SiloX-GPT

Content Search

Datensilos verbinden mittels Multi-Agenten-Systemen

Data2Day 2024



Moritz Glauner

Head of Data Science @ Bertelsmann





Nico Kreiling

Data Scientist @ scieneers

Host of <u>techtiefen.de</u>







Why classical RAG was not an option...



€20.2 Billion

Group revenues



€1,326 Million

Group profit



Gütersloh

Headquarters



€3,119 Million

Operating EBITDA



80,418

Employees









BERTELSMANN

arvato group



Bertelsmann **Education Group**







At our starting-point, is was not yet clear, that LLMs can work with Knowledge-Graphs (very well)

Initial Situation:

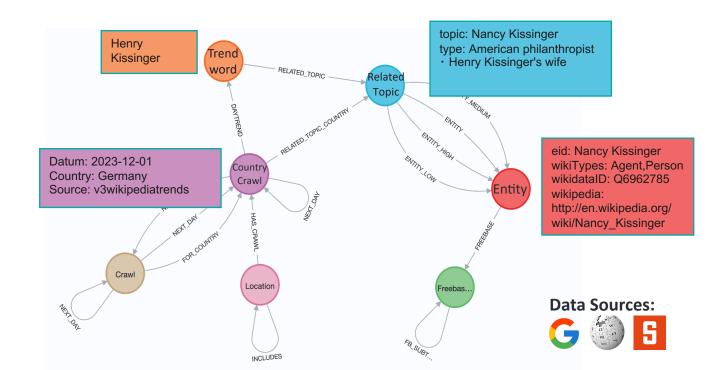
Existing knowledge graph from predecessor project in Neo4J

Research-Question:

Can natural questions be answered by an LLM and a Knowledge-Graph?

Learnings:

- GPT4 can write decent cypher querries when prompted with schema and some examples
- Simple-intuitive schemas work better then complex-formel
- We want to have a natural-language answer



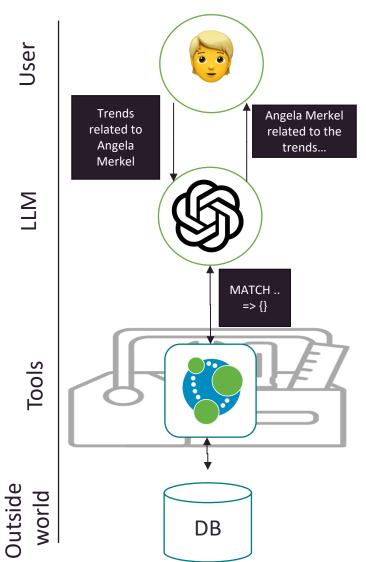




Agents enable LLMs to do real work

Agents give LLMs the ability to interact with the world by executing programs

- Minimal version: Simple function-call with one parameter
- Complex version: Browsing or writing and testing own source code



User

Welche Trends stehen in Bezug zu Angela Merkel?

LLM

Trigger function: execute_cypher
With cypher="MATCH
(c:CountryCrawl) - [d:DAYTREND] > (t:Trendword)
WHERE t.trend= 'Angela Merkel'

Tool

[{year: 2015, topic: Flüchtlingskriese}, {year: 2020, topic: Corona Pandemie}]

LLM

Relevante Trends in Bezug auf Angela Merkel und ihre Kanzlerschaft waren:

- * Flüchtlingskrise: 2015 traf Merkel die kontroverse Entscheidung, Deutschlands Grenzen für Flüchtlinge offen zu halten.
- * Corona-Pandemie: In ihrer letzten Amtszeit war die Bewältigung der COVID-19-Pandemie(2020)

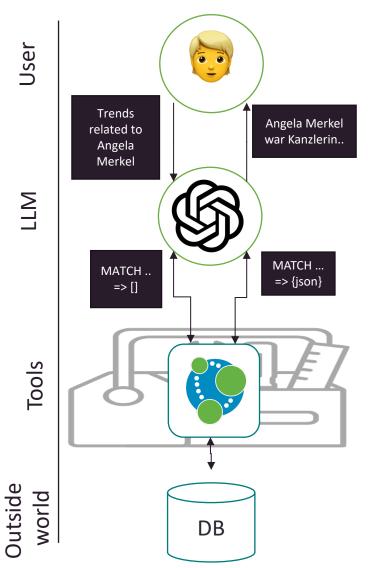




Agents enable LLMs to do real work

Agents give LLMs the ability to interact with the world by executing programs

- Minimal version: Simple function-call with one parameter
- Complex version: Browsing or writing and testing own source code



User

Welche Trends waren besonders relevant für die Kanzlerschaft von Merkel?

LLM

Trigger function: execute_cypher
With cypher="MATCH ... WHERE
t.trend= 'Kanzlerschaft
Merkel'

Tool

[]

LLM

Trigger function: execute_cypher
With cypher="MATCH ... WHERE
t.trend= 'Kanzler'

Tool

[{topic: Angela Merkel}, {topic: Olaf Scholz}]

LLM

Angela Merkel war Kanzlerin der Bundesrepublik Deutschland. Olaf Scholz ist ihr Nachfolger.





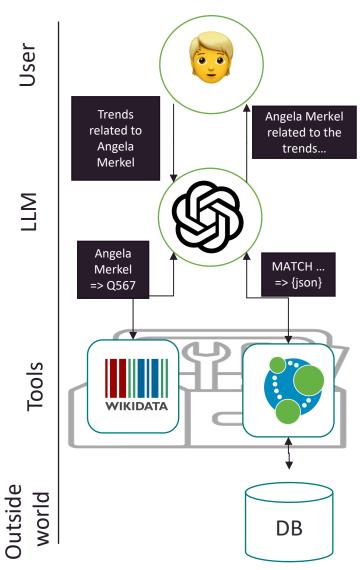
Agents enable LLMs to do real work

Agents give LLMs the ability to interact with the world by executing programs

- Minimal version: Simple function-call with one parameter
- Complex version: Browsing or writing and testing own source code

Learnings:

- Agents are much more powerfull then simple LLMs
- Important to keep the focus of an agent



User

Welche Trends waren besonders relevant für die Kanzlerschaft von Merkel?

LLM

Trigger function: lookup_wikidata_id
With name="Angela Merkel"

Too

Q567

LLM

Trigger function: execute_cypher
With cypher="MATCH (c:CountryCrawl) [d:DAYTREND] -> (t:Trendword)
WHERE t.wikidata id = 'Q567'

Tool

[{year: 2015, topic: Flüchtlingskriese}, {year: 2020, topic: Corona Pandemie}]

LLM

Relevante Trends in Bezug auf Angela Merkel und ihre Kanzlerschaft waren:

- * Flüchtlingskrise: 2015 traf Merkel die kontroverse Entscheidung, Deutschlands Grenzen für Flüchtlinge offen zu halten.
- * Corona-Pandemie: In ihrer letzten Amtszeit war die Bewältigung der COVID-19-Pandemie(2020)



Agents are similiar to humans: Specialication and Collaboration increases the scope of possibilities – and the complexity

Using multiple agents increases flexibility of the system

- Use different LLMs for different tasks
- Have clear and focused system-prompts
- Control the length of the chat-history
- Gain more

But they also increase the complexity

- Requires communication accross agents
- General technical complexity increases







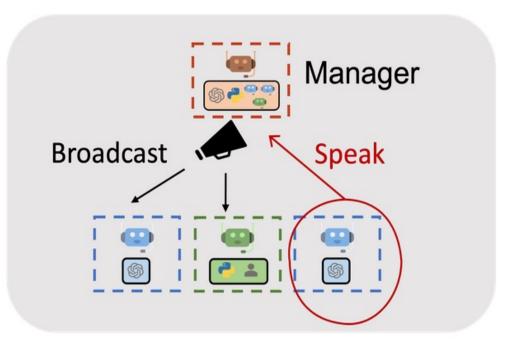
AutoGen uses an open-discussion-style communication

AutoGen in a nutshell:

- AutoGen was the first project that specificly targeted cooperation among multiple agents to solve tasks
- Message flow looks like an open discussion between agents
- Has dedicated agents for user, that is also responsible for tool execution

Learnings:

- Open message flow limits system relieabilty
- No support for parallel execution of agents
- Customization requires deep interventions in code









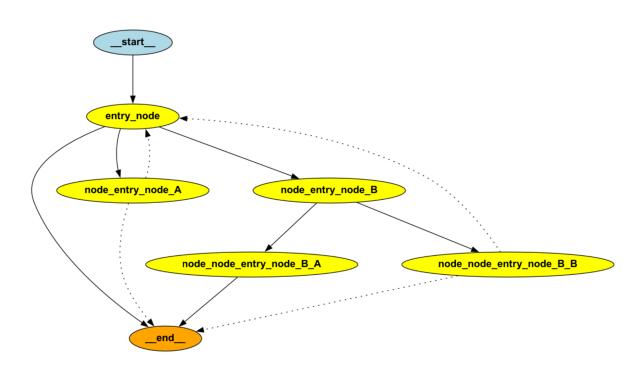
LangGraph uses a graph to design the message flow

LangGraph in a nutshell:

- Released with LangChain v0.1
- Graph design inspired by networkx
- Provides a nice way to realize very complex message flows in a deterministic way
- LangChain ecosystem brings great tool support
- Much better then early LangChain versions, but still not always intuitive

Learnings:

- Graph-Design suits much better to our use-case
- LangChain ecosystem seams more productionready

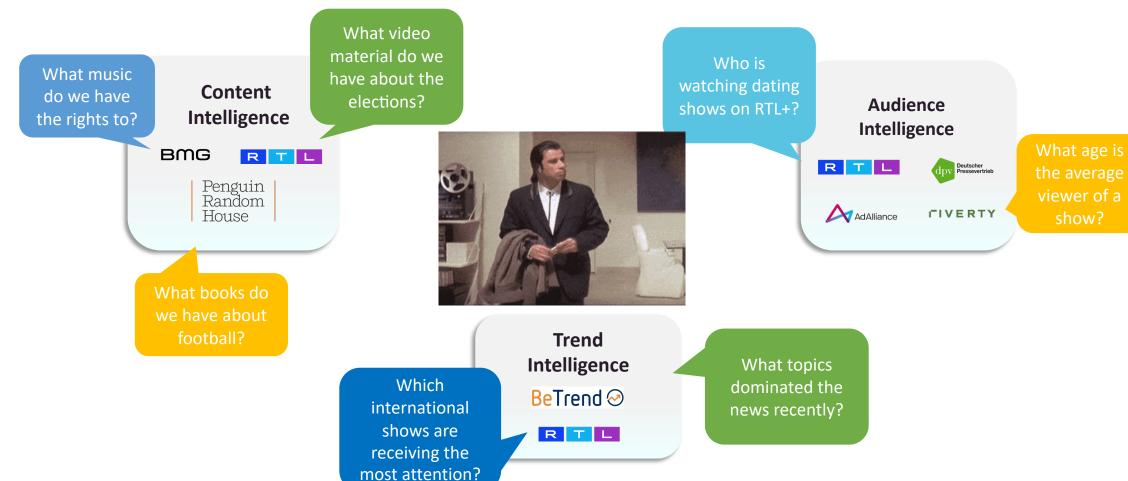








Each division has so much individual knowledge! But it's sometimes hard to make sense of it







How can we query this data?

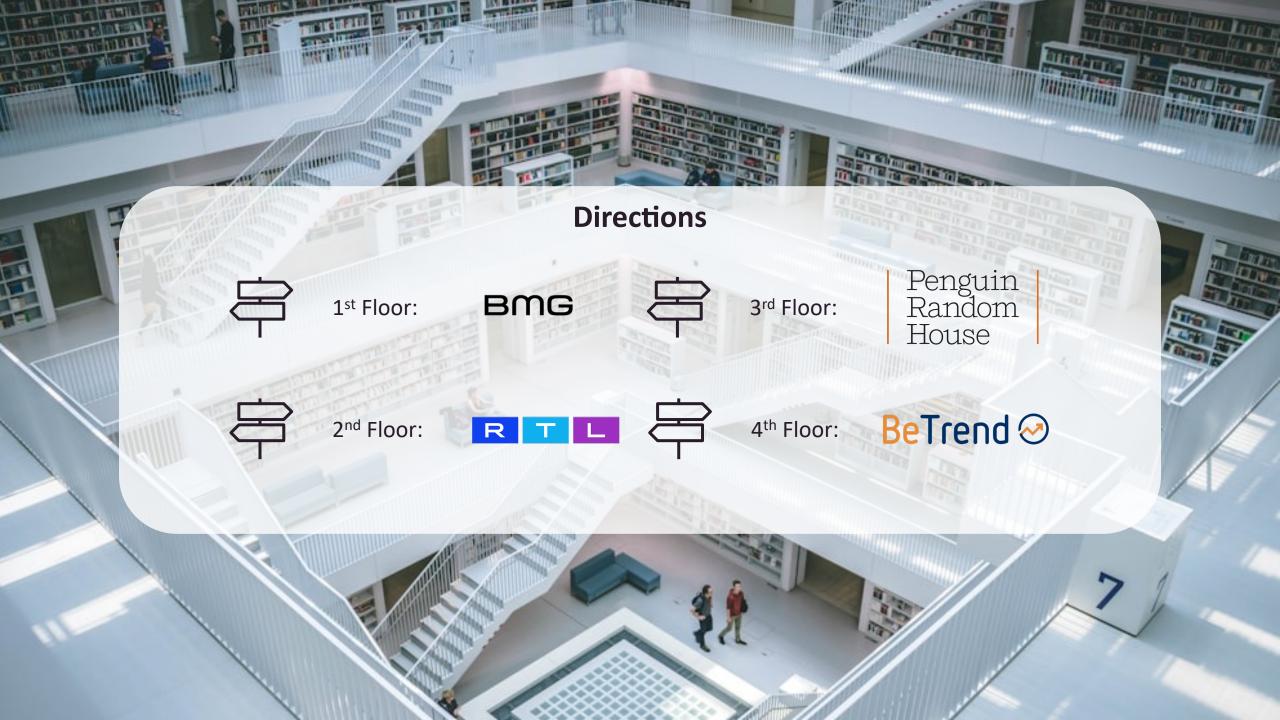
















Different agent-categories are used to access different types of data



Fremantle

BENET

Agents using vector search:

Similar to classical RAG, but with the possibility to add filters and to use tools multiple times

Tools:



IPRNOW



Penguin Random House Verlagsgruppe **API-based Agents**

Using tools that wrap the relevant parts of the specific APIs

Only custom Tools



Graph-Based Agents:

Executes dynamically filled Cypher-Template-Querries



Tools:



Q Websearch

Co-Pilot

Other Agents:

Perform web-search and add relevancy information for the selected agents

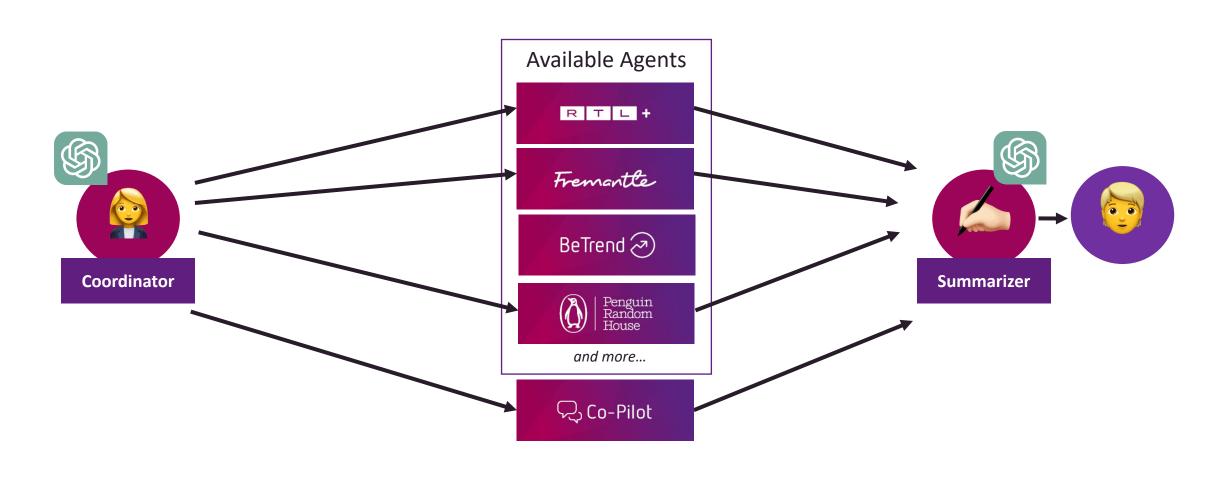
Tools:

Tavily





Based on the user request the relevant agents get triggered to combine them in a single answer





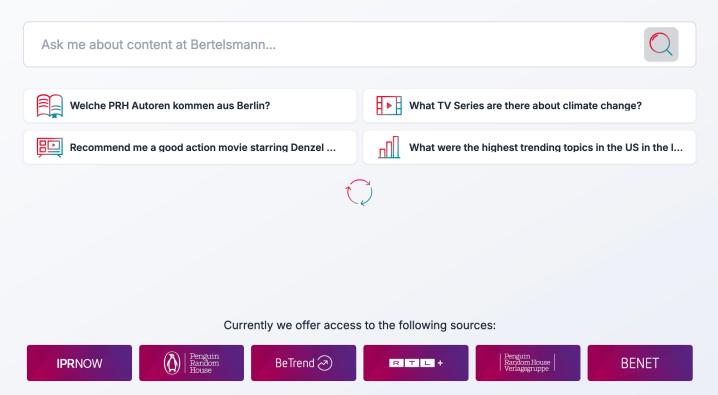
About

FAQ



It's demo time!







The LangChain Ecosystem Offers Much

Most Popular High-Level LLM Building Framework

Getting (a bit) more production ready

- (Mostly) Backwards compatible with major versions now
- v0.3 now with Pydantic 2 support
- \$10M Seed funding

Chains as Core Concept

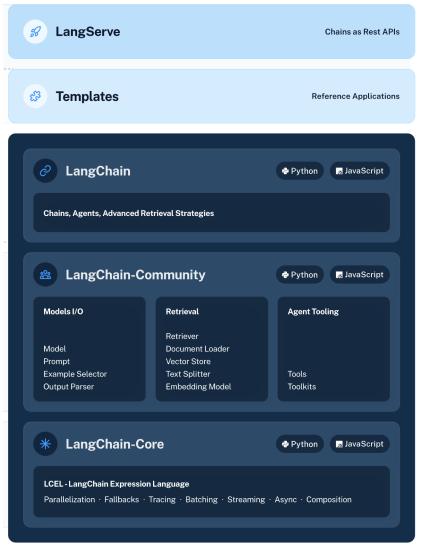
- Chain = Input + Prompt + LLM
- Plus, optional components







LangChain Overview - the core package to create LLM chains







The LangChain Ecosystem goes beyond the LangChain package



Build individual components by combining LLM, storage and prompts



Orchestrate complex flows through one or more components

LangServe

Wrap LangChain chains available as FastAPI endpoints

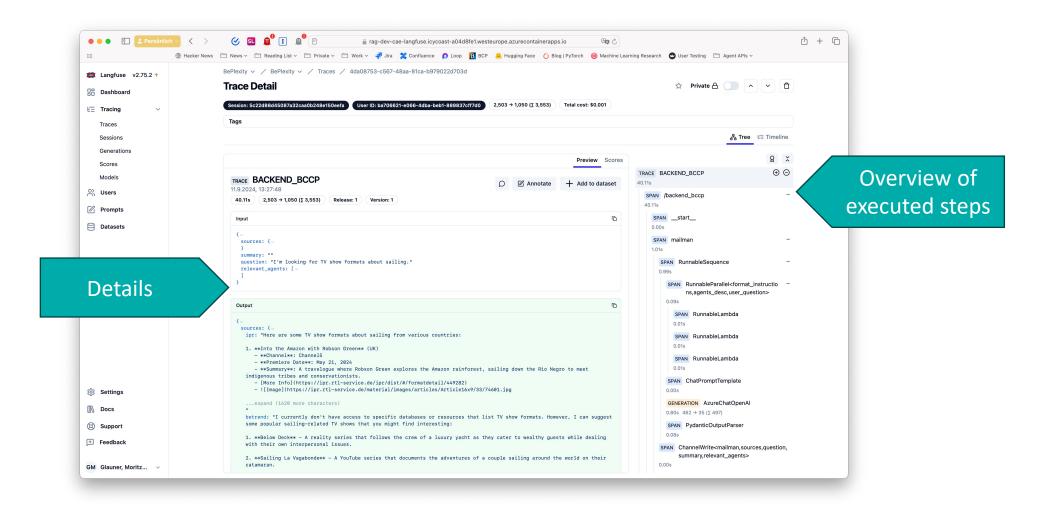


Monitor and continuously evaluate applications





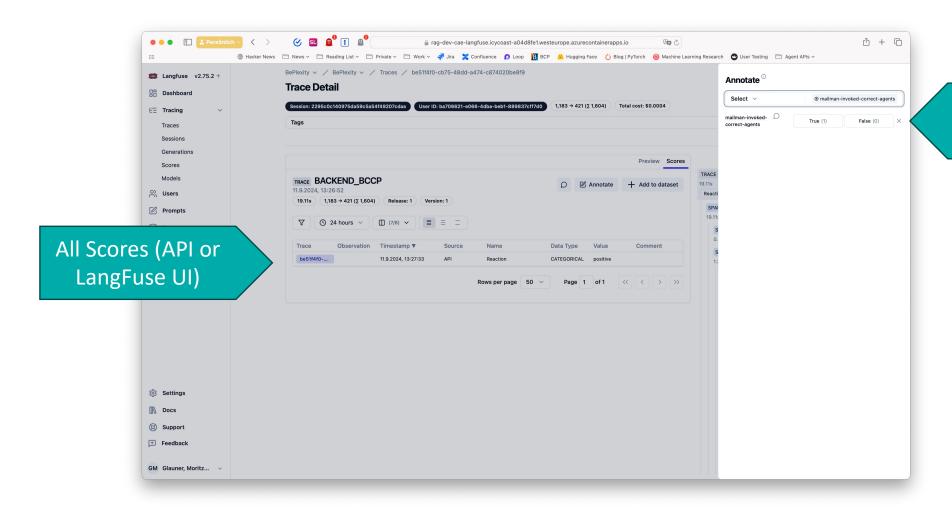
LangFuse is the LLMOps jack-of-all-traits – Tracking and Tracing







LangFuse is the LLMOps jack-of-all-traits – Evaluation (Scoring)

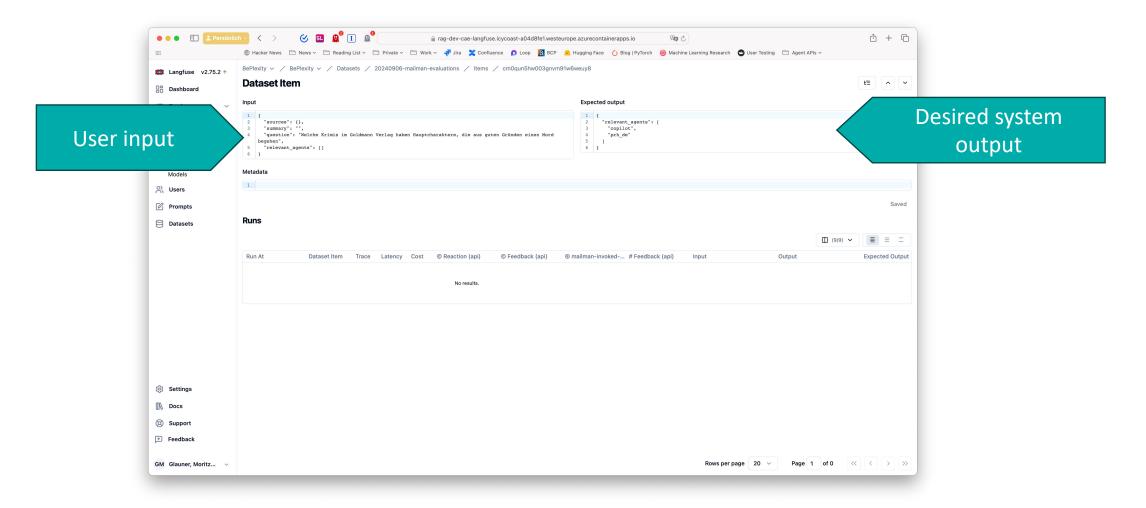


Manual annotation





LangFuse is the LLMOps jack-of-all-traits – Evaluation (Annotation & datasets)







Azure OpenAl Latency - What we expected

- LLM-Calls are send to the Azure Open-Al Endpoint, which routes those to the next free GPU.
- Execution time depends on the Input, the Model and the regional system load
- Region of the Azure OAI Endpoint matters, but not the subscription or model

LLM-Calls

Azure OAl-Endpoint





















Azure OpenAl Latency - What we got

- LLM-Calls are send to the Azure Open-Al Endpoint, that routes all to the same GPU
- The GPU does not handle requests in FIFOorder but splits its token generation capacity to all requests equally
- Execution time scales linearly with the number of concurrent requests

LLM-Calls

Azure OAl-Endpoint













GPUs







Azure OpenAl Latency - How we dealt with it

- We deployed dedicated Azure Open-Al Endpoints per Agent (all serving the same model). Those endpoints route to different GPUs.
- Different agents are don't affect the execution time of others.
- Multiple requests to the same agent still scale linearly.

Azure OAI-







Endpoint

















Fast technology exploration and productive software development require different skillsets and workflows

Technology Exploration

Software Development

Goal



Quick-Insights



Reliable Software

Team



A few creative allrounders



Interdiscipilnary team including frontend & infrastructure

Collaboration



Quick-Direct Communication, Great personal Freedom to test and play

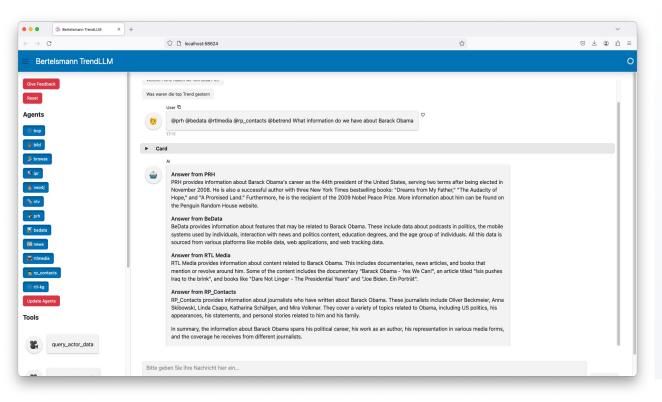


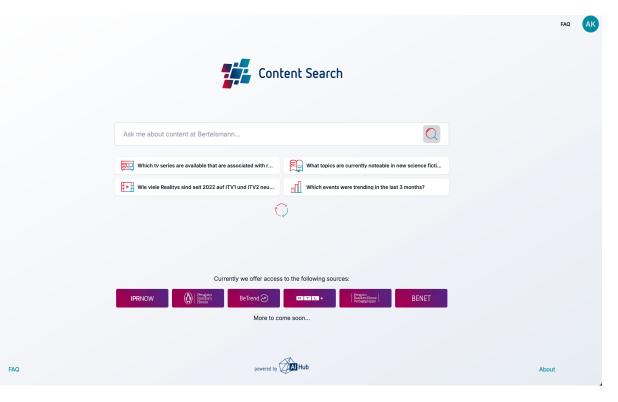
Kanban/ Scrum with Dailies Clear responsibilities





Show, don't tell! Building prototypes is helpful...





UI Explorative Phase:

Focus on Usability (Panel / Python)

Final UI:

Focus on User-Experience (React)





Also the technical components required grow in complexity

Technology Exploration

A LLM app that handles most cases

Single dump of data

A simple frontend

Deployment on localhost



A LLM app that handles all cases

Scheduled ETL pipelines incl. update logic

A sophisticated user interface

Deployment in cloud environment

IT security

Load balancing and scaling

Logging, monitoring & alerting

Identity and access management (IAM)



Best-Practices from classical software development stay relevant in the LLM-Era

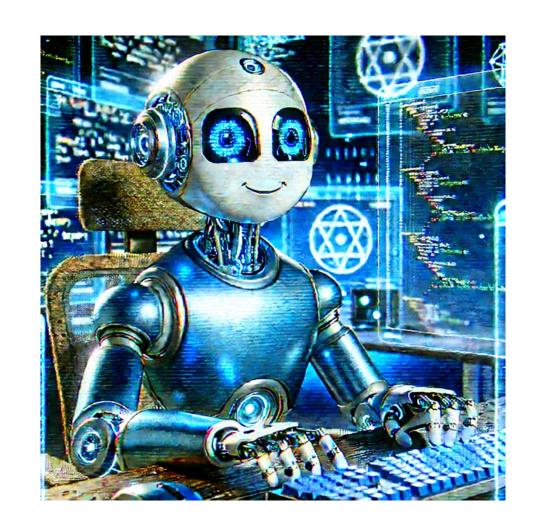
Transforming PoCs into **stable** and **reliable software is costly**, due to security, stability and UX/UI claims.

Tracing and **Monitoring** are crucial, to understand the system and its limitations

Multi-Agent-Systems are the Microservice-Design of LLMs. It increases maintainability, makes side-effects controllable and overall predictability

Unix-Rules apply: Make each program do one thing.

Tools and LLMs shall have a clear purpose, don't expect magic.





Feedback und Evaluation

Evaluation is hard and requires expert knowledge

- Working with users and data source owners is important
- Confirmation bias stemming from confident LLM responses

Integrating Feedback buttons early helps

- With gaining an intuition for the system performance
- Curating test sets for automated test & evaluation runs

UX of the feedback button matters

- Position the button centrally, in case of doubt add a second one
- Carefully consider lickart scale ratings vs. binary feedback

Logging user traces is valuable but can be legally challenging

- Valuable as it allows to adapt system for user requirements
- Remember it has GDPR implications, pseudonymisation helps





Next Steps

Improve quality and range of feedback data

- Automate scoring of traces to fill feedback gaps
- Gain holistic impression of system performance

Balance System improvements vs. extensions

- Onboard new data sources
- Improve existing Agents e.g. through advanced RAG design patterns





A&Q



Moritz Glauner

Head of Data Science @ Bertelsmann <u>moritzglauner</u>



Nico Kreiling

Data Scientist @ scieneers Host of <u>techtiefen.de</u> <u>nico-kreili</u>