From Zero to Hero: Agent and Multi-Agent AI

Ricardo Santos, Staff AI Engineer @ Complyance

LLMs triggered a new era: a new industrial revolution

The democratization of AI and the advanced capabilities of text generation models and services, enable new ideas and powerful use cases

End-to-end process automation is now possible by harnessing GenAI

Business processes, document analysis, and communications management can be achieved through GenAI capabilities

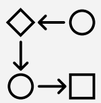
Reasoning capabilities open a new world of possibilities

Most recent LLM models, with reasoning capabilities, enable a wider array of use cases and open the door for a more helpful AI

We pushed GenAI beyond information retrieval

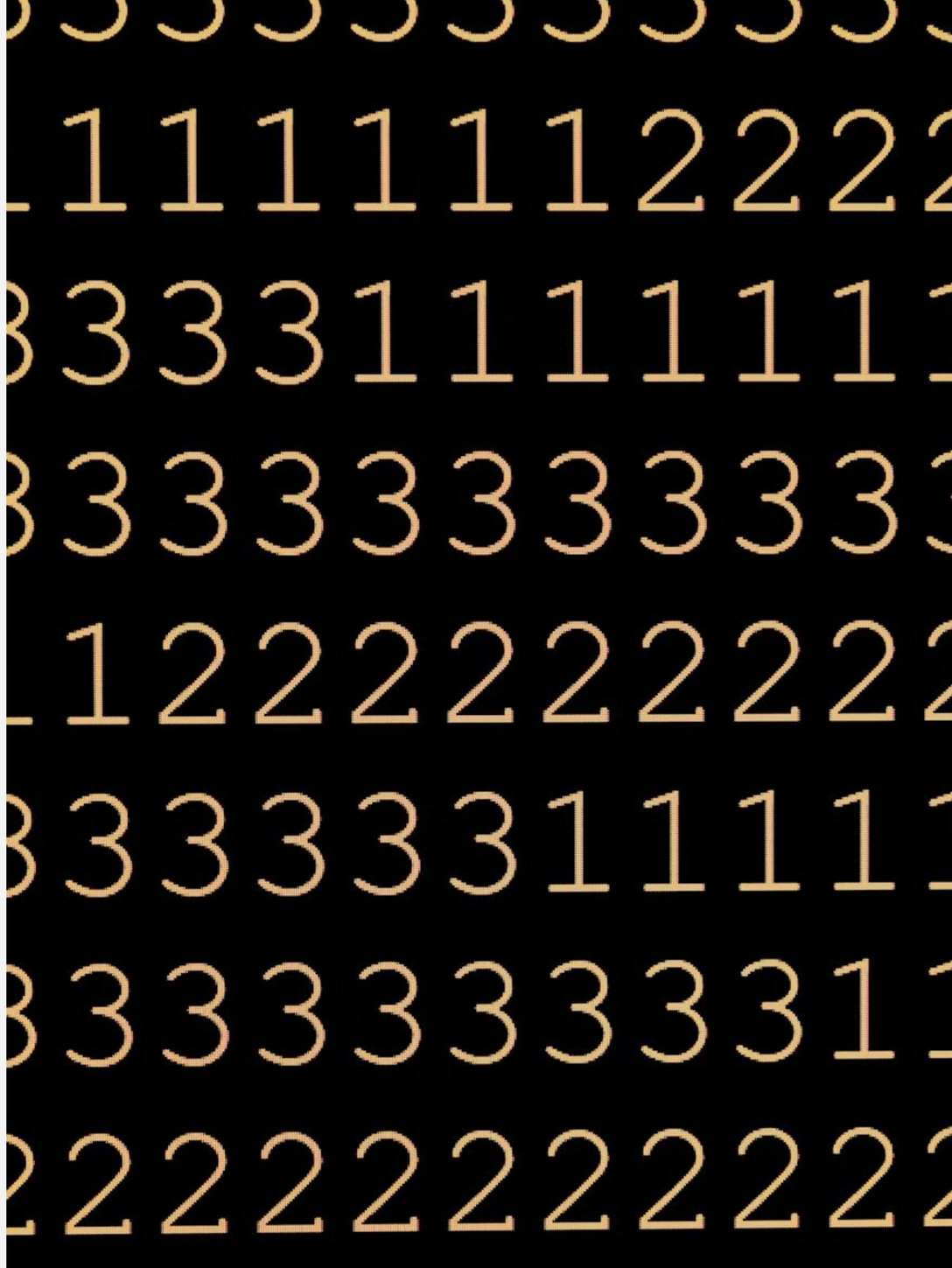
LLMs at their core are text generators, optimized for chat-like human interaction:

Optimized for information retrieval, text redaction, and creativity



Given the capability to return semi-structured objects and text

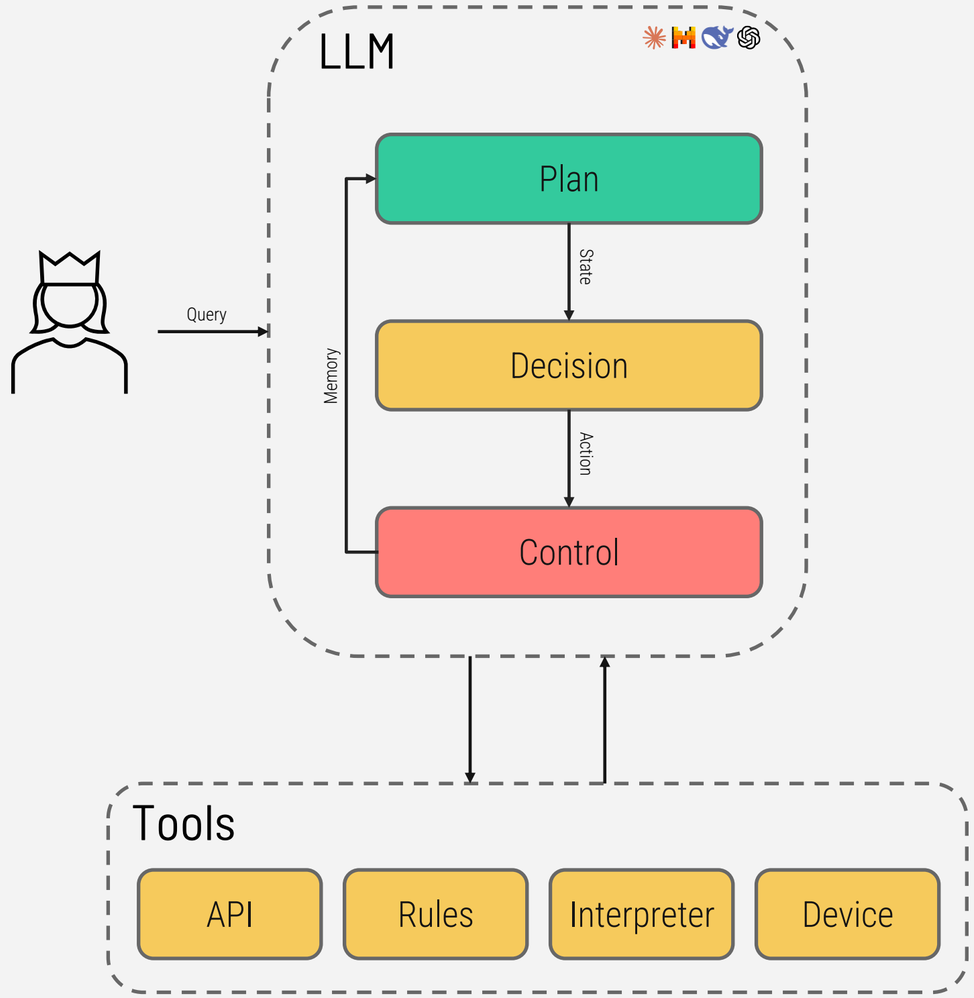
Given capabilities extra to a text canvas, and can execute and call functions



GenAI Agents: initial e2e automation approach

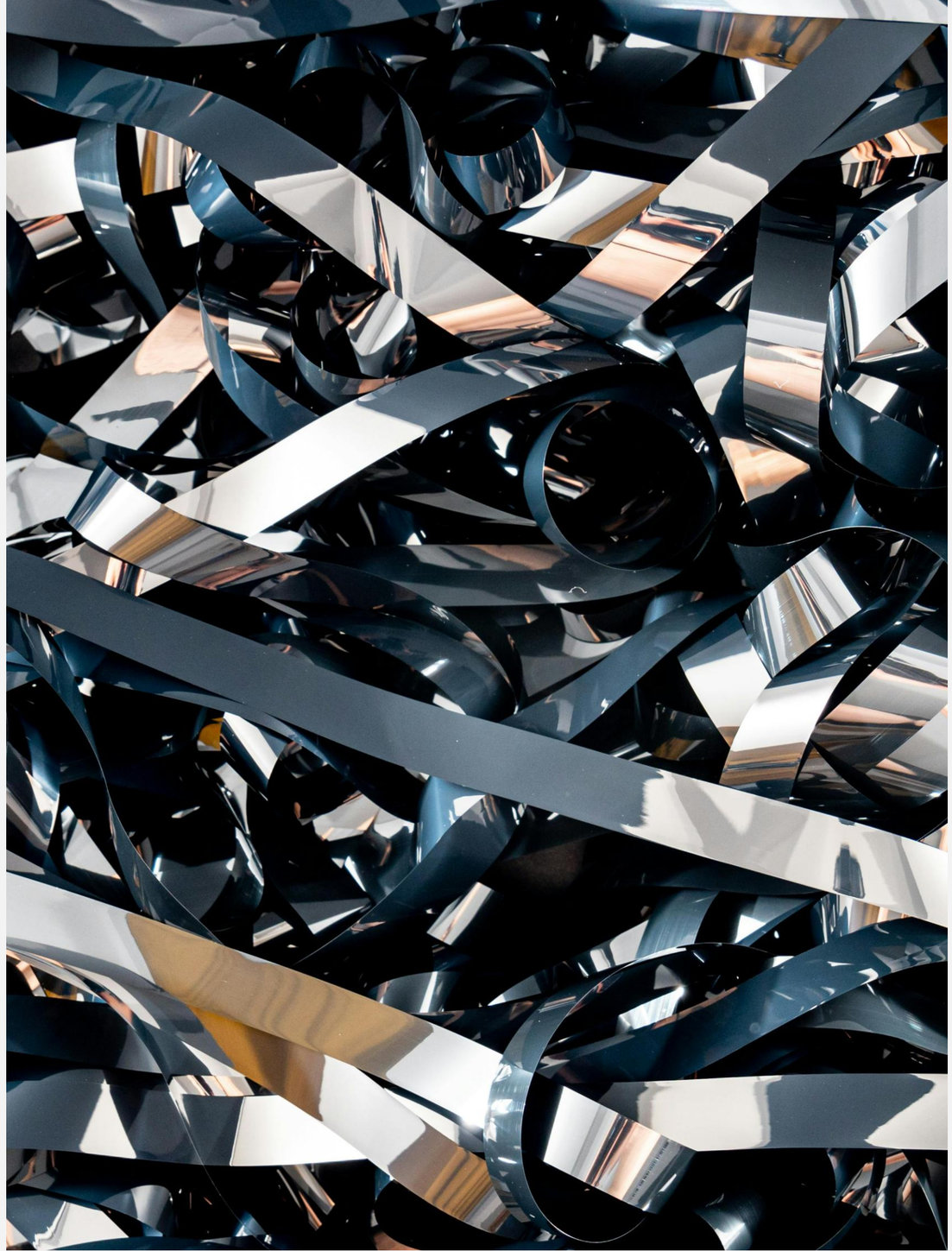
Software capable of taking the driver's seat in end-to-end processes:

- Rely on LLMs as reasoning engines
- Follow instructions through known techniques like CoT or ReAct
- Capable of using and orchestrating tools



Igniting Language Intelligence: The Hitchhiker's Guide From Chain-of-Thought Reasoning to Language Agents, https://arxiv.org/abs/2311.11797

Let's build a simple Software Development Agent with LangChain and LangGraph



Agents struggle with complex problems

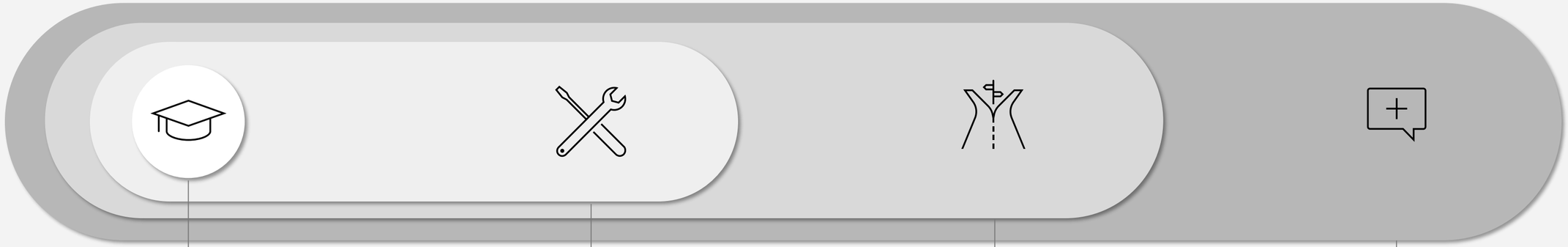
There are impressive use cases where agents successfully took the driving seat, but the failure rate for complex workflows was too high.

- Single LLMs with long instructions fail to achieve the desired process results
- When the number of tools and use cases grow, the failure rate grows as well
- Single GenAI-based agents fail to demonstrate strategic reasoning*

* Simulating Strategic Reasoning: Comparing the Ability of Single LLMs and Multi-Agent Systems to Replicate Human Behavior, https://arxiv.org/pdf/2402.08189v2

A Multi-Agent approach implements the division of work and enables agents to become specialists

Multi-agent solutions let agents interact through a directed graph, and each agent has the following capabilities:



Specialization

Different inception prompts and models

Capable of specializing in a field of action

Tooling

Different tools available per agent

Required capabilities to achieve its goal

Decision making

Individual Agents decide an approach

Each decision influences the solution approach

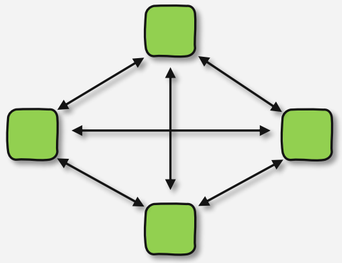
Communication

Data flows between agents in the network according to rules and paths

Researchers concluded that Multi-Agent solutions showcase a 33% increase in success rate for complex problem-solving*

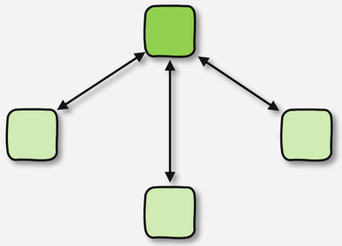
* Simulating Strategic Reasoning: Comparing the Ability of Single LLMs and Multi-Agent Systems to Replicate Human Behavior, https://arxiv.org/pdf/2402.08189v2

Multi-agent solutions can follow different architectures and a mix of best-in-class models



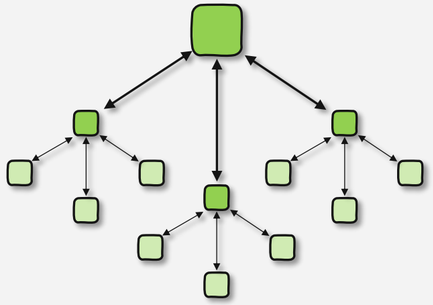
Network

Each agent can communicate with every other agent. Any agent can decide which other to call next



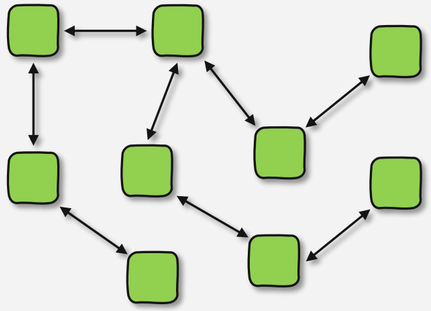
Supervisor

Each agent communicates with a supervisor agent, who decides which agent should be called next



Hierarchical

Mult-agent system with a supervisor of supervisors. Each supervisor manages a team of agents



Custom

Each agent communicates only with a subset of agents. Parts of the flow are deterministic, and some agents decide who to call next

Agents are represented as `Nodes`, and communications are either `Commands` or `Edges`, carrying an updated `State`

* LangGraph - Multi-agent Systems, https://langchain-ai.github.io/langgraph/concepts/multi_agent/


Let's improve our solution, and
let's add a Multi-Agent setup.

Multi-agent systems can be as flexible as needed: Modularity, Specialization, and Control

Modularity

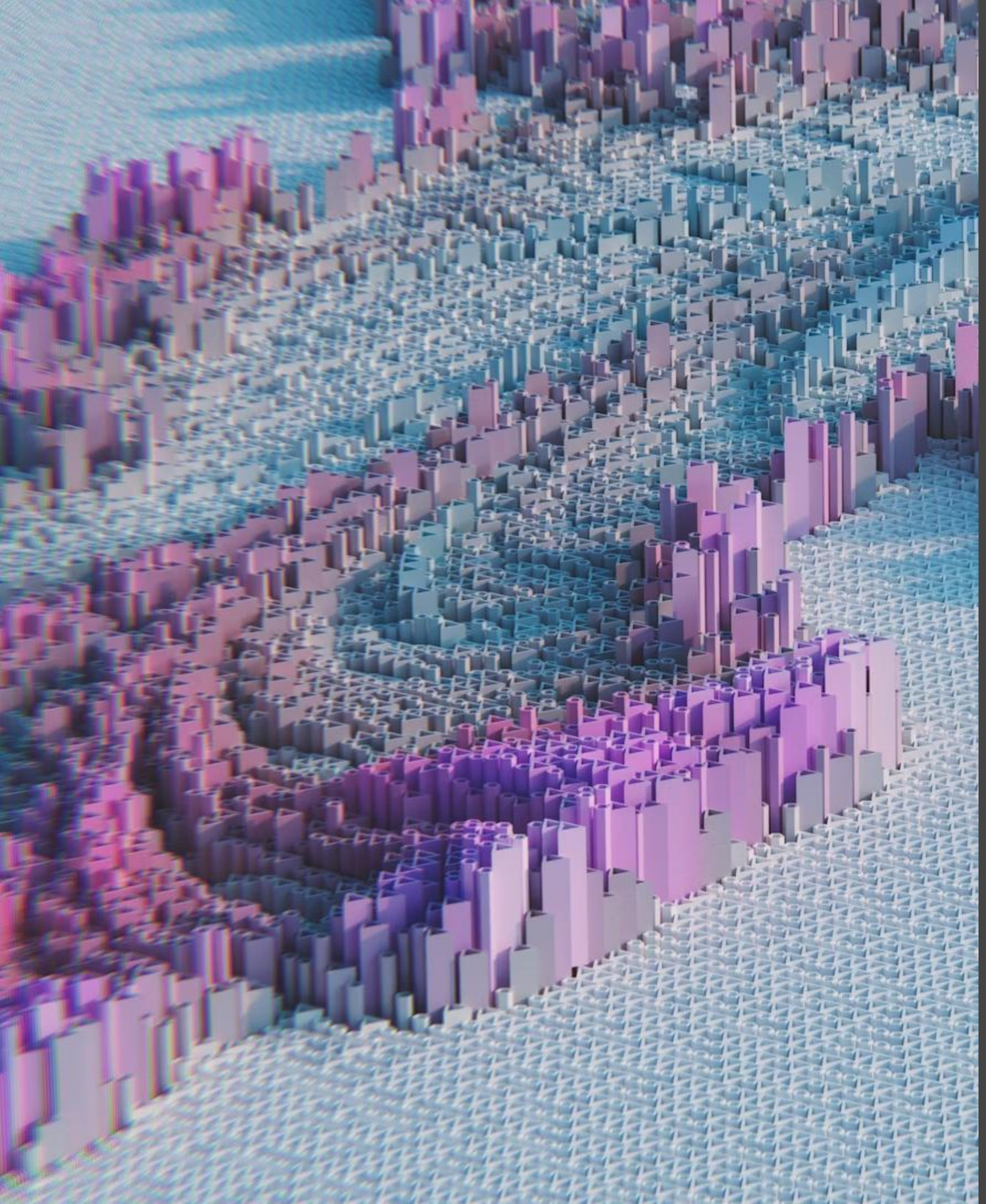
Graphs can be easily extended with the addition of new nodes that easily integrate within the multi-agent architecture, and enhance the service value offering

Specialization

Expert agents, with detailed roles, models, and capabilities, can focus on specific domains, achieving the best performance on specific tasks

Control

Agent communication can be controlled, or parametrized, allowing us, developers, to manage the data flow within the network nodes



We are only scratching the surface

- There are hundreds of tools to implement Multi-agent Solutions
- Reasoning capabilities will greatly improve multi and single-agent solutions
- Memory optimization techniques will allow bigger networks and complex pipelines

Thank You

https://www.youtube.com/@RicardoSantosDiaz

https://github.com/Tibiritabara

https://www.linkedin.com/in/ricardosantosdiaz/