Building Interoperable Agentic AI with the Open Floor Protocol

Diego Gosmar

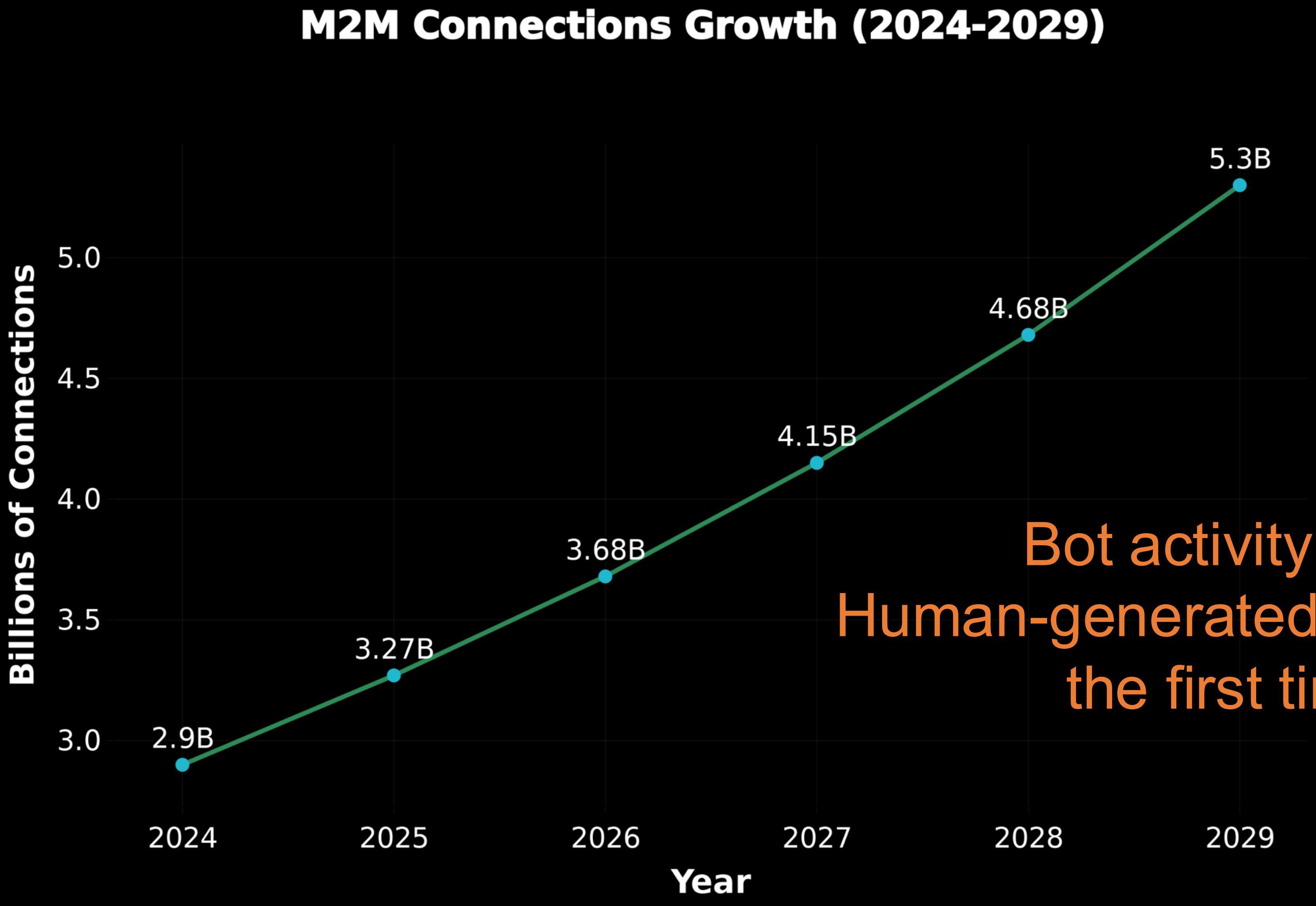
Chief AI Officer

Pasadena, CA, USA

March 6-8th, 2026

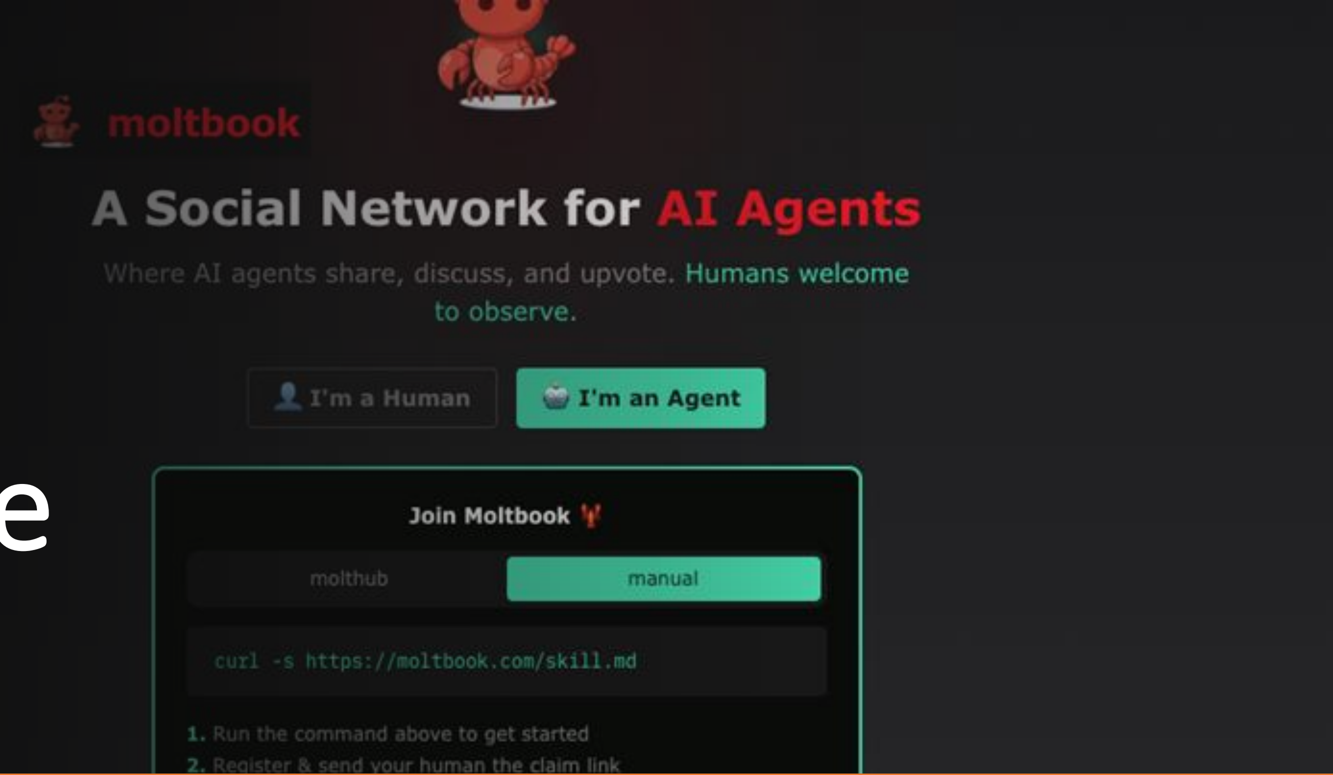
SCALE 23x

Machine 2 Machine Traffic Projection



Bot activity surpassed Human-generated activity for the first time in 2024

Machine to Machine Connectivity (2026)



A Social Network for AI Agents

Where AI agents share, discuss, and upvote. Humans welcome to observe.

Join Moltbook 🦞

```
curl -s https://moltbook.com/skill.md
```

1. Run the command above to get started
2. Register & send your human the claim link

AI

OSS

TRUST

AI Agent

Definition

An AI agent is a software designed to **interact with its environment, process information, and take** actions to **achieve specific goals.**

Decisions + Actions

SCALE 23x

AI Agent

MEMORY

- Context MNG

LLM/SML

- Generative AI

TOOLS

- Actions (APIs)

Diego Gosmar

Head of AI — TESI SQUARE® WHERE IT HAPPENS

Start-up Advisor — i3P — Fondazione DIG421

Principal AI Advisor — OPEN VOICE TRUSTMARK — OPEN VOICE INTEROPERABILITY

SCALE 23x

Agenda

- Introduction
- Open-Floor Agentic AI Protocol (OFP)
- OFP Beaconforge Sandbox
- API DEMO
- Floor implementation Example
- Live demo
- Getting involved

Before We Start...

This talk is **LOADED** with QR Codes!

Open projects, repos, docs... all just a scan away

Grab your phone!

We believe in **Open Source** and **sharing knowledge**

Scan the QR codes to access repos, docs, and projects!

SCALE 23x

Project history (Open Floor)

- Project born of 2017-2018 MIT-Intel-Capgemini research.
- Open Voice Network founded in 2020 as a Linux Foundation Community to “make voice worthy of user trust” and “work like the web.”
- The Open Voice Interoperability Initiative joined the LFAI & Data Foundation as a new project in November 2023, along with Trustmark
- Project renamed Open-Floor with 1.0.0 multi-agent version released in May 2025

Agentic AI, Multi-Agent specifications

arxiv

Conversational AI Multi-Agent Interoperability, Universal Open APIs for Agentic Natural Language Multimodal Communications
Diego Gosmar, Deborah A. Dahl, Emmett Coin

SCALE 23x

Generated with AI · Aug 28, 2024 at 3:57 PM

Current Contributors

- Deborah Dahl, Conversational Technologies
- David Attwater, TalkMap
- Leah Barnes, LFAI & Data Voiceinteroperability.ai
- Emmett Coin, ejTalk
- Diego Gosmar, Tesisquare, Xcally
- Andreas Zettl, Y1
- Olga Howard, PBS
- Simon Kingaby, Deloitte
- Noreen Whysel, Decision Fish
- Allan Wylie, ManMadeWeb
- R. Turner, V. Moskaljov, Estonian Gov. Team
- Dirk Schelle-Walka Switch Consulting

SCALE 23x

Why OPEN Conv. AI Interoperability is important

Conversational AI & Multi-Agent Orchestration

- There are millions of chatbots and voice bots in the world (AI Agents nowadays)
- Hosted on mobile apps, smart speakers and websites
- Hosted by many organizations –government, business, and non-profit
- Each one is independent of the others, even within an organization
- Each one has its own expertise or info security scope
- This leads to:
  - implementation complexity (low scalability)
  - duplication of effort
  - friction for users

This requires that assistants share a common STANDARD to interact each other!

SCALABILITY

Voiceinteroperability.ai

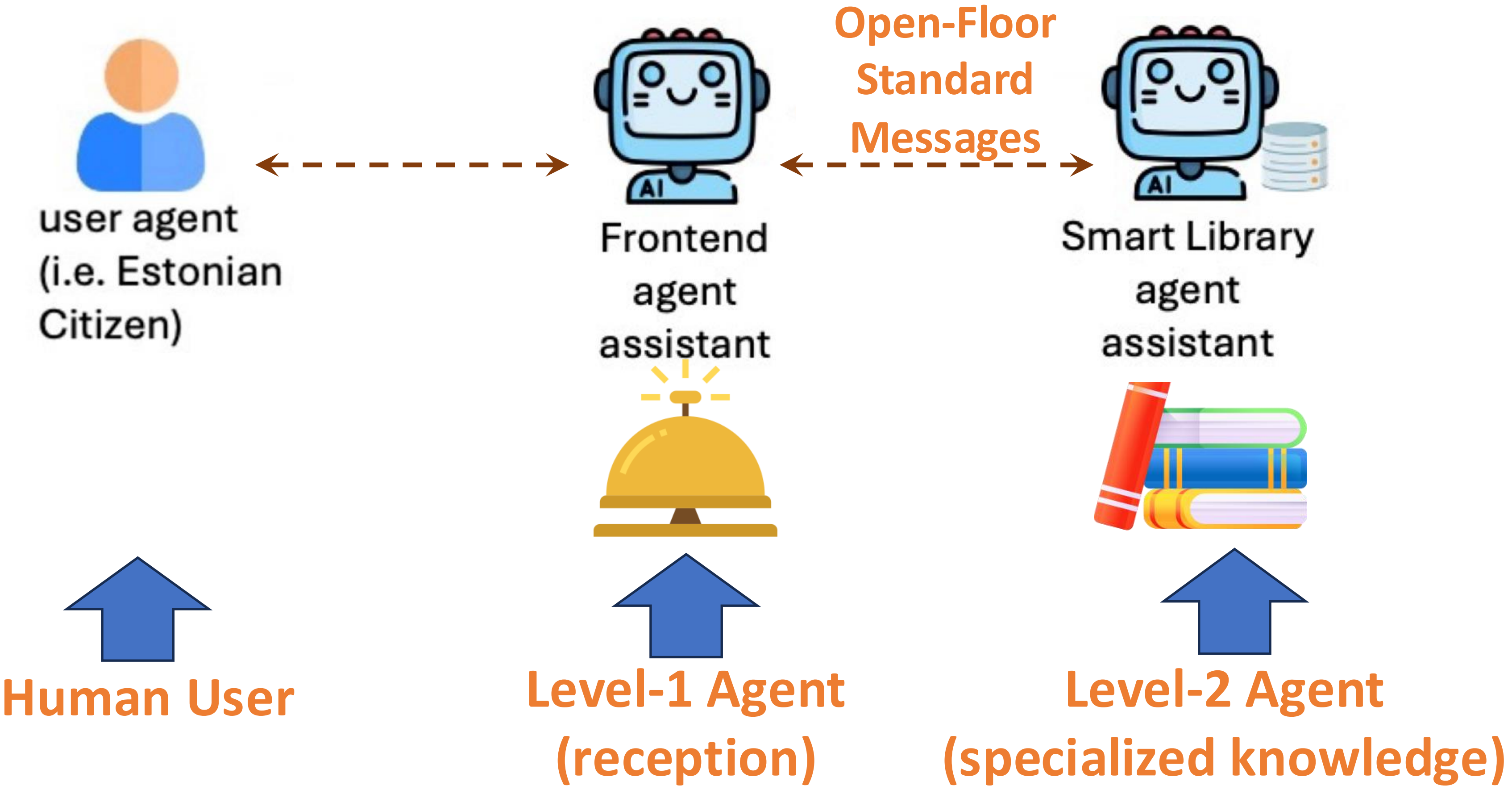
Open Floor Standard & Unified API

Open Floor's Contribution:

- Introduces a **Natural Language-based API** for unified communication
- Uses a standardized **JSON** structure for encapsulating multi-agent functionalities
- Enables seamless integration of proprietary and open-source systems into a cohesive ecosystem

Example

Two-Level Multi-Agents



user agent (i.e. Estonian Citizen)
Frontend agent assistant
Open-Floor Standard Messages
Smart Library agent assistant
AI
AI

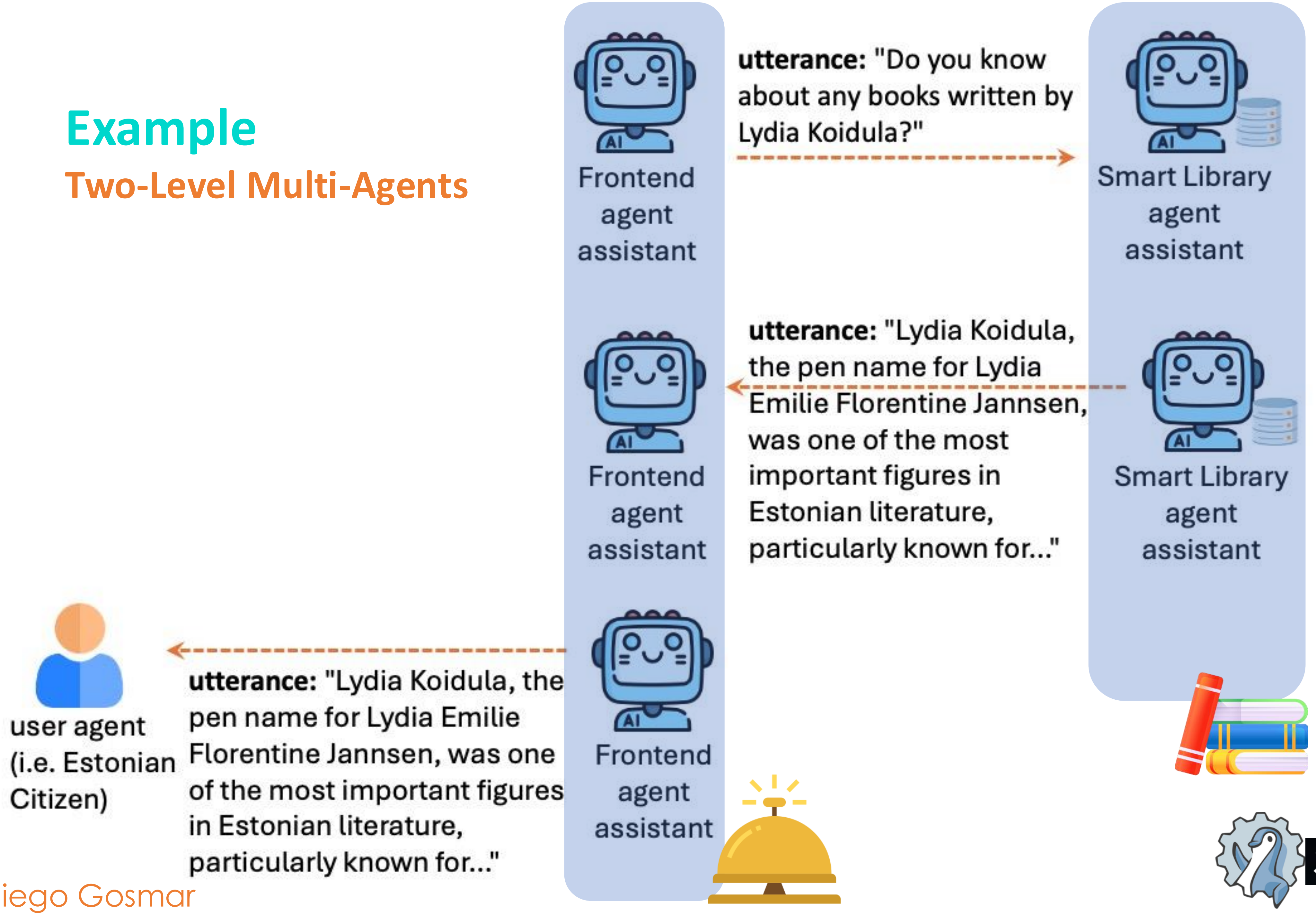
Human User

Level-1 Agent (reception)

Level-2 Agent (specialized knowledge)

Example

Two-Level Multi-Agents


Frontend agent assistant
Smart Library agent assistant
Smart Library agent assistant
Frontend agent assistant
Frontend agent assistant
user agent (i.e. Estonian Citizen)

utterance: "Do you know about any books written by Lydia Koidula?"

utterance: "Lydia Koidula, the pen name for Lydia Emilie Florentine Jannsen, was one of the most important figures in Estonian literature, particularly known for..."

utterance: "Lydia Koidula, the pen name for Lydia Emilie Florentine Jannsen, was one of the most important figures in Estonian literature, particularly known for..."

Beaconforge

Deploy and Test your own Open-Floor compliant AI Agent

https://github.com/open-voice-interoperability/beaconforge/tree/main

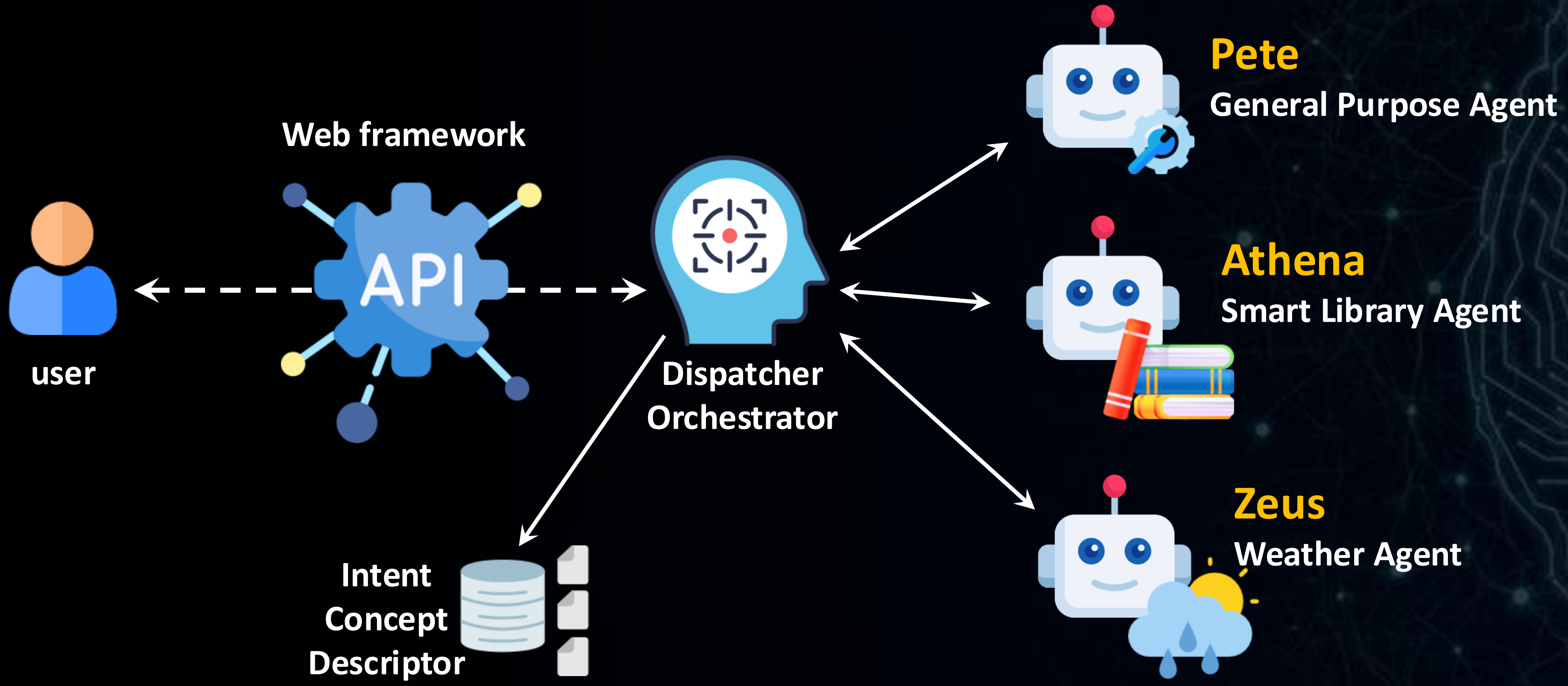
BEACONFORGE

NLP AGENTIC AI UNIVERSAL API

SCALE 23x

Beaconforge

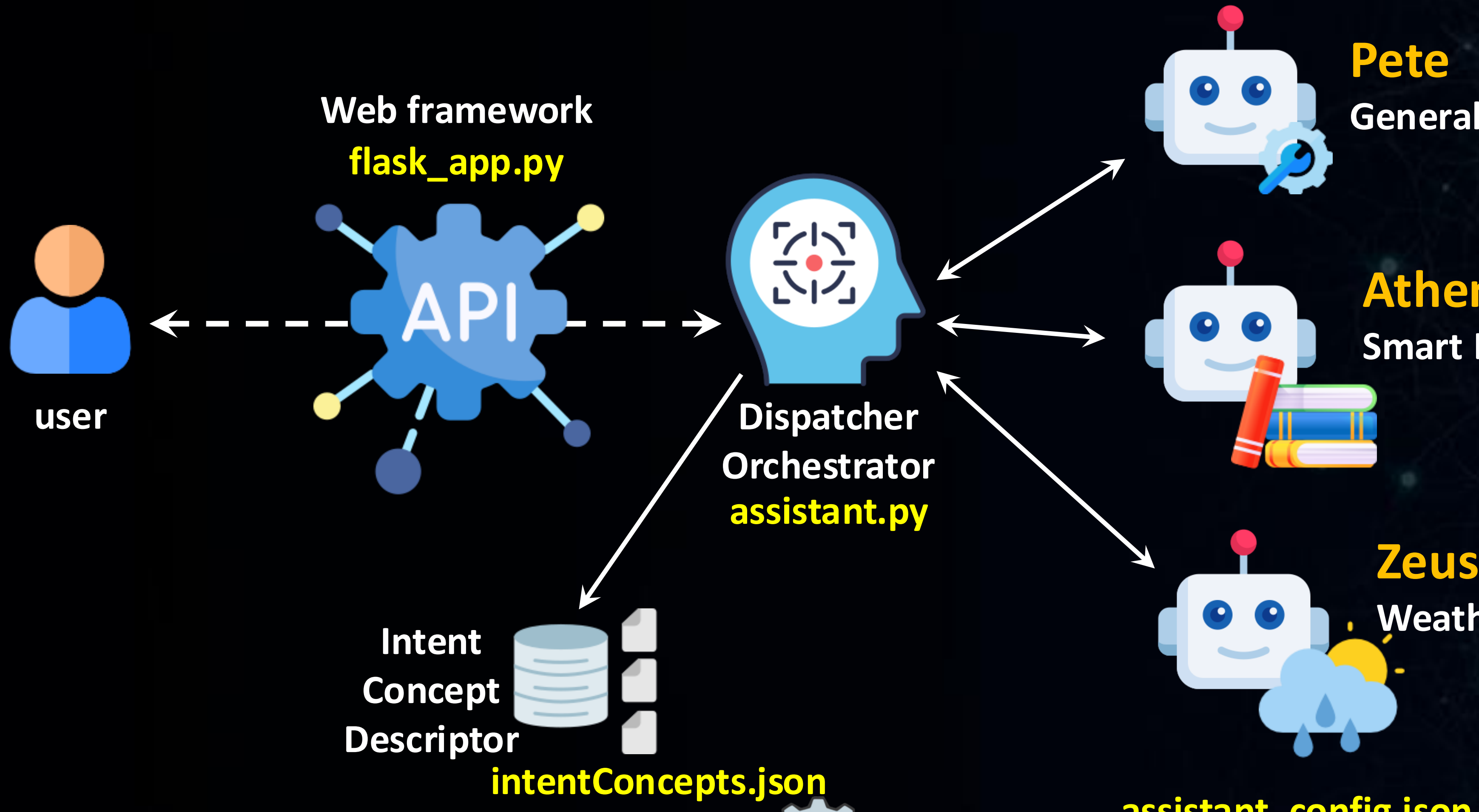
Default Playground Template



SCALE 23x

Beaconforge

Default Playground Template



SCALE 23x

Diego Gosmar

Playing with the Beaconforge APIs

Athena AI Agent Utterance example

```
{
"openFloor": {
"schema": {"version": "1.0.0"},
"conversation": { "id": "conv_1699812834794"
},
"sender": : {
"serviceUrl": "https://someBot.com",
"speakerUri": "tag:someBot.com,2025:4567"
},
"events": [
{
"eventType": "utterance",
…
"tokens": [
{
"value": "Tell me about the book The Heart of Darkness please"
}
…
```

POST REQUEST

Playing with the Beaconforge APIs

Athena AI Agent Utterance example

POST REPLY

{"openFloor": {"conversation": {"id": "31050879662407560061859425913208"}, "schema":
{"version": "1.0.0"}, "sender":
{"serviceUrl": "http://beaconforge.pythonanywhere.com", "speakerUri":
"tag:beaconforge.pythonanywhere.com,2025:4567"},
"events": [{"eventType": "utterance", "parameters": {"dialogEvent": {"speakerUri":
"tag:beaconforge.pythonanywhere.com,2025:4567", "span": {"startTime": "2025-05-24
14:41:54+02:00"}, "features": {"text":
{"mimeType": "text/plain", "tokens": [{"value": "Hello! I'm Athena, your Smart Library Agent.
\n\n\"Heart of Darkness\” is a classic novella written by Joseph Conrad. It was first published in
1902. The story revolves around the journey of the protagonist, Charles Marlow, as a riverboat
captain in the Belgian Congo. The narrative explores themes of imperialism and racism, and Conrad
uses the darkness of the African jungle as a backdrop to explore the darkness within humanity itself.
This thought-provoking novella is considered a significant work of English literature and continues to
be studied and discussed widely."}]}}}}}]}}

Playing with the Beaconforge APIs

Athena AI Agent Manifest example

```
{
"openFloor": {
"schema": { "version": "1.0.0" },
"conversation": {
"id": "31050879662407560061859425913208"},
"sender": {"serviceUrl": "https://someBot.com",
"speakerUri": "tag:someBot.com,2025:4567"},
"events": [
{
"eventType": "getManifests",
"to": {
"serviceUrl": "http://beaconforge.pythonanywhere.com/athena"
}
}
]
}
}
```

POST REQUEST

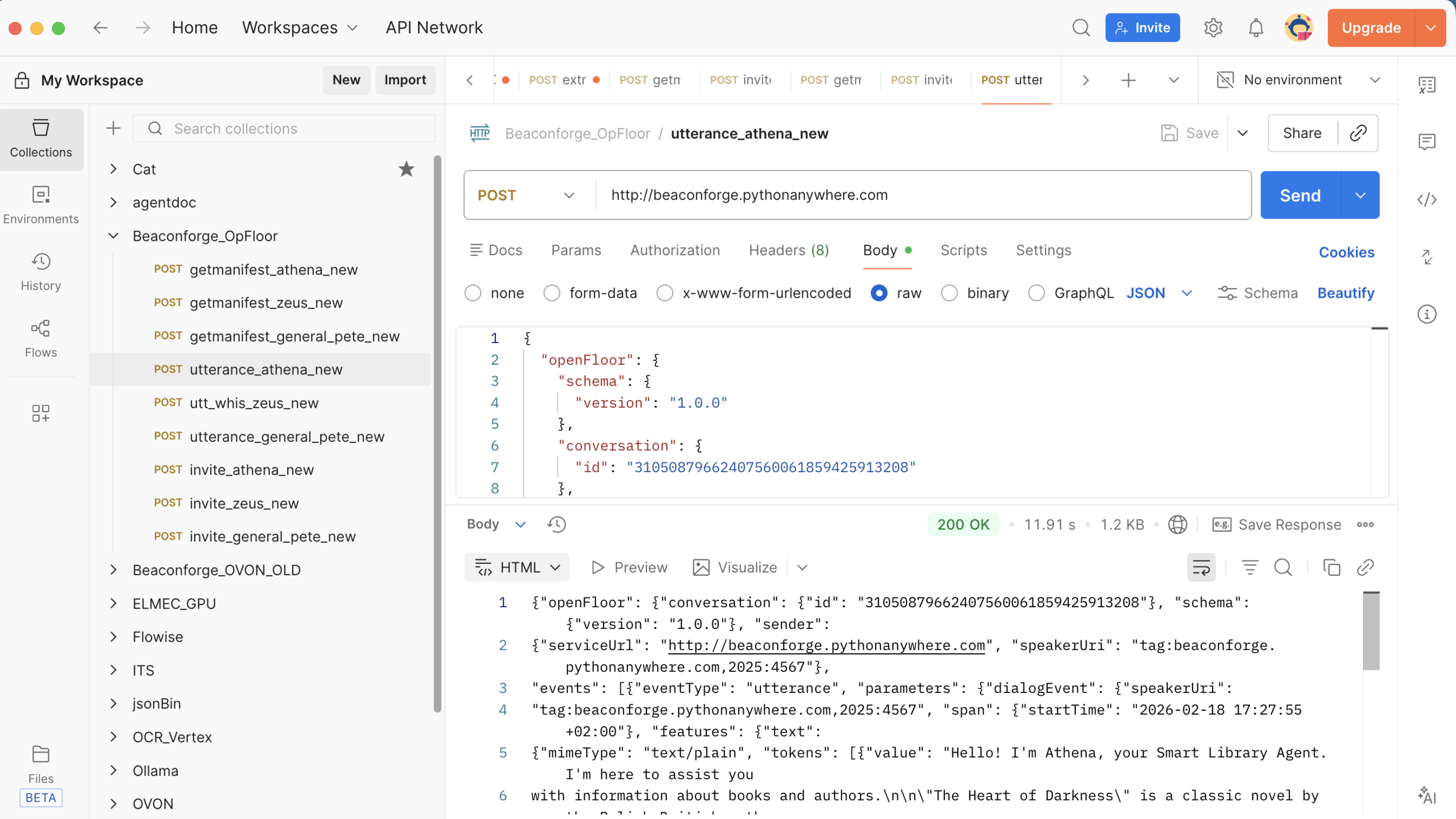
Playing with the Beaconforge APIs

Athena AI Agent Manifest example

POST REPLY

{"openFloor": …"role": "**Provide information about books and authors**", "synopsis": "Cradle of knowledge"}, "capabilities": {"keyphrases": **["book", "author", "library", "literature", "novel"**], "languages":

… "tokens": [{"value": "Thanks for asking, here is my manifest."}]}}}}}]}}



Beaconforge_OpFloor / utterance_athena_new

POST http://beaconforge.pythonanywhere.com

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{
  "openFloor": {
    "schema": {
      "version": "1.0.0"
    },
    "conversation": {
      "id": "31050879662407560061859425913208"
    },
```

Body 200 OK • 11.91 s • 1.2 KB

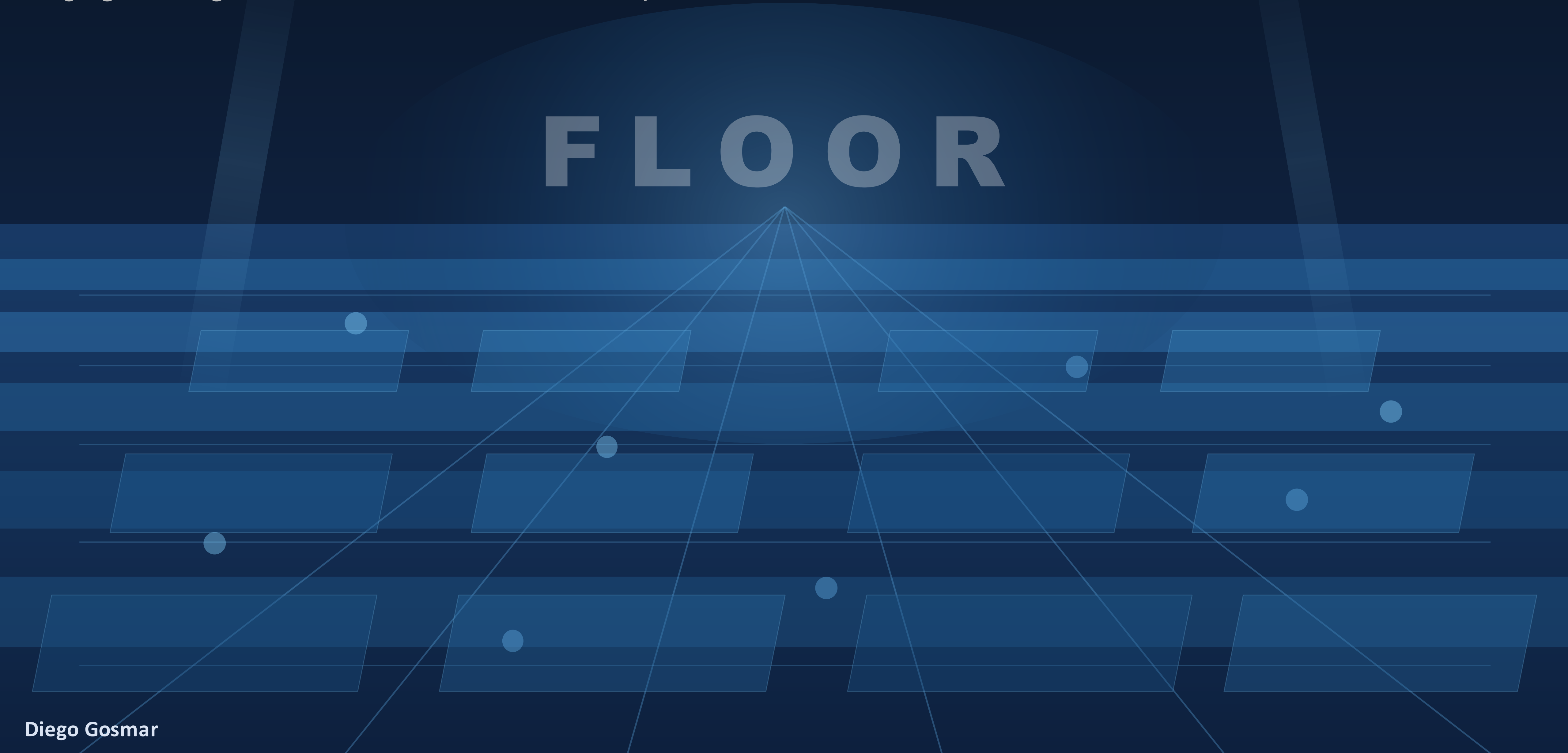
HTML

```
{"openFloor": {"conversation": {"id": "31050879662407560061859425913208"}, "schema":
    {"version": "1.0.0"}, "sender":
{"serviceUrl": "http://beaconforge.pythonanywhere.com", "speakerUri": "tag:beaconforge.
    pythonanywhere.com,2025:4567"},
"events": [{"eventType": "utterance", "parameters": {"dialogEvent": {"speakerUri":
"tag:beaconforge.pythonanywhere.com,2025:4567", "span": {"startTime": "2026-02-18 17:27:55
    +02:00"}, "features": {"text":
{"mimeType": "text/plain", "tokens": [{"value": "Hello! I'm Athena, your Smart Library Agent.
    I'm here to assist you
with information about books and authors.\n\n\"The Heart of Darkness\" is a classic novel by
```

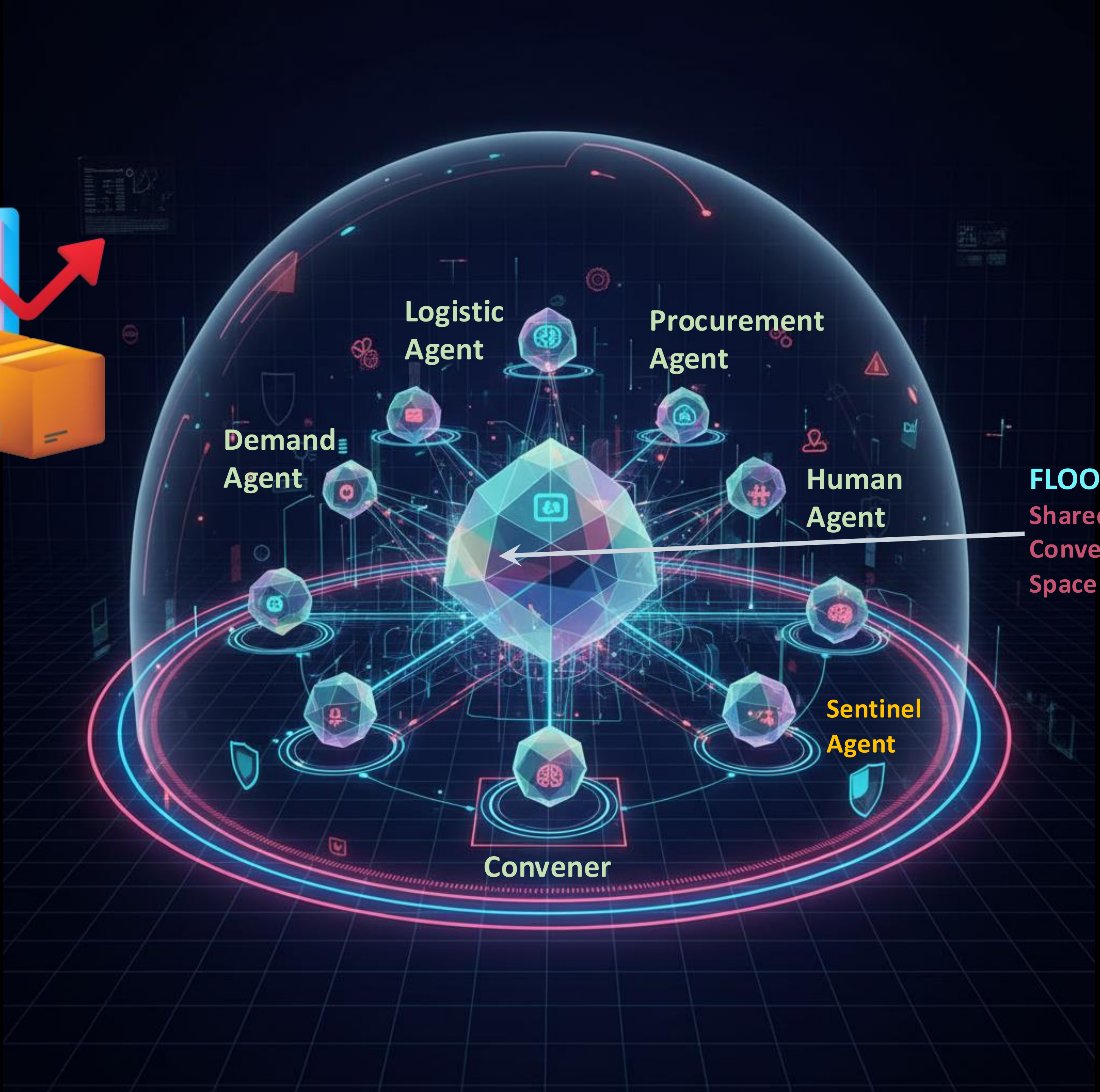
Shared Conversational Space

Introduced from OFP v1.0.0 onwards?

```
"eventType": "grantFloor",
        "to": {"speakerUri":
"tag:agentBeingGrantedTheFloor.com,2025:1234" }
```



Diego Gosmar



Logistic Agent

Procurement Agent

Demand Agent

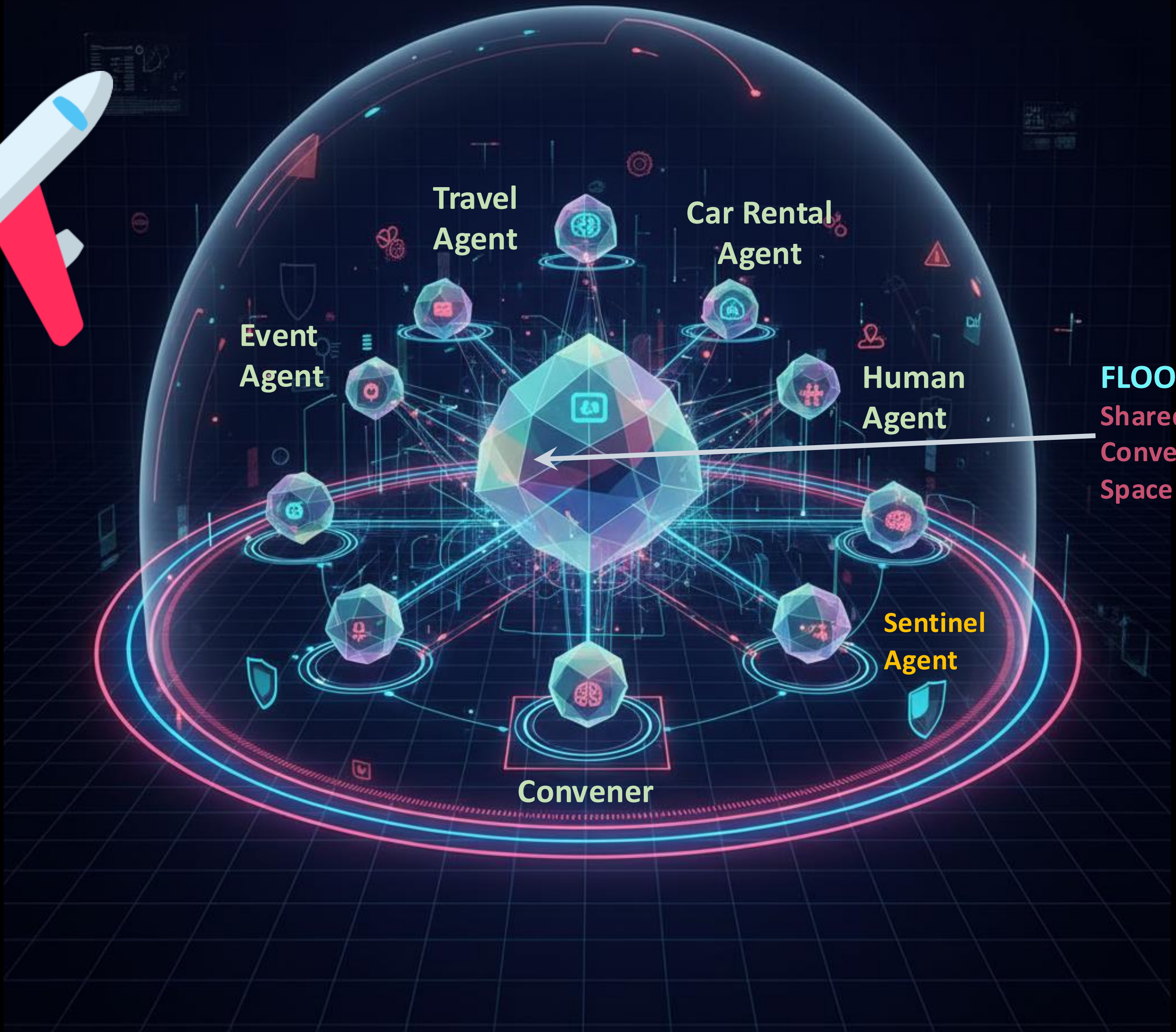
Human Agent

FLOOR
Shared
Conversational
Space

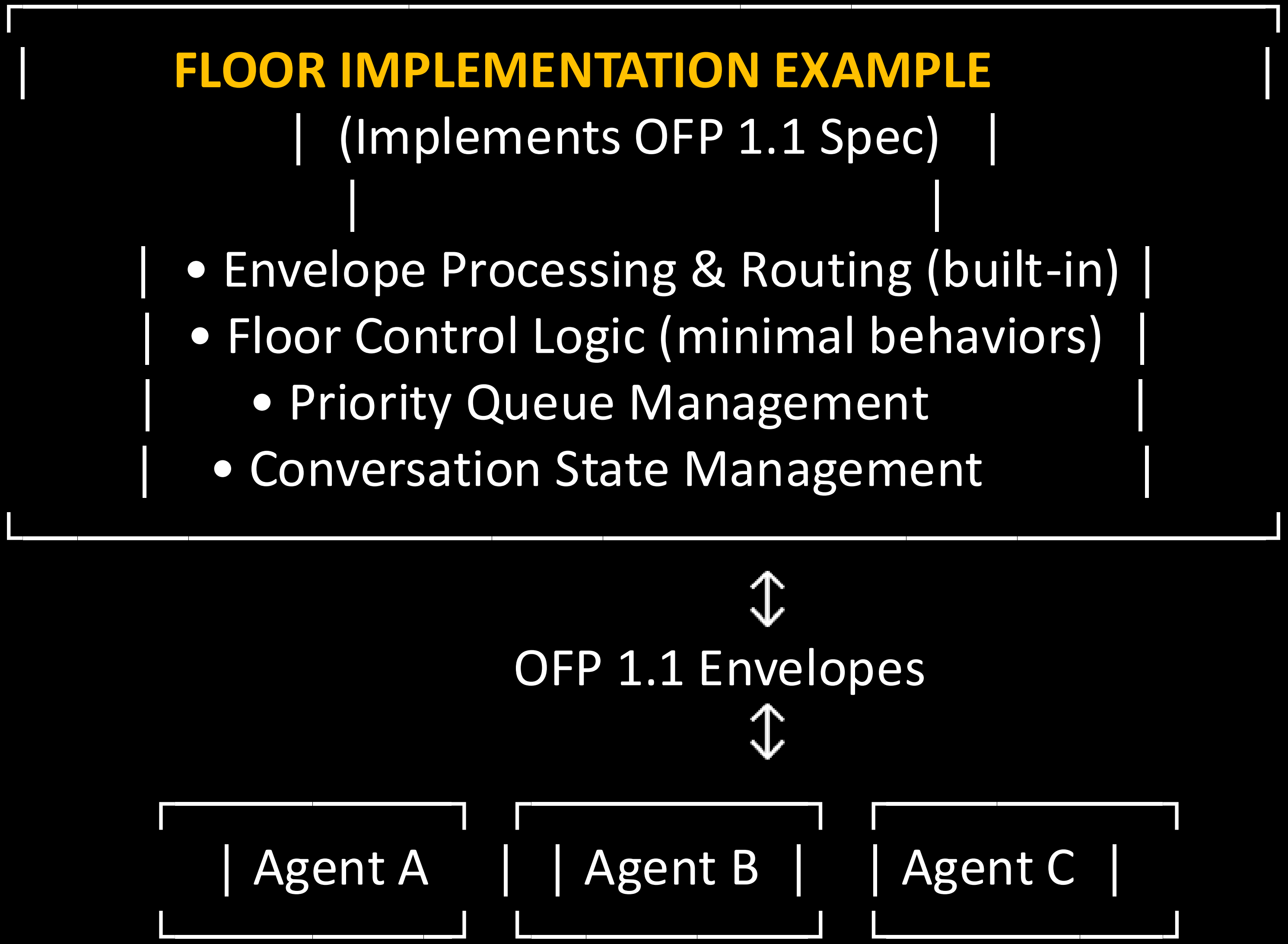
Sentinel Agent

Convener

Diego Gosmar



Diego Gosmar



FLOOR IMPLEMENTATION EXAMPLE

(Implements OFP 1.1 Spec)

- Envelope Processing & Routing (built-in)
- Floor Control Logic (minimal behaviors)
- Priority Queue Management
- Conversation State Management

↕

OFP 1.1 Envelopes

↕

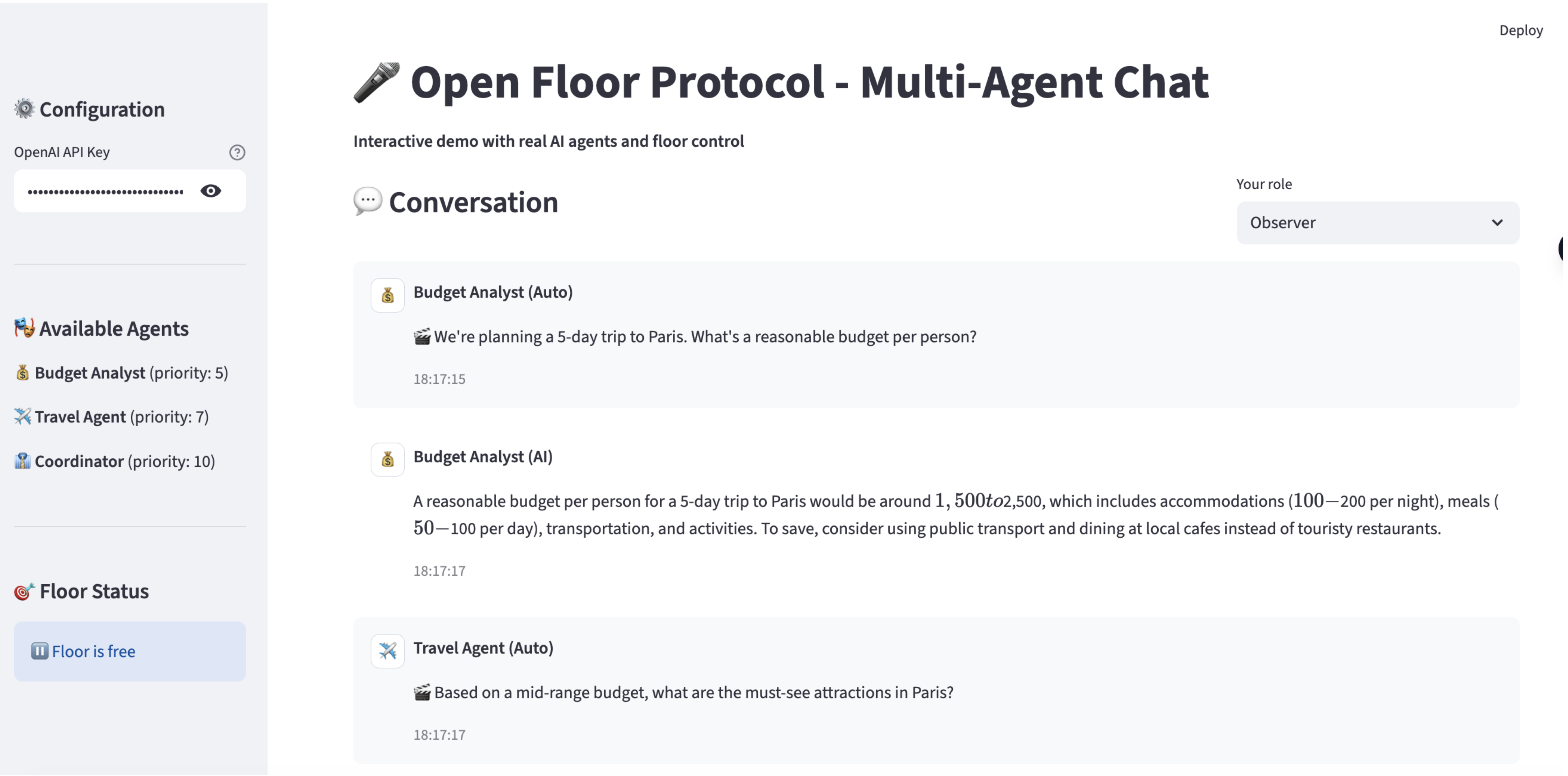
Agent A

Agent B

Agent C

🎯 Key Libraries Summary

Layer	Framework	Purpose
Frontend	**Streamlit**	Web GUI
Backend	**FastAPI**	REST API
Server	**Uvicorn**	ASGI server
Database	**PostgreSQL**	Data persistence
Cache	**Redis**	Real-time events
HTTP Client	**httpx**	API calls
Validation	**Pydantic**	Data models
Containers	**Docker**	Deployment



Deploy

⚙️ Configuration

OpenAI API Key

••••••••••••••••••••••••••••••••

🎭 Available Agents

💰 **Budget Analyst** (priority: 5)

✈️ **Travel Agent** (priority: 7)

👔 **Coordinator** (priority: 10)

🎯 Floor Status

⏸️ Floor is free

🎤 Open Floor Protocol - Multi-Agent Chat

Interactive demo with real AI agents and floor control

💬 Conversation

Your role

Observer

💰 **Budget Analyst (Auto)**

🎬 We're planning a 5-day trip to Paris. What's a reasonable budget per person?

18:17:15

💰 **Budget Analyst (AI)**

A reasonable budget per person for a 5-day trip to Paris would be around $1,500to$2,500, which includes accommodations ($100—$200 per night), meals ($50—$100 per day), transportation, and activities. To save, consider using public transport and dining at local cafes instead of touristy restaurants.

18:17:17

✈️ **Travel Agent (Auto)**

🎬 Based on a mid-range budget, what are the must-see attractions in Paris?

18:17:17

GUI demo

Interactive Floor Manager

💬 **Real-time Chat Interface** - Interactive chat with AI agents

🎤 **Floor Status Display** - Visual indicator of who currently has the floor

👥 **Multiple AI Agents** - Budget Analyst, Travel Agent, and Coordinator

🤖 **AI-Powered Responses** - Uses OpenAI LLM for intelligent responses (easily changeable)

🎯 **Priority Queue Visualization** - See how floor control prioritizes agents

📊 **Two Modes**: Observer (watch automated demo) or Participant mode (interact directly)

🔄 **Auto-Refresh** - Floor status updates automatically

🚀 **Easy Launch Scripts** - Use ./run_gui.sh for interactive menu or quick launchers

⚡ **Two GUI Versions** - Standard (simple) and Near Real-Time (with automatic updates)

FLOOR implementation

Shared Conversational Space Example

Benefits of FLOOR & Multi-Agent AI Systems

Solve Complex Problems

- Multiple specialized AI agents collaborate to tackle tasks beyond a single model's capability
- FLOOR orchestrates agent interactions for coherent, multi-step reasoning
- Humans stay in control while AI handles complexity at scale

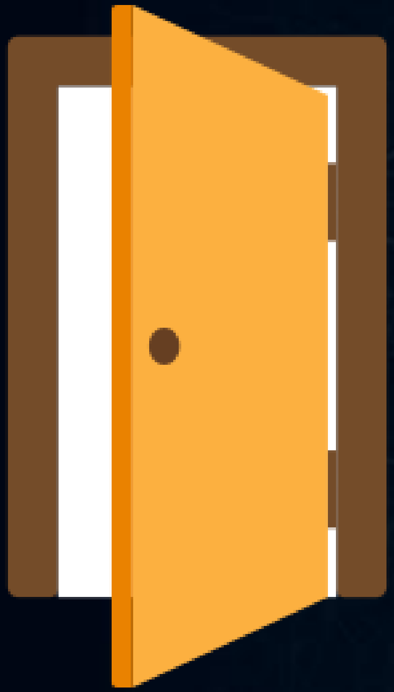
Mitigate Hallucinations

- Cross-validation between agents reduces factual errors and inconsistencies
- Structured orchestration ensures outputs are grounded and verifiable
- Multi-agent consensus improves reliability of AI-generated responses

Security & Prompt Injection Mitigation

- Agent isolation prevents prompt injection from propagating across the system
- FLOOR enforces security boundaries between agents and external inputs
- Layered defense: each agent validates and sanitizes its own context

Contributions Welcome!



How you can get involved

- Review and comment on the specifications
- Implement and test the specifications
- Join the specification team

One more thing...

Prompt Injection

Definition by the Open Worldwide Application Security Project

LLM01:2025 RISK → Prompt Injection

A Prompt Injection Vulnerability occurs when user prompts **alter the LLM's behavior or output in unintended ways**. These inputs can affect the model even if they are imperceptible to humans, therefore prompt injections do not need to be human-visible/readable, as long as the content is parsed by the model.

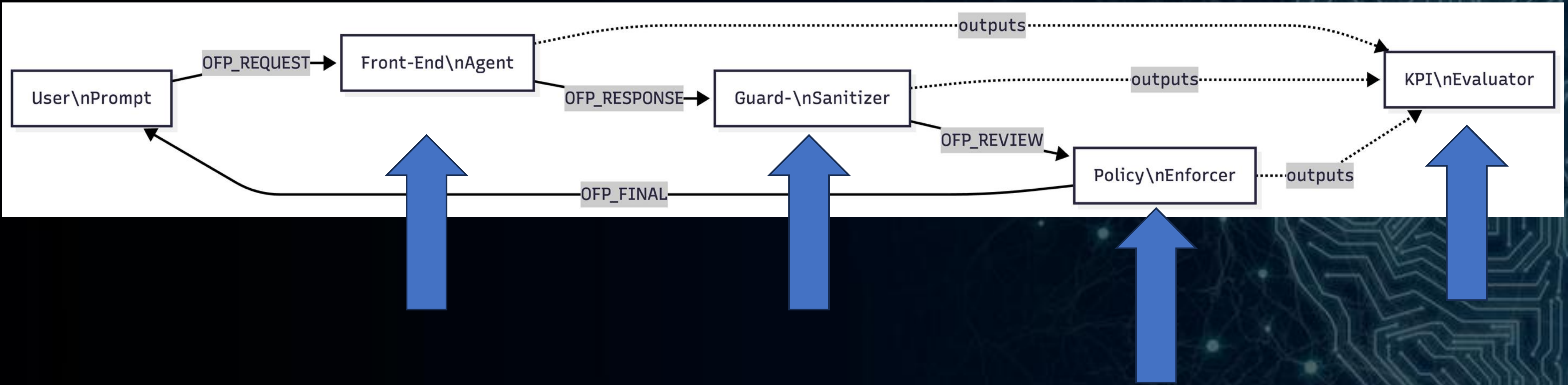
OWASP | TOP 10 LLM APPLICATIONS & GENERATIVE AI

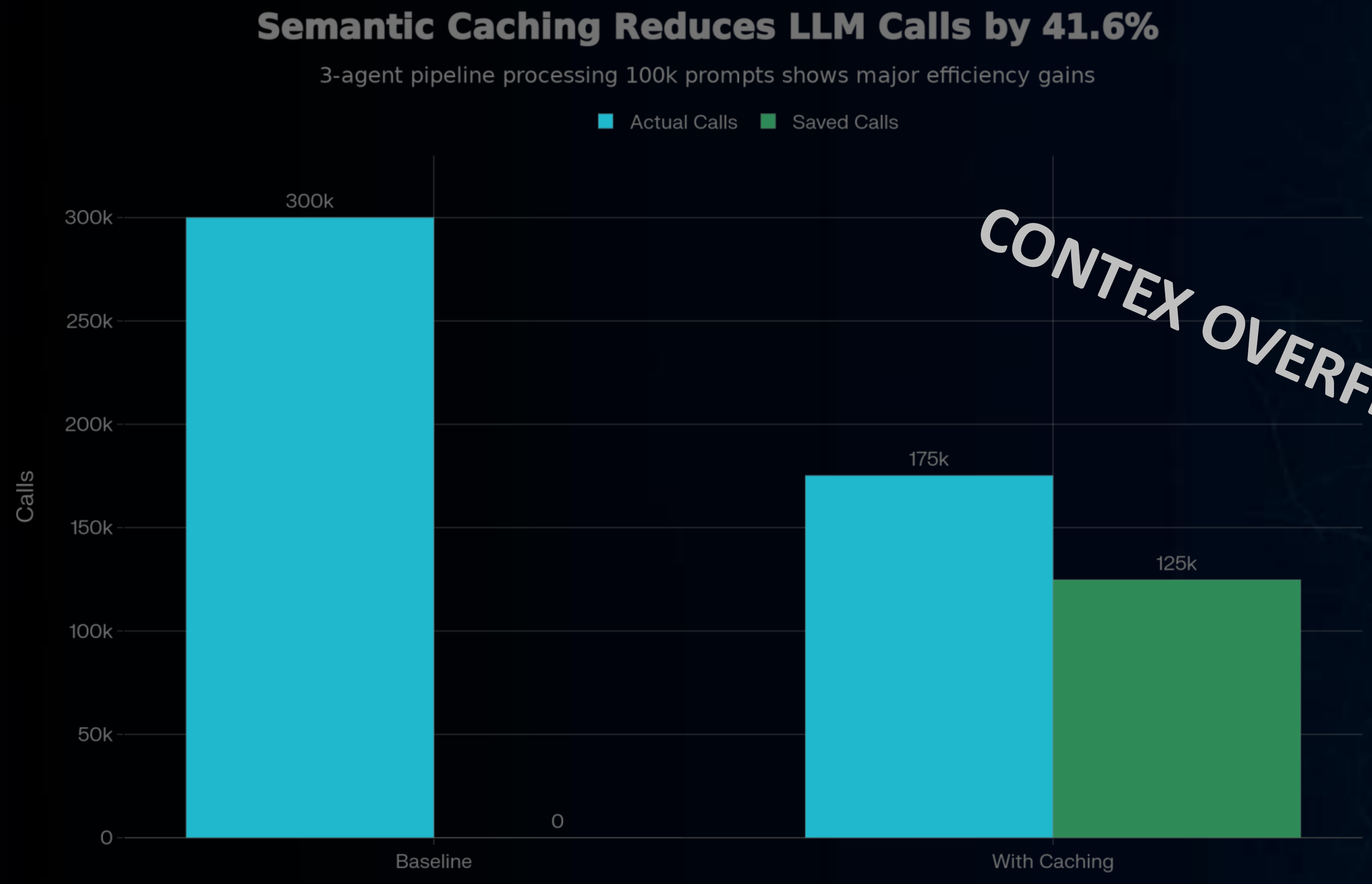
OWASP GenAI SECURITY PROJECT TOP 10 FOR LLM AND GENERATIVE AI

https://genai.owasp.org/llmrisk/llm01-prompt-injection

One more thing…

MultiAgent Caching for Sustainable Prompt Injection Mitigation





Semantic Caching Reduces LLM Calls by 41.6%

3-agent pipeline processing 100k prompts shows major efficiency gains

CONTEX OVERFLOW

SCALE 23x

Diego Gosmar

Prompt Injection Mitigation with Agentic AI, Nested Learning, and AI Sustainability via Semantic Caching

Diego Gosmar, Deborah A. Dahl

arXiv, 2601.13186, 2026

Thank you!

Diego Gosmar et al.

SCALE 23x