LLM-powered Automated Workflow Management

EnergyNorway 2024

Jungwon Seo Ph.D. Candidate in IDE NCS2030 WP5









Previous In Energy Norway



Federated Knowledge Cloud

Blockchain-Powered Digital Asset Management and Access Control for Federated Learning



Jungwon Seo, Nan Zhang, Chunming Rong

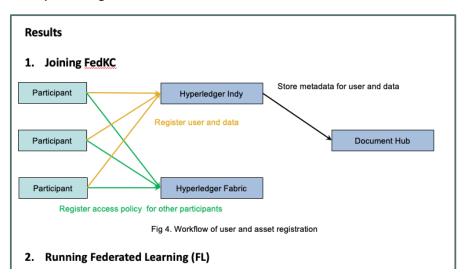
University of Stavanger

Introduction

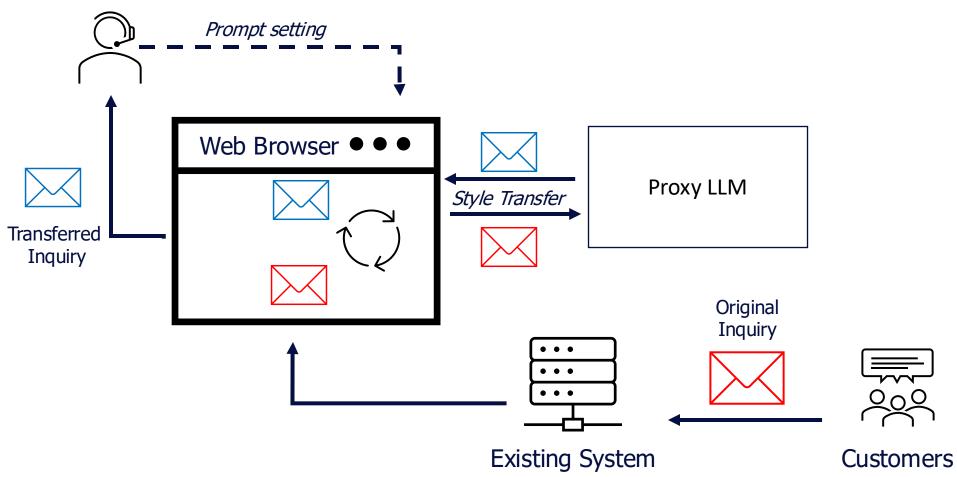
The Federated Knowledge Cloud(FedKC) is a platform where participants can collaborate in the machine learning process through federated learning. To ensure the security and trustworthiness of the platform, we propose the system design of a robust asset management system using Decentralized Identities (DIDs) to represent tokenized assets, such as data and models, and prove ownership and establish a clear chain of custody. Additionally, to automate access control and align with Zero Trust Architecture principles, we will utilize smart contracts to verify and authenticate users and their actions, allowing for the immediate revocation of access if necessary. This smart contract-based system will ensure the security and automation of the FedKC and foster a collaborative and secure environment for data and model training.

Objectives

- · Collaboration and knowledge sharing by moving computation where data is.
- Providing secure and privacy-preserving digital asset management and access control.







Federated Knowledge Cloud



?

Large Language Model



Blockchain

(Access Control, Digital Asset Management, Incentive)

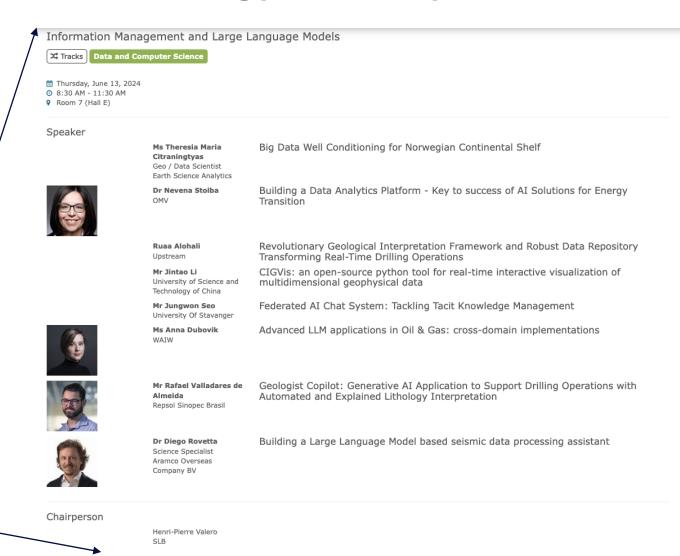


Large Language Model (LLM)

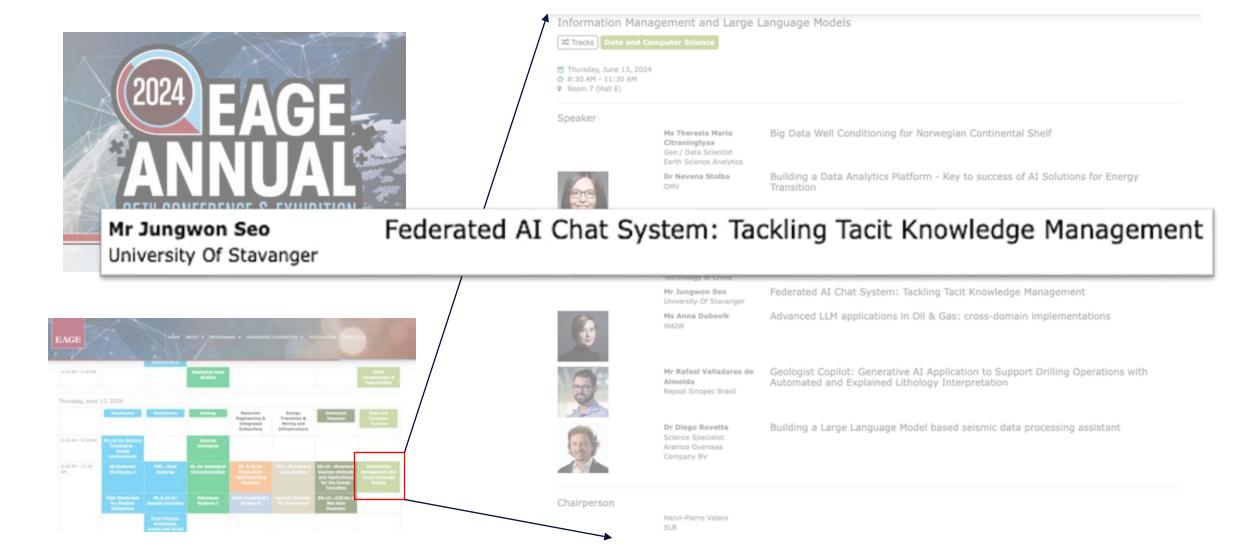
Large Language Model in Energy Industry







Large Language Model in Energy Industry



Large Language Model

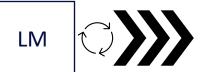
Probabilistically predicting next words

Where is UiS?



UiS typically refers to the University of Stavanger...

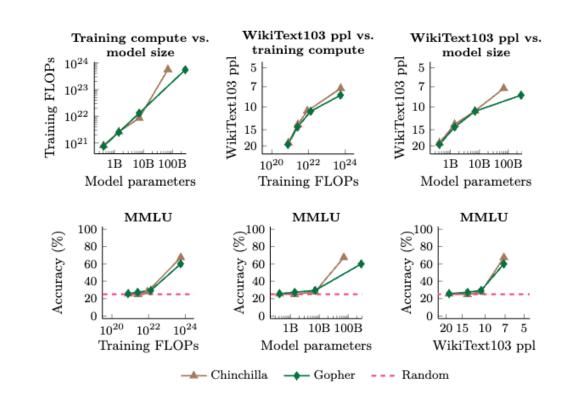




LM ...platform for networking, knowledge sharing ...

"Large" Language Model vs. Language Model

- Architecture point of view:
 - Larger parameter
- O Performance point of view:
 - Emergent Abilities
 - Not explicitly trained ability
 - General-purpose
 - Task-specific: Machine Translation



What LLM (solely) can / cannot

O Can

- Understand and generate text
- Answer questions
- Translate languages
- Summarize content
- Predictive text and autocompletion
- ...

Cannot

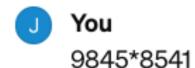
- Access to real-time information
- Calculate precise mathematical operation
- •

We need to differentiate between LLM and ChatGPT

ChatGPT 4 is a complete system in addition to LLM.

Example: Mathematical Calculation

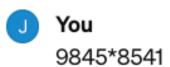
ChatGPT 3.5 V



9845 multiplied by 8541 equals 84,134,745.

() () 5 T

ChatGPT 4 ~



ChatGPT

The result of multiplying 9845 by 8541 is 84,086,145.



Example: Real-time Information Access 1

ChatGPT 3.5 V





You

Who is the winner of ATP Miami Open 2024



I'm sorry, but I can't provide real-time information as my training only includes data up to January 2022, and I don't have access to the internet to fetch real-time data. To find the winner of the ATP Miami Open 2024, I suggest checking the latest news updates, the official ATP website, or reliable sports news sources.

ChatGPT 4 v





You

Who is the winner of ATP Miami Open 2024



Jannik Sinner won the ATP Miami Open 2024, defeating Grigor Dimitrov in the final with a score of 6-3, 6-1 (ATP Tour).

Example: Real-time Information Access 2

ChatGPT 3.5 V



What time is it now in Norway?

ChatGPT

I'm sorry for any confusion, but as an Al, I don't have real-time capabilities or access to current data such as the current time. Therefore, I can't provide the current time in Norway or any other location. You can easily check the current time in Norway by using various online tools such as world clocks, websites, or smartphone apps.

ChatGPT 4 ~



What time is it now in Norway?



The current time in Norway is 15:33 CEST on April 8, 2024. [>-]

What's the difference?

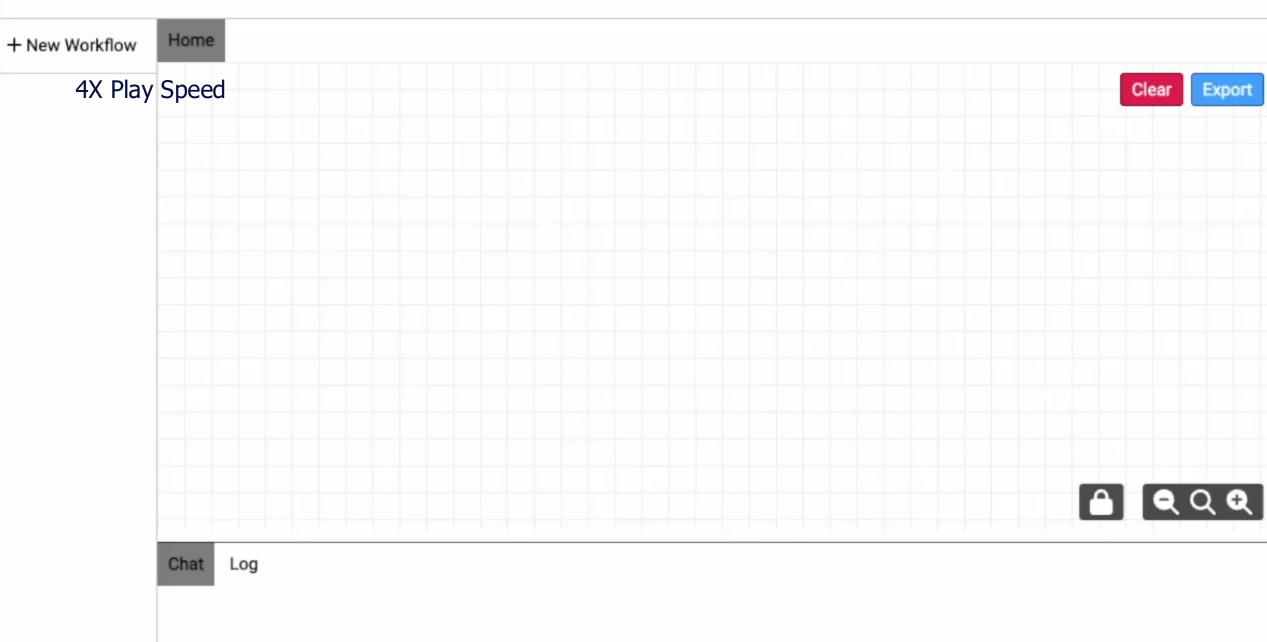
Non-agentic Workflow (Zero-shot)

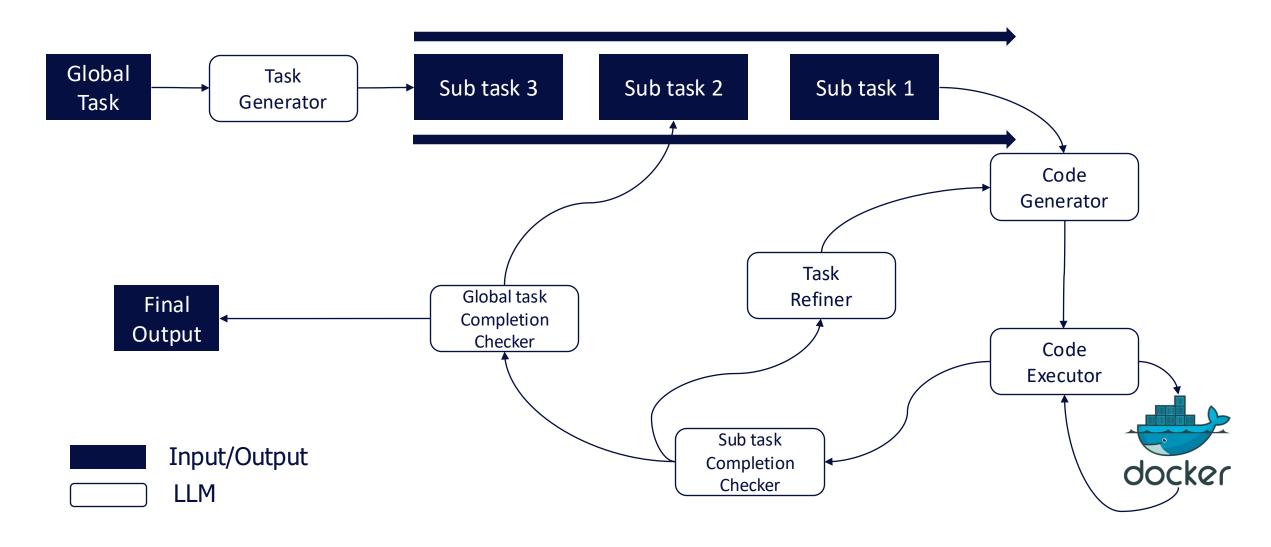


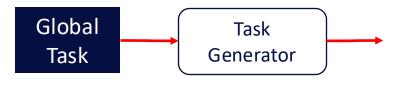
Agentic Workflow Input Do you need more data? Do you need to search? Do you need to code? Do you need a plan? Output



LLM-powered Automated Workflow Management (Demo)



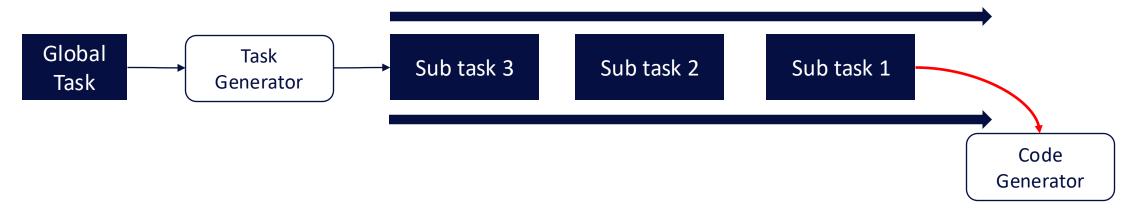




Split into sub-tasks

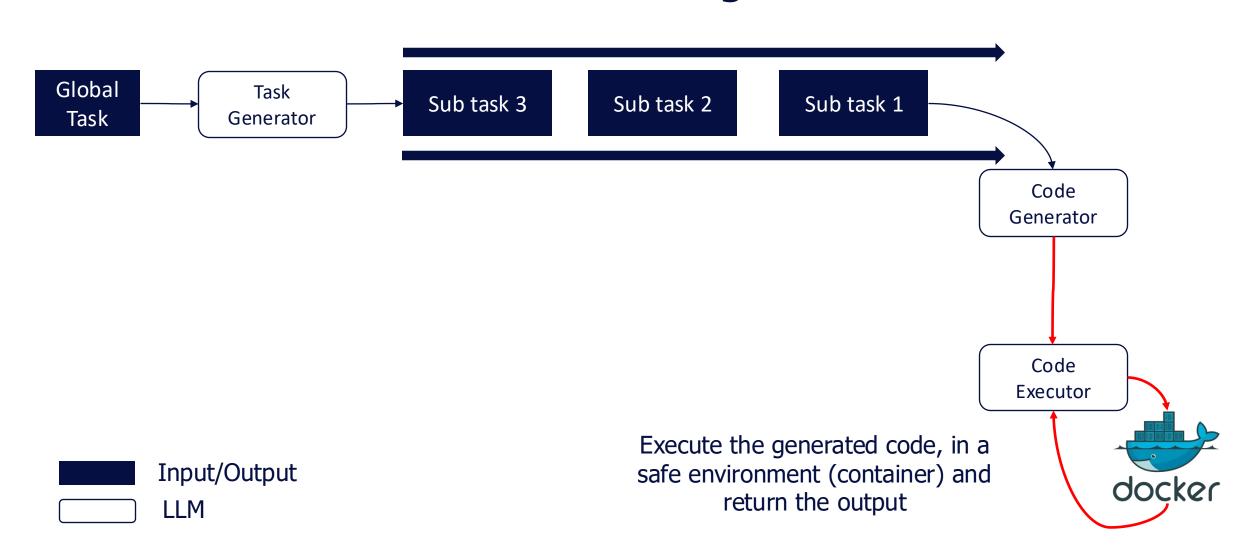


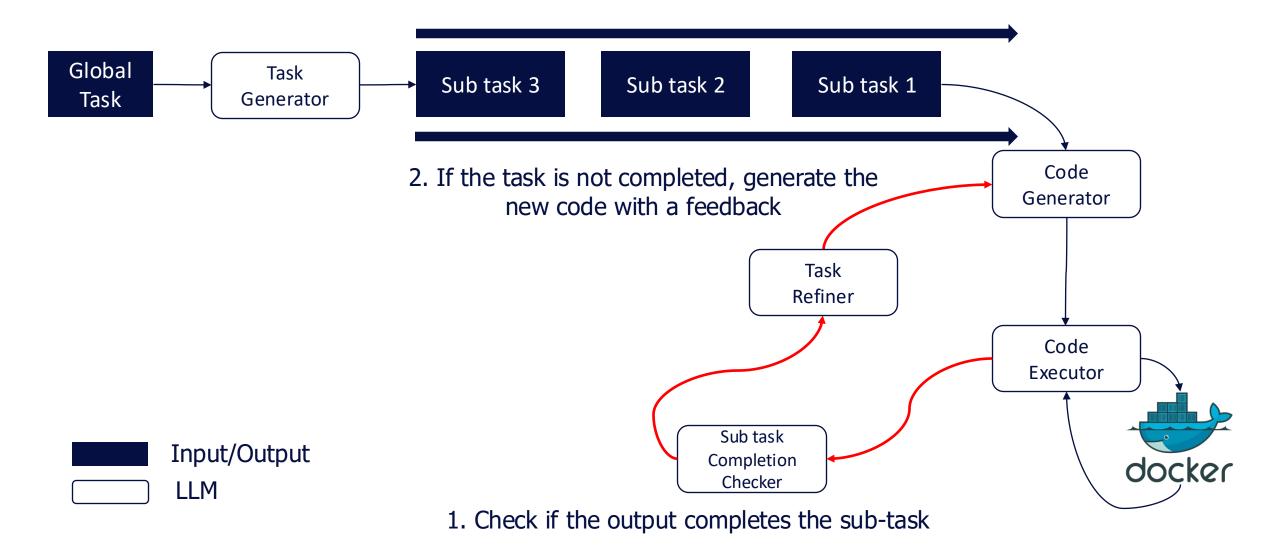


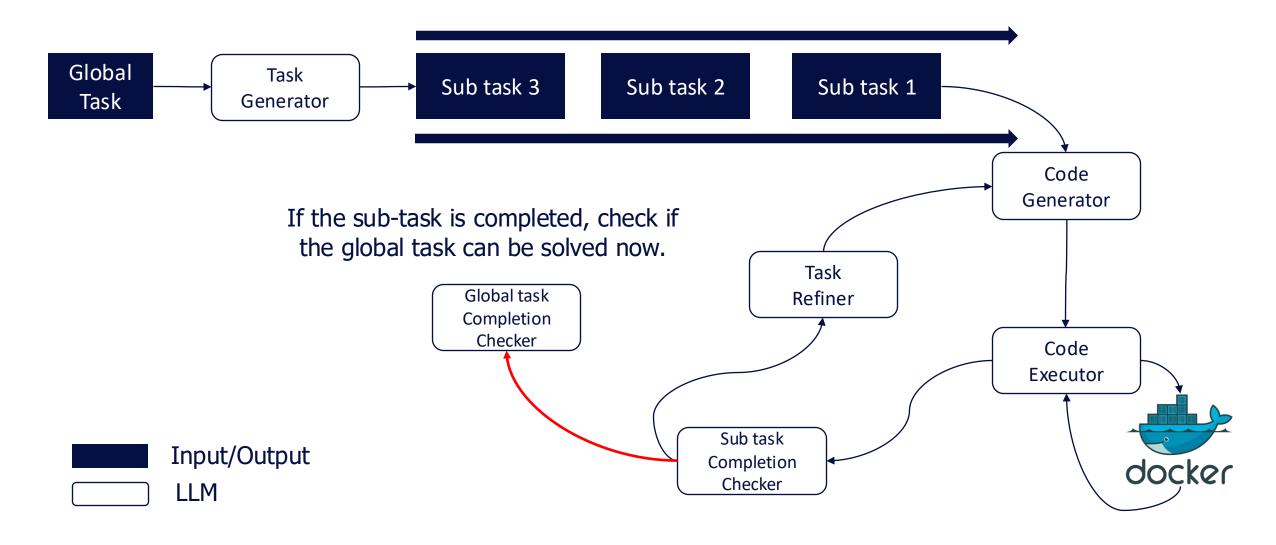


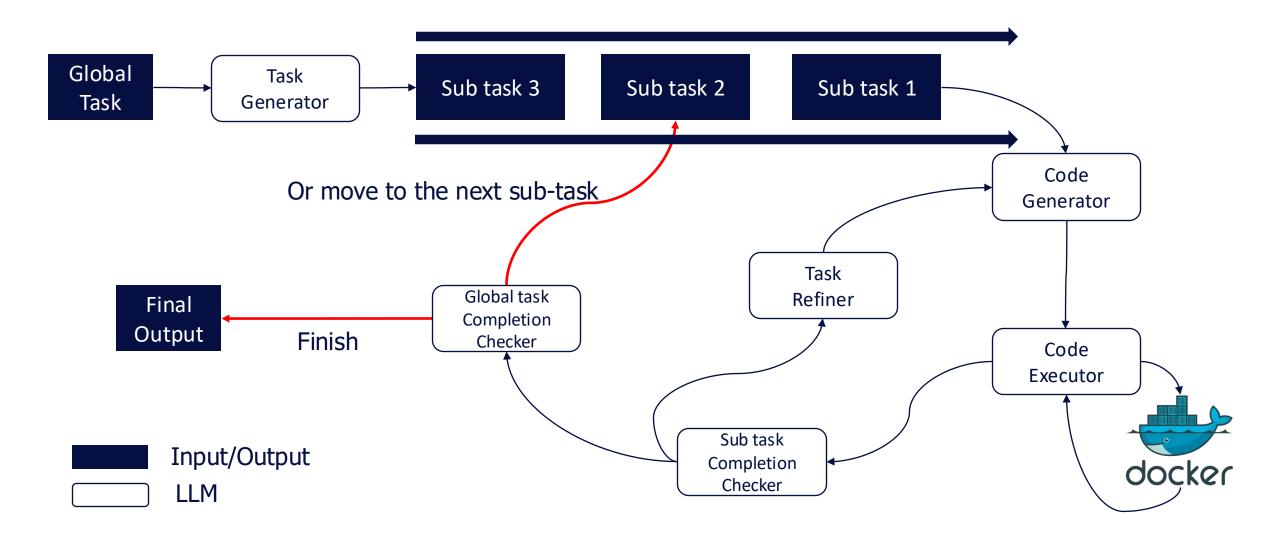
Choose one sub-task and generate a code to solve it.











Agentic Reasoning Design Patterns*

O Reflection

- Madaan, Aman, et al. "Self-refine: Iterative refinement with self-feedback." Advances in Neural Information Processing Systems 36 (2024).
- Shinn, Noah, et al. "Reflexion: Language agents with verbal reinforcement learning." Advances in Neural Information Processing Systems 36 (2024).

O Tool use

- Patil, Shishir G., et al. "Gorilla: Large language model connected with massive apis." arXiv preprint arXiv:2305.15334 (2023).
- Yang, Zhengyuan, et al. "Mm-react: Prompting chatgpt for multimodal reasoning and action." arXiv preprint arXiv:2303.11381 (2023).

O Planning

- Wei, Jason, et al. "Chain-of-thought prompting elicits reasoning in large language models." Advances in neural information processing systems 35 (2022): 24824-24837.
- Shen, Yongliang, et al. "Hugginggpt: Solving ai tasks with chatgpt and its friends in hugging face." Advances in Neural Information Processing Systems 36 (2024).

Multi-agent Collaboration

- Qian, Chen, et al. "Communicative agents for software development." arXiv preprint arXiv:2307.07924 (2023).
- Wu, Qingyun, et al. "Autogen: Enabling next-gen Ilm applications via multi-agent conversation framework." arXiv preprint arXiv:2308.08155 (2023).

Robust technoloy

Emerging technology

^{*} Sequoia Capital. (2024, March 26). What's next for AI agentic workflows ft. Andrew Ng of AI Fund [Video]. YouTube. https://www.youtube.com/watch?v=saI78ACtGTc

Development Consideration

LLM API (ChatGPT)

Open Source (Local LLM)

Speed

Fast

Local machine dependent

Performance

Great

Parameter size dependent

Cost

High

Low

Privacy

Low

High







Development Consideration

LLM API (ChatGPT)

Open Source (Local LLM)

Speed

Fast

Local machine dependent

Performance

Great

Parameter size dependent

Cost

High

Low

Privacy

Low

High





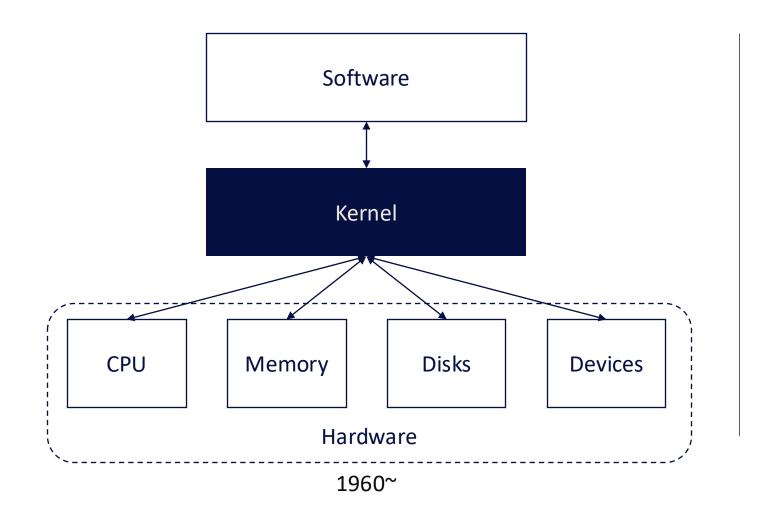


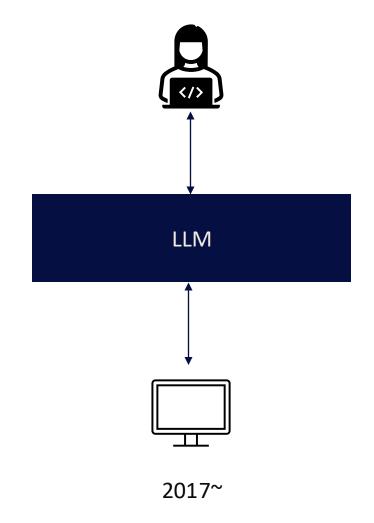


The Role of Large Language Model



The Role of LLM

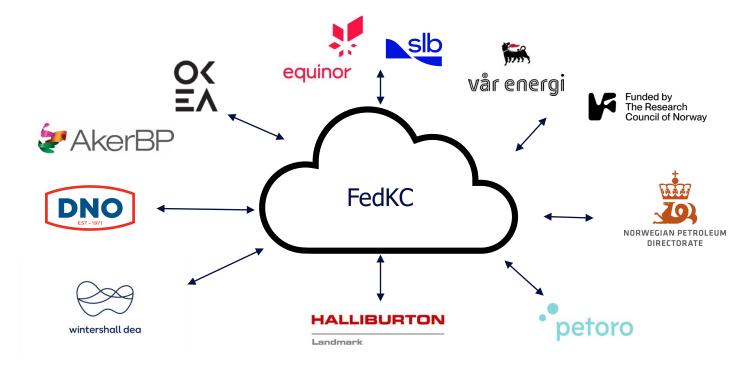




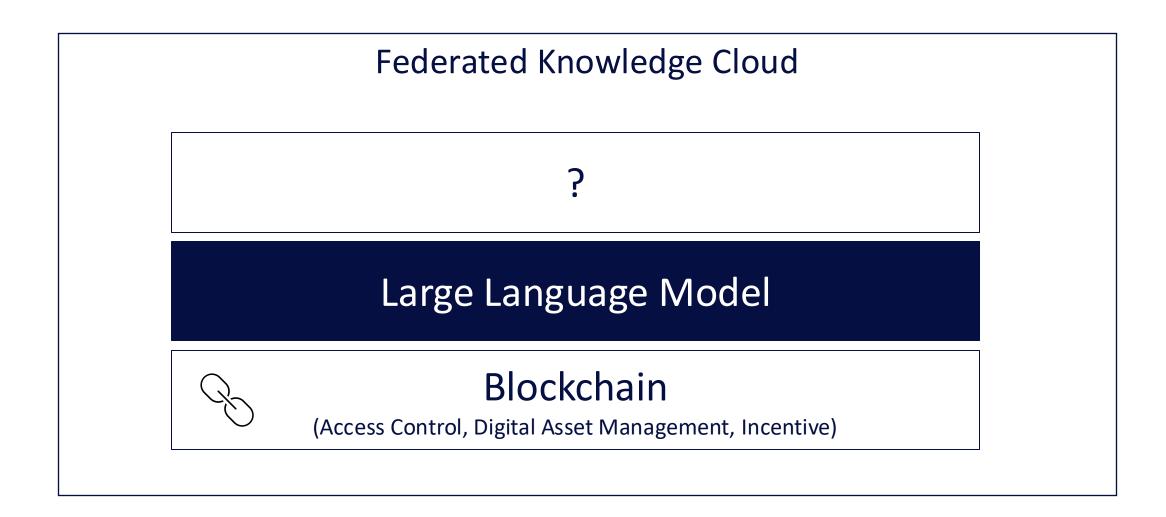
Why is LLM important for FedKC?

To optimize collaboration and streamline efforts

- You just develop however you want.
- LLM will find the way to use it.



What is missing now?



Conclusion

Federated Knowledge Cloud 2025

Domain Knowledge

(insight, code, data, model..)

Large Language Model



Blockchain

(Access Control, Digital Asset Management, Incentive)



Thank You!

See you at the stand!



National Centre for Sustainable Subsurface Utilization of the Norwegian Continental Shelf

University of Stavanger









Acknowledgement

The author(s) acknowledge the Research Council of Norway and the industry partners of NCS2030 – RCN project number 331644 – for their support.









User partners & observers





























