#ScottishSummit2024

Securing the Realm

SCOTTISH SUMMIT

#ScottishSummit2024

Securing the Realm

✦ ✦ ✦

An adventure with an Apprentice Wizard in 3 parts

SCOTTISH SUMMIT

Thank You to our Sponsors...

Platinum Sponsor

Capgemini

Gold Sponsors

resco

ARROW

dox42

automate your documents
integrate your data

kerv Digital

#ScottishSummit2024

Thank You to our Sponsors...

SCOTTISH SUMMIT

With Thanks

AGILECADENCE
POWERING INNOVATION. SIMPLIFYING TECHNOLOGY.

Telefónica Tech

LightningTools

Cloud Surge
UNLEASH YOUR POWER

LOGIQAPPS

DYNAMICS MINDS
powered by DOCENTRIC

mscrm-addons.com
Your company for MS-CRM ADD-ONS!

Noteworthy .Support

PROMX

Syskit

Click

riada CONSULTANCY

QUBIX

PROXIMO3

360

#ScottishSummit2024

Authors (your speakers)

Josh McDonald

Modern Work, Security & AI at Avanade

Chris Lloyd-Jones

Microsoft MVP in AI Strategy & Architecture @ Avanade

#ScottishSummit2024

Contents (the agenda)

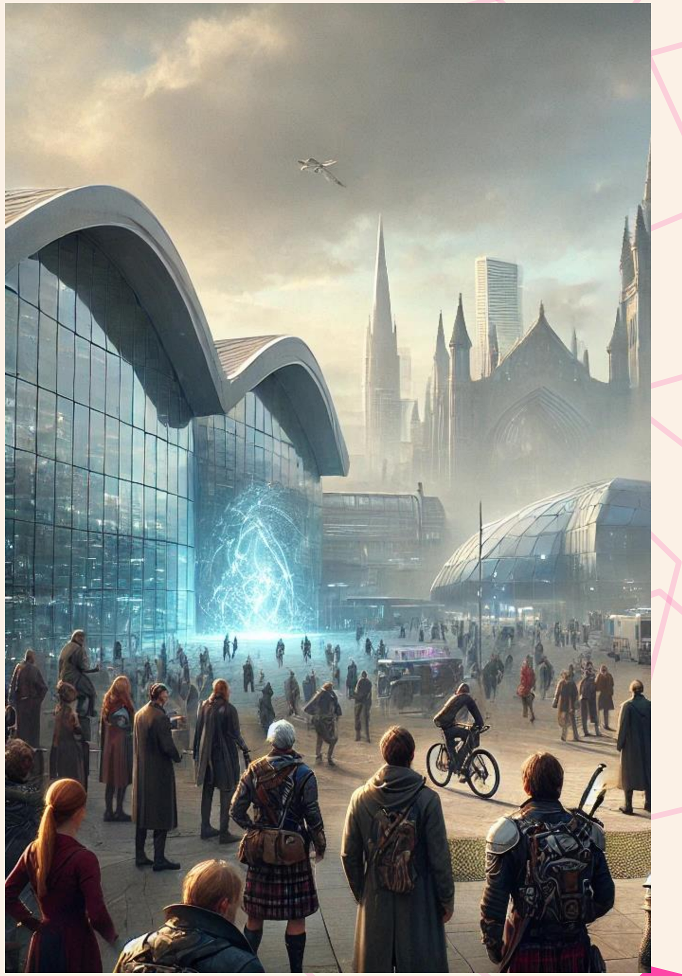
Prologue – The Apprentice Wizard's Task
Prototyping

Act 1 – Summoning the Kobold
Starting a campaign, safely, in Azure OpenAI

Act 2 – Training the Kobold
Building immersive experiences in Generative AI

Act 3 – Kobold goes Awry
Using statefulness to enhance the experience

Epilogue – The Apprentice' Master is Pleased… for now
Roadmap



Foreword (what this talk is about)

What this is

- A story in multiple acts, demonstrating how to layer Azure AI services together
- Broad walk-through of technical, design, security & compliance, and end-user considerations
- A chance to ask questions/comment/discuss

What this isn’t

- Overview of LLM’s/SLM’s
- An introduction or deep dive of Microsoft/Azure AI services
- Boring (hopefully)

WHY?

Why?

✦✦✦

All these concepts are applicable to AI 'at work'
...and it's fun!

Prologue

The Apprentice Wizard’s Task

Prologue (how did this all start)

ChatGPT

The GPT Builder, a mighty tool for an apprentice wizard

Systems Reference Document/OGL

Open source (not without controversy), courtesy of the Wizards of the Coast

Data

Yes, it was done on Excel!

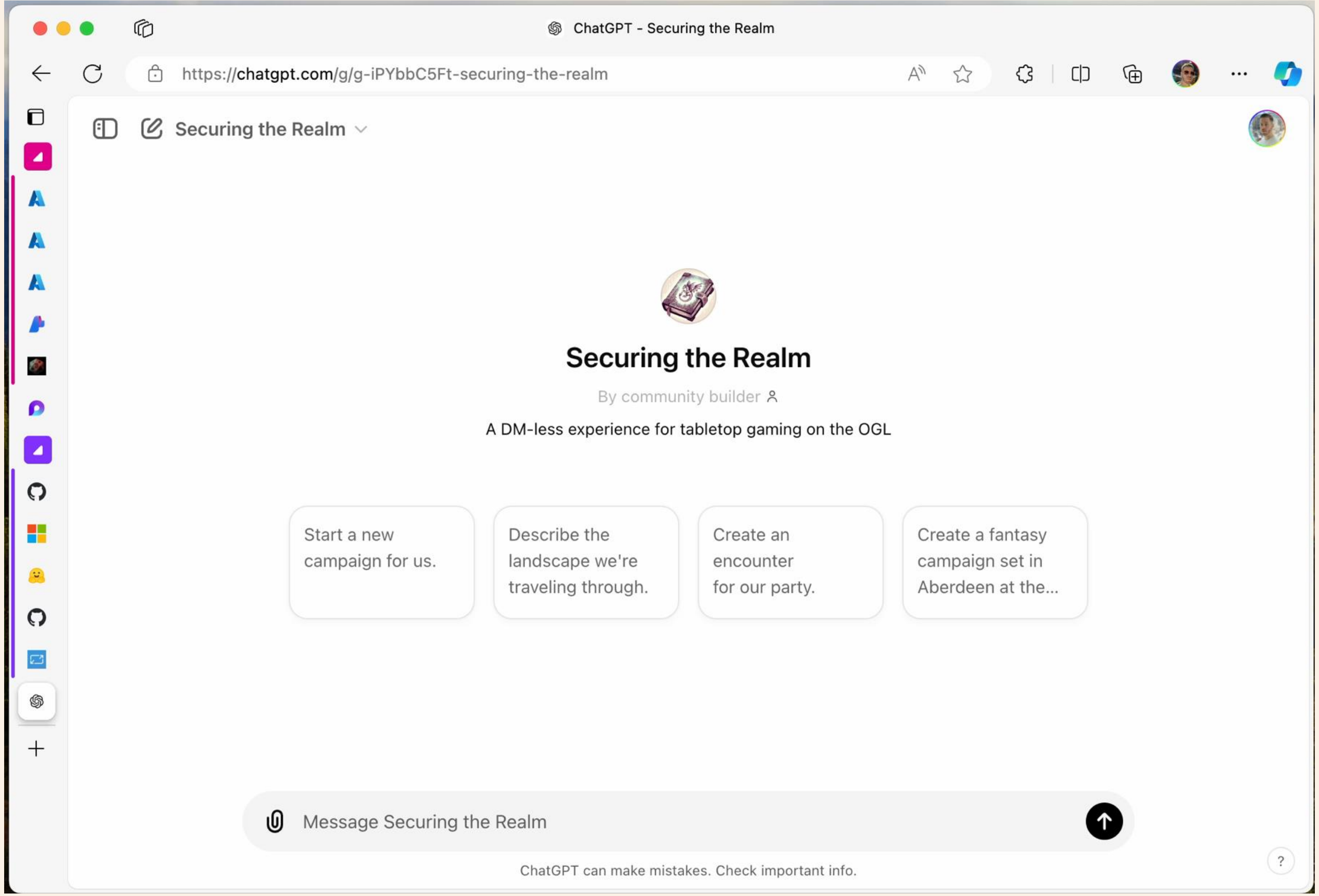
DEMO 1 - Functional Prototype

- Pretty good to get going!
- Bound by limitations at the platform level
- Shouldn't be afraid of starting this way (subject to compliance and sensitivity of data)

ChatGPT Prototype – scan to test!

https://chatgpt.com/g/g-iPYbbC5Ft-securing-the-realm

DEMO RECORDING



ChatGPT - Securing the Realm
https://chatgpt.com/g/g-iPYbbC5Ft-securing-the-realm
Securing the Realm

Securing the Realm

By community builder

A DM-less experience for tabletop gaming on the OGL

Start a new campaign for us.

Describe the landscape we're traveling through.

Create an encounter for our party.

Create a fantasy campaign set in Aberdeen at the...

Message Securing the Realm

ChatGPT can make mistakes. Check important info.

#ScottishSummit2024

Prologue (do you see the theme now?)

Enchantments

- Rapid time-to-MVP
- Rapid iteration
- Excellent prototyping
- Prompt and data source driven

Hexes

- Lack of statefulness
- Difficulty tracking character/story progress - token constraints
- Hallucinations
- Lack of integration, impacting UX and usefulness of data

Not a DM…

The Adventure Begins!

AI DM vs DM-less

A difference between augmenting vs automating human fulfilled processes

Hardening

How might we mitigate against security/IP/safety risks?

ACT I

Summoning the Kobold

ACT I – Campaign Creation

Baby Steps

Let's see what we can recreate, just using an Azure OpenAI deployment.

Systems Reference Document

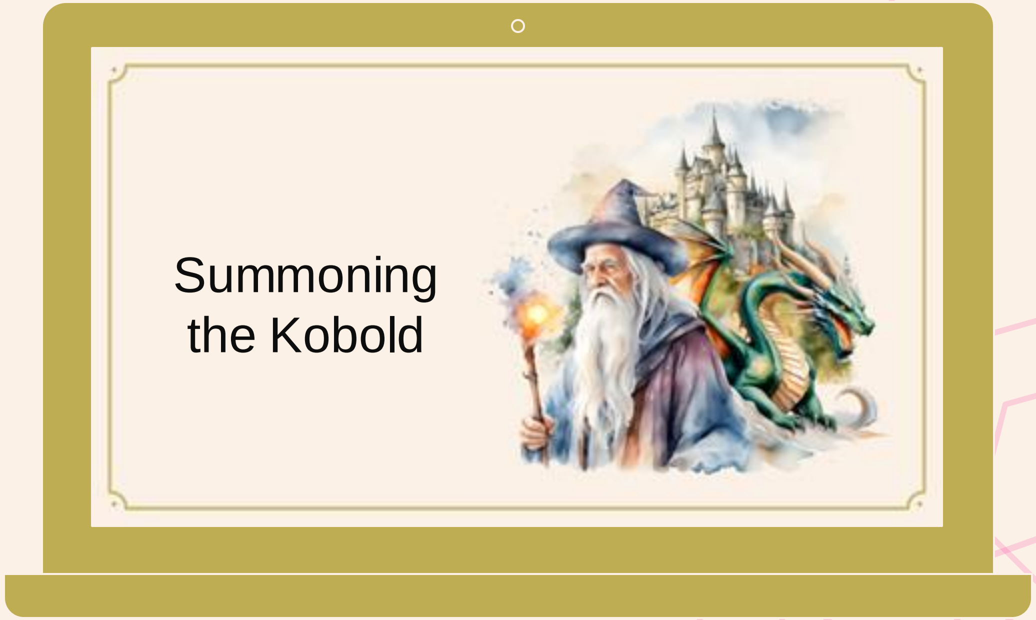
Not yet referenced – let's see what the model already has in its dataset.

Data

We start by using the player interaction to guide the interaction.

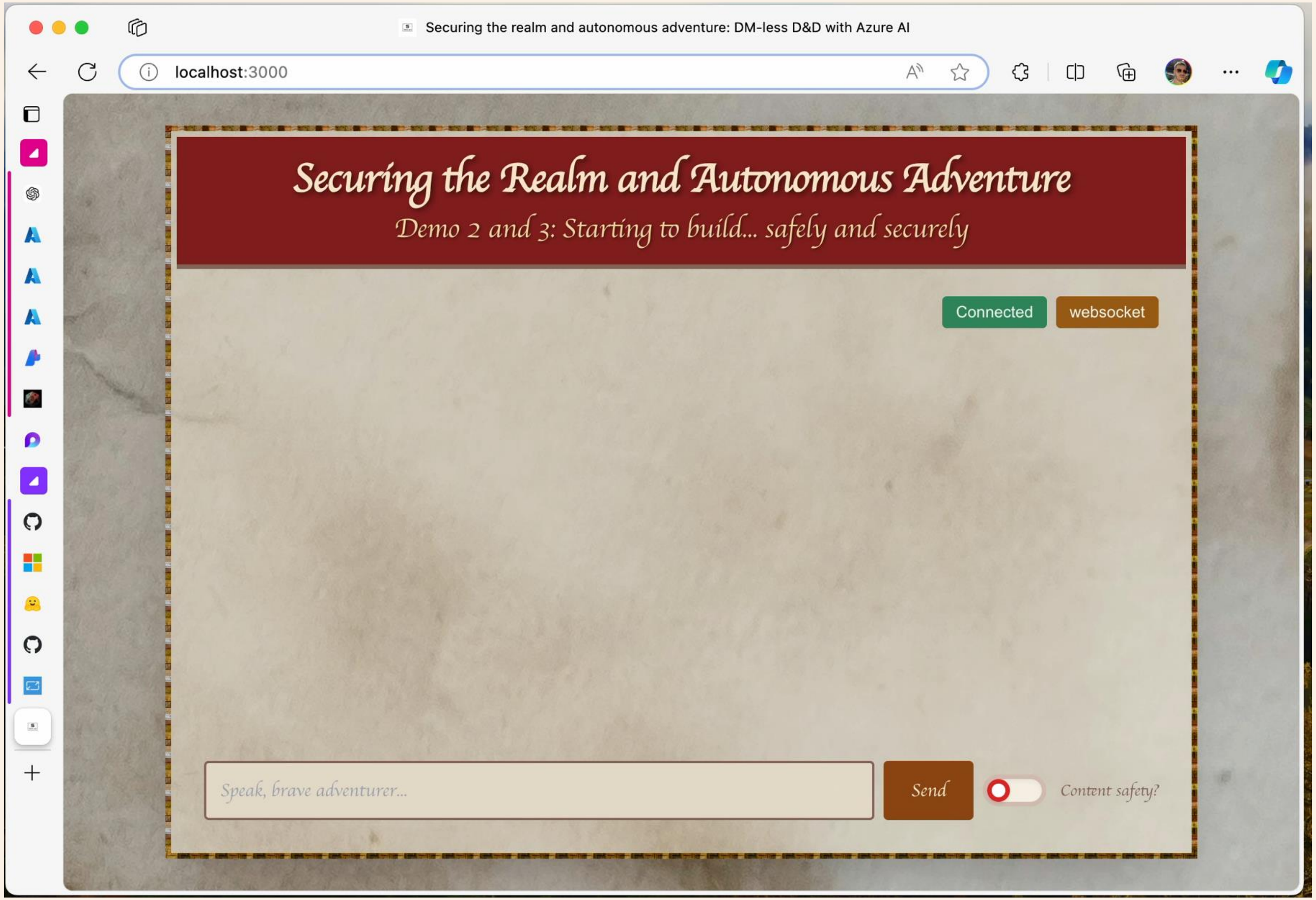
DEMO 2 – Start a Campaign

- Understand the player’s wishes
- Set out a world based upon the vision of the player
- Understand and introduce their character(s)



Summoning
the Kobold

DEMO RECORDING



Securing the realm and autonomous adventure: DM-less D&D with Azure AI

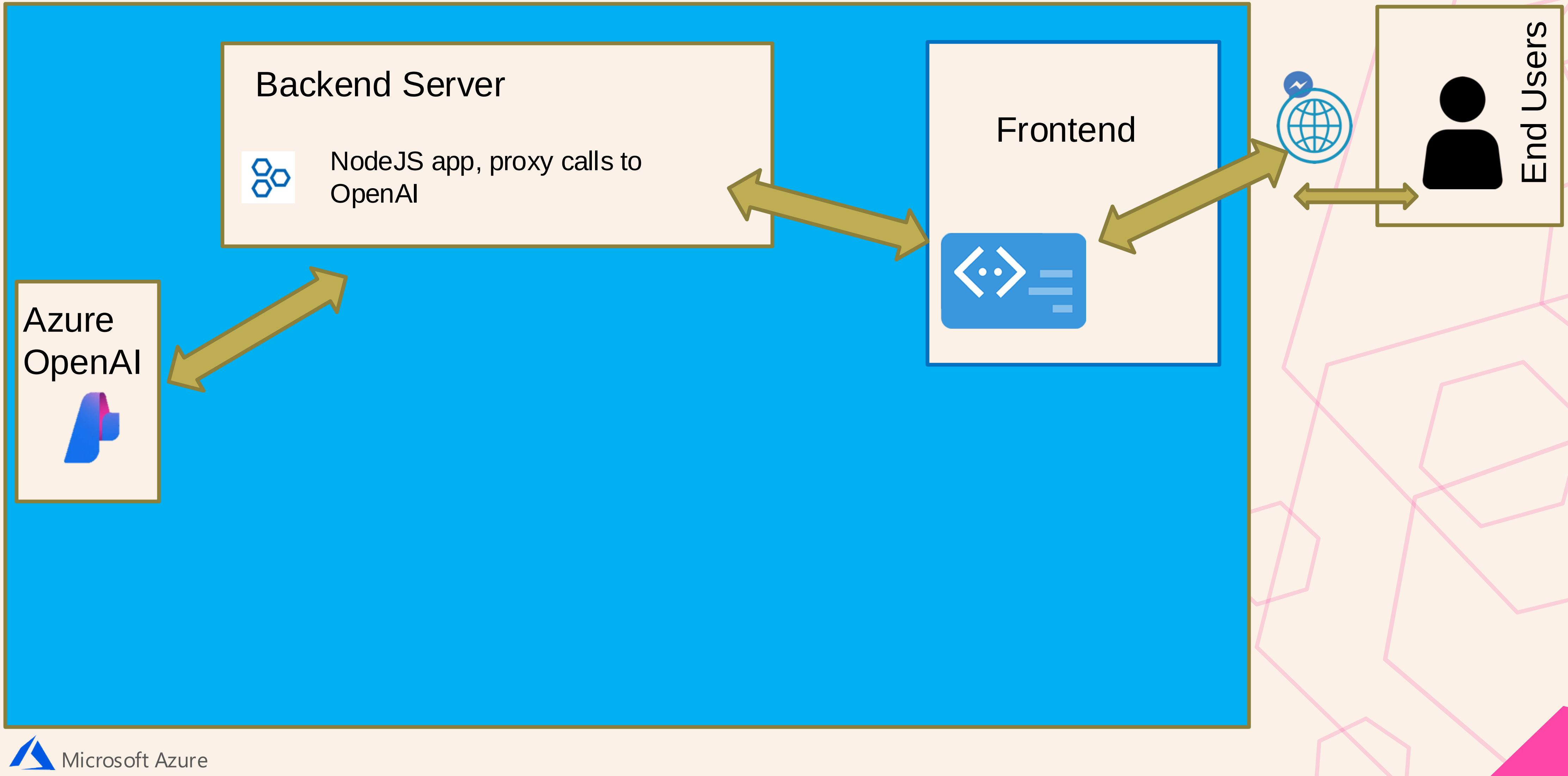
localhost:3000

Securing the Realm and Autonomous Adventure

Demo 2 and 3: Starting to build... safely and securely

#ScottishSummit2024

DEMO 2 – Initial architecture



ACT I – A Threat!

Threat

✦ ✦ ✦

We need our hero...

#ScottishSummit2024

ACT I – Enter Azure Content Safety

Fighting Back

✦✦✦

Putting the safety into D&D

#ScottishSummit2024

ACT I – How we Implemented this

Azure Prompt Shield

- Protects LLMs from malicious or harmful inputs, known as "prompt injection" attacks
- Can scan models in real time
- Can also scan attached documents

Azure Content Safety

- Already turned on for Azure OpenAI deployments
- Scans outputs for risk of harm, sexual content, violence, etc

Let’s look at the configuration options in Azure...

DEMO 3 -The Quest Hook

- Player takes their first steps and interacts with the world around them
- The plot begins!
- Interact with some Non-Player Characters (NPC's)

Constraining the Kobold

ACT I – What else could we consider?

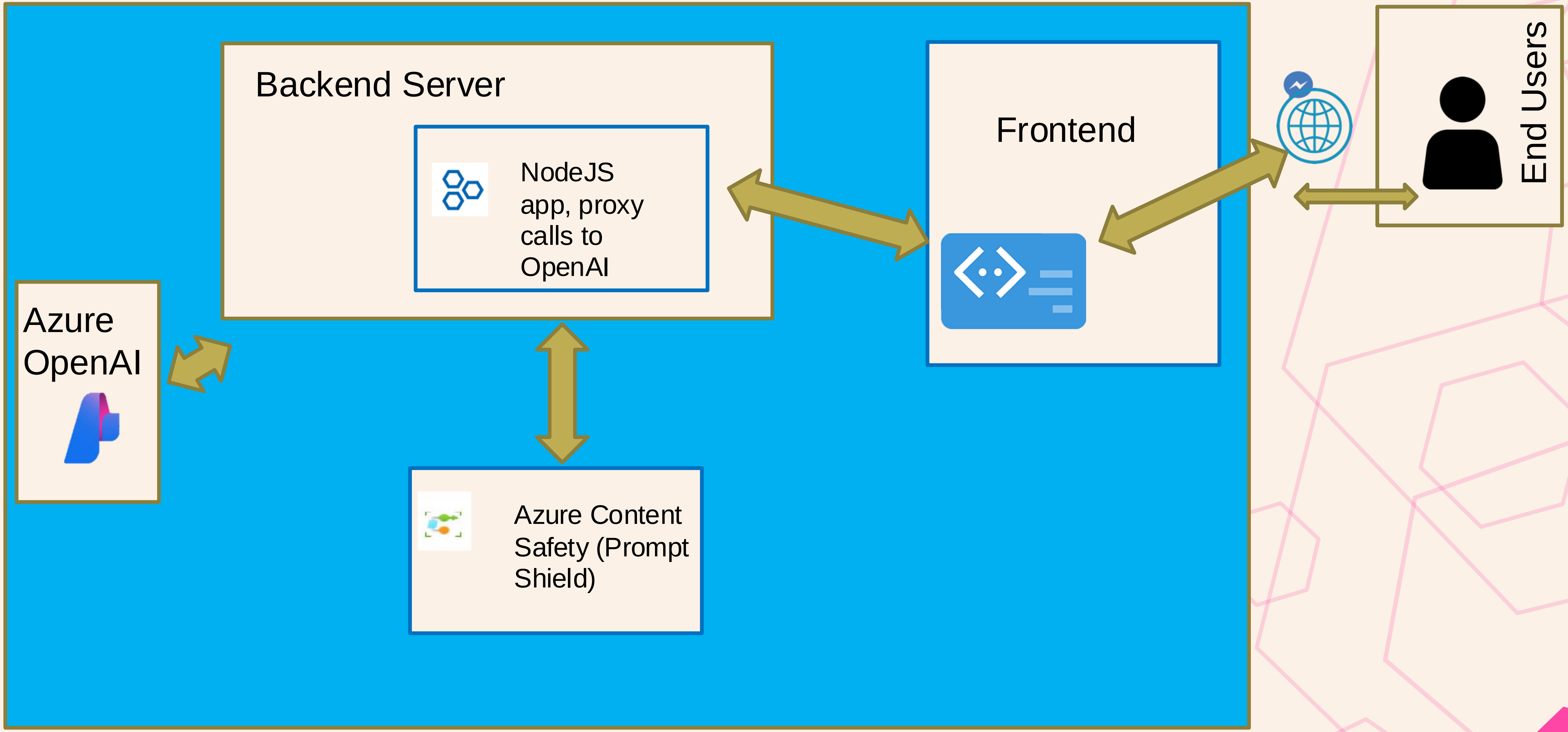
Groundedness API

- Also part of AI Azure AI Content Safety
- Q&A type functionality – checks the model is responding using information provided
- Content source is player character sheets
- Reasoning not required, would slow down interaction

Protected Material API

- You get the idea… it's an AI Content Safety feature
- Prevents you emitting protected intellectual property
- Help mitigate accidental breach of Open Game License
- We could prevent use of third-party IP (Dungeons & Dragons or independent publications)
- Plug & play

DEMO 3 – Updated architecture


Backend Server
NodeJS app, proxy calls to OpenAI
Frontend
End Users
Azure OpenAI
Azure Content Safety (Prompt Shield)

Microsoft Azure

#ScottishSummit2024

ACT I – Summary

Enchantments

- More targeted completion quality
- Greater potential for optimised retrieval
- Extended services (e.g. Content Safety)

Hexes

- Lack of statefulness
- Difficulty tracking character/story progress - token constraints
- Hallucinations
- Lack of integration, impacting UX and usefulness of data

Something is missing from the immersion...

ACT II

Training the Kobold

ACT II – Enhancing the Experience

Images

Generating images to showcase what the area looks like.

Voice

A dungeon master doesn’t furiously type…

SLMs

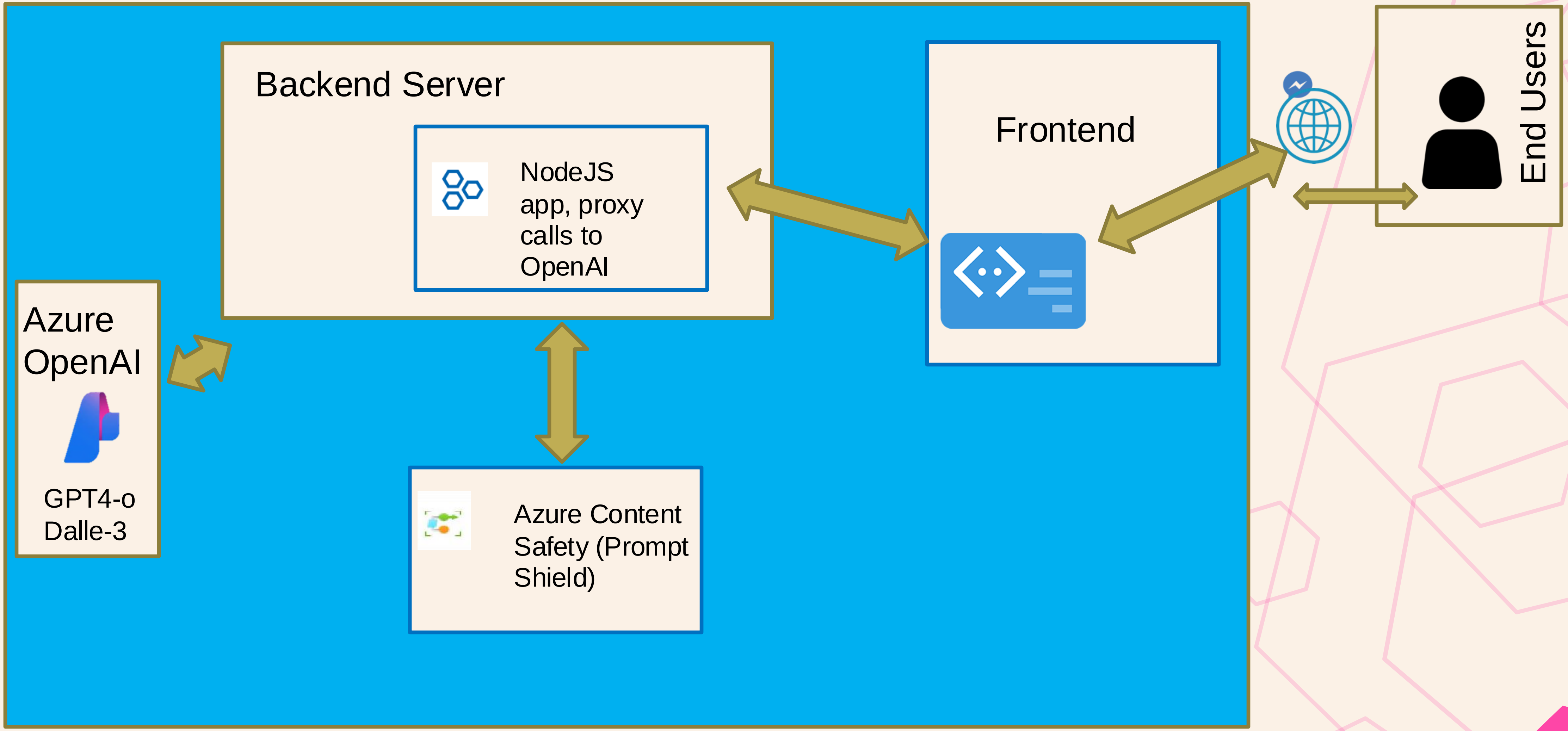
Using SLMs to generate ambient effects in the background.

DEMO 4 –Image Generation

- The player is challenged
- Learning that not everything needs a modern technology solution
- Model reactions based upon the roll of the die (and verifying the die influenced the outcome)

Kobold Projects Images to See

DEMO 4 – Updated architecture


Backend Server
NodeJS app, proxy calls to OpenAI
Frontend
End Users
Azure OpenAI
GPT4-o
Dalle-3
Azure Content Safety (Prompt Shield)

Microsoft Azure

#ScottishSummit2024

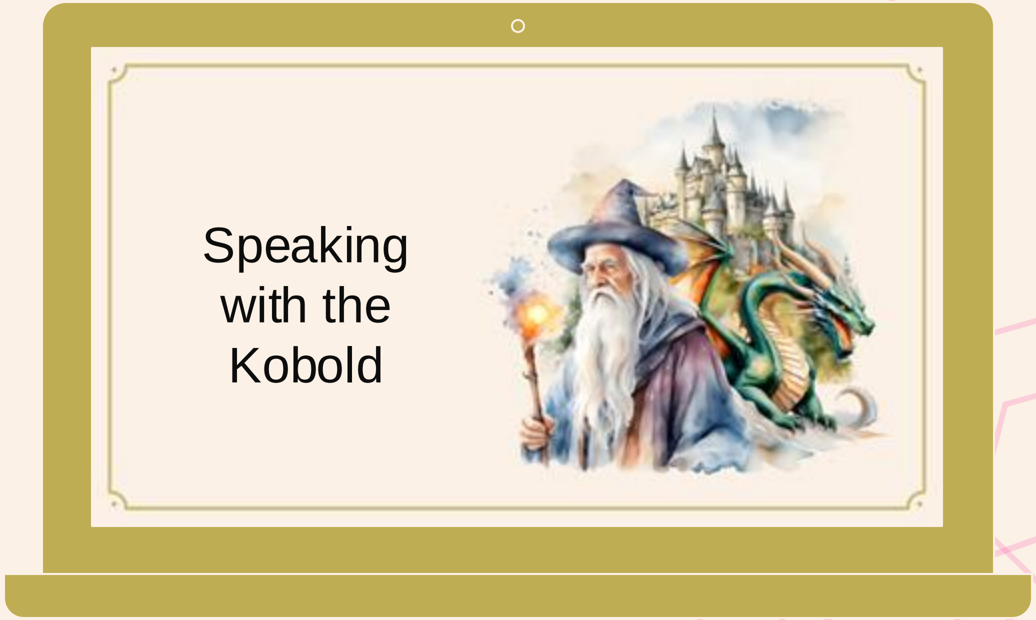
Roleplay

✦✦✦

- Natural conversation
- Conversing with NPCs

DEMO 5 – Time to barter

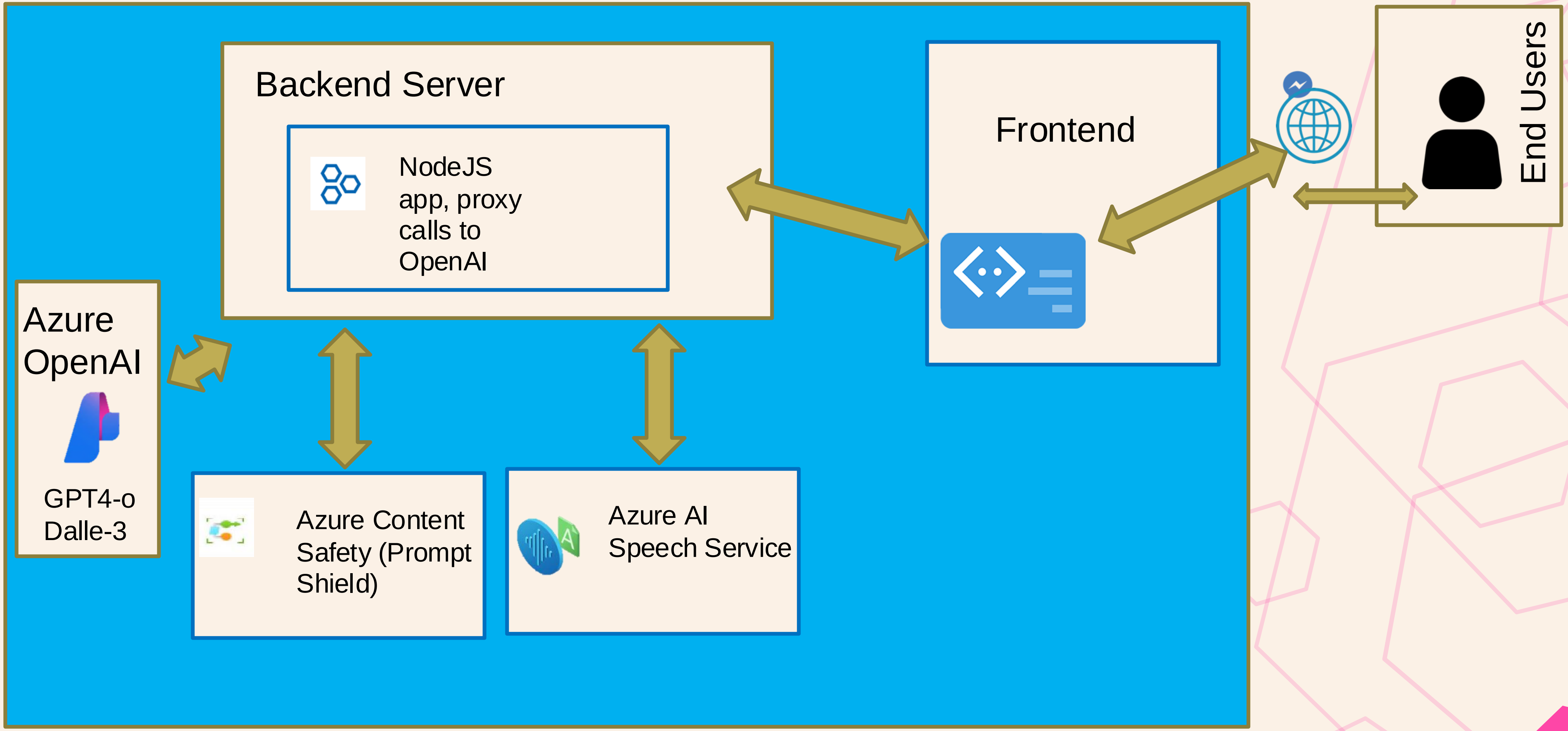
- Using natural language to engage with the NPC
- Purchasing goods from the trader
- Haggling for gold



Speaking with the Kobold

#ScottishSummit2024

DEMO 5 – Updated architecture

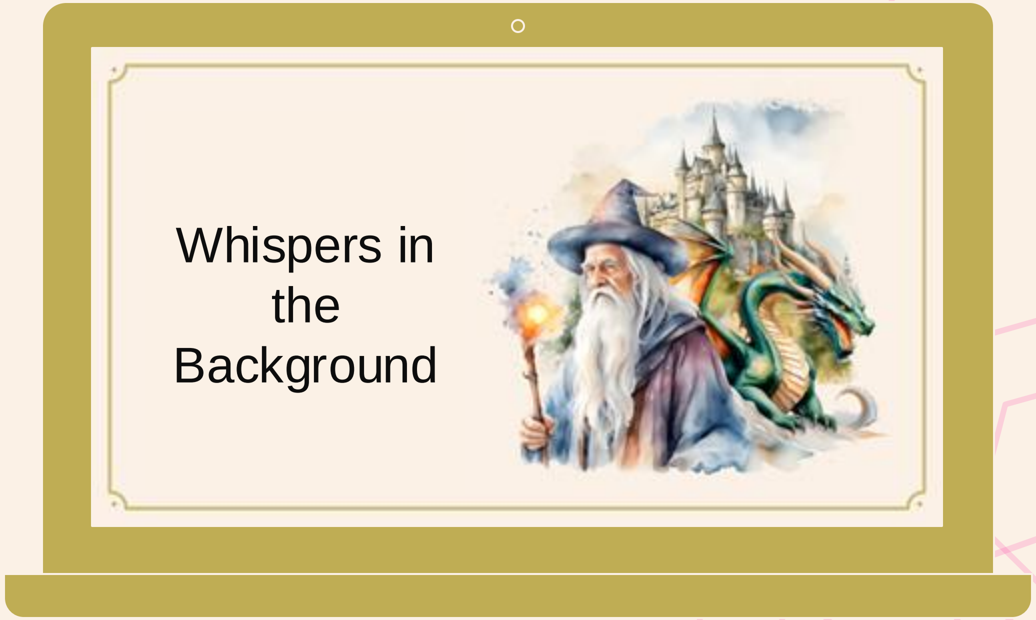


Microsoft Azure

#ScottishSummit2024

DEMO 6 – What's going on over there?

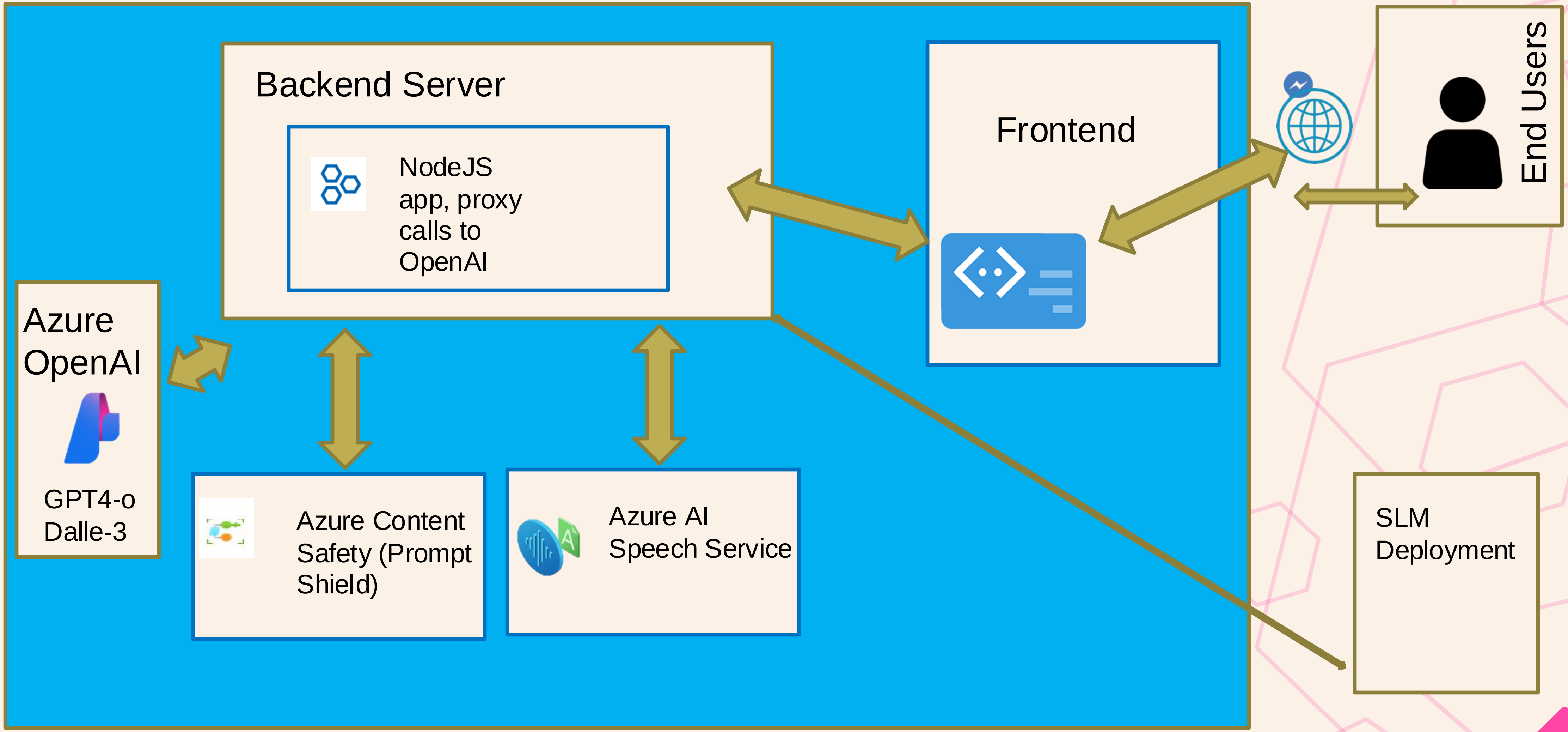
- Using SLMs (the smallest model suitable for the job) to provide ambient effects
- Supporting additional immersion, demonstrating what's going on around the player



Whispers in the Background

#ScottishSummit2024

DEMO 6 – Updated architecture



Microsoft Azure

#ScottishSummit2024

ACT II – Summary

Enchantments

- Image wizardry – now we can see
- Ongoing background chatter
- Voice! We can now talk to the Kobold
- A step towards ambient compute?

Hexes

- Lack of statefulness
- Difficulty tracking character/story progress - token constraints
- Hallucinations
- Lack of integration, impacting UX and usefulness of data

Pretty good…

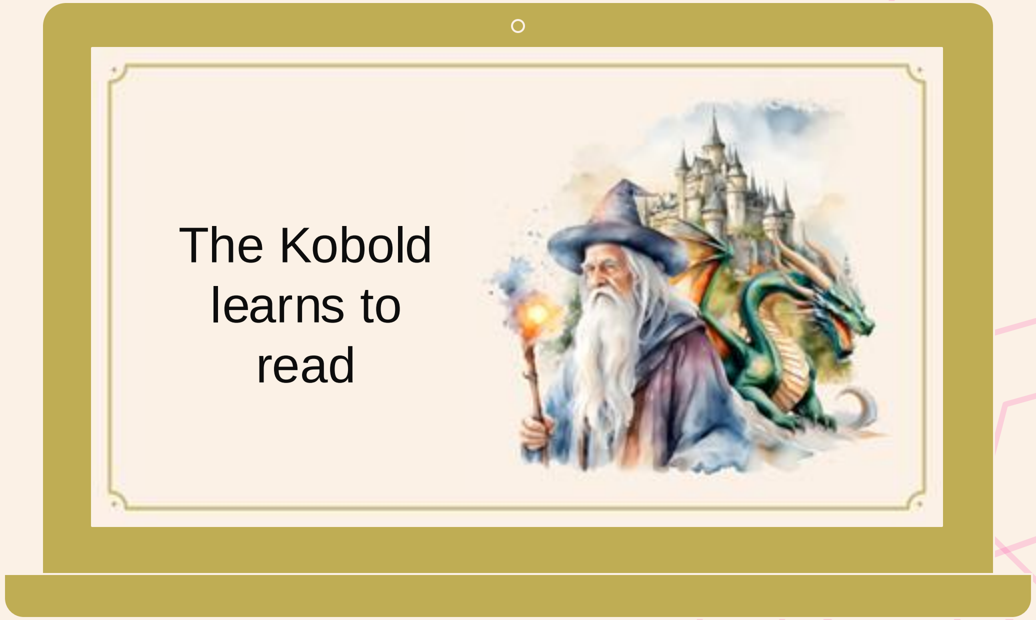
#ScottishSummit2024

ACT III

Kobold goes Awry

ACT III – Time to learn

- Comparing different approaches - Retrieval Augmented Generation vs Finetuning



The Kobold learns to read

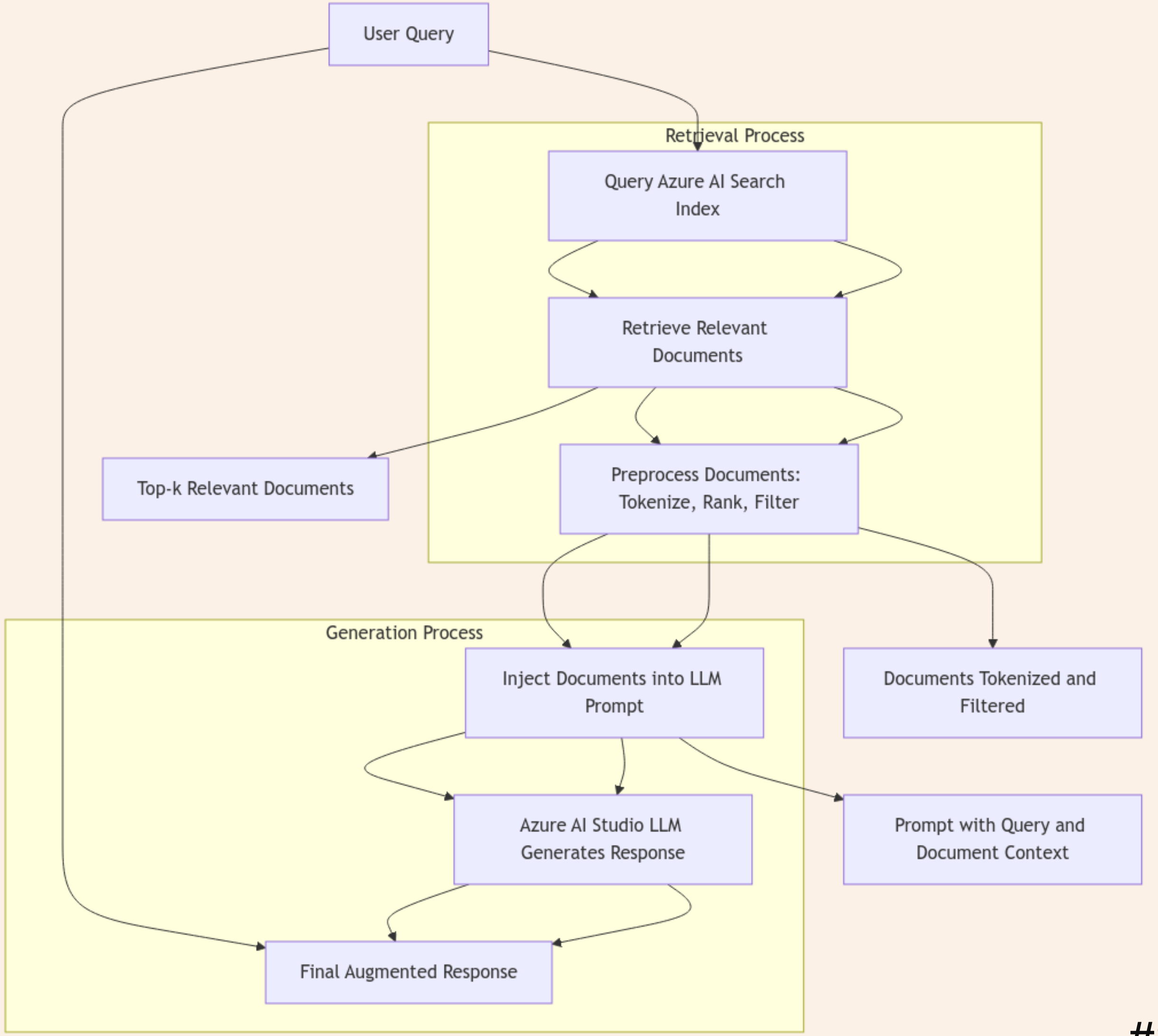
ACT III – How does finetuning work?

- Azure AI fine-tuning allows you to take a pre-trained AI model and customise it to better fit your specific task or data, without having to train a model from scratch.
- For Azure AI Chat Completions, data is uploaded in a JSONL Q/A pair, like so:

```
{"messages": [{"role": "system", "content": "You are an Xbox
customer support agent whose primary goal is to help users with
issues they are experiencing with their Xbox devices. You are
friendly and concise. You only provide factual answers to queries,
and do not provide answers that are not related to Xbox."},
{"role": "user", "content": "Is Xbox better than PlayStation?"},
{"role": "assistant", "content": "I apologize, but I cannot
provide personal opinions. My primary job is to assist you with
any issues related to your Xbox device. Do you have any Xbox-
related issues that need addressing?"}]}
```

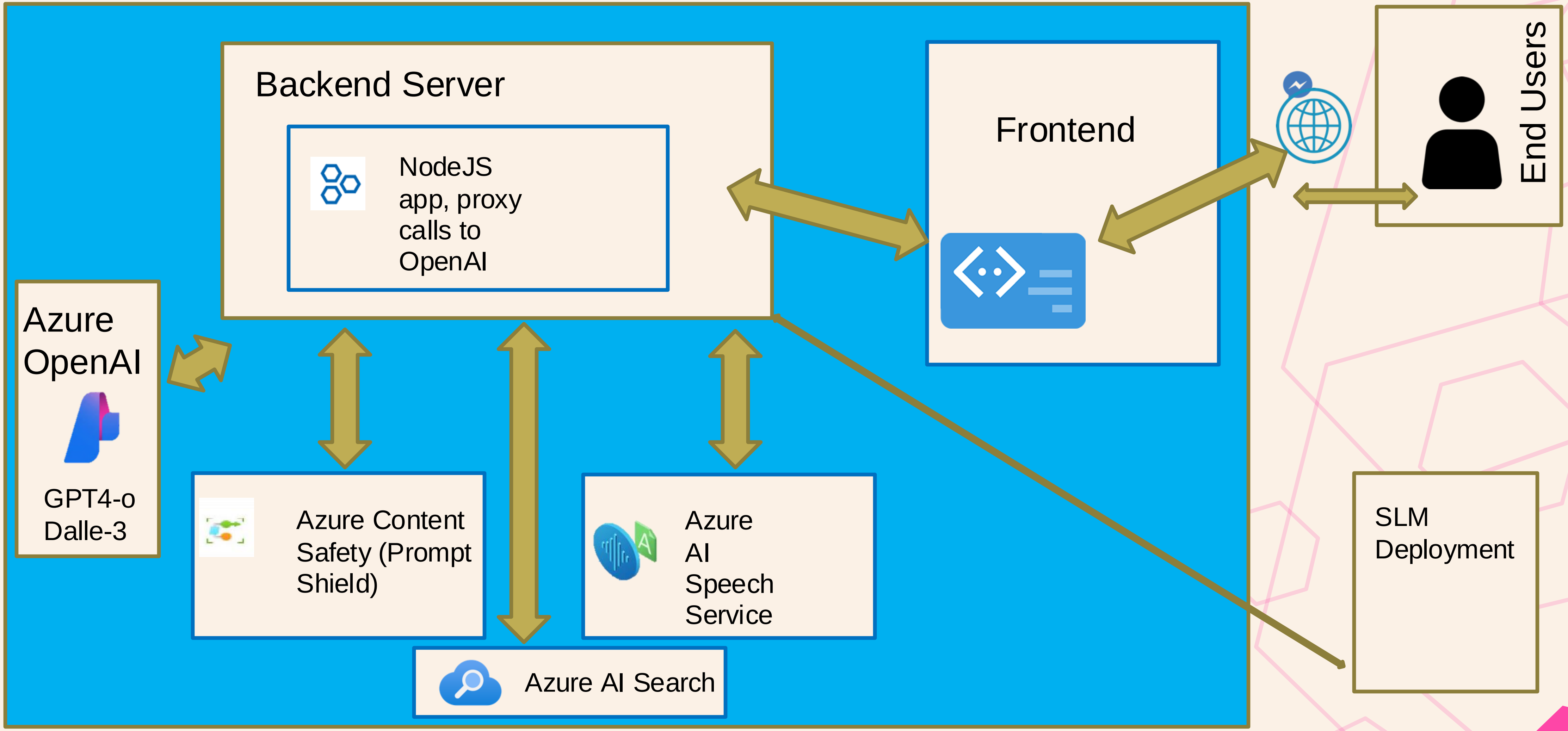
Source: Microsoft, Customize a model with fine-tuning

ACT III – How does RAG work?


User Query
Retrieval Process
Query Azure AI Search Index
Retrieve Relevant Documents
Top-k Relevant Documents
Preprocess Documents: Tokenize, Rank, Filter
Generation Process
Inject Documents into LLM Prompt
Documents Tokenized and Filtered
Azure AI Studio LLM Generates Response
Prompt with Query and Document Context
Final Augmented Response

#ScottishSummit2024

~~DEMO 7~~ - Updated architecture



Microsoft Azure

#ScottishSummit2024

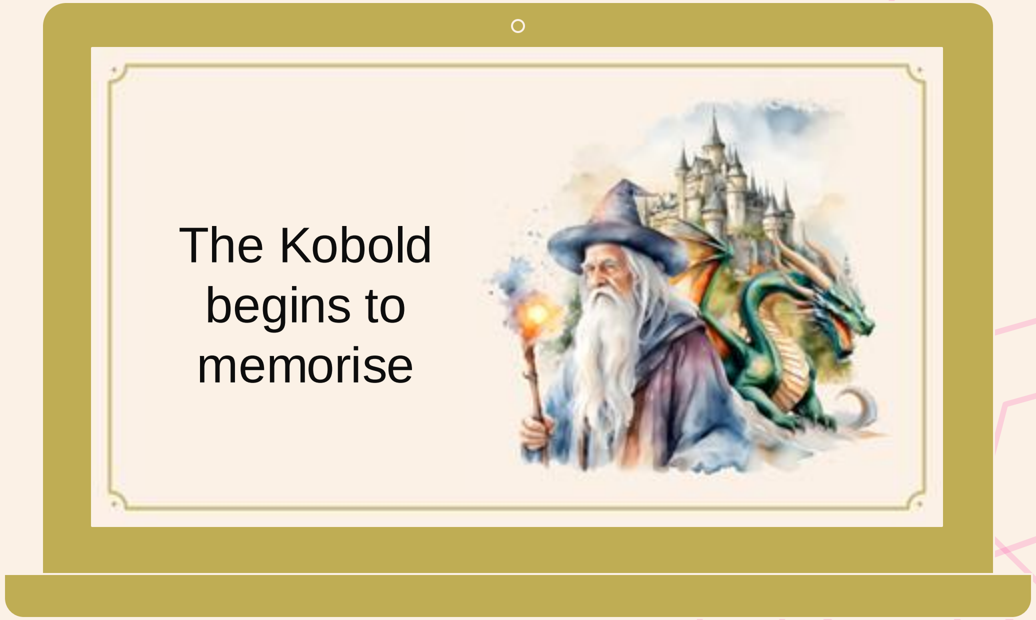
ACT III – Encounters

Encounters

- State (including time)
- Emulating Space
- Lots of rules

ACT III – BATTLE STATIONS!

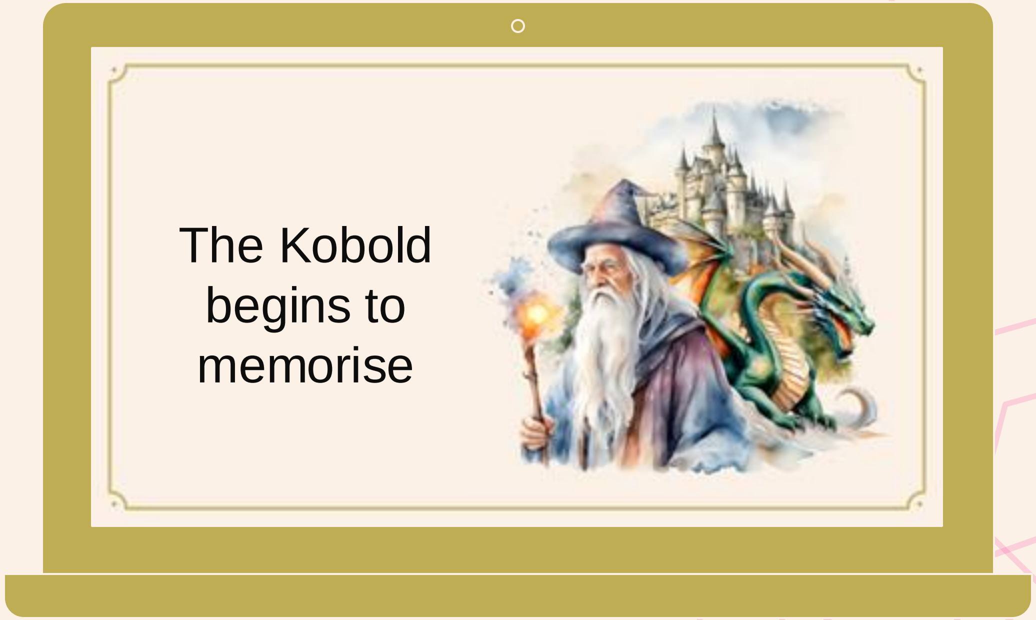
- Identify distance and validate its contextual significance
- Update a character stat
- The voice of the storyteller



The Kobold begins to memorise

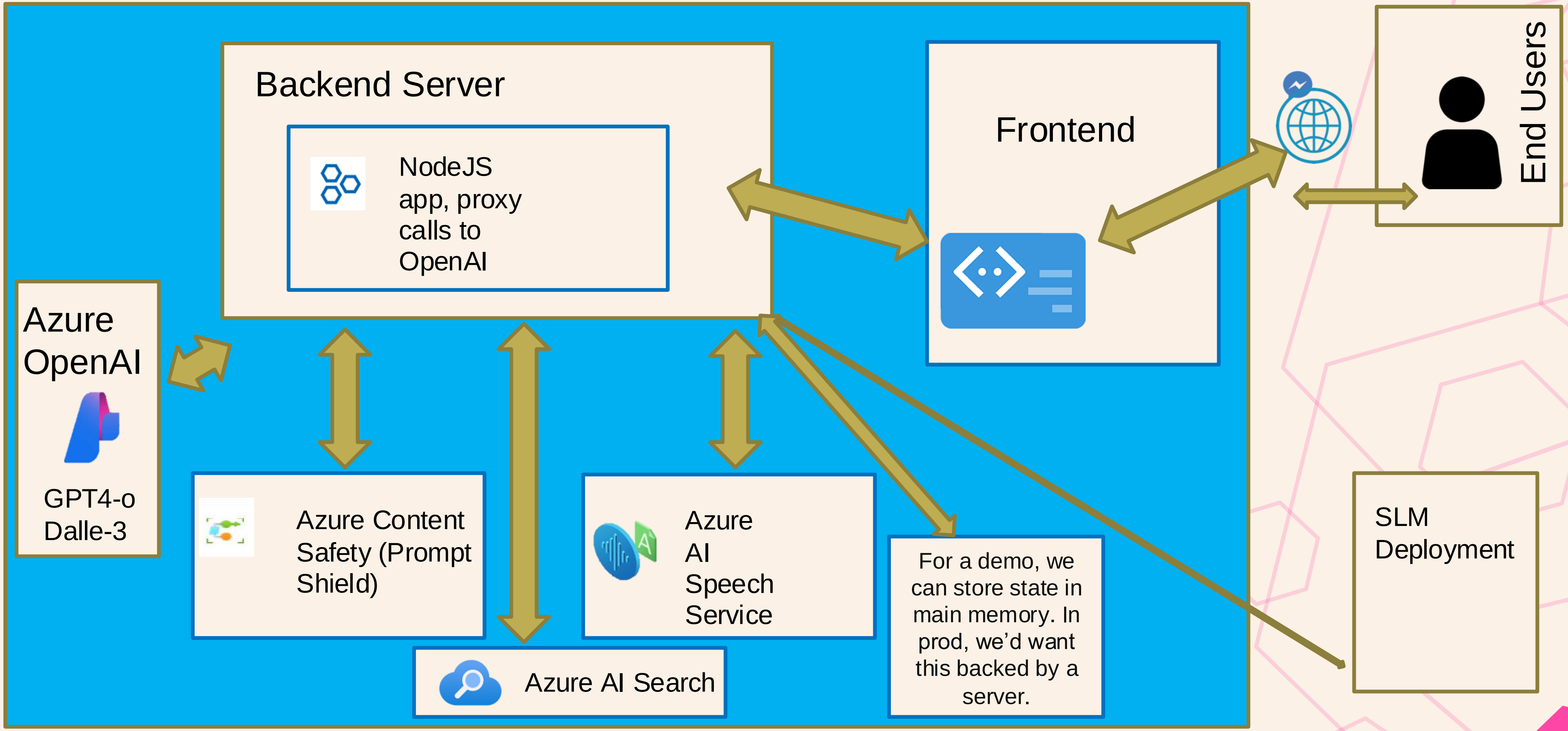
ACT III – Time to remember

- How best to store state?
- This system wasn't designed agentically – for a future iteration, and with multiple player characters, that's probably a more flexible approach
- Providing tools to the model to store, and retrieve specific information



The Kobold begins to memorise

DEMO 8 – Updated architecture



For a demo, we can store state in main memory. In prod, we'd want this backed by a server.

Microsoft Azure

#ScottishSummit2024

ACT III – Summary

Enchantments

- Voice
- State
- Ambient notifications from SLMs

Hexes

- No real tracking of different characters
- Not the best understanding of the rules

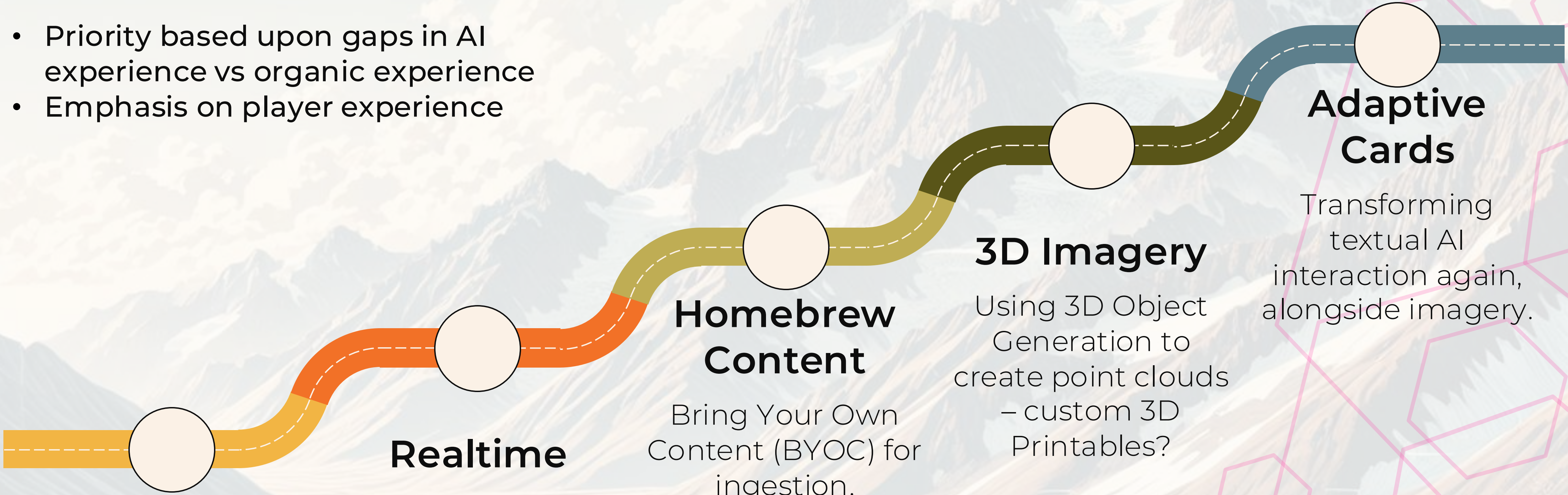
Lots we could build on in the future...

Epilogue

The Apprentice’ Master is Pleased… for now

Epilogue – What Next?

- Priority based upon gaps in AI experience vs organic experience
- Emphasis on player experience



Maps/Terrain

Pre-generated, followed by procedural.

Realtime

Swapping voice to the latest GPTo Realtime model for back-and-forth discussions, considering how that could work with multiple players.

Homebrew Content

Bring Your Own Content (BYOC) for ingestion.

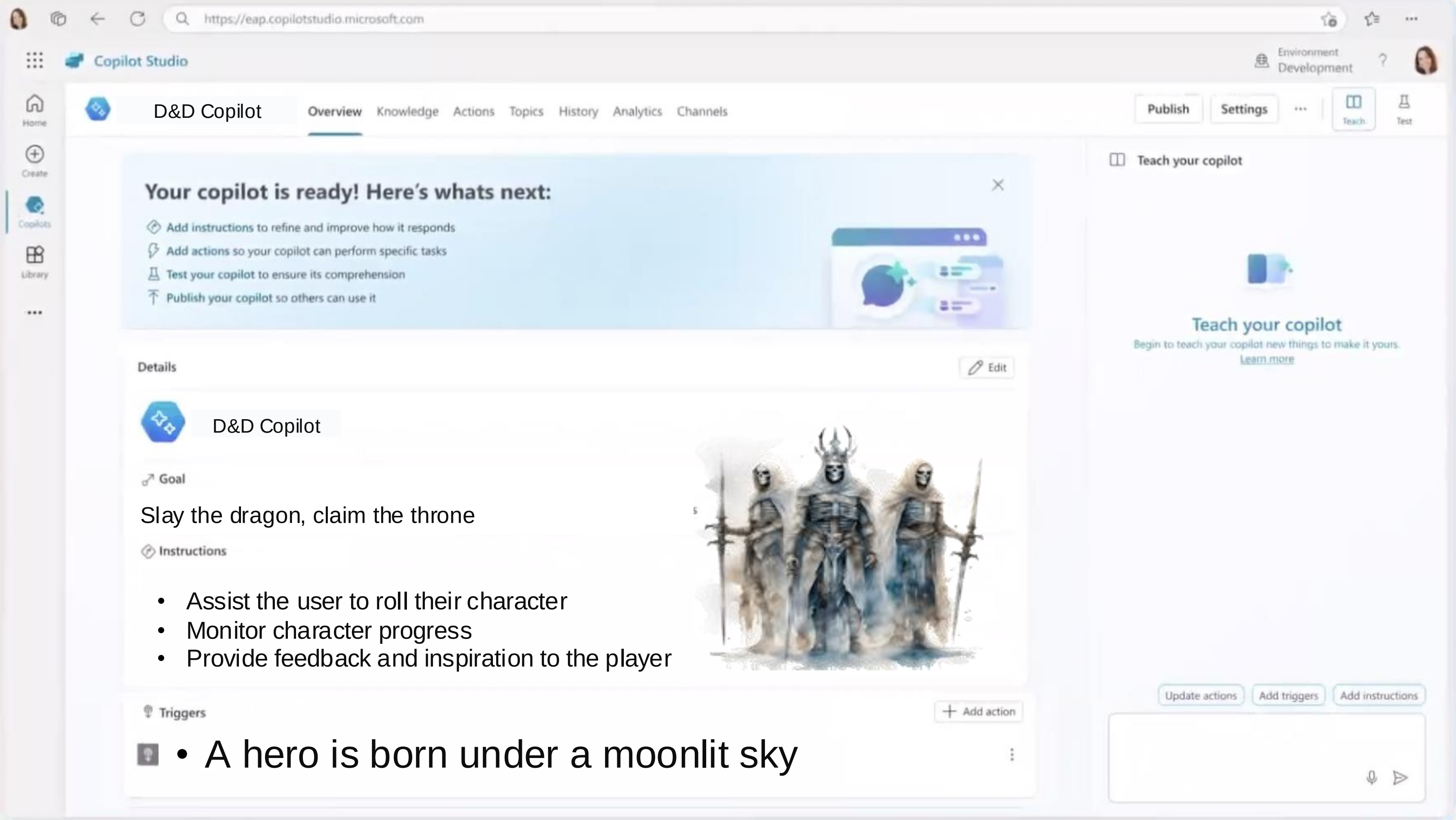
3D Imagery

Using 3D Object Generation to create point clouds – custom 3D Printables?

Adaptive Cards

Transforming textual AI interaction again, alongside imagery.

Epilogue – And of course...



Your copilot is ready! Here's whats next:

- Add instructions to refine and improve how it responds
- Add actions so your copilot can perform specific tasks
- Test your copilot to ensure its comprehension
- Publish your copilot so others can use it

Teach your copilot

Teach your copilot

Begin to teach your copilot new things to make it yours.
Learn more

Details

D&D Copilot

Goal

Slay the dragon, claim the throne

Instructions

- Assist the user to roll their character
- Monitor character progress
- Provide feedback and inspiration to the player

Triggers

- A hero is born under a moonlit sky

#ScottishSummit2024

Epilogue – The Apprentice’ Journey

To be continued…?

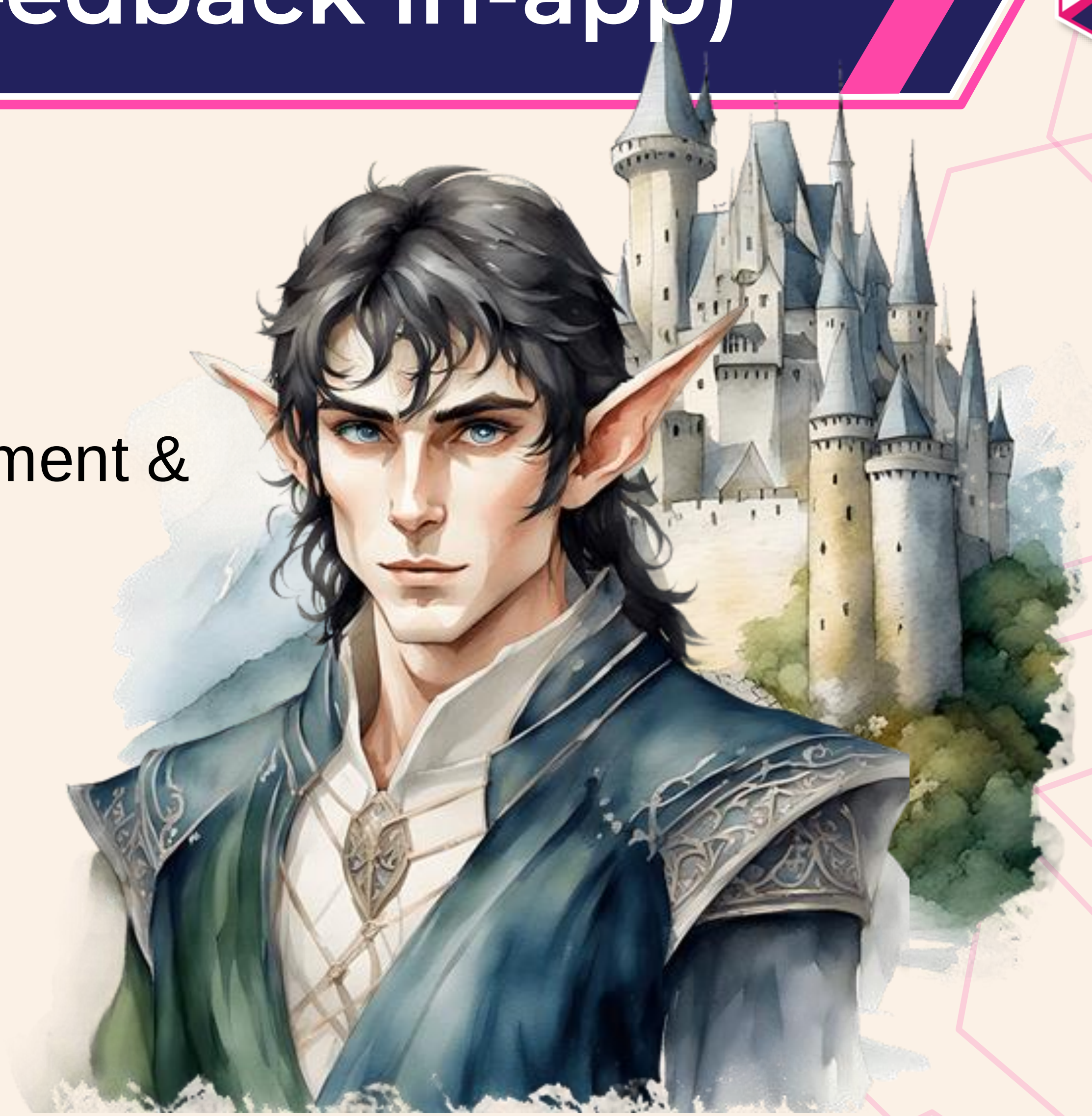
✦✦✦

Q&A (and please leave feedback in-app)

ChatGPT Prototype

System Reference Document & Open Game License

The slides will be shared on the Scottish Summit site – and will include a link out to https://github.com/Sealjay/scottish-summit-dnd (currently marked private.)



Thank You to our Sponsors...

SCOTTISH SUMMIT

Platinum Sponsor

Capgemini

Gold Sponsors

resco

ARROW

dox42®
automate your documents
integrate your data

kerv Digital

#ScottishSummit2024

Thank You to our Sponsors...

SCOTTISH SUMMIT

With Thanks

AGILECADENCE
POWERING INNOVATION. SIMPLIFYING TECHNOLOGY.

Telefónica Tech

LightningTools

Cloud Surge
UNLEASH YOUR POWER

LOGIQAPPS

DYNAMICS MINDS
powered by
DOCENTRIC

mscrm-addons.com
Your company for MS-CRM ADD-ONS!

Noteworthy
.Support

PROMX

Syskit

Click

riada
CONSULTANCY

QUBIX

PROXIMO3

360

#ScottishSummit2024