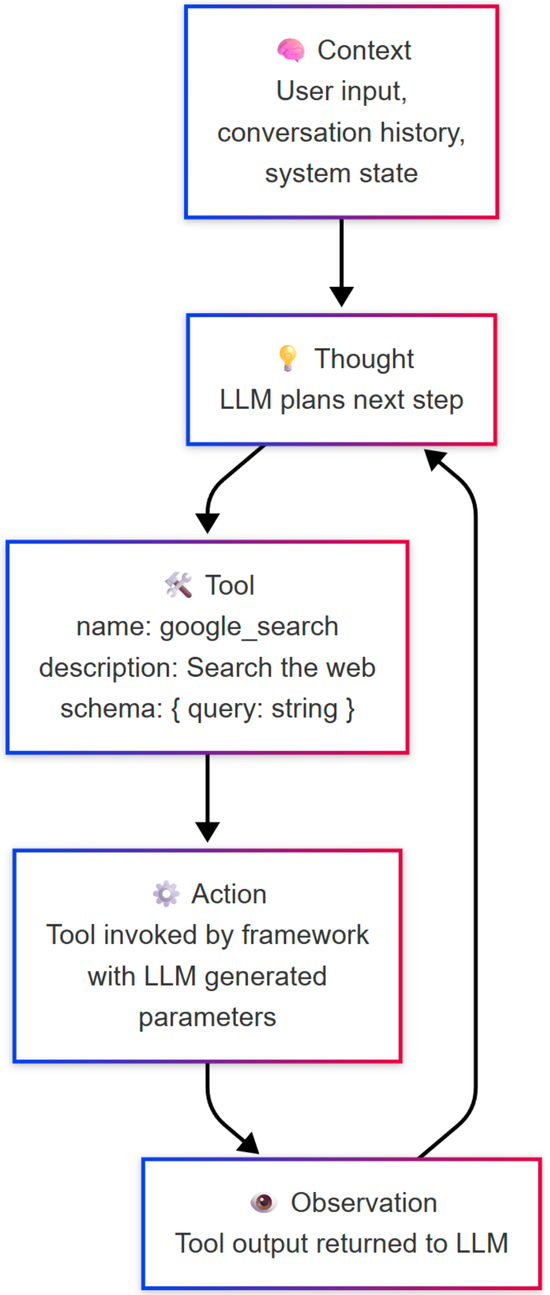
Large Language Models call Tools through "Agentic Frameworks”;
The LLM selects the right tool and parameters based on its description, then processes the output.

Example

```
name: google_search
description: Use this tool to search the internet, providing an input prompt.
input schema: {"query": "Latest News"}
```

MCP standardizes how AI Agents interact with Tools

- MCP de-couples AI Tools from the Agentic Platform
- Without MCP, each framework or AI tool would duplicate work, and LLMs couldn't be 'fine tuned' for standardized tool calling.



https://github.com/IBM/mcp-context-forge

Model Context Protocol (MCP) – "the USB-C for AI tools"

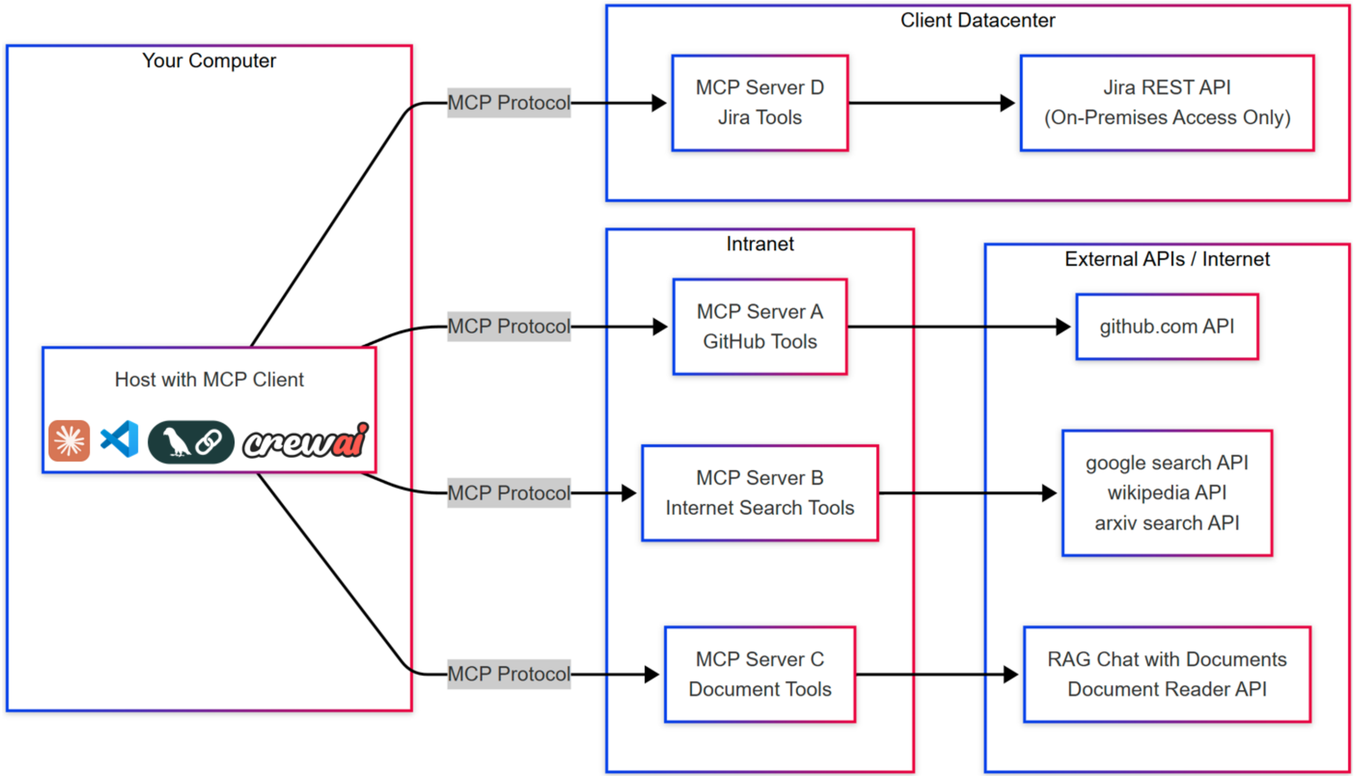
MCP Overview

- An open protocol introduced by Anthropic in November 2024 to standardize tool calling
- Enables a consistent interface to define how Agents and applications discover, invoke, and interact with tools and other context (prompts, resources)

Widely adopted: 15,000+ community servers developed since launch; wide adoption by major vendors

Still Evolving: the standard is rapidly evolving to resolve gaps in security, granular access controls, transparent tool usage, and user interaction, but many tools only implement a partial or older spec

ContextForge addresses these gaps



MCP Hosts: applications or AI tools that want to access data via MCP (VSCode+ Copilot/Cline/Continue, Langchain, Crew.AI, Claude Desktop)

MCP Clients: Protocol clients that maintain 1:1 connections with servers

MCP Servers: Lightweight programs that each expose specific capabilities through Model Context Protocol

https://github.com/IBM/mcp-context-forge

ContextForge addresses challenges with the MCP Ecosystem

MCP challenges

MCP gained rapid adoption — but the ecosystem evolved unevenly. Many tools only partially implement the spec, and integration challenges remain:

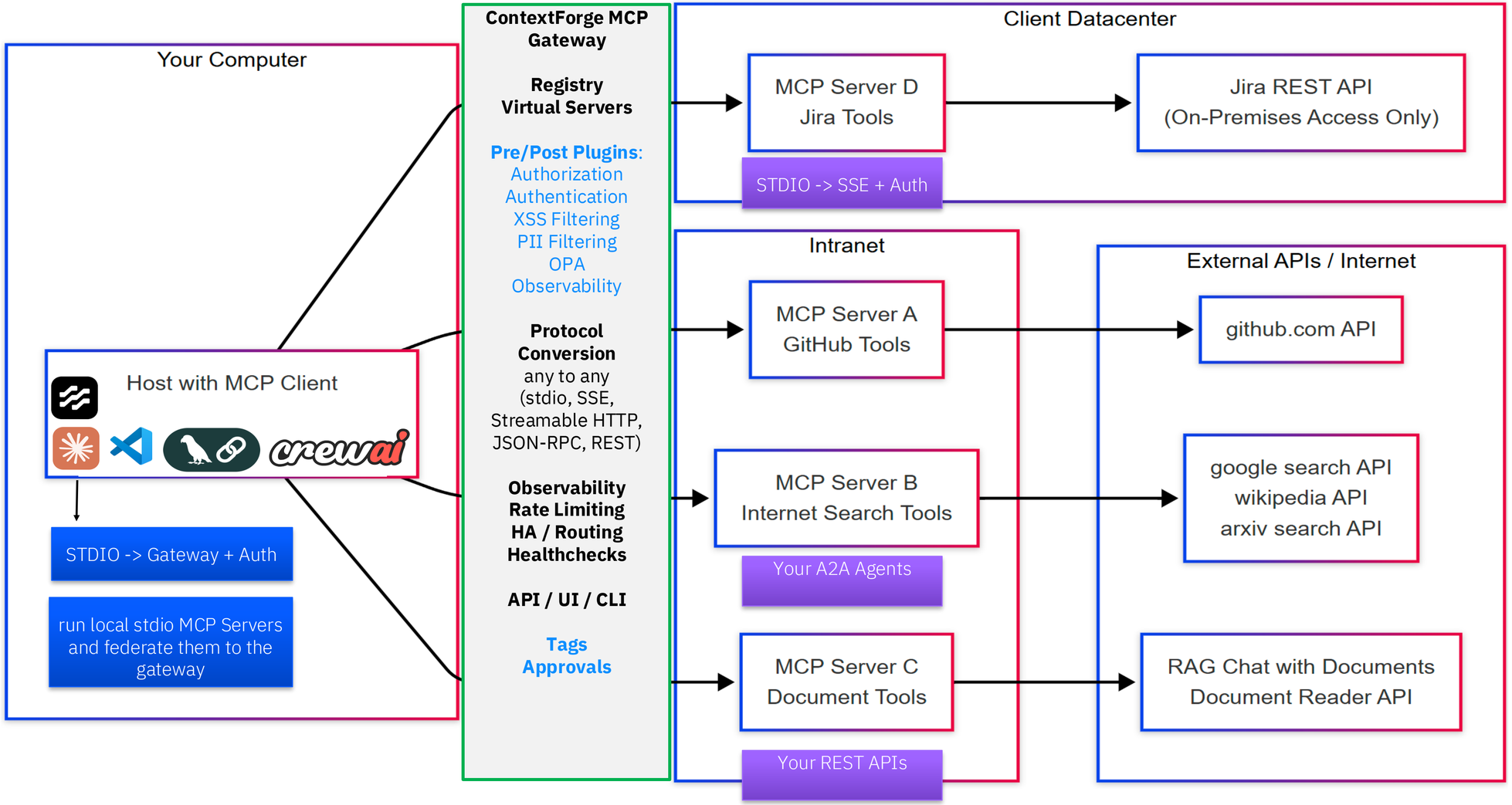
- Existing tools: REST endpoints must be rewritten to become MCP-compliant.
- Protocol and security inconsistency: some use JWT authentication, others OAuth2, many use nothing at all – while most servers are still developed to stdio / SSE transport (instead of the newer streamable HTTP).
- Integration complexity: tools are scattered across servers, each with its own config, retry logic, and monitoring gaps

MCP Gateway emerges as a mandatory pattern when deploying MCP in the enterprise

- Acts as a secure, unified proxy between AI agents and tool servers, easily deployable in remote environments.
- Convert between different transports, add authorization, security, observability, retry logic, and tool lifecycle controls – allowing you to quickly convert non-compliant MCP servers to the latest standard, and add security, observability, etc.
- Wrap any REST API and exposes it as a typed, discoverable MCP-compatible tool
- Reusable building block, easily embedded into other products and tools

https://github.com/IBM/mcp-context-forge

ContextForge: open source secure, modular proxy for MCP



https://github.com/IBM/mcp-context-forge

Security-first design

Core Security Mission

Protect against untrusted MCP servers

Sanitize all inputs/outputs

Policy-based access control

Pluggable security middleware

Isolation Capabilities

Separate tool namespaces

Independent auth configs

Per-server rate limits

Custom security policies

Enterprise Security

Policy as Code with OPA

SSO Integration (OAuth/SAML), JWT

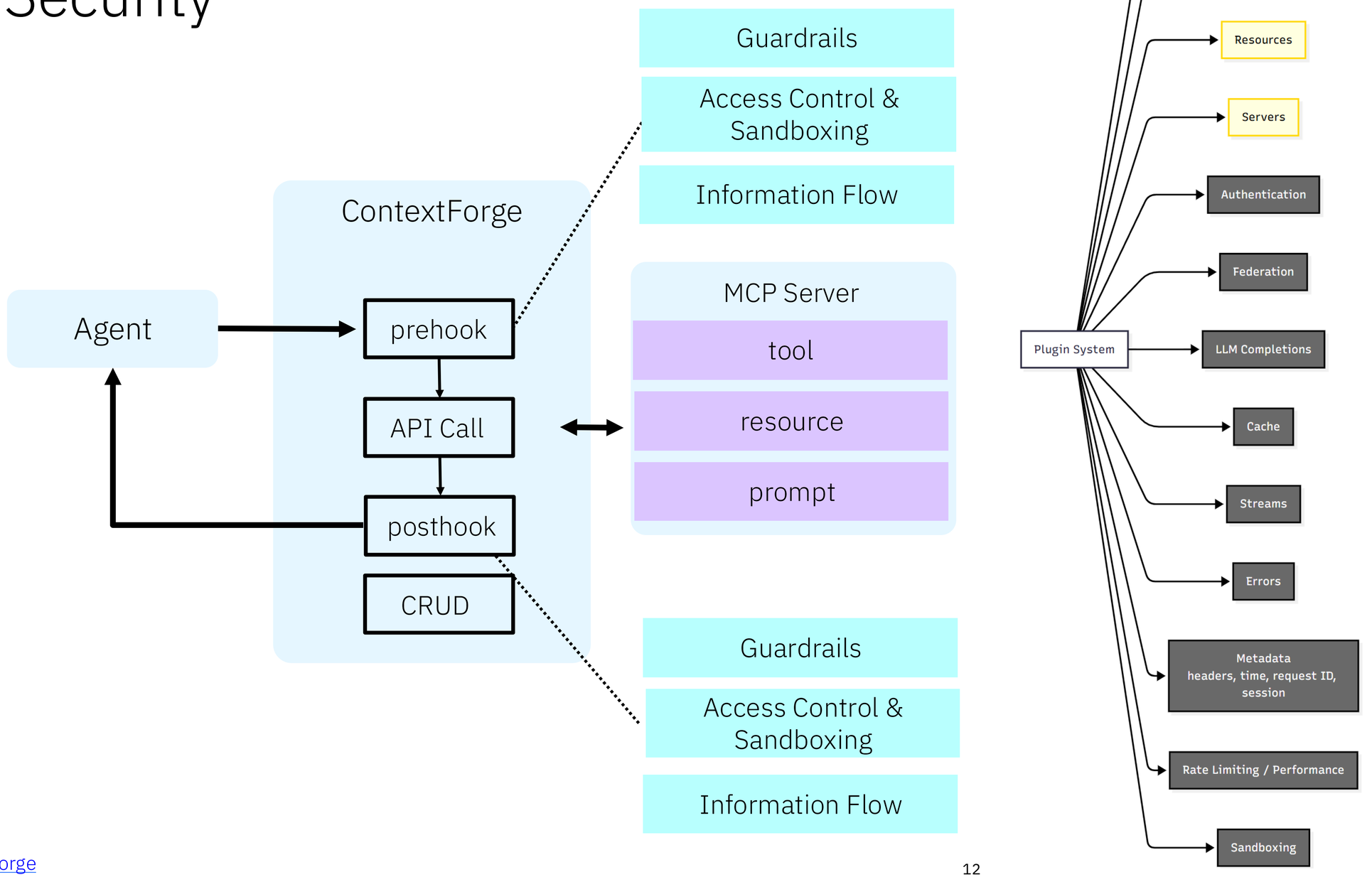
RBAC, Multi-tenancy, Database Encryption

Observability (OpenTelemetry)

https://github.com/IBM/mcp-context-forge

ContextForge with Pluggable Security

Security extensions implemented as LSM-style hooks to ContextForge



Community engagement and growth

2.6k+ stars

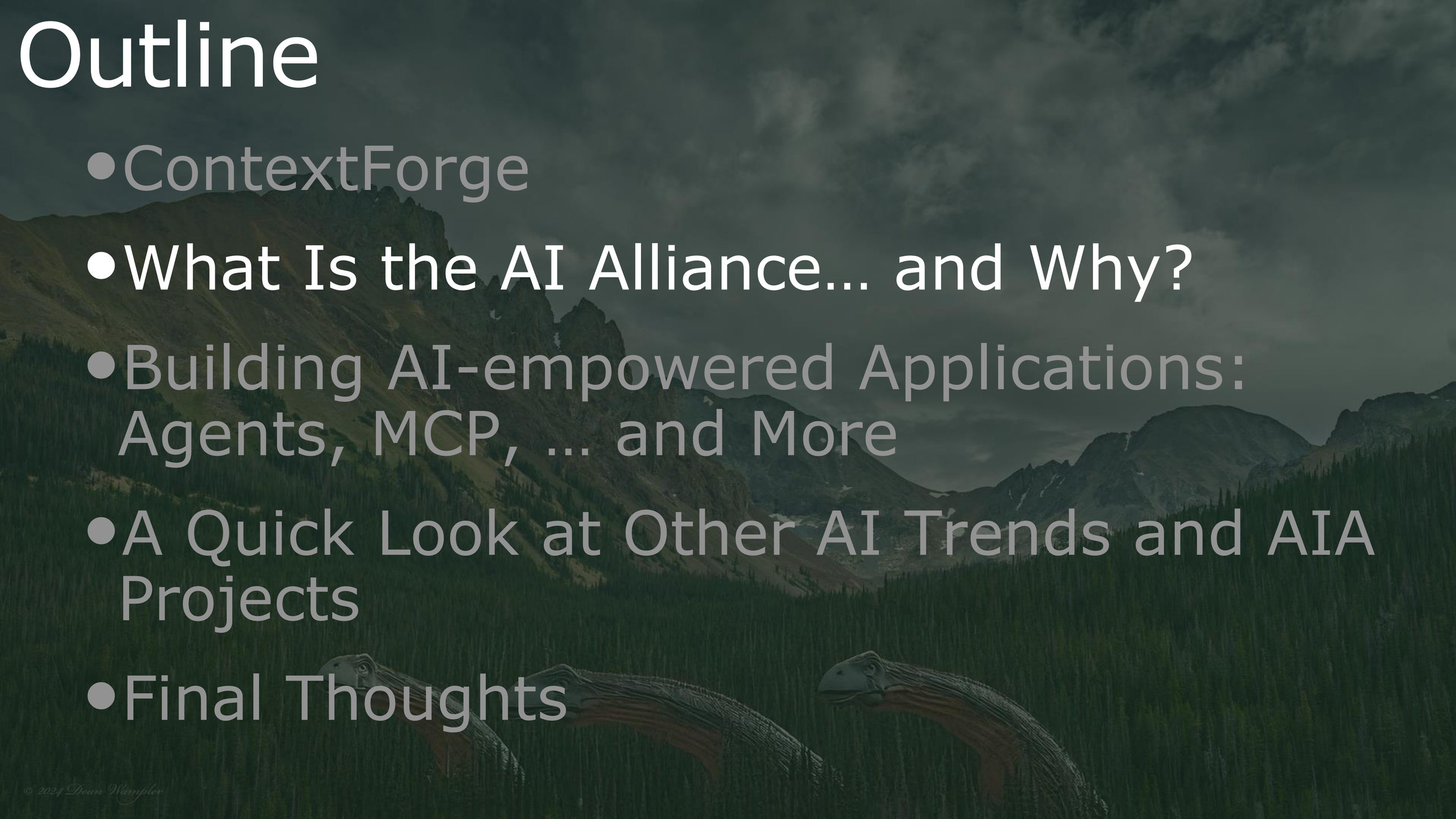
319 forks

57 contributors

The most popular MCP Gateway! – with highest number of features and a security focus

Outline

- ContextForge
- What Is the AI Alliance… and Why?
- Building AI-empowered Applications: Agents, MCP, … and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts



Trends in Artificial Intelligence - Closed or Open?

ANNALS OF TECHNOLOGY

THE INSIDE STORY OF MICROSOFT'S PARTNERSHIP WITH OPENAI

The companies had honed a protocol for releasing artificial intelligence ambitiously but safely. Then OpenAI's board exploded all their carefully laid plans.

By Charles Duhigg

December 1, 2023

AI Alliance

Meta

IBM

LUX ET VERITAS

Meta and IBM form open-source alliance to counter big AI players

NASA, Intel, Yale University and more related bodies are involved.

Sarah Fielding

Tue, Dec 5, 2023 · 2 min read

1

FRONTIER MODEL FORUM

THE LINUX FOUNDATION

NASA

intel

"The future of AI is open — no matter what some say."

Dario Gill, SVP and Director of Research, IBM

aialliance.org

The AI Alliance brings together organizations, people, and resources to accelerate ***open innovation***, ***technology development*** and ***adoption***.

Launched December 5, 2023

linkedin.com/company/the-aialliance/

bsky.app/profile/aialliance.bsky.social

AI Alliance

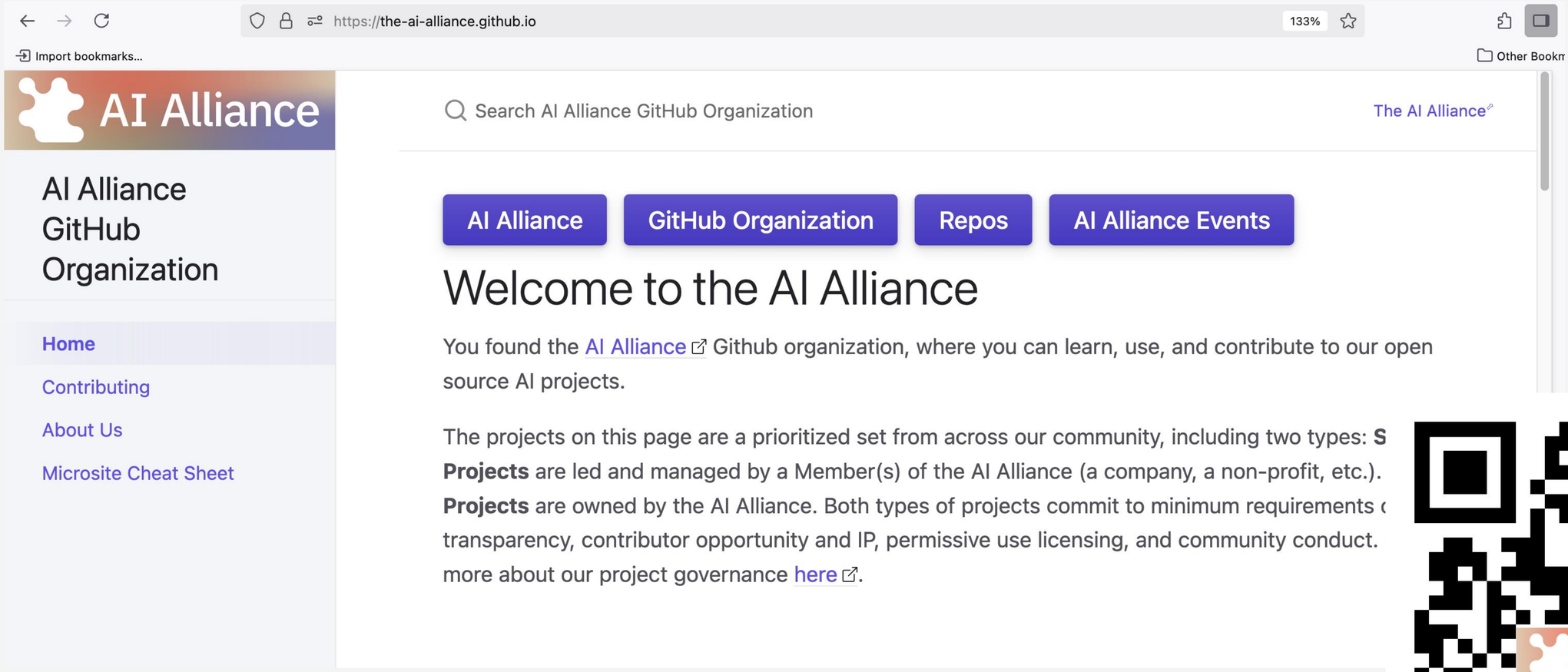
Map of Members

Member organizations in the AI Alliance comprise academia, commercial, research and non-profits and span the globe.

Our core beliefs in AI that is open is the tie that binds us, despite our differences.

The AI Alliance is made up of ~200 organizations in 24+ countries, and growing

Numerous Projects:



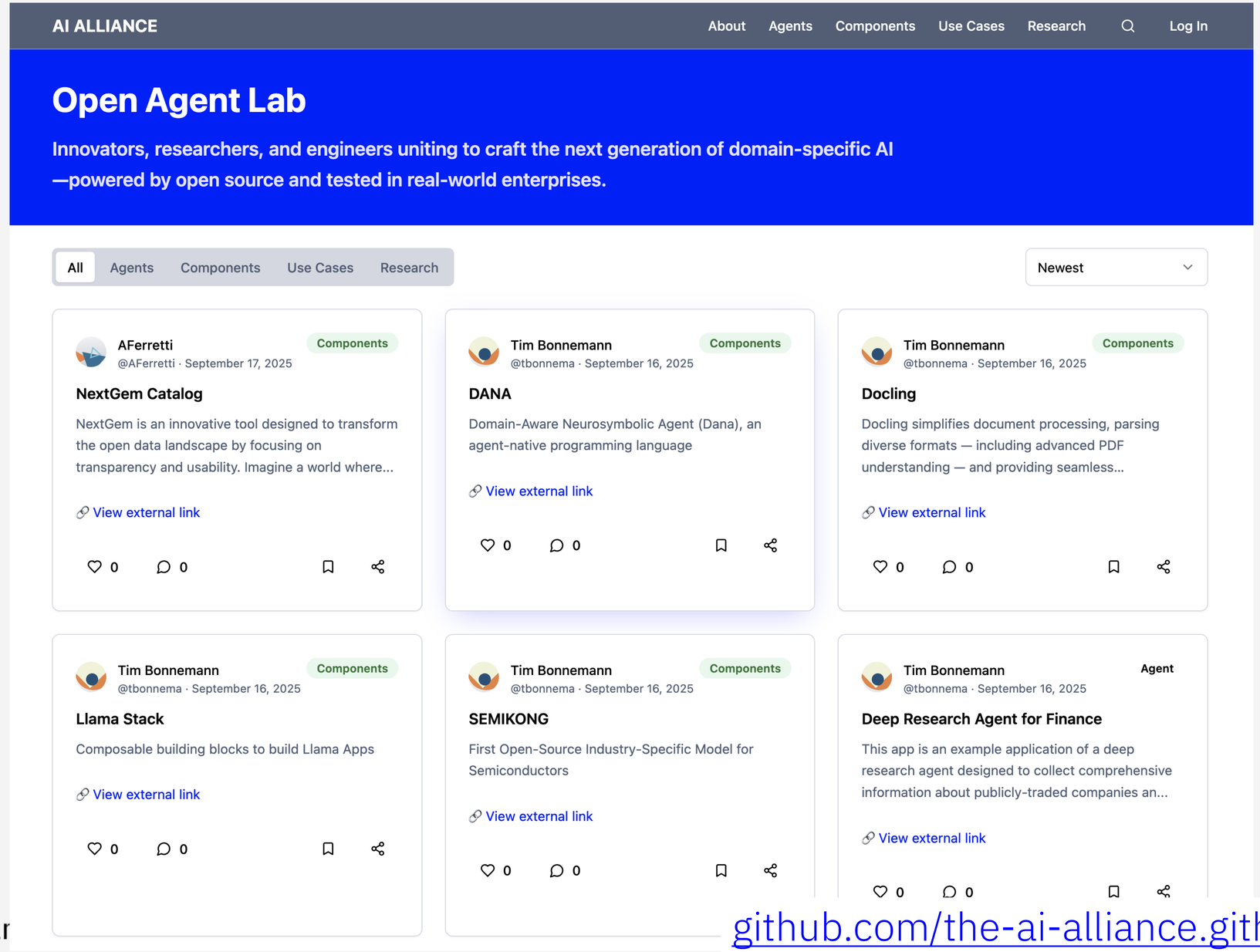
AI Alliance

github.com/the-ai-alliance.github.io

Outline

- ContextForge
- What Is the AI Alliance… and Why?
- Building AI-empowered Applications: Agents, MCP, … and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts

Open Agent Lab

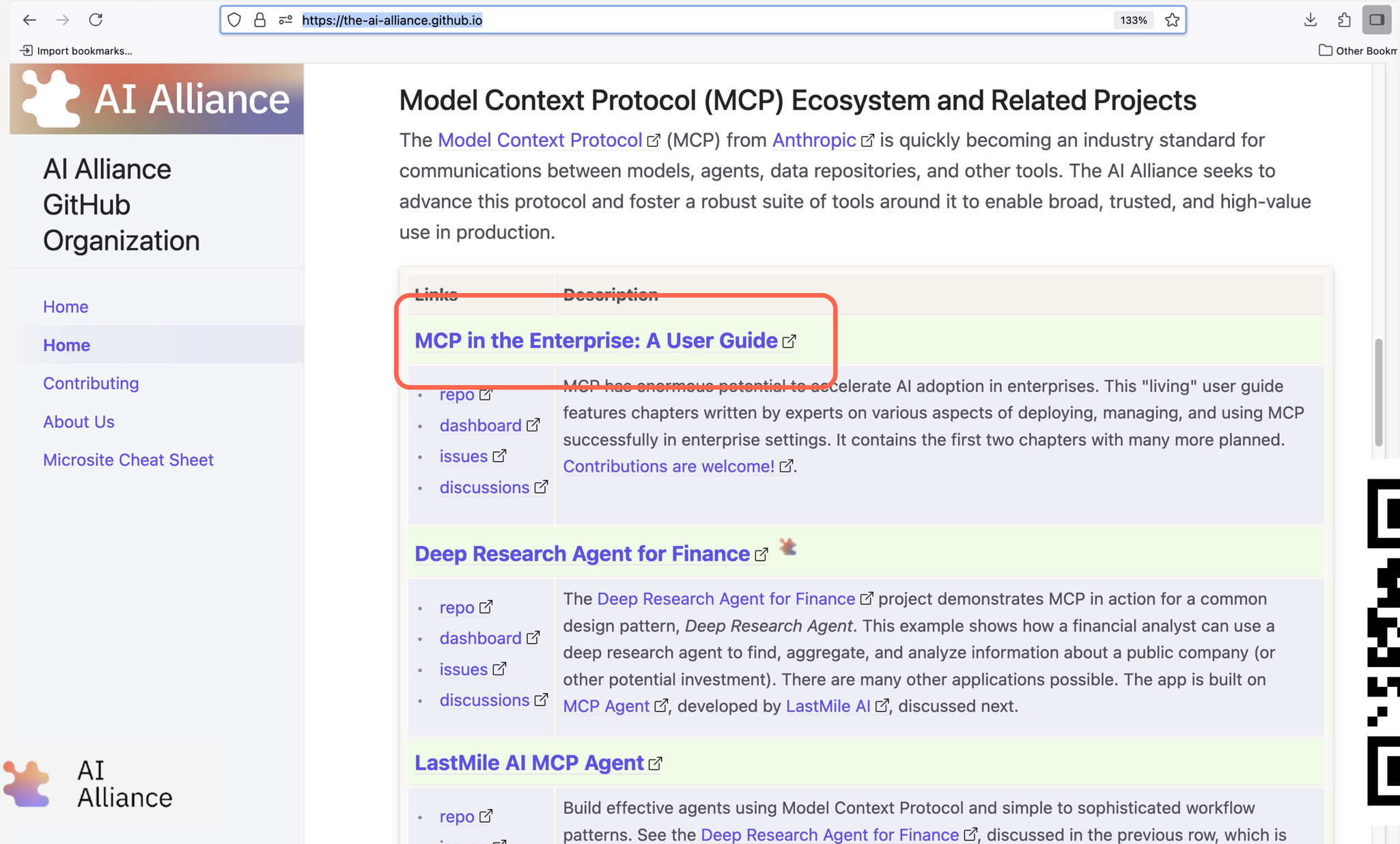


AI Alliance

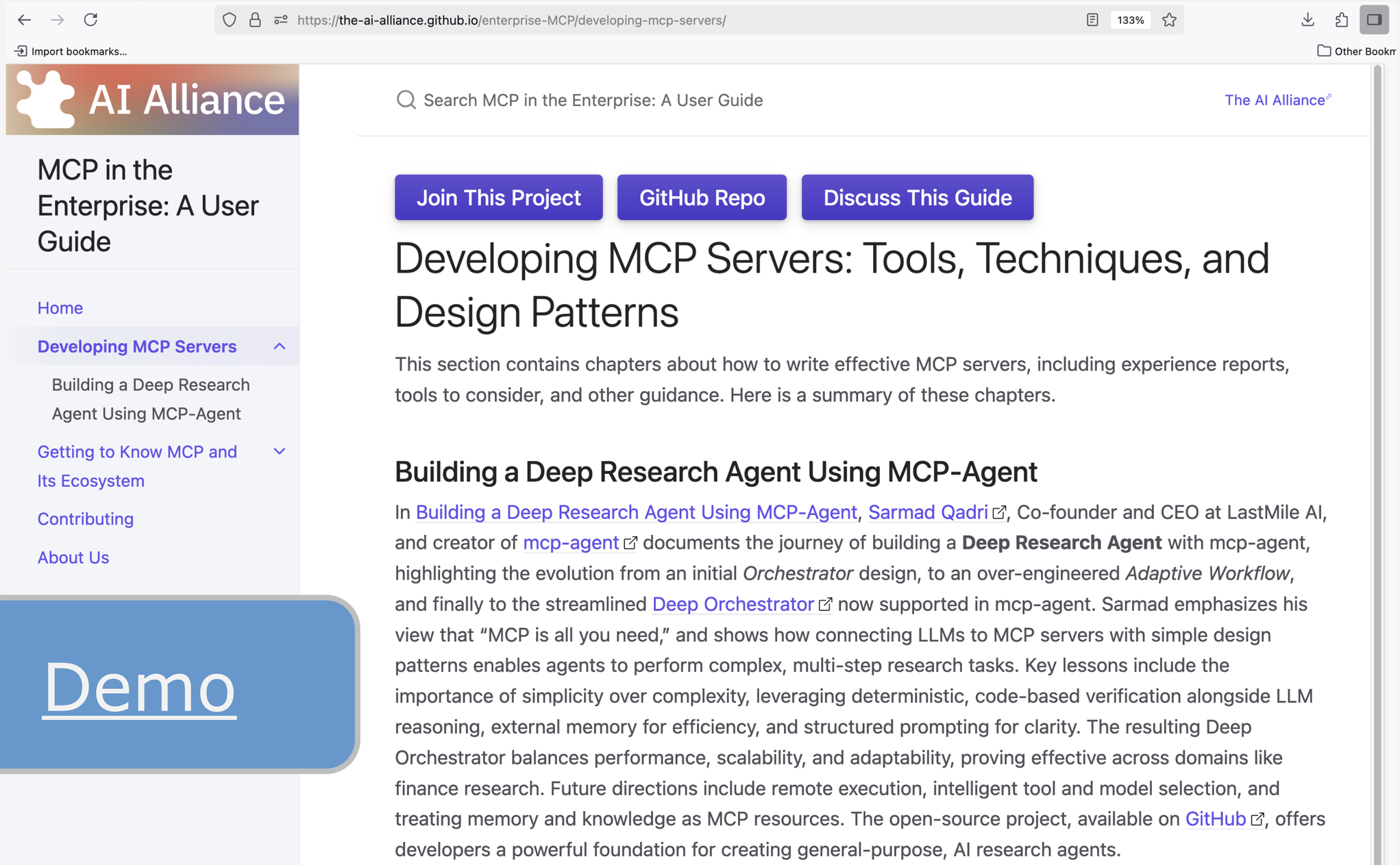
github.com/the-ai-alliance.github.io

AI Alliance

MCP Projects



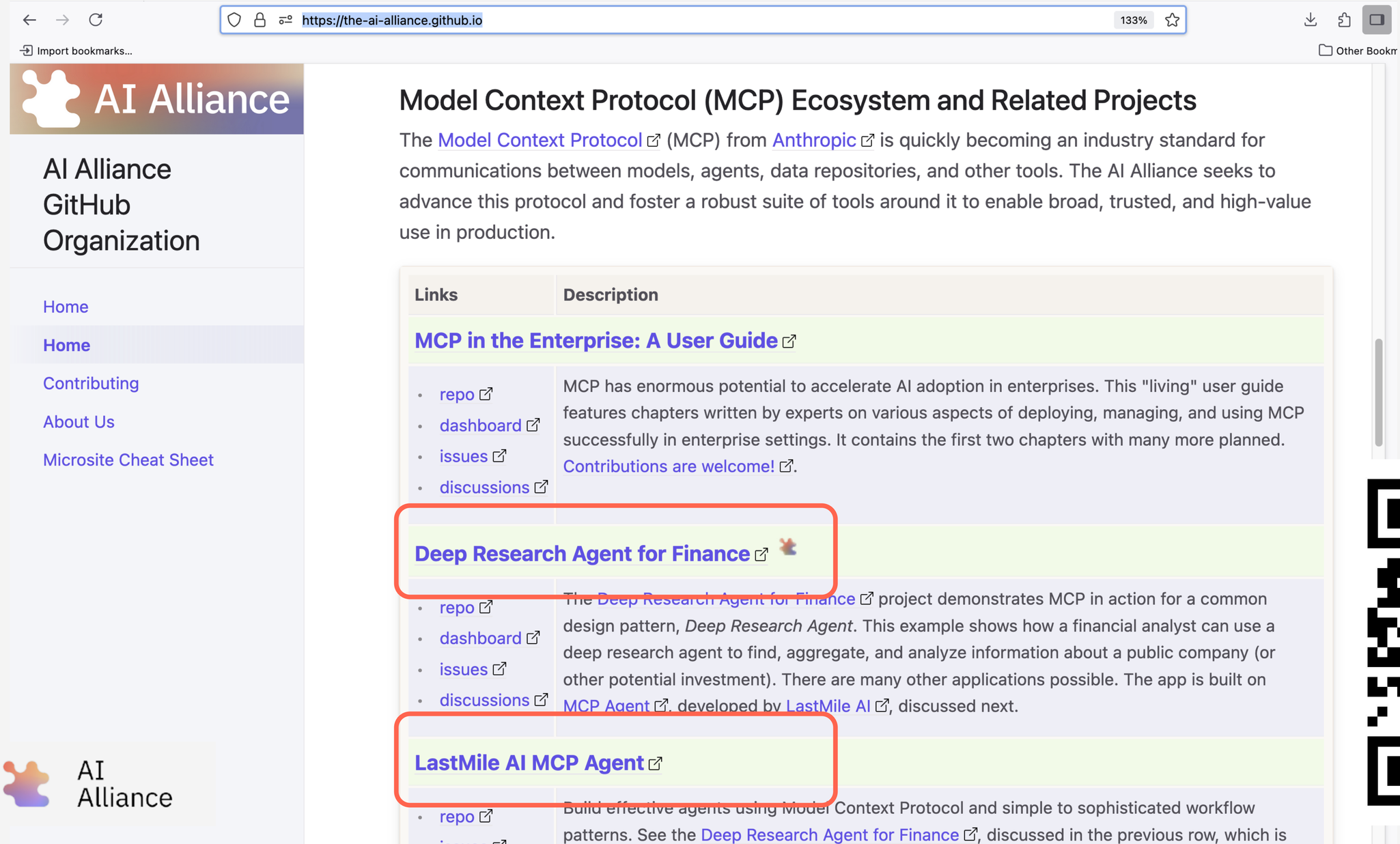
User Guide: MCP in the Enterprise



Demo

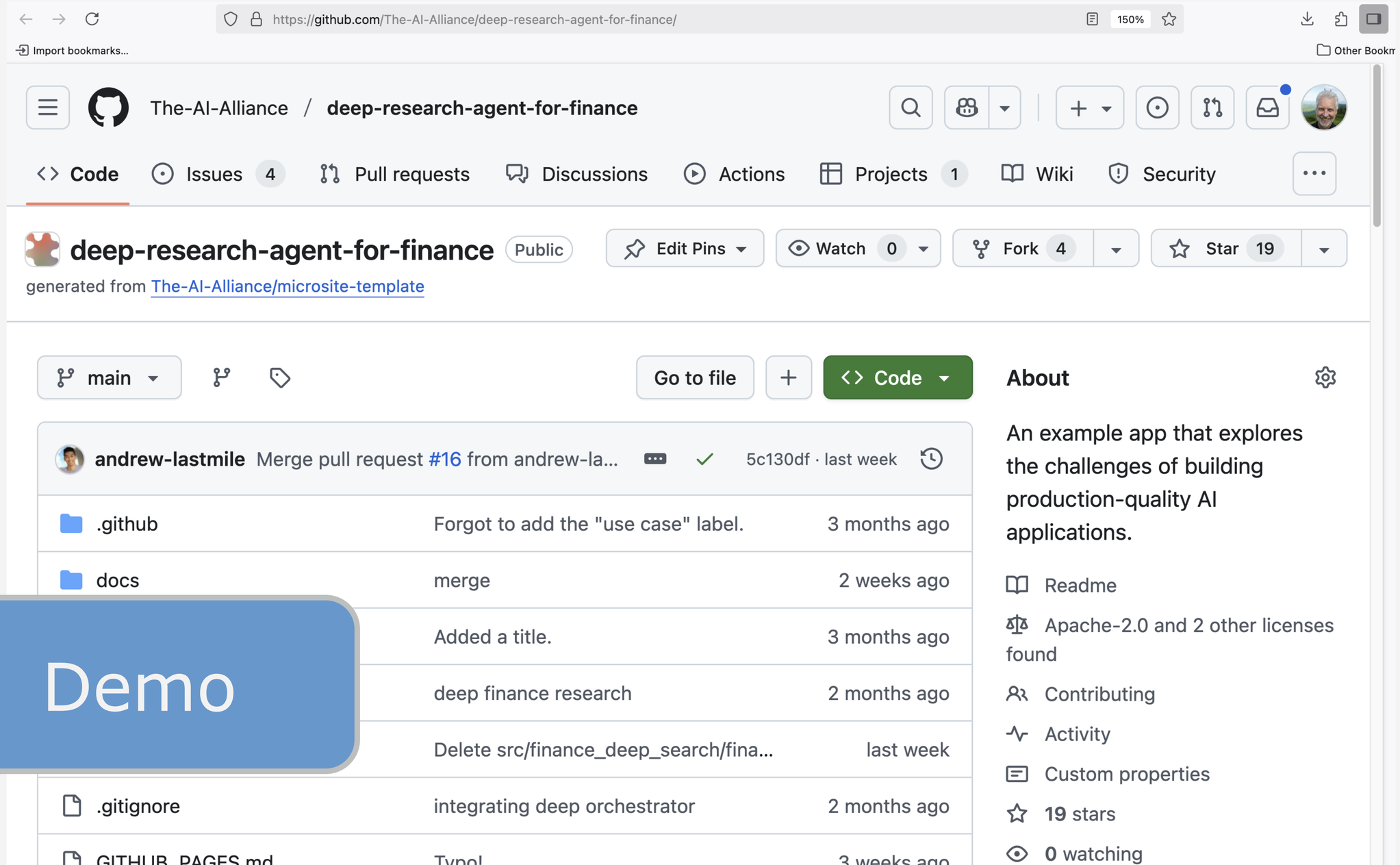
AI Alliance

MCP + Agents



AI Alliance

MCP + Agents: Deep Research App

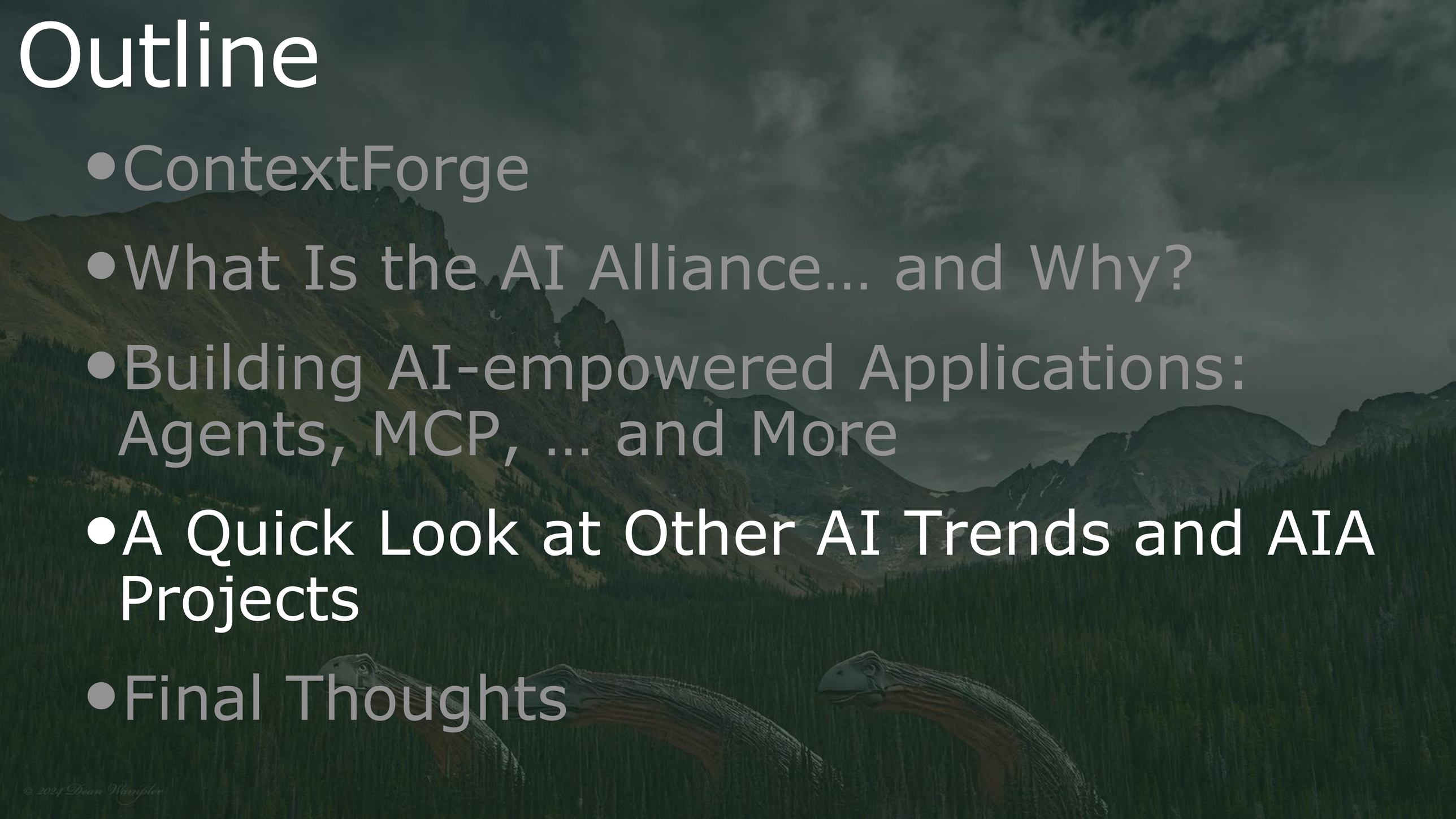


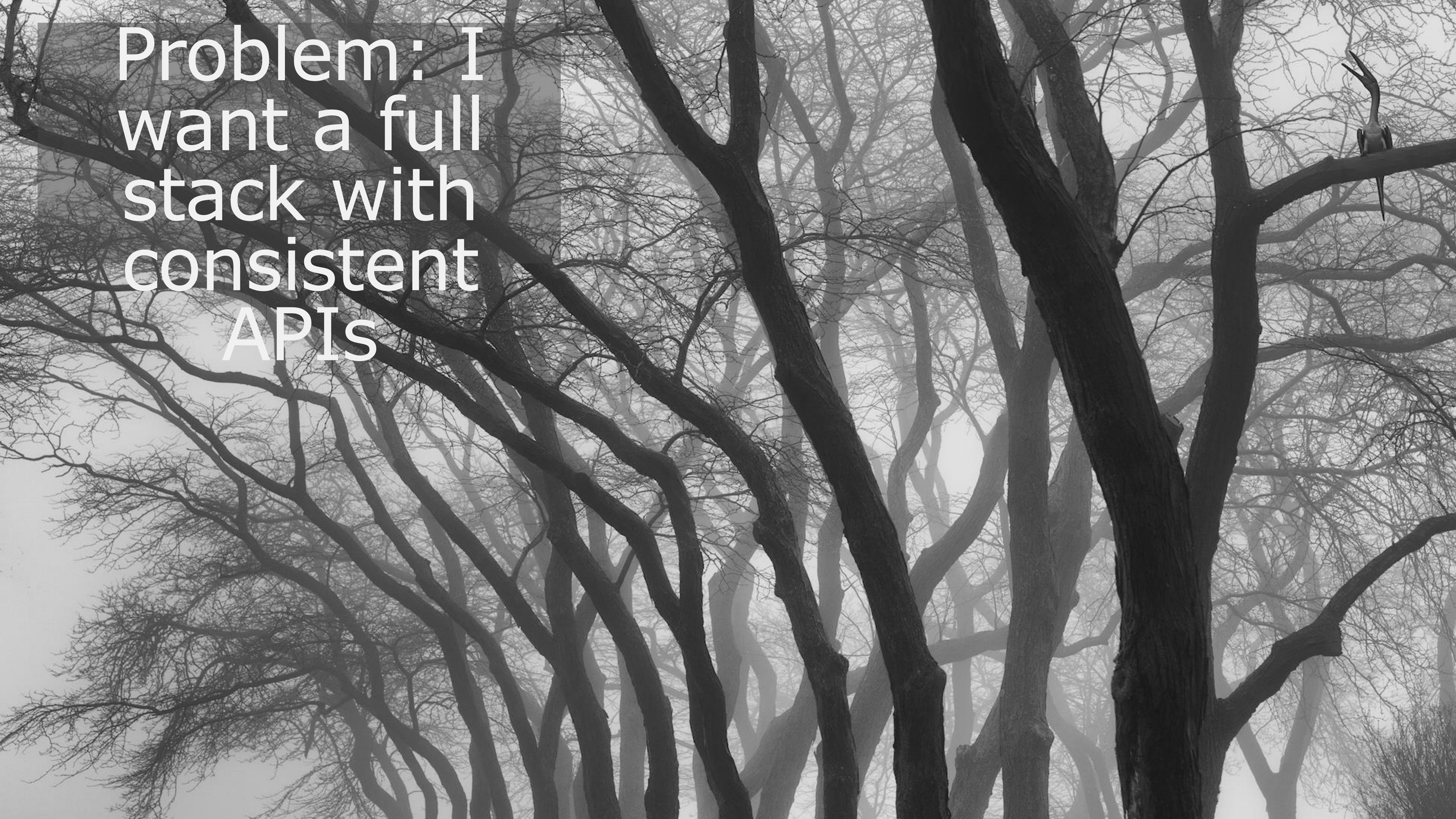
Demo

AI Alliance

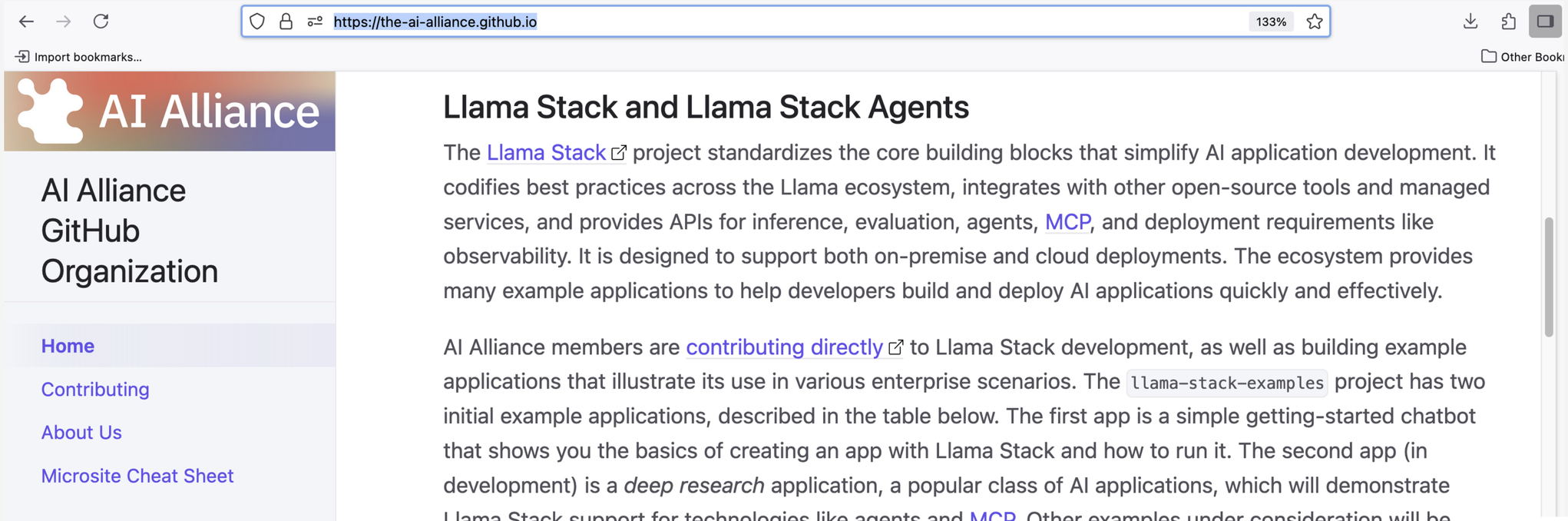
Outline

- ContextForge
- What Is the AI Alliance… and Why?
- Building AI-empowered Applications: Agents, MCP, … and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts




Problem: I want a full stack with consistent APIs

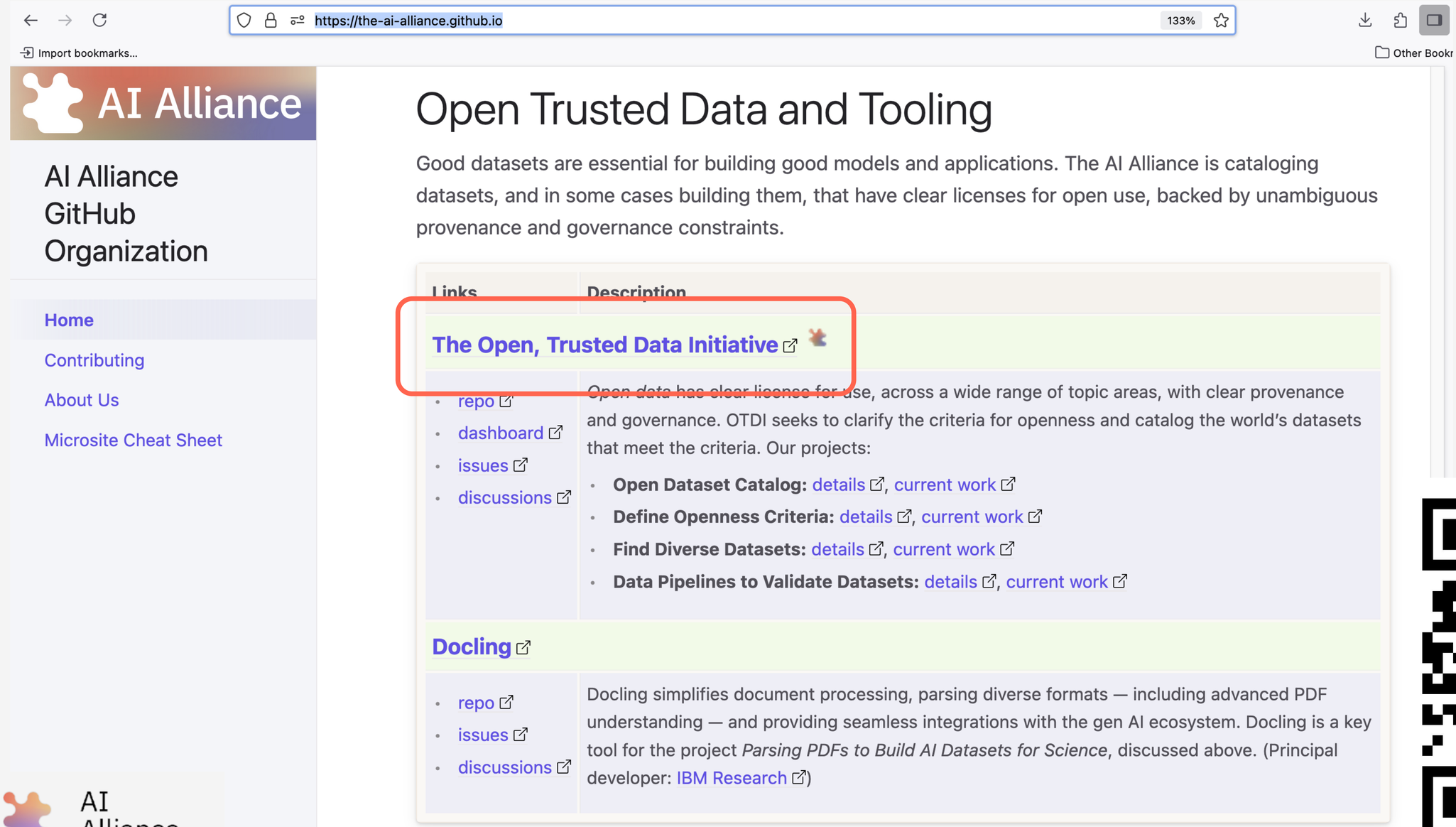
Solution: Llama Stack



AI Alliance

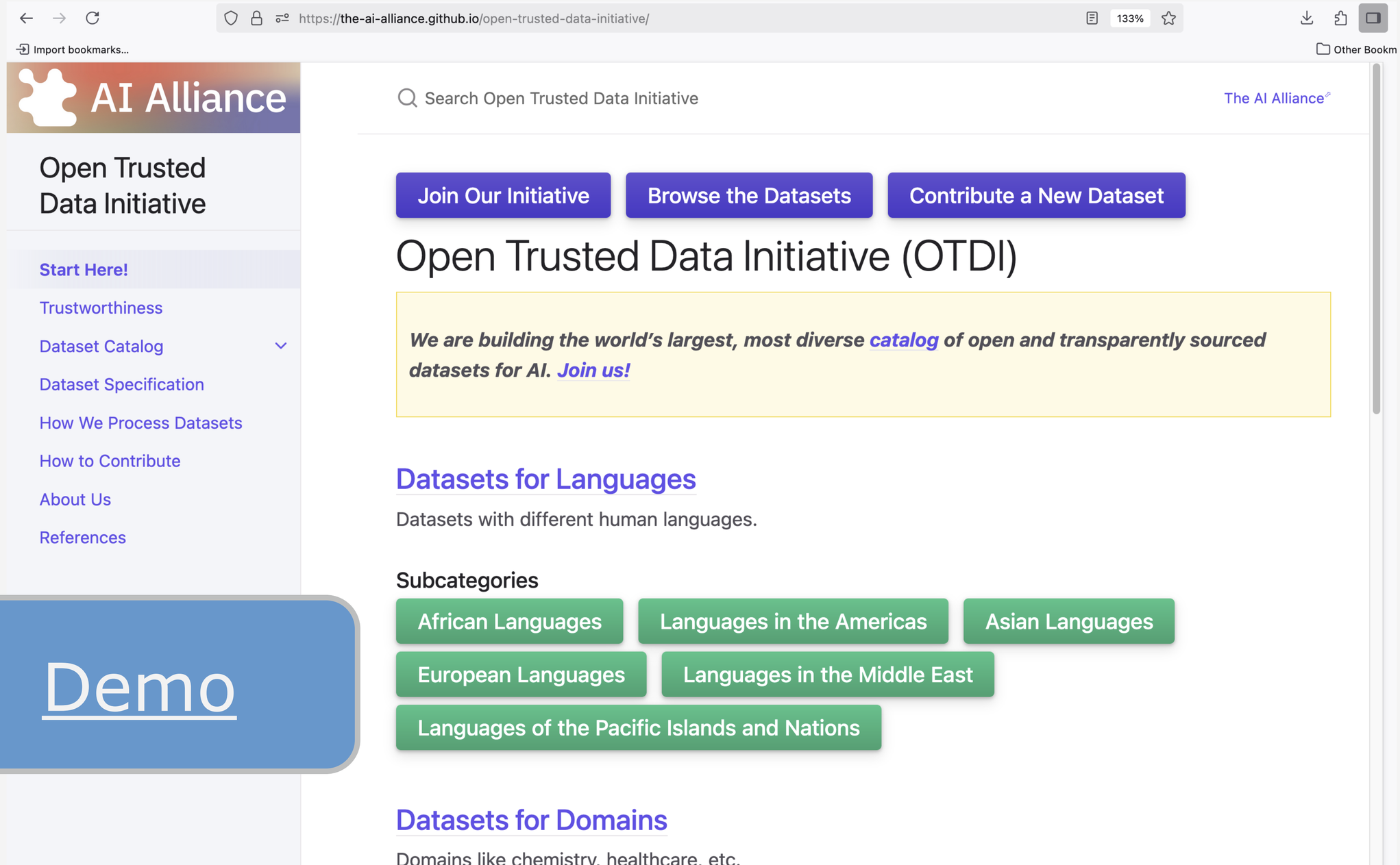

Problem: I need open, trusted datasets

Solution: Open Trusted Data Initiative



AI Alliance

Solution: Open Trusted Data Initiative

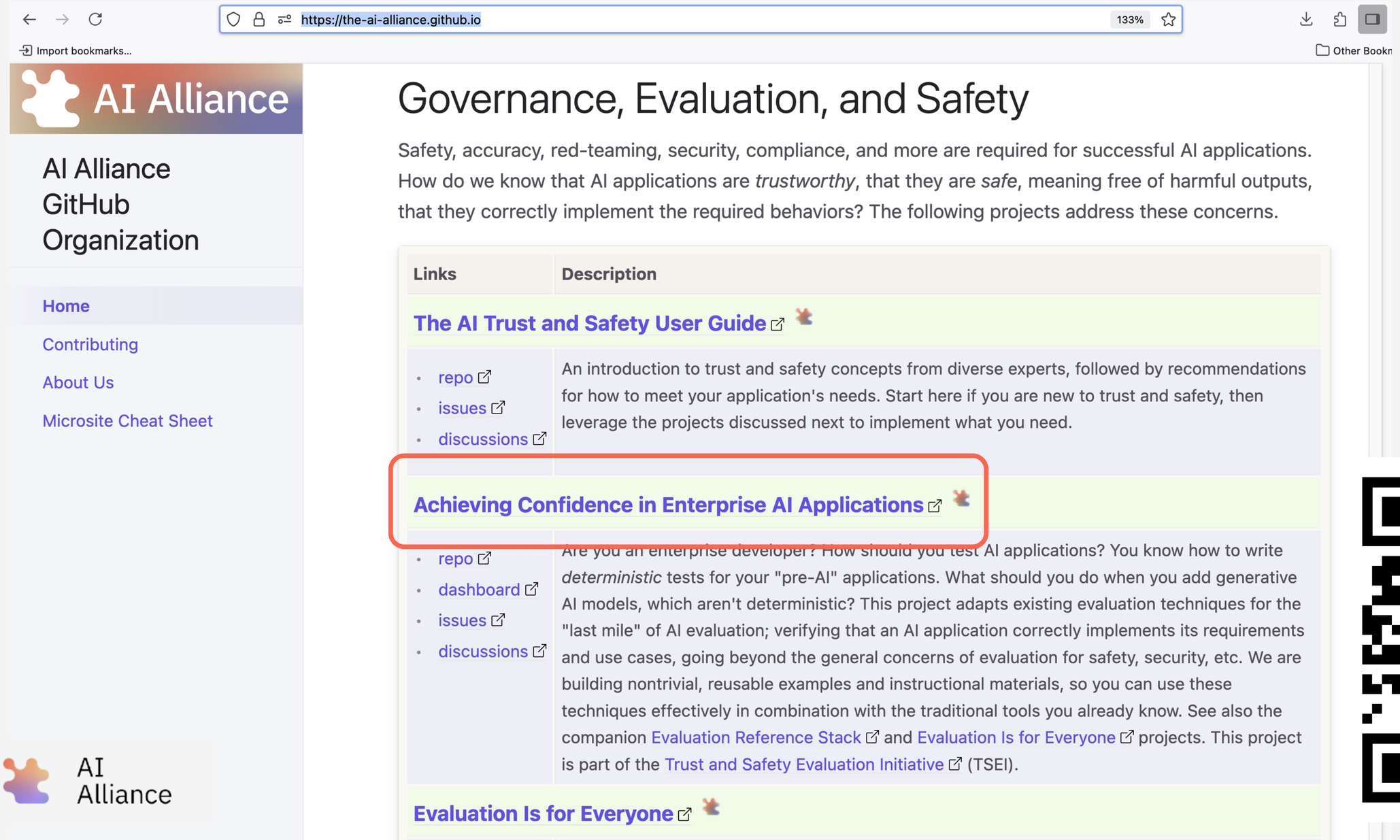


Demo

AI Alliance

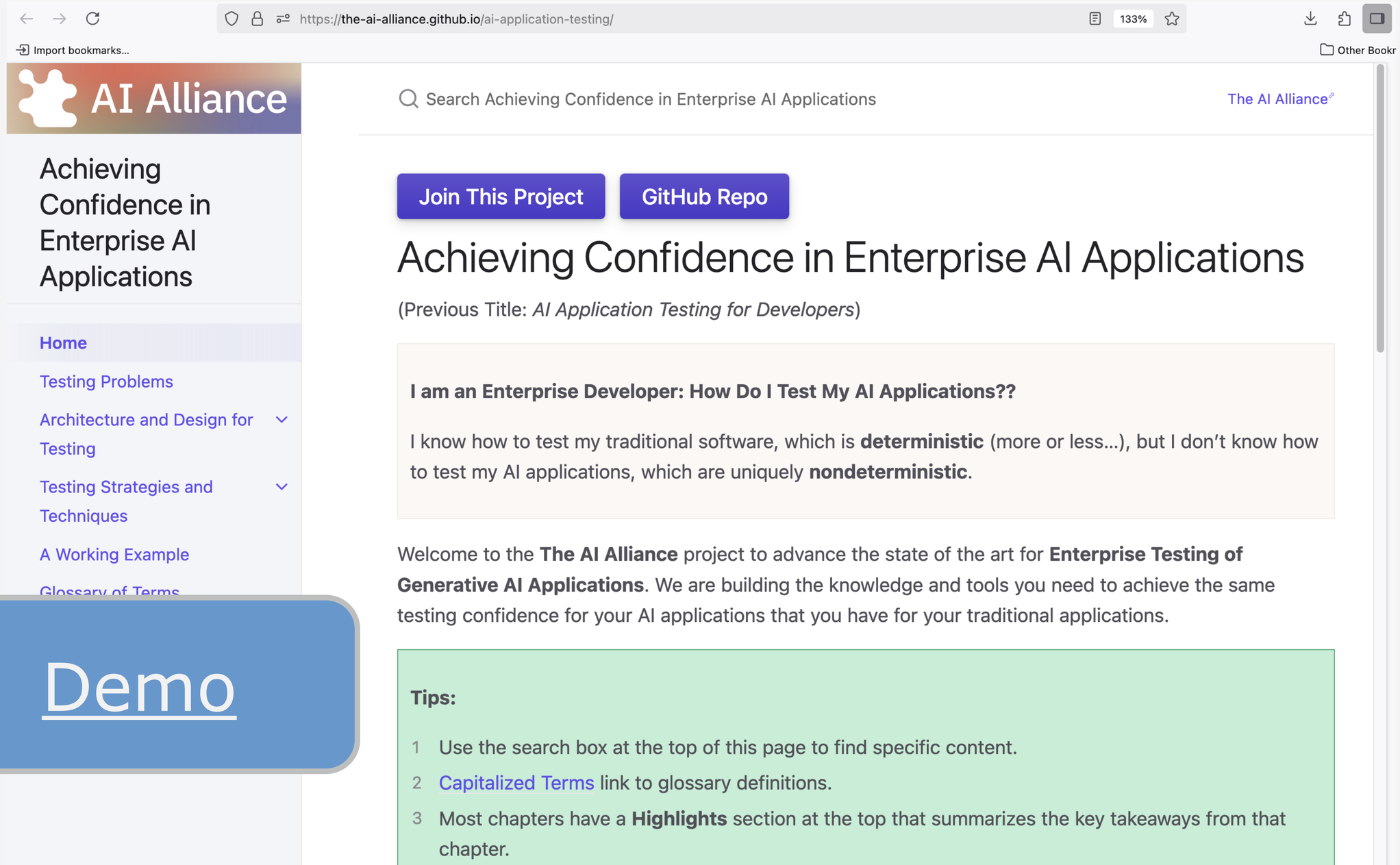

Problem: I don’t know how to test AI-enabled apps!

Solution: Evaluation and Safety



AI Alliance

Solution: Evaluation and Safety



Demo

AI Alliance

Outline

- ContextForge
- What Is the AI Alliance… and Why?
- Building AI-empowered Applications: Agents, MCP, … and More
- A Quick Look at Other AI Trends and AIA Projects
- Final Thoughts

Final Thoughts

ContextForge - Meets many requirements for enterprise deployments of MCP.

The AI Alliance - Strives to make all users able to safely and successfully use AI.

ContextForge - N
many requireme
for enterprise
deployments of

Fill out our Trust and Safety survey! What are you doing? What concerns do you have?

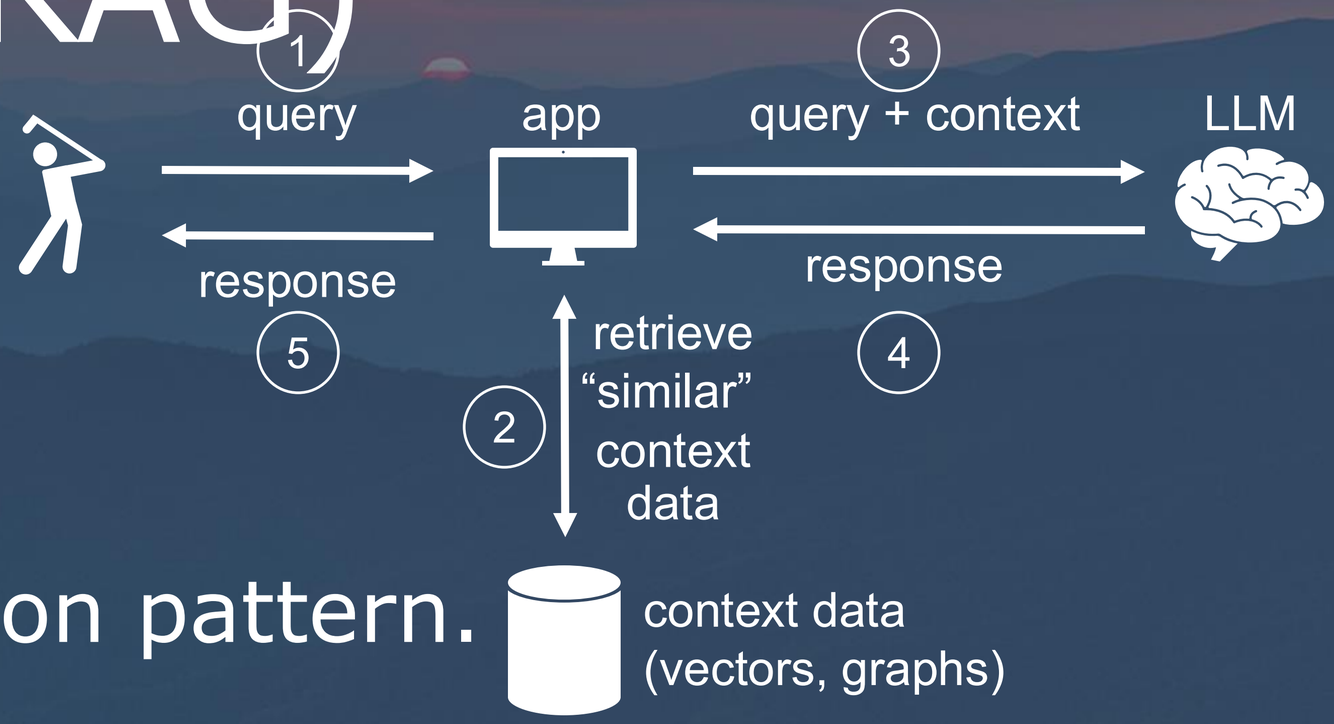
I Alliance -
s to make all
able to safely
ccessfully use

Extra Slides

Extra Slides

Retrieval-augmented Generation (RAG)

Retrieval-Augmented Generation (RAG)



The first GenAI application pattern.

- Improves alignment.
- Incorporates new knowledge after training was done.
- Incorporates proprietary domain or use-case knowledge.

AllyCat

README Apache-2.0 license

license Apache-2.0 issues 16 open Stars 56

AllyCat

AllyCat is full stack, open source chatbot that uses GenAI LLMs to answer questions about your website. It is simple by design and will run on your laptop or server.

Why?

AllyCat is purposefully simple so it can be used by developers to learn how RAG-based GenAI works. Yet it is powerful enough to use with your website, You may also extend it for your own purposes.

⭐ **Found this tool helpful? Give it a star on GitHub to support the project and help others discover it!**

🗞️ Allycat news - releases and new features!

How does it work?

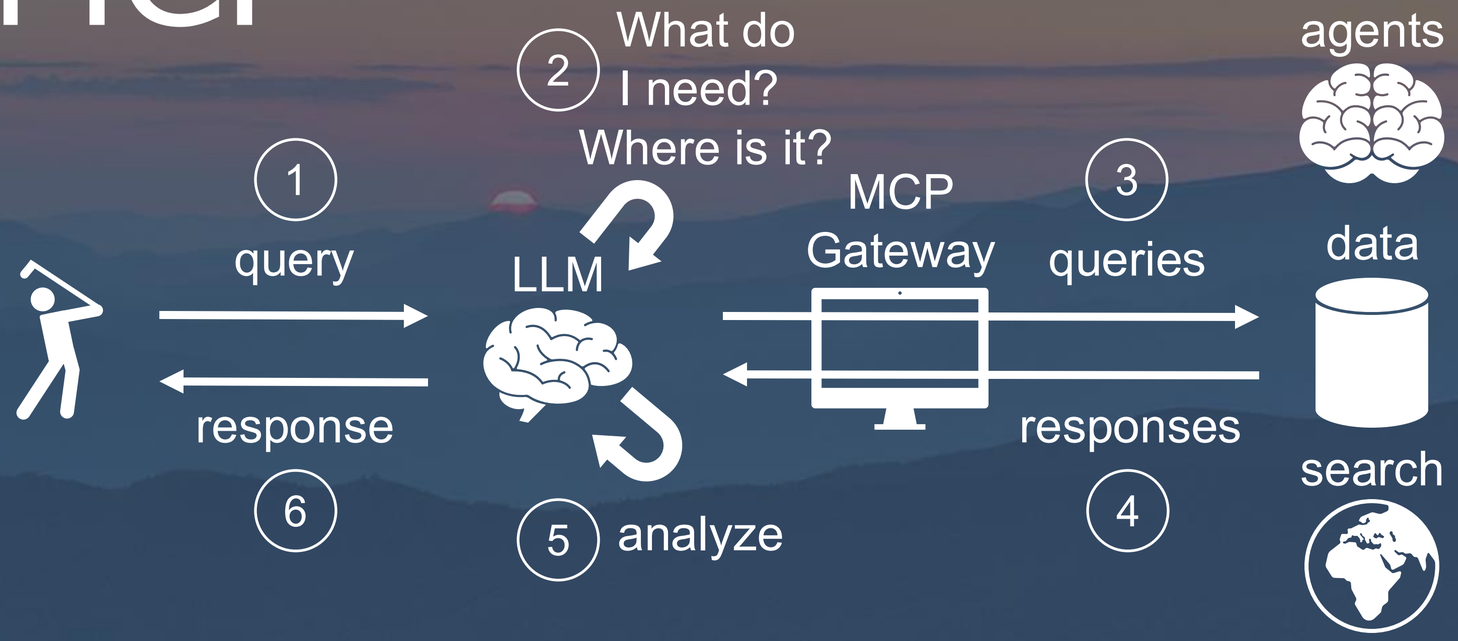
AllyCat uses your choice of LLM and vector database to implement a chatbot written in Python using RAG architecture. AllyCat also includes web scraping tools that extract data from your website (or any website).

github.com/The-AI-Alliance/AllyCat/

Extra Slides

Agents and Model Context Protocol (MCP)

Agents and MCP



The second+ GenAI application pattern(s).

- LLMs do what they do best. Other tools do what they do best, orchestrated together.
- Flexible for very diverse use cases.