# The LLM Development Stack

**Rob Barton and Jerome Henry** 

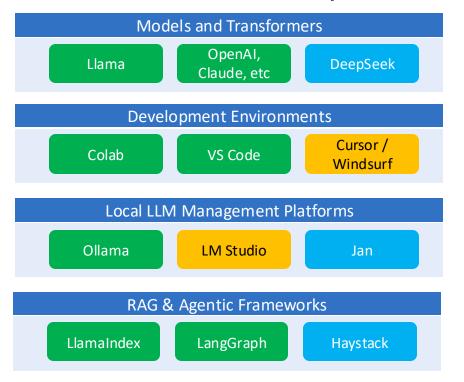


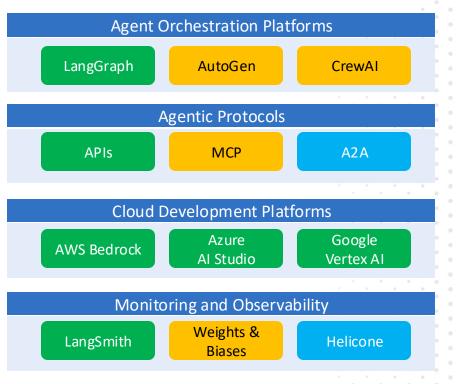
#### Course Overview

- Lesson 1: LLM Development Fundamentals
- Lesson 2: Building Applications with LLMs
- Lesson 3: Agentic Al Development Tools
- Lesson 4: Agentic Al Protocols
- Lesson 5: Cloud-Based LLM Platforms
- Lesson 6: LLM Benchmark and Optimization Tools



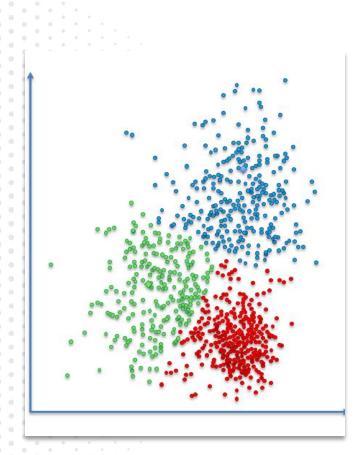
### The LLM Development Stack









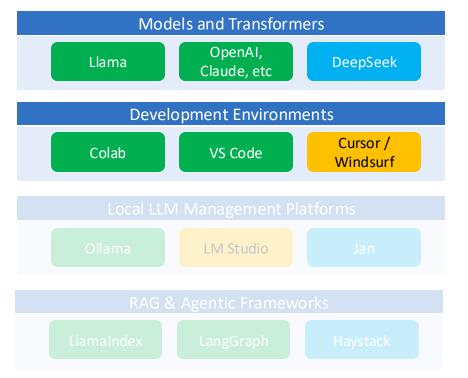


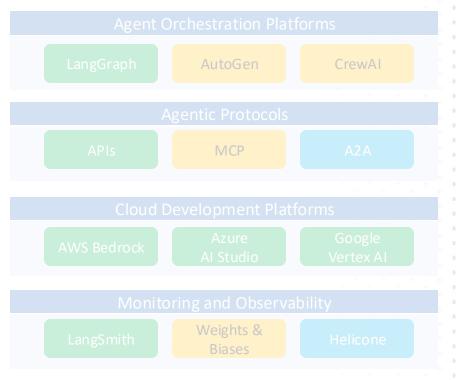
# Lesson 1: Foundational Tools

#### Objectives

- Choosing a model: cloud vs local, open vs closed
- Hugging Face for model selection
- Google Colab to run development and experiments
- Tracking progress: Wandb

# Models, Transformers, and Development Environments









#### **LLM Development Phases**

LLM development creates an LLM from scratch, or modifies an LLM, it has 3 components:

# **Step 1: Model and data selection**

Train from scratch?
Augment/distill? Which model base?
(compromise between task (specialization), size and precision). Which data to train from?

# Step 2: Environments and tools selection

Cloud? On prem? Link to data lake? Link between agents?

# Step 3: Tracking and Testing

Log experiments to remember outcomes? Evaluate model performances? Optimize?



## Private-Source vs. Open-Source LLMs

	Closed-Source	Open-Source
Examples	ChatGPT, Google Gemini, Claude	BERT, LLaMA, Mistral, etc.
Fine Tuning Capability	Limited to none (RAG only)	Depends on the LLM, but generally possible
Embodiment	Public-Cloud (aaS model)	Private cloud, on-prem
Security	Difficult to control	Easy (you control the model)
Typical Model Size	Huge	Smaller, but can be more focused
Price	aaS pricing model	Generally capital cost only



#### Business Lens: Closed vs. Open-Source Models

- 1. Cost: OpenAl claims GPT-4 cost them over \$100 million to develop. This cost means the models will likely stay under the control of the organization who developed it (forcing users to send data to the service either via the web interface or API)
- 2. Privacy and Security: Commercially available LLMs are something of a "black box" for users. The users have no control over how they were trained, bias, etc.
- **3. Training Gap:** Private-source LLMs are hard to keep up to date, and can typically be 1-2 years old
- **4. Fine Tuning:** Open-Source models can generally be fine-tuned, allowing them to be smaller for a specific purpose



### Finding Open-Source Models – Hugging Face

- What is Hugging Face?
- An AI company which has become the world's largest repository of open-source transformers

Open-Source Models Open-Source Datasets

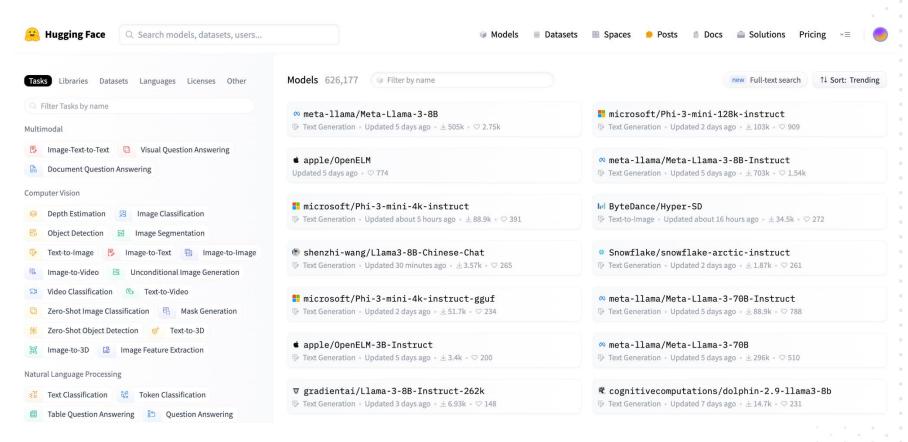
Spaces (platform to build and deploy LLMs)

**Python Transformers Library** 

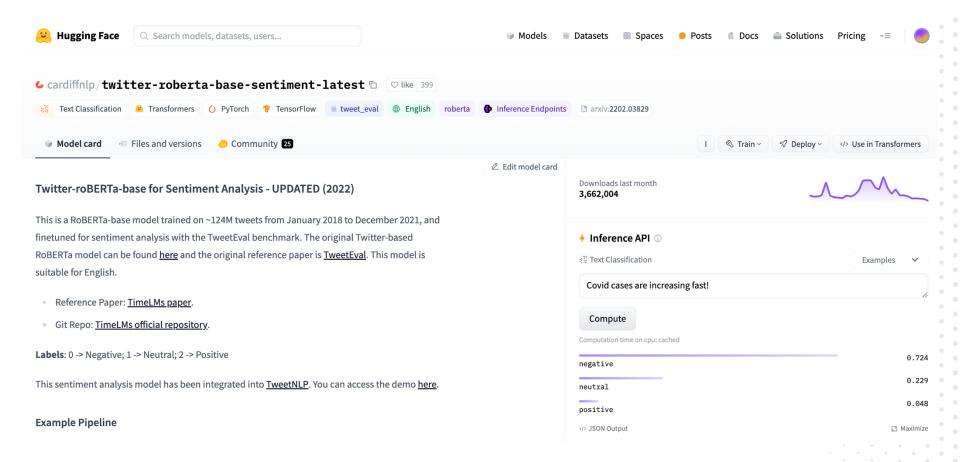


## Hugging Face Open Source LLM Repository

huggingface.co/models



#### **Model Cards**



#### Transformers Library

Open-source Python library that provides:

- **pretrained models (**(e.g., BERT, GPT, T5, LLaMA, etc.)
- Tools for tokenization, model training, fine-tuning, and inference
- APIs to download and manage models from the Hugging Face Model Hub

**Not only for Natural Language Processing (NLP)** but also for related tasks such as vision and audio processing using **transformer-based architectures** 



#### LLM Development Components

LLM development creates an LLM from scratch, or modifies an LLM, it has 3 components:

# Step 1: Model and data selection

Each model is a compromise between task (specialization), size and precision.

#### **Step 2: Environments**

Use commands to point the model(s) to the right data and generate the training

# Step 3: Experiment Tracking

Log your experiments to remember outcomes.



# Google Colab: Code + Cloud + GPUs



- LLM development is used by researchers, startups, and hobbyists
- Fast iteration is key when working with LLMs.
- Tools must be accessible, flexible, and well-integrated
- Google Colab:
  - free (or "can be free")
  - integrated with Google drive (to store data) and/or Gituhub
  - features a simple Jupyter interface

# Google Colab Alternatives



- Your own Jupyter server (with GPU local or on another machine)
- Rented virtual environments (e.g. RunPod)
- Cloud-based environments e.g., AWS, Vertex (more advanced)

#### LLM Development Components

LLM development creates an LLM from scratch, or modifies an LLM, it has 3 components:

# Step 1: Model and data selection

Each model is a compromise between task (specialization), size and precision.

#### **Step 2: Environments**

Use commands to point the model(s) to the right data and generate the training

# Step 3: Experiment Tracking

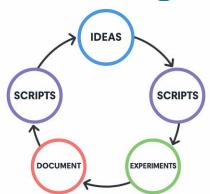
Log your experiments to remember outcomes.

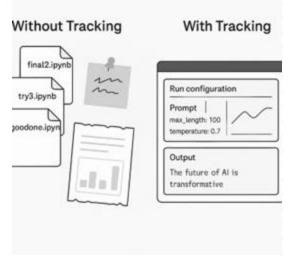


# Keeping Track

Pearson

- LLM development is an iterative process
- It is difficult to remember what (and why) you did several weeks/months ago
- Hard if you work alone, a nightmare when working in teams ("final2.ipynb" syndrome)
- A tracking system allows you reduce investigative wasted time





# Tracking Solutions



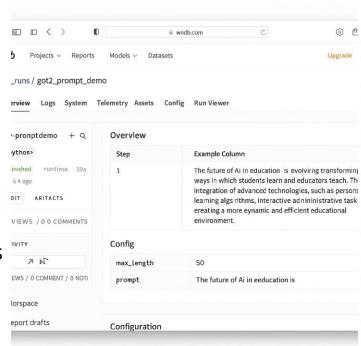
Non exhaustive list of main players

<b>B</b> (Beginner)	ClearML (Mid-level)	Aim (Open source, minimal UI)
hed, cloud UI	Very detailed	Lightweight & modern
•	Medium (more config)	Easy CLI, but less guidance
•	<b>✓</b>	
e links, teams	Team support	Git-style project mgmt
,, 0	Larger pipelines	Minimalist open- source workflows
	B (Beginner)  Shed, cloud UI  est (Colab- ndly) (via wandb ne)  e links, teams otyping & ing	shed, cloud UI Very detailed  est (Colab- ndly) Medium (more config)  (via wandb le)  e links, teams Team support  otyping & Larger pipelines

# Tracking Solutions



- Wandb (Weights and Biases, W&B)
  - Free and beginner-friendly (integrates well with Colab & Jupyter)
- Track:
  - prompts
  - parameters (e.g., temperature, model)
  - generated outputs
  - Visualize results across multiple runs
  - Share, resume, or compare experiments with a single link



# Google Colab with Hugging Face



**DEMO** 

 Colab easily integrates with Hugging Face APIs, so you can call a Hugging Face model from Colab... and check the experiments from Wandb