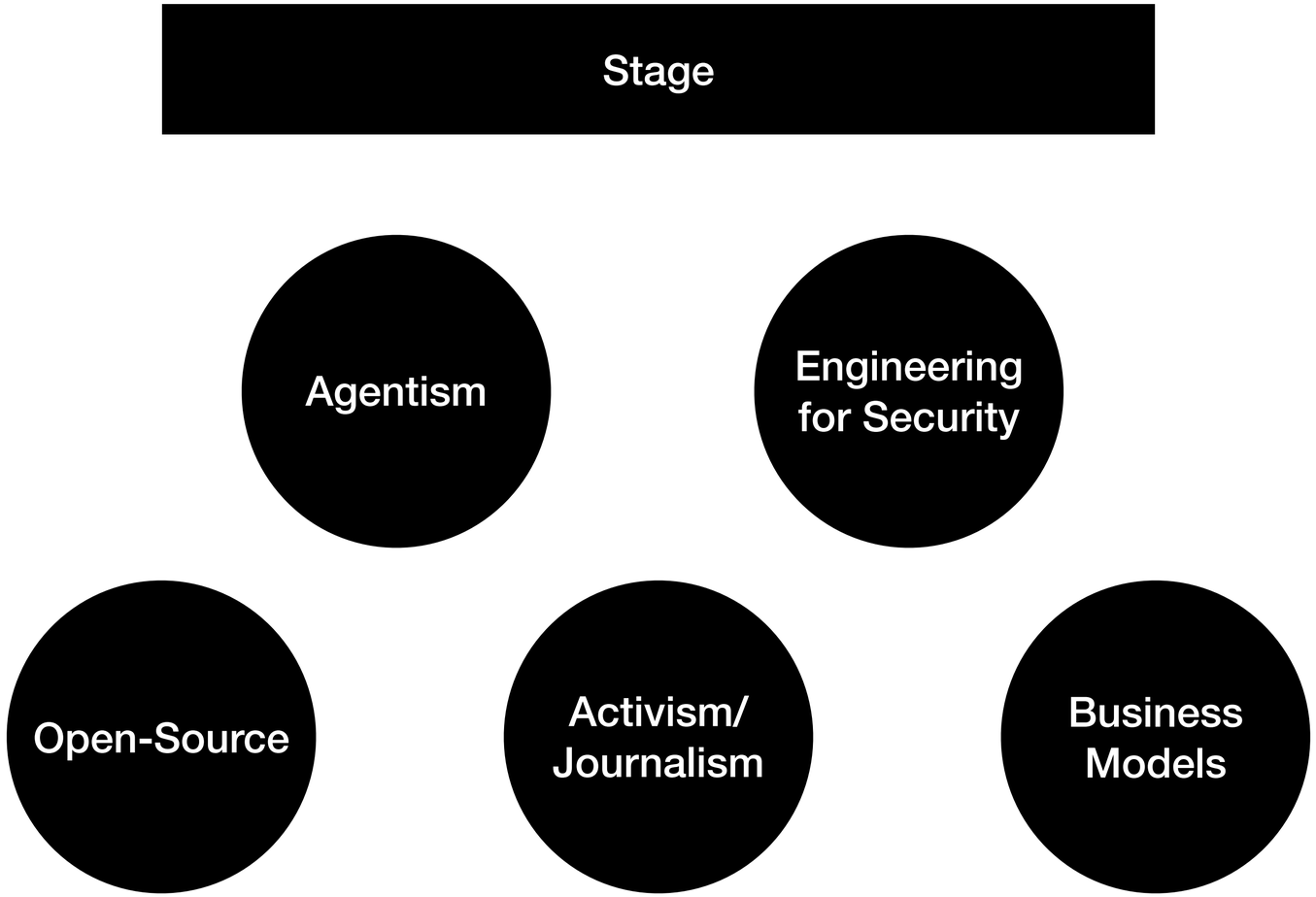
LLM Agents Meetup

Indraos@37c3

Proposed Topics



Open-Source

- There are open-source LLMs
- We have open-source models
- Which models could we see for open-source LLM agents?
  - Like an operating system?
  - Easier sharing for end users/ huggingface model?
- [Deliverable: Visionaries/Futures]

Business Models

- Let’s imagine future business models for LLM agents
- What does this mean for Big Tech?
- How will LLMs be shaped based on incentives inherent in Business models?
- [Deliverable: Visionaries/Futures]

- Current LLMs are next-token predictors
- Where do we need proper long-term planning?
- Which use cases?
- Is there hope this will work?
- [Focus: List of Use Cases]

Engineering for Security

- We see how LLM agents are vulnerable to injections and extraction of information
- They don’t seem to be capable to meaningfully enforce client-side security
- What are models or ways out?
- [Deliverable: Path towards technical artifacts]

Activism/
Journalism

- What are good ways to showcase in which way LLMs fail us?
- How does this integrate with other activism?
- What is needed (technically/ knowledge/resources) to be meaningfully active?
- [Example of an activist action]

Please take Notes in Docs