Foundation Models and Agentic AI

For Engineering Professionals

Bishal Sapkota
Lead Software Engineer &
Co-founder at Outback Yak

Yuba Raj Panta
Software Engineer at
PageUp Google Developer
Group Organizer

SNE Vic Career Conference 2025 31/08/2025

Agenda

01
History of Artificial Intelligence

02
Emergence of Foundation Models

03
Pitfalls and Limitations

04
What is Agentic AI

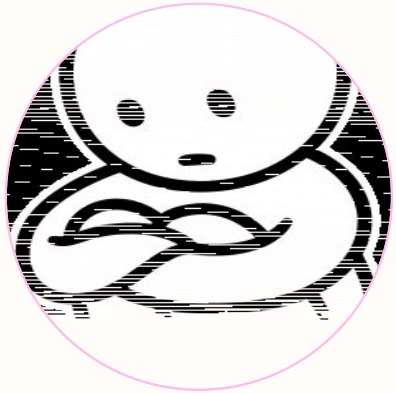
05
Agentic AI in Enterprise Today

06
Scenario of AI Agents in Engineering

07
Demo

08
QnA

Lets start with a story of a PM



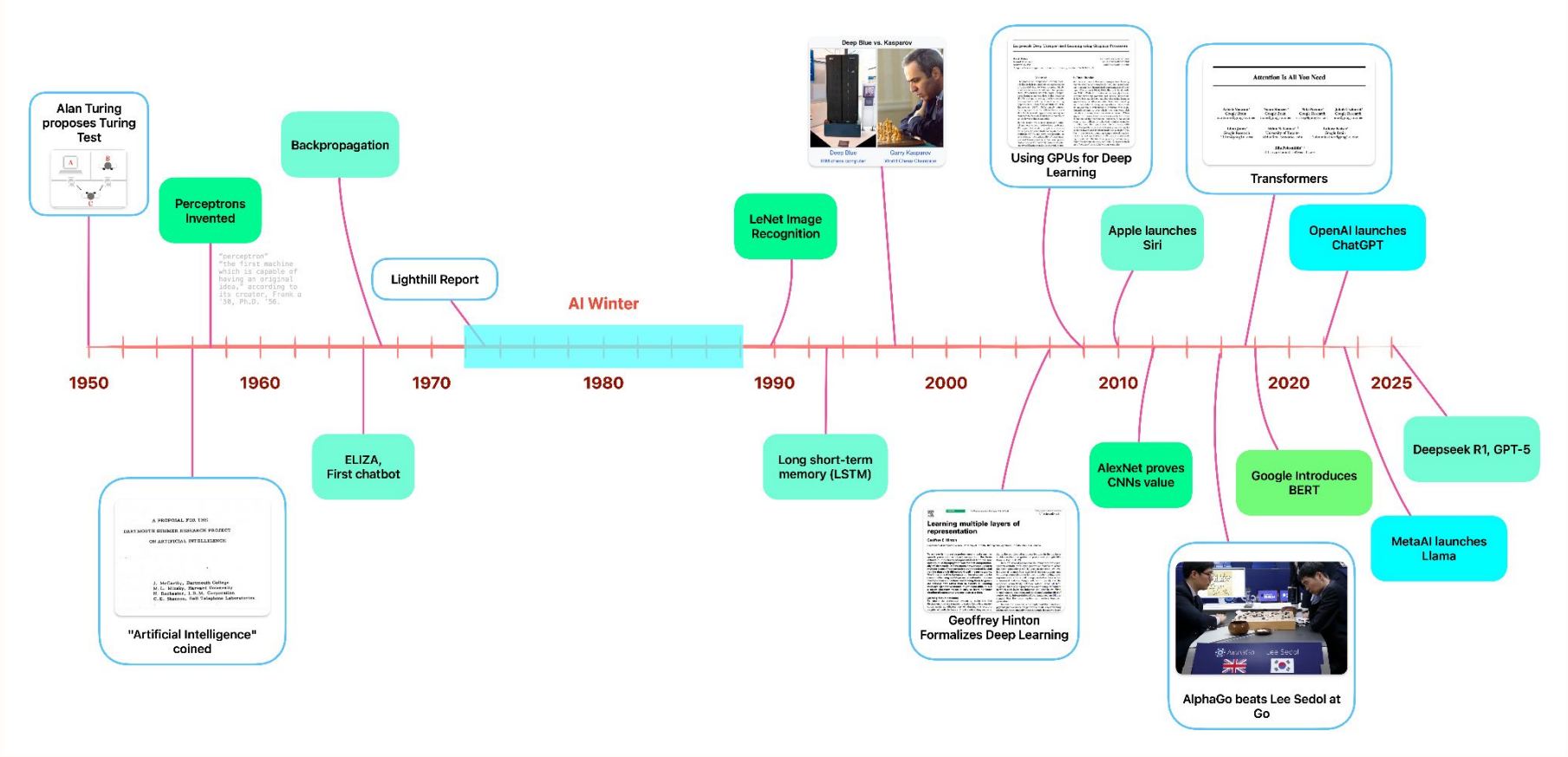
It is 10 AM, on a wednesday. You are a Senior Project Manager working on Epping Road Upgrade. One of your excavation teams in Zone 3 reports “*we've hit something. Looks like an old cast-iron pipe. It's not on the plans.”.*

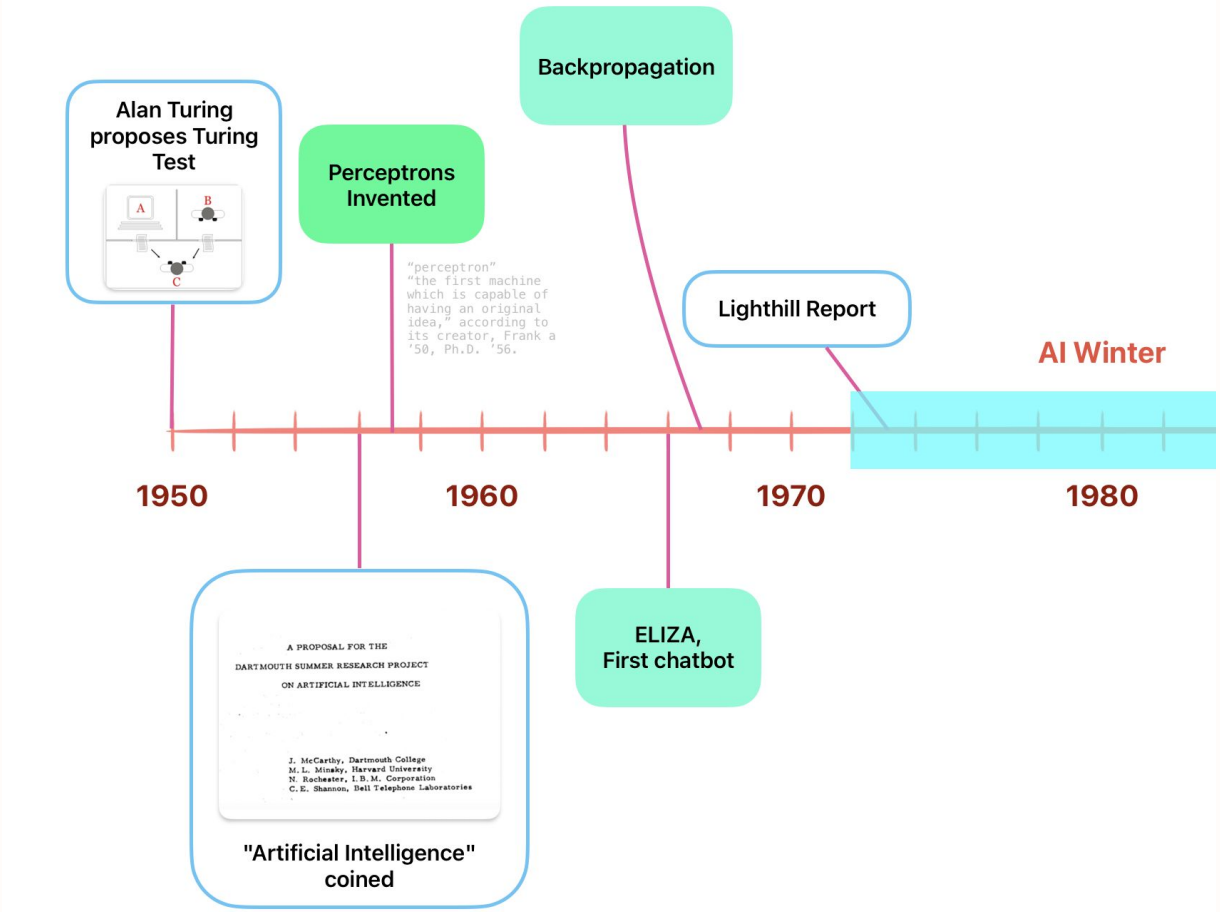
Chaos begins. Work freezes. You are hastily trying to refer back to plans for Water, Gas, and other Utilities. You are on a phone with the local council, who are not helpful, despite their efforts.

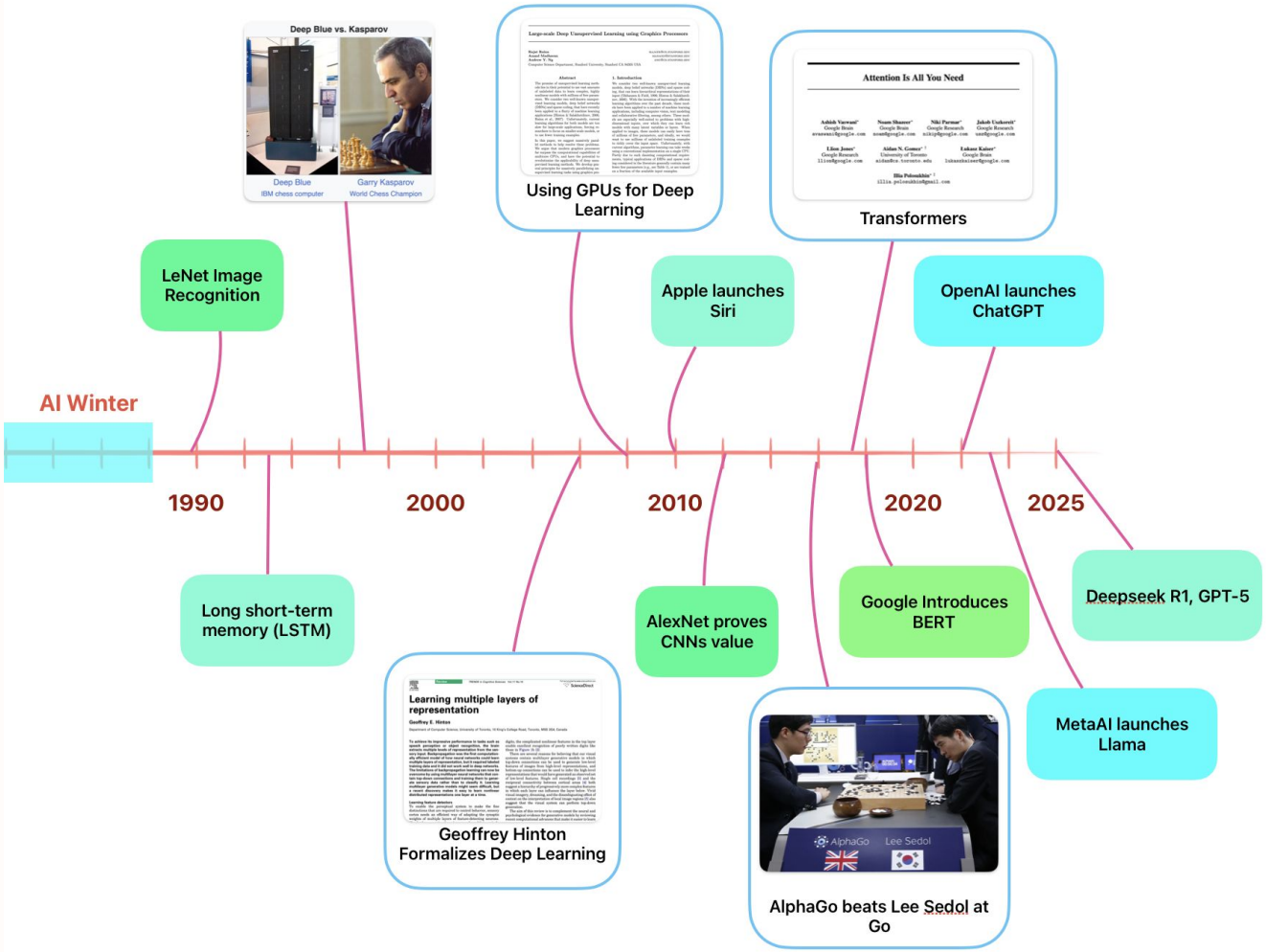
You get a call from the project steering committee

By lunchtime, three hours have passed. The pipe is still unverified, the crew has been unproductive all morning, and your entire project schedule is now in jeopardy. You’ve been a crisis manager, not an engineer.

History of Artificial Intelligence




Alan Turing proposes Turing Test
A
B
C
Perceptrons Invented
"perceptron"
"the first machine which is capable of having an original idea," according to its creator, Frank a '50, Ph.D. '56.
Backpropagation
Lighthill Report
AI Winter
1950
1960
1970
1980
A PROPOSAL FOR THE
DARTMOUTH SUMMER RESEARCH PROJECT
ON ARTIFICIAL INTELLIGENCE
J. McCarthy, Dartmouth College
M. L. Minsky, Harvard University
N. Rochester, I. B. M. Corporation
C. E. Shannon, Bell Telephone Laboratories
"Artificial Intelligence" coined
ELIZA, First chatbot


Deep Blue vs. Kasparov
Deep Blue
IBM chess computer
Garry Kasparov
World Chess Champion
Using GPUs for Deep Learning
Transformers
LeNet Image Recognition
Apple launches Siri
OpenAI launches ChatGPT
AI Winter
1990
2000
2010
2020
2025
Long short-term memory (LSTM)
AlexNet proves CNNs value
Google Introduces BERT
Deepseek R1, GPT-5
MetaAI launches Llama
Learning multiple layers of representation
Geoffrey Hinton
Geoffrey Hinton Formalizes Deep Learning
AlphaGo
Lee Sedol
AlphaGo beats Lee Sedol at Go

Emergence of Foundation Models

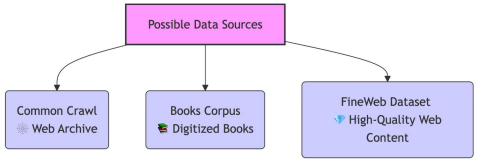
Emergence of Foundation Models

Data Collection & Preprocessing 🔑

Foundation Models: Built on a World of Information 🌍

To truly understand and generate **human-like text**, models need to learn from a **VAST** and **DIVERSE** range of information. Diversity ensures the model can:

- 🧠 Generalize across topics & styles
- 💪 Perform robustly in different contexts



Let's See Tokenization in Action! 🎬

Imagine we have this sentence:

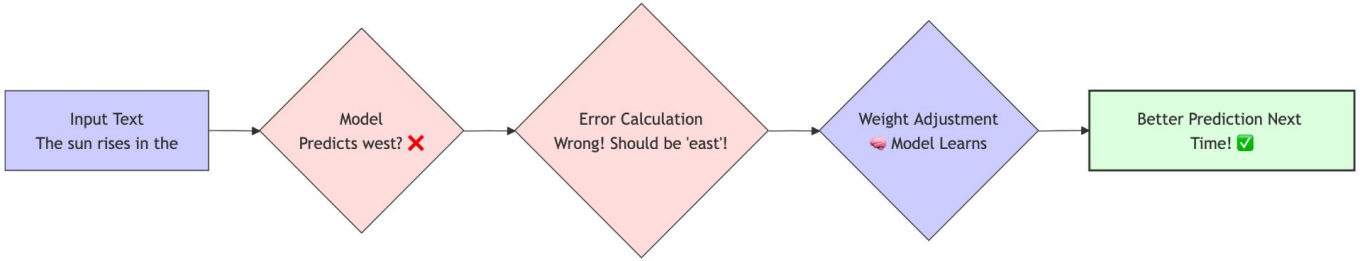
`"Artificial Intelligence is amazing."`

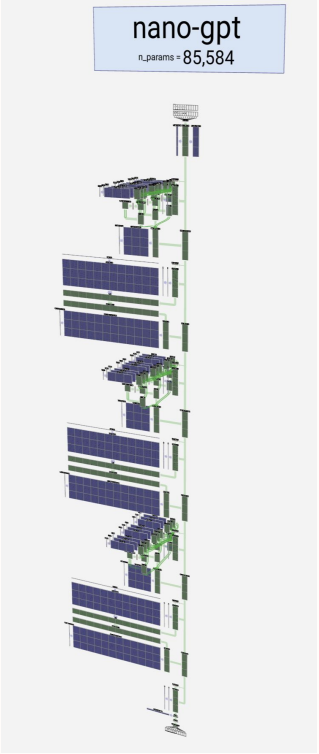
⬇️ Tokenization

```
Tokens:  ['Artificial', ' Intelligence', ' is', ' amazing'
```

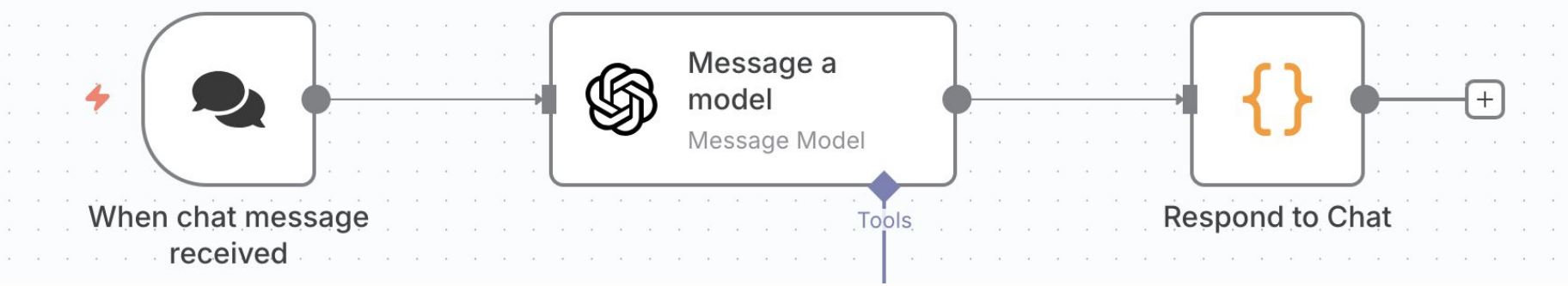
⬇️ Numerical Conversion ⬇️

```
Numbers:  [ 1234,  567,  89,  1011,  12 ]  (Example IDs)
```





Using a Foundation Models



Properties of Foundation Models

- Trained on massive datasets (text, images, documents, books, code, etc.)
- General-Purpose AI: Adaptable to a wide range of downstream tasks
- Examples: GPT-5, Gemini, and other large language and multimodal models 🌐

✨ Key Traits of Foundation Models

- Scale: Billions or Trillions of parameters - enormous model size 🐘
- Transfer Learning Power: Pre-trained knowledge transferable to new tasks with minimal fine-tuning 🔄
- Emergent Capabilities: Exhibiting complex behaviors not explicitly programmed

Foundation Models

	Text	Vision	Video	World Models
Features	→ Long context, tool/function calling, → Multilingual	→ Text→image, image→image, in/out-painting	→ Text/image→video · Shot/camera/keyframe control → Audio support?	→ generate interactive training environments
Strengths	→ Reasoning + assistants · Huge context (up to ~1M tokens) for long docs	→ High fidelity & coherence	→ Increasing temporal consistency & physics realism → Cinematic control	→ Bridges to robotics via VLA (vision-language-action)
Examples	→ GPT 5 → Deepseek R1	→ DALL-E → Imagen 4	→ Veo3, Leonardo AI, Grok	→ Genie 2 / Genie 3 (interactive, playable worlds)

Limitations of Foundation Models

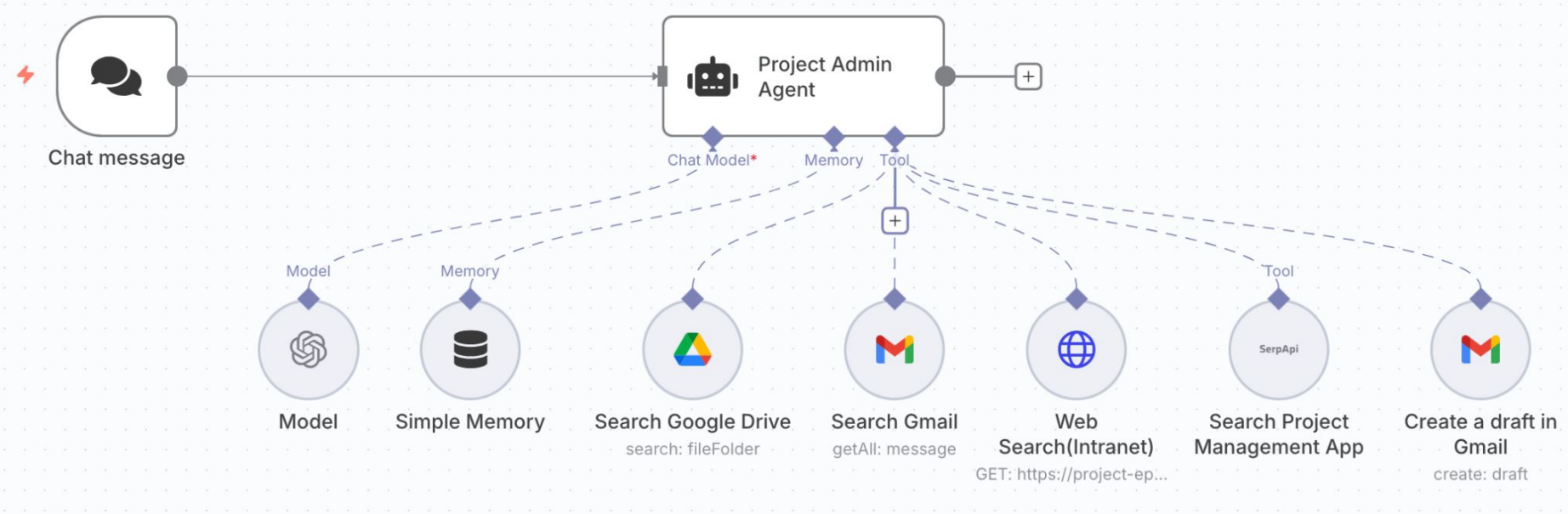
- Model Bias
- Trustworthiness
- Hallucination
- Transparency Issues
- Explainability
- Data Privacy and Regulatory Issues

What is **Agentic AI**

- Foundation models are not aware of the real world
- They can not influence the real world
- Foundation models respond to user input in one turn
- Do not have long term memory

- What is foundation models were aware of the real world
- What if they could influence(act) the real world
- What if they could take multiple turns to formulate their responses
- What if the models could have long term memory, and learn for its interactions

Anatomy of an Agent



Let’s see it in **Action!**

Agentic AI in Enterprise Today

Generative Design & Simulation

Engineers are using generative AI to come up with design alternatives or optimise designs under constraints

Knowledge Management and Troubleshooting

Large language models can be fine-tuned on a company's internal technical documentation, standards, and past project archives.

Administrative and Productivity Tasks

AI in everyday Productivity. mundane, but they free up time for engineers to focus on creative problem-solving.

Coding and Scripting Assistance

autocomplete boilerplate code or translate pseudocode into a real programming language, which is a boon for engineers who code as part of their work.

Real-time Monitoring and Decision Support

agent-based automation is seen as a way to enable real-time, adaptive supply chains, where an AI orchestrates decisions faster than a human could

Values & Risks

Automates complex tasks and workflows, saving time and effort for engineers

Enables real-time decisions in operations (e.g., supply chains) by monitoring data and making adjustments faster than a human could.

Augments human capabilities and boosts productivity – acting as a tireless assistant that can draft documents, write code, or explore design alternatives in minutes

Frees engineers for innovation by handling drudge work (AI lets human engineers focus on creative and complex problem-solving that truly requires human insights)

Security risks like prompt injection attacks, where malicious inputs could trick the AI into unwanted actions .

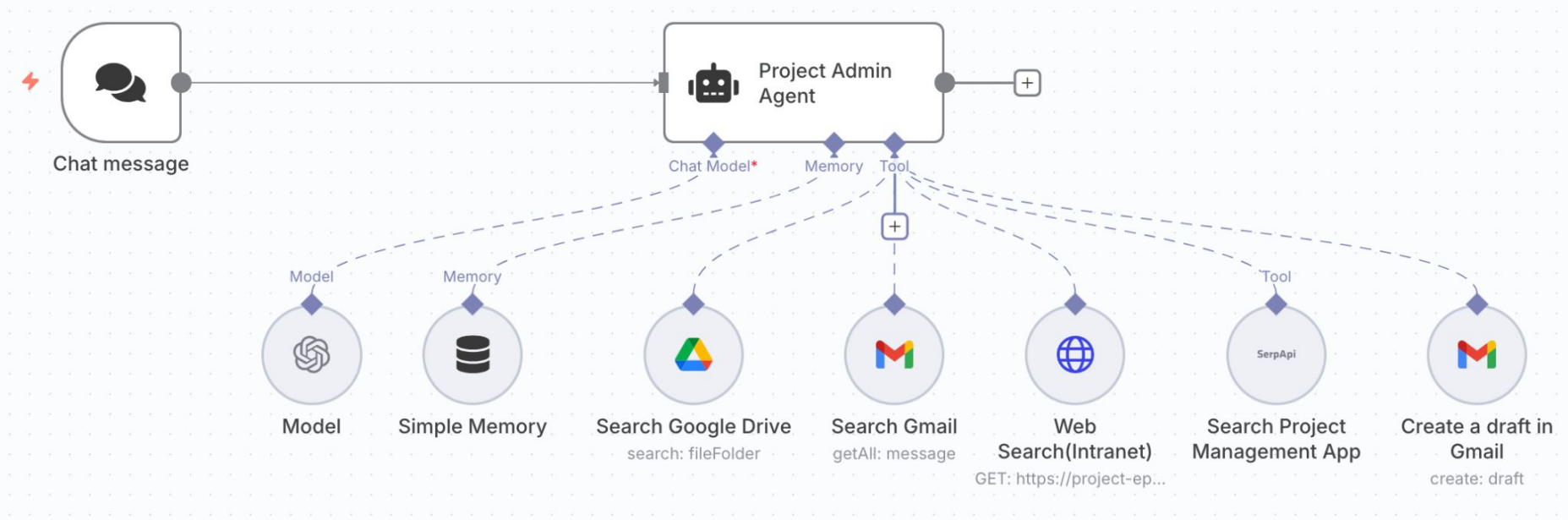
Lack of transparency in AI decision-making ("black box" effect). Deep models often don't explain why they made a recommendation

Data privacy and compliance issues – foundation models trained on public data may inadv rtently leak sensitive info.

Potential for biased or harmful outcomes if the AI has biases in training data. In engineering, this could mean biased risk assessments or exclusion of certain design options.

Lets go back to the Project Manager

Lets go back to the Project Manager



Lets go back to the Project Manager

It’s now 10:15 AM. The pipe is still in the ground. The crew is still waiting. The problem has not magically vanished.

But the entire administrative and communication fire drill that previously took hours is now complete. The right people are informed with consistent data. The formal inquiries are underway. A single source of truth for the incident has been created.

And Liam? He is now free. He has his most valuable asset back: his time and focus.

That is the practical power of Agentic AI. It's not about replacing the engineer; it's about clearing the chaos so the engineer can do their job.

Key Takeaways

- AI has evolved from pattern recognisers to action-takers (Agents).
- We're in a phase of high potential but practical limitations. Start simple.
- Use AI Models as thinking partners, not assistants.
- AI is inevitable. Use it or be left behind.

Thank you!

Bishal Sapkota
bishalspkt
bishal@outbackyak.io

Yuba Raj Panta
yuba-raj-panta
uvishere@gmail.com