Agentic for Enterprise

Challenges and Opportunities in the “Wild”

Eser Kandogan

Megagon Labs

Megagon Labs

Compound AI Systems

Data AI Symbiosis

RECRUIT

Megagon Labs

indeed

CSI Companies

glassdoor

CHANDLER MACLEOD GROUP

unique

Staffmark Group

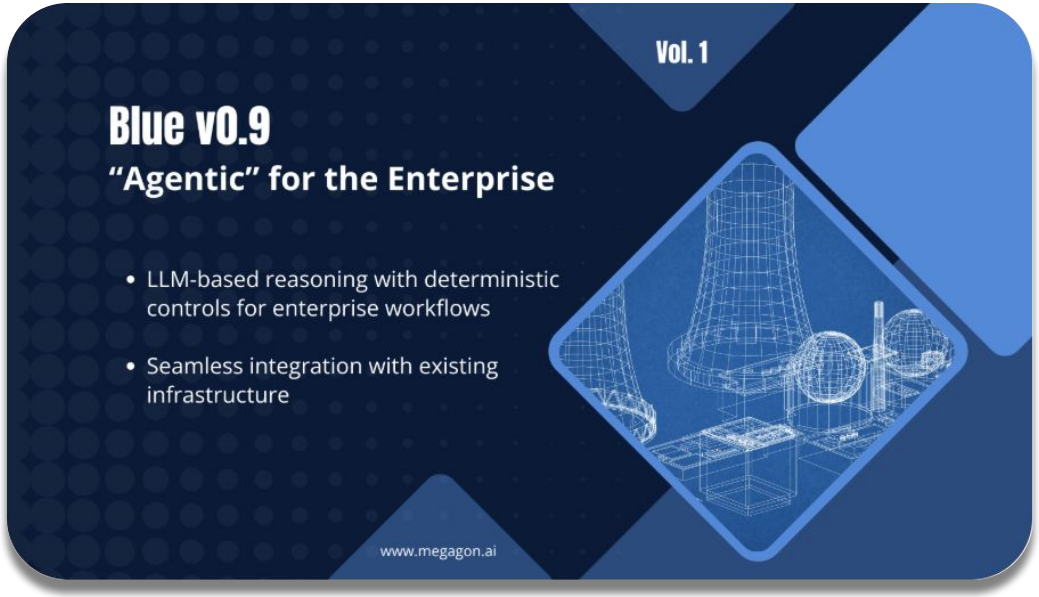
Quandoo

LLMs and NLP

Human-Centered AI

Megagon Blue

The Blue architecture is a next-generation AI system built on the **principles of CoupoundAI Systems**, with an emphasis on **integrating databases and domain knowledge** to handle **complex tasks** and **adapt** to specific industries.



megagon.ai/research/compound-ai-system/

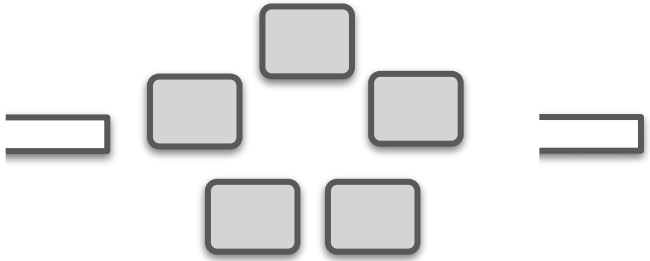
megagon.ai

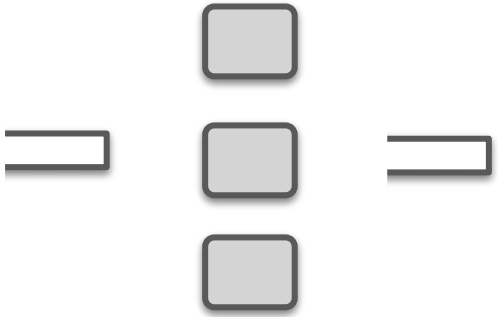
LLMs changed everything...

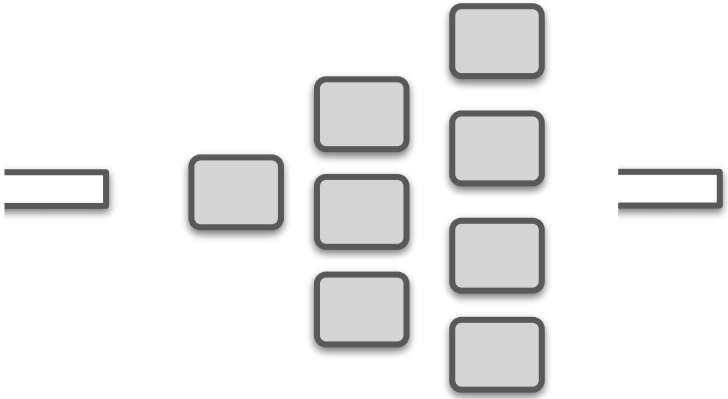
Adopting LLMs has been challenging...

...
hallucination,
context length,
prompt sensitivity,
fairness,
ethics,
...

Emergence of Agentic Patterns



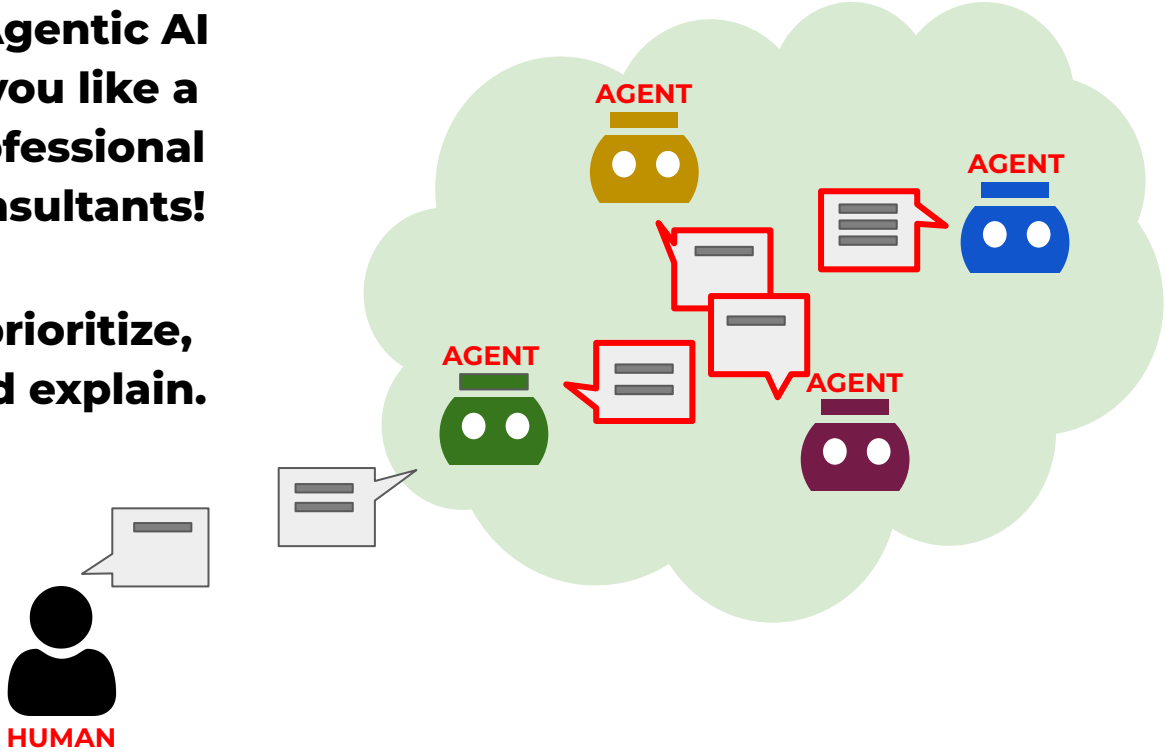




Agentic AI

Agentic AI works with you like a professional consultants!

...to analyze, prioritize, and explain.



Agents

Skills and Abilities in a Domain

Autonomy to Make Decisions

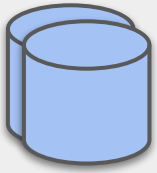
External Tools and Resource

Memory, Knowledge

Agentic Use Cases

Customer Support

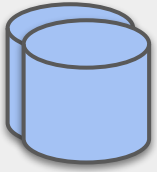
Exploit past issues to provide solutions, with explanations



Customer DB
Issue Tracker

Finance

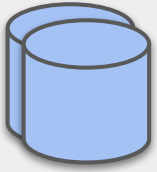
Automate monthly reports, perform anomaly detection



Accounting DB

Sales

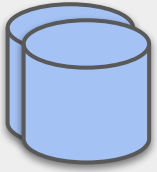
Identify leads, create proposals



Client DB
Product DB
Sales DB

HR

Compare candidates to job reqs, scores and explains fit

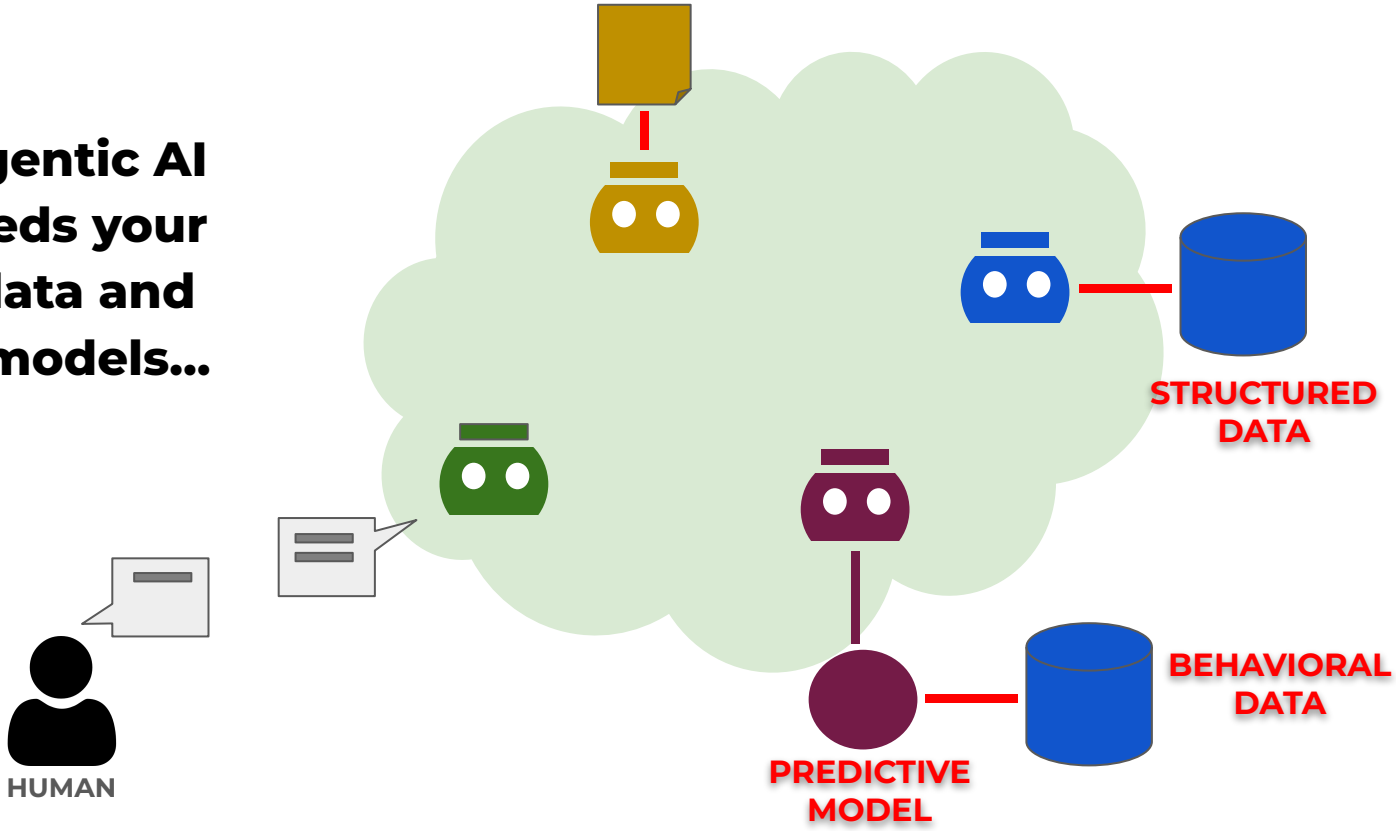


Jobs DB
Resumes DB
Applications DB

I am looking for a house...

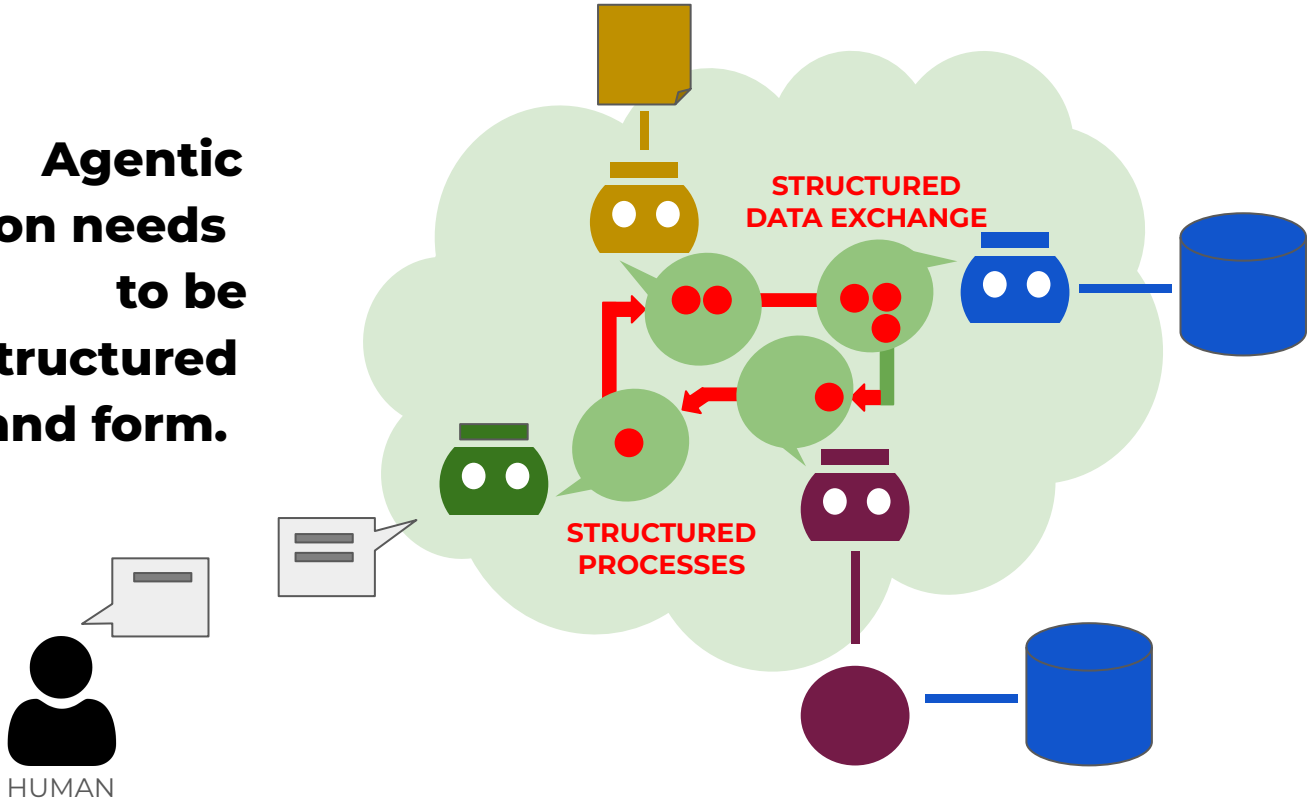
Agentic AI: Data and Models

Agentic AI needs your structured data and models...



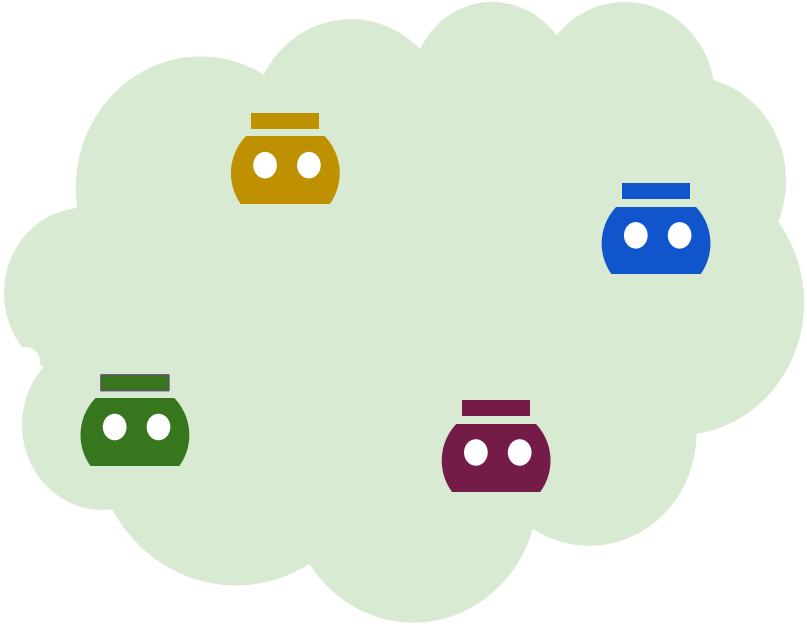
Agentic AI: Structured Conversation

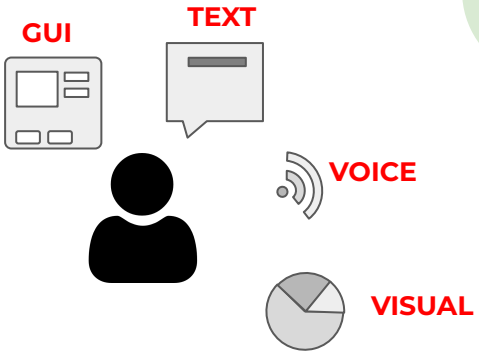
Agentic collaboration needs to be structured in content and form.



Agentic AI: User Interaction

Support multiple modalities in user interactions, GUI, VIS, Text, Voice...





Agentic for Enterprise

Scalability

Efficiency

Controllability

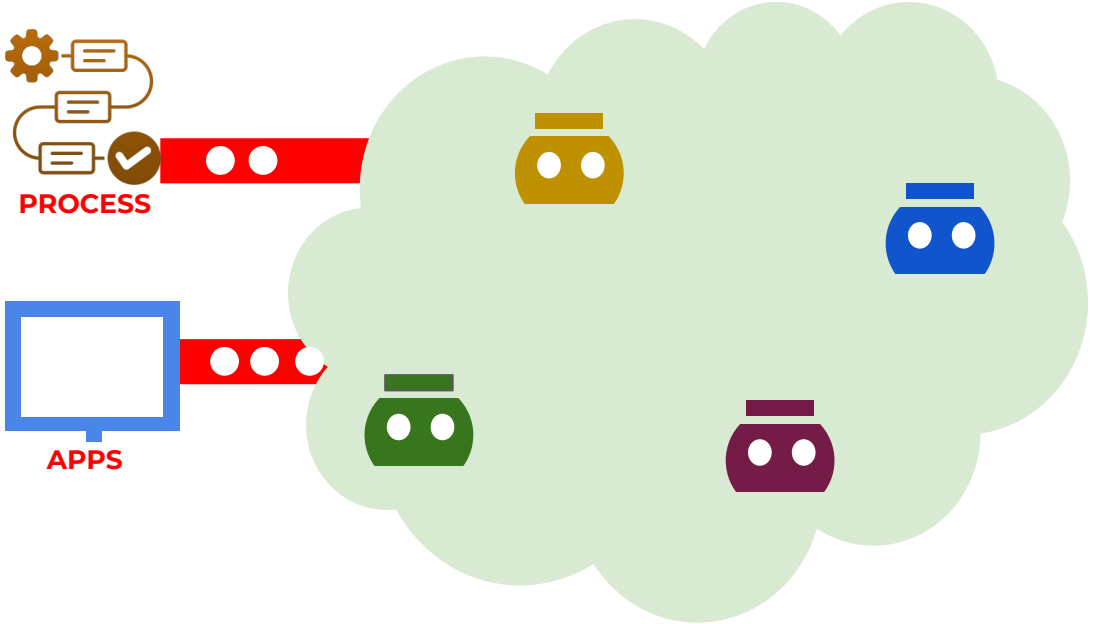
Observability

Measurability

Configurability

Agentic Enterprise AI: Touchpoints

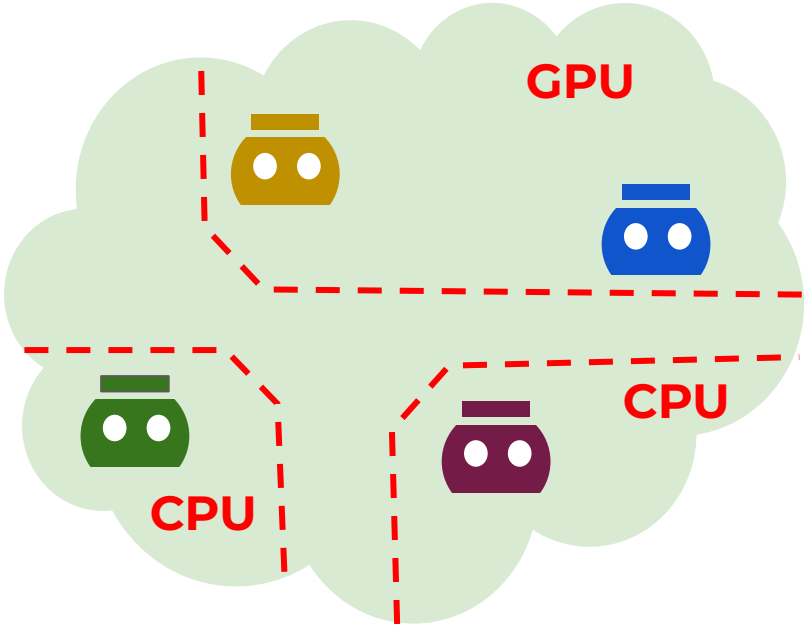
Connect your 'agentic workflows' to your applications and business processes.



Agentic Enterprise AI: Infrastructure

Exploit enterprise infra when necessary for scale and efficiency.

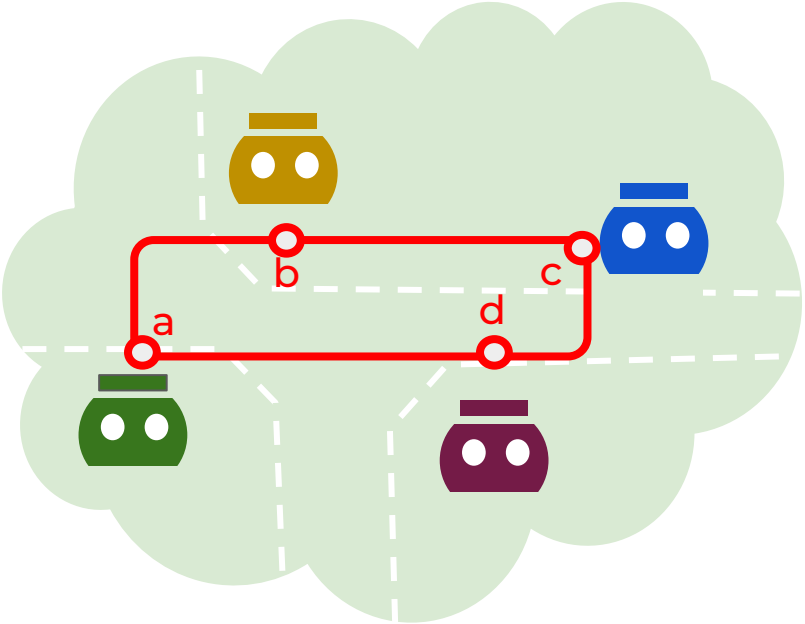
Allocate the right compute resources for agentic.



Agentic Enterprise AI: Infrastructure

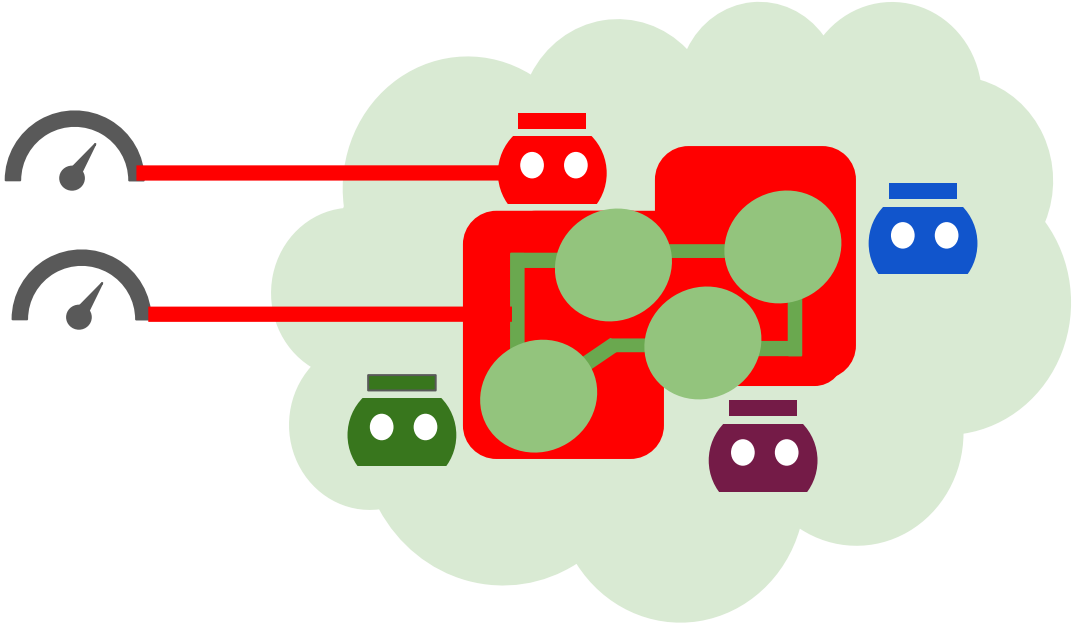
Discover and address agentic resources in the infrastructure.

Establish means to distribute data and tasks.



Agentic Enterprise AI: Monitoring, QoS

Instrument Agentic AI to collect QoS metrics, at multiple granularity/scope per agent, per session, per task.



logic

algorithmic

apriori

probabilistic

in-situ

data

structured	unstructured
symbolic	parametric
domain-specific	common-sense
private	public
single-source	multi-source

interaction

direct-manipulation
masses

agentic
personal

Computing...

‘Prescribed’		‘Learned’
algorithmic apriori	→	probabilistic in-situ
symbolic structured domain-specific private	→	parametric unstructured common-sense public
direct-manipulation masses	→	agentic personal

Computing… *hybrid*

… **data transformed** into different modalities,

moving between compute,

mix of **algorithmic and probabilistic**

applications comprised from multitude of compute(s)

some application logic designed a **priori, some on-the-fly**

interacting with users / agents in **bursts but w/ gaps**

Thesis

rethink...

...how we **define application**?

...how we **acquire and process data**?

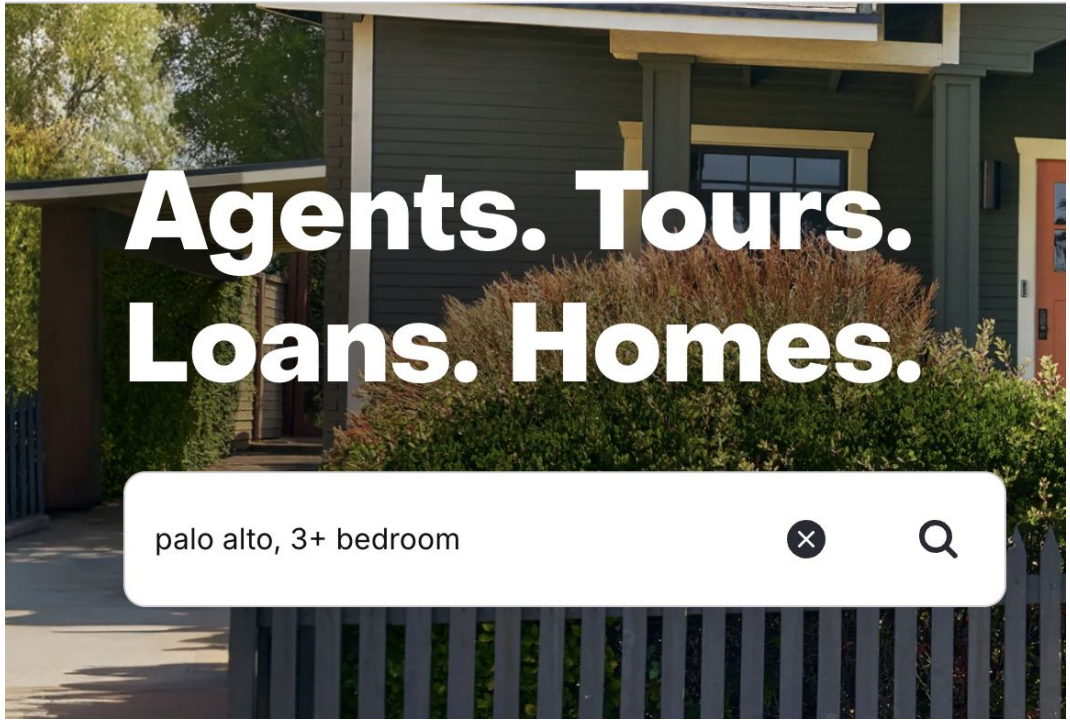
...how we **interact** to the user?

...how we **develop** software?

...how we **deploy** applications?

I am looking for a house...

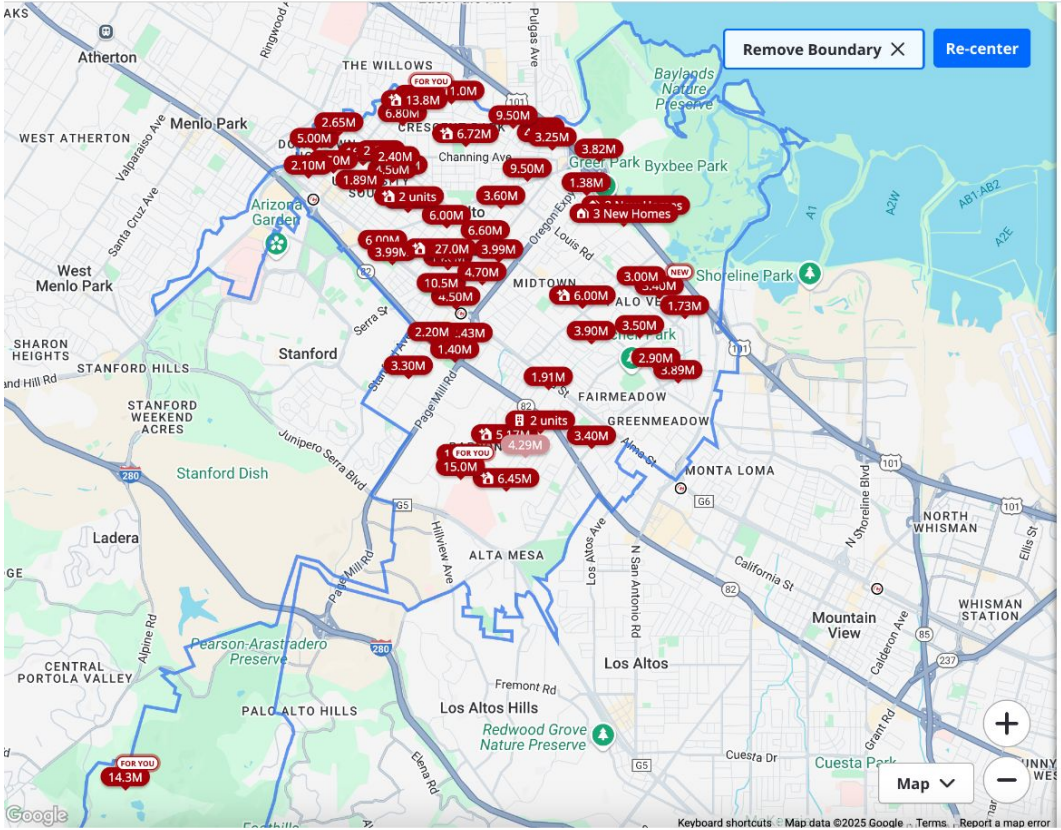
Buy Rent Sell Get a mortgage Find an Agent



palo alto, 3+ bedroom

For Sale | Price | 3+ bd, 0+ ba | Home Type | More | Save search

87 Saved Homes



Palo Alto CA Real Estate & Homes For Sale

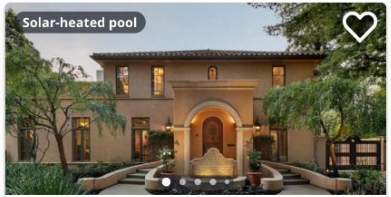
62 results

Sort: Homes for You

$13,800,000

7 bds | 9 ba | 7,915 sqft - New construction

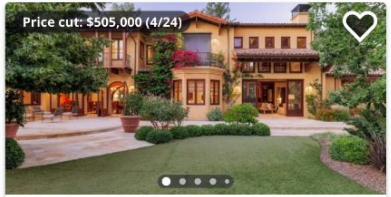
1307 University Ave, Palo Alto, CA 94301



$16,500,000

5 bds | 7 ba | 7,180 sqft - House for sale

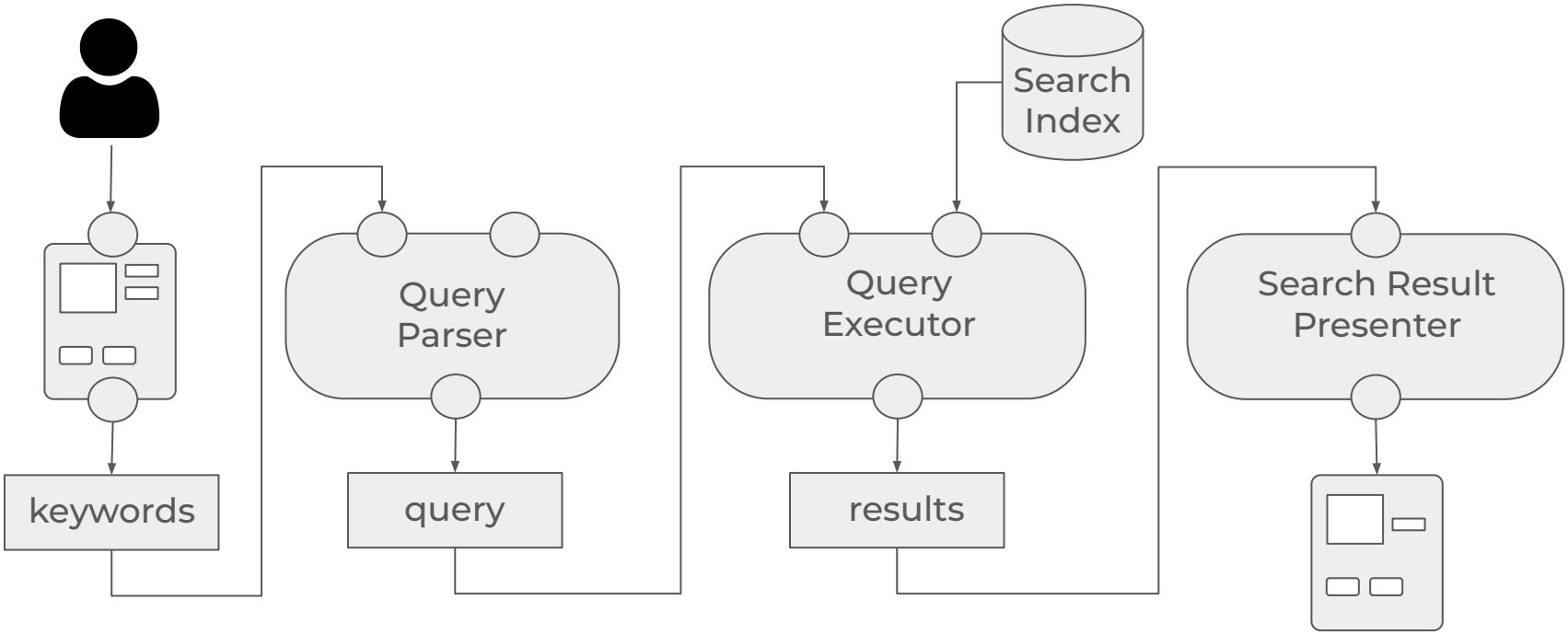
420 Palm St, Palo Alto, CA 94301



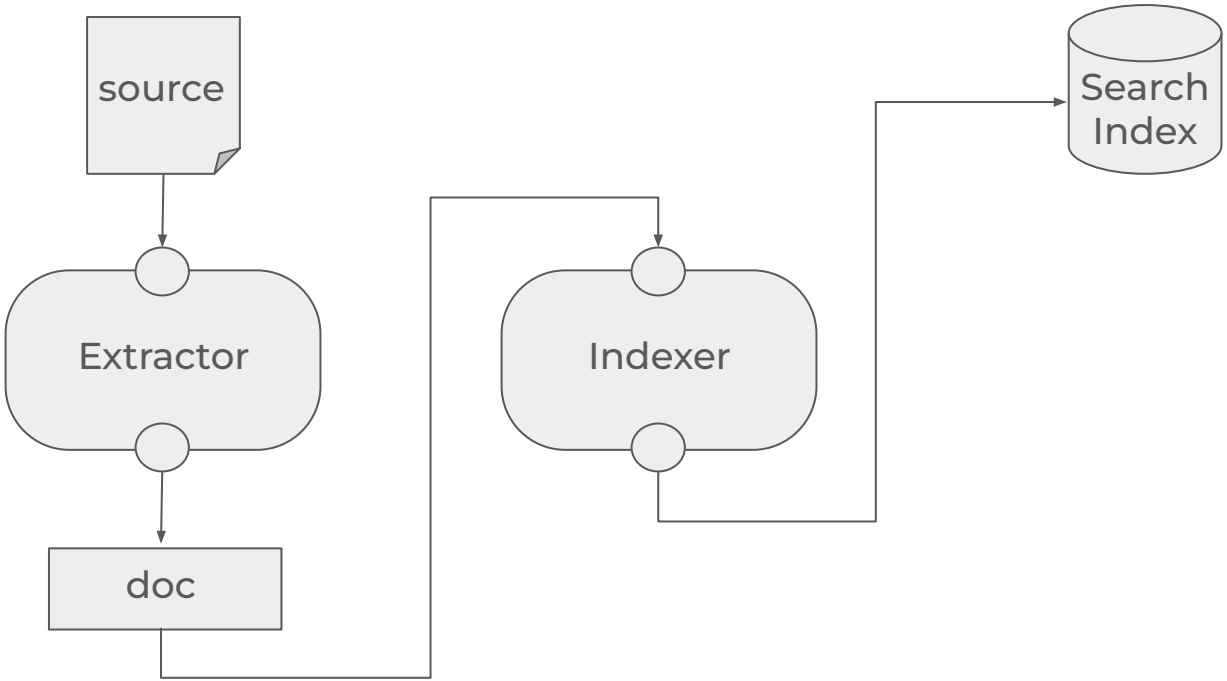
$14,995,000

4 bds | 6 ba | 6,850 sqft - House for sale

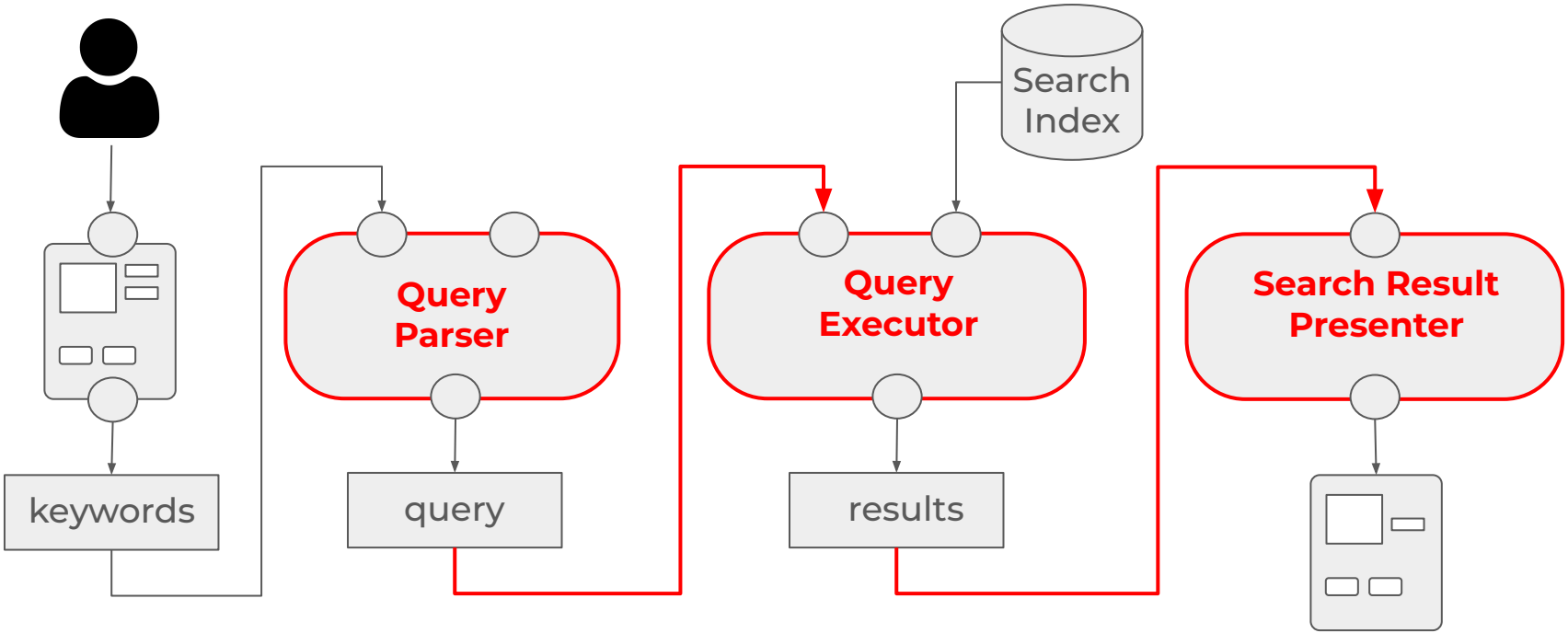
995 Matadero Ave, Palo Alto, CA 94306


Search Index
Query Parser
Query Executor
Search Result Presenter
keywords
query
results

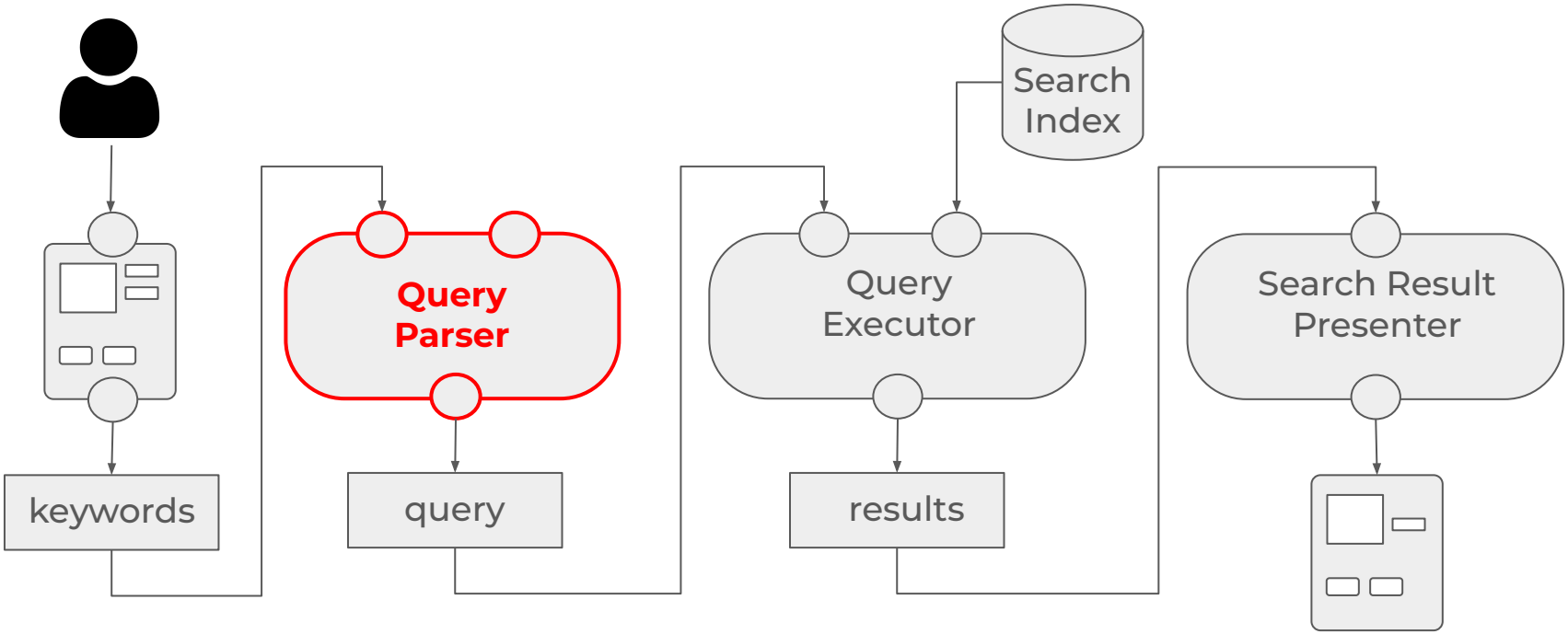
Offline



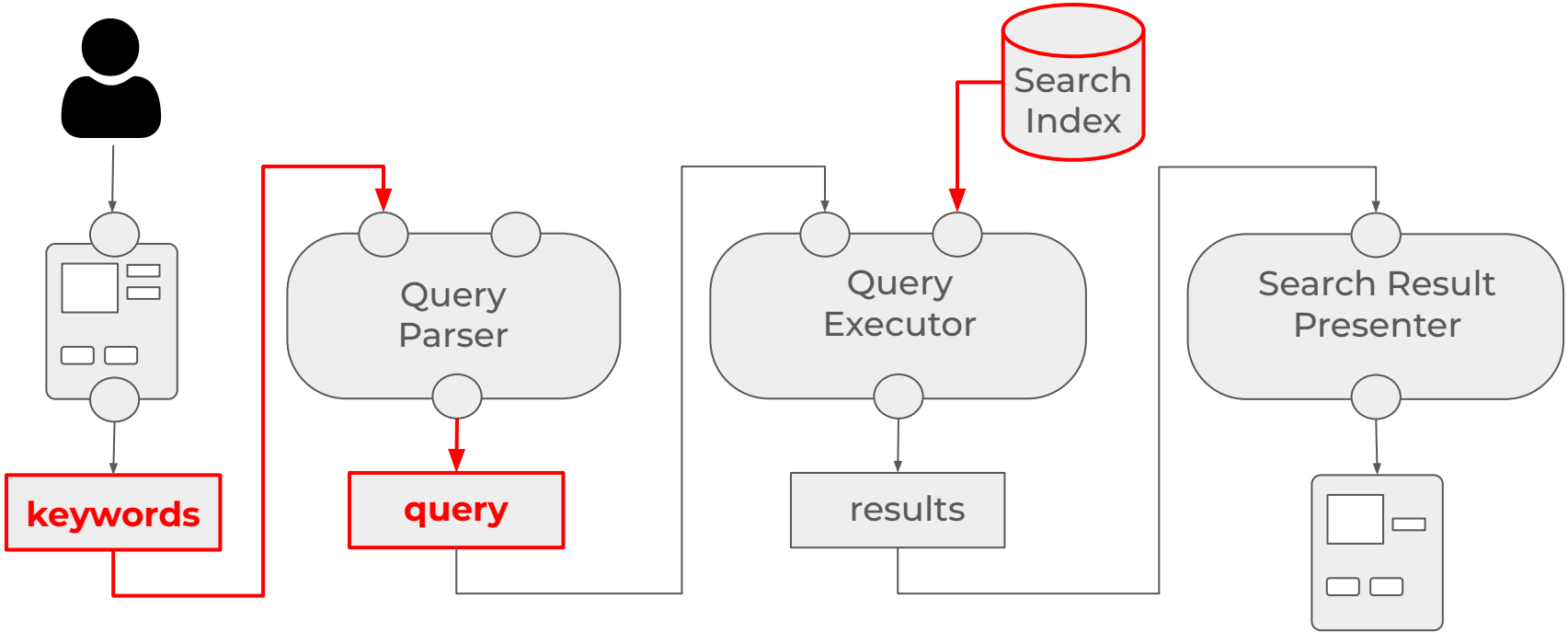
Algorithm


Search Index
Query Parser
Query Executor
Search Result Presenter
keywords
query
results

Functions


Search Index
Query Parser
Query Executor
Search Result Presenter
keywords
query
results

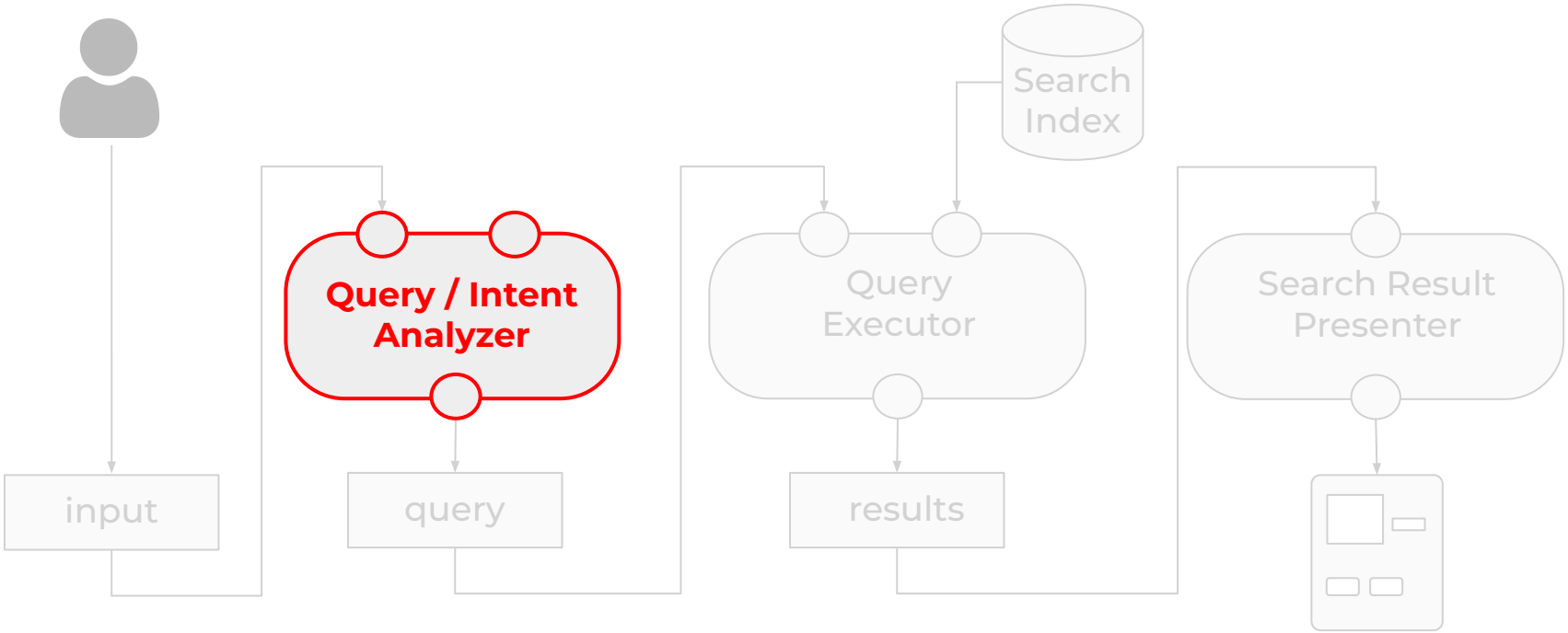
Data


Search Index
Query Parser
Query Executor
Search Result Presenter
keywords
query
results

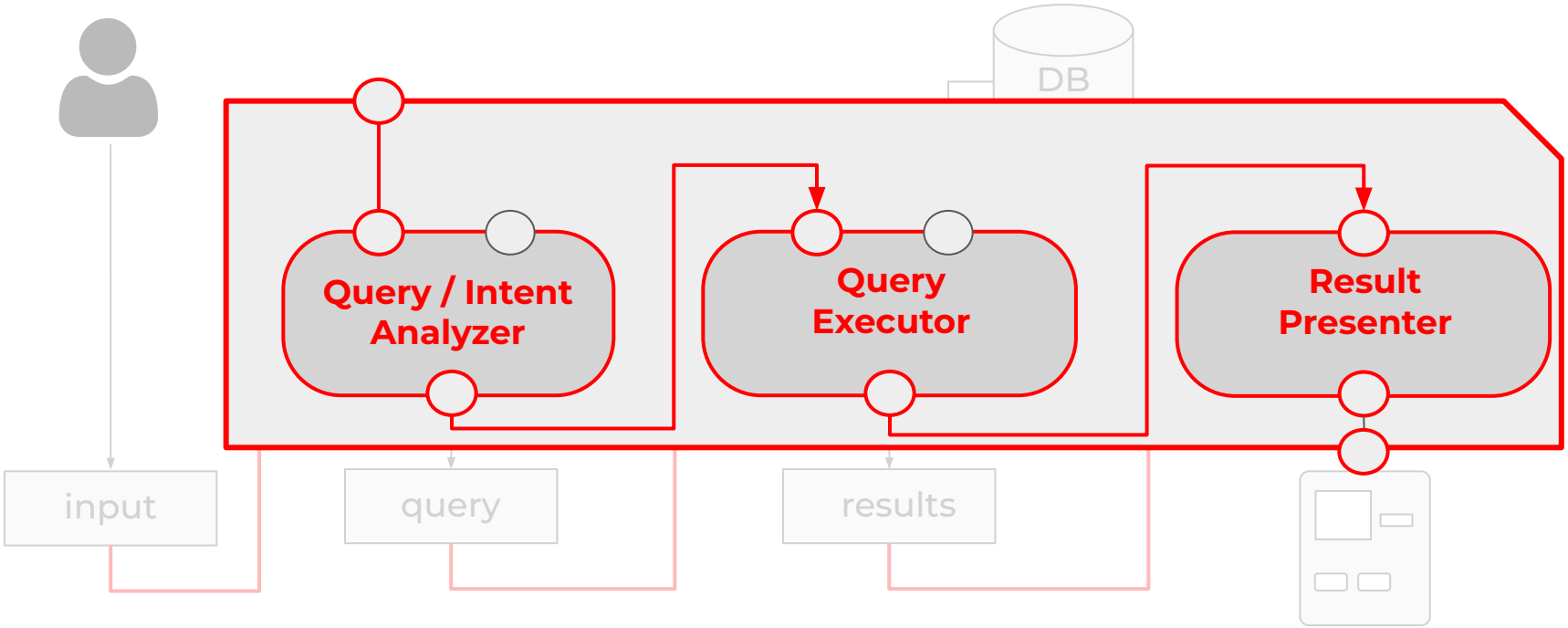
In the Agentic World

“I am looking for a house…”

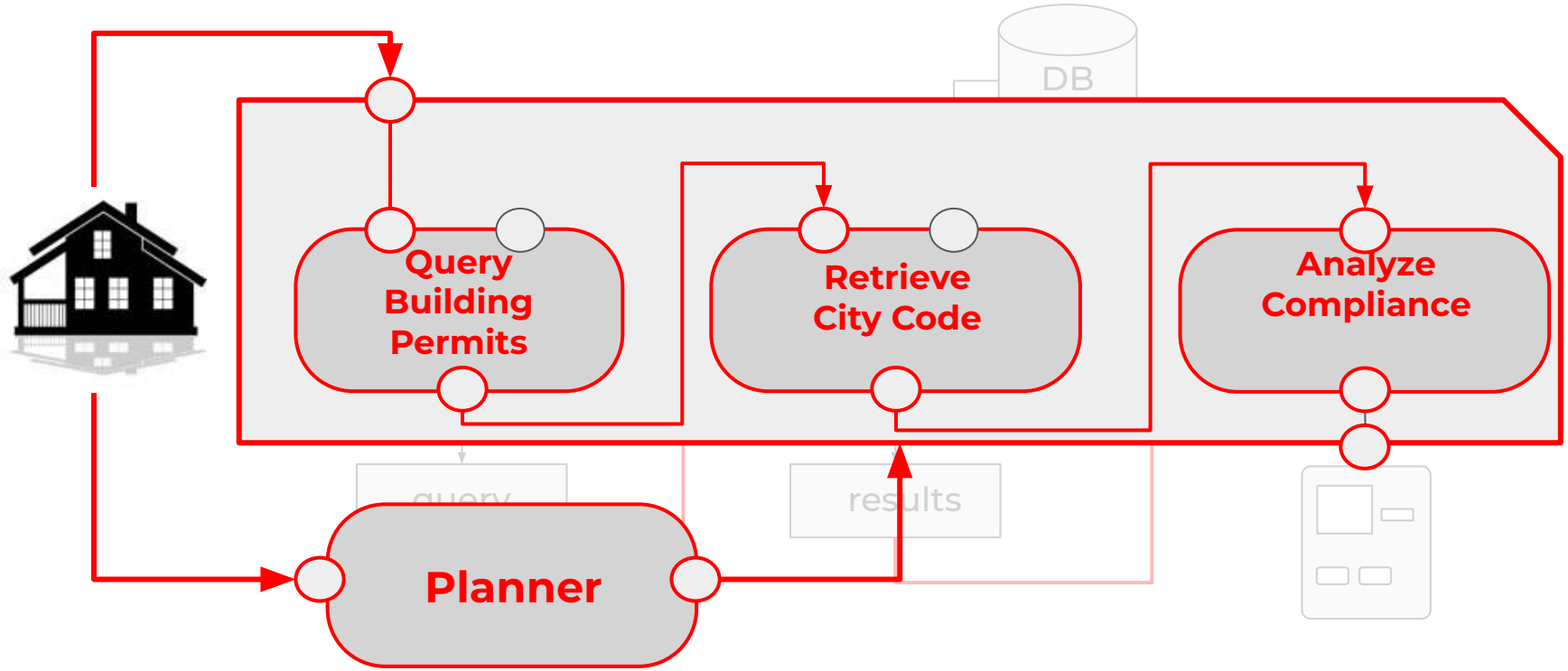
Agent


Search Index
Query / Intent Analyzer
Query Executor
Search Result Presenter
input
query
results

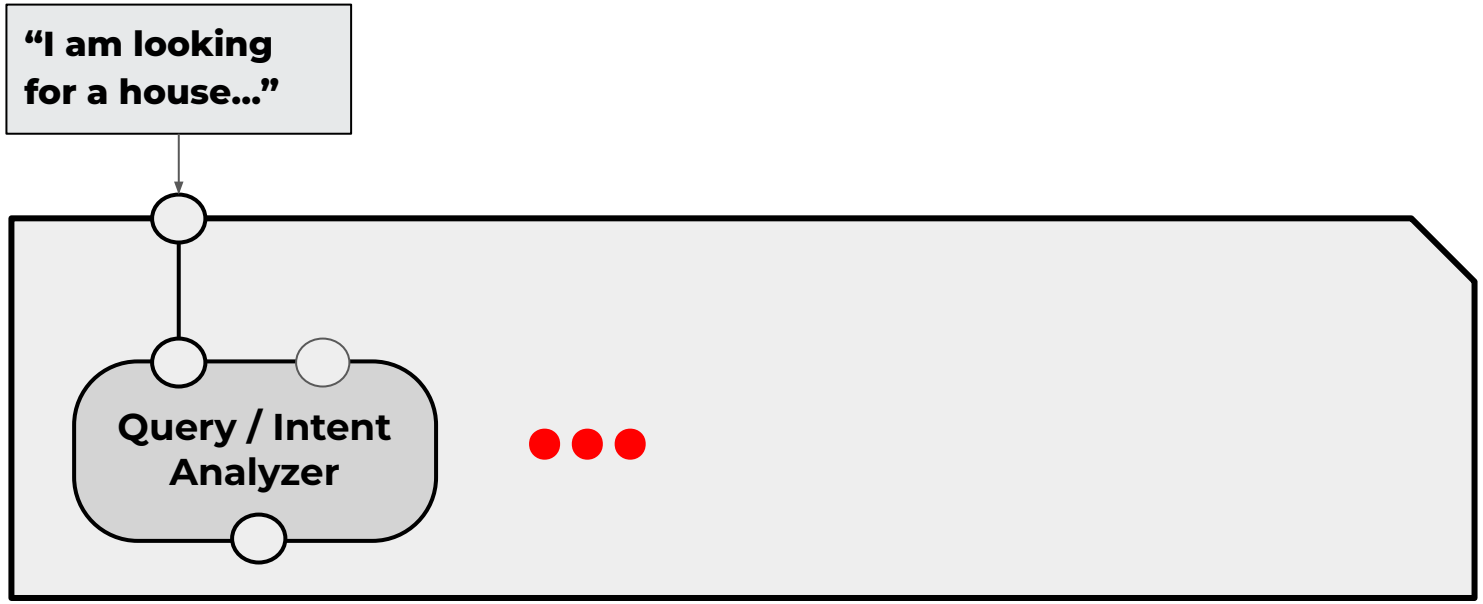
Plan


DB
Query / Intent Analyzer
Query Executor
Result Presenter
input
query
results

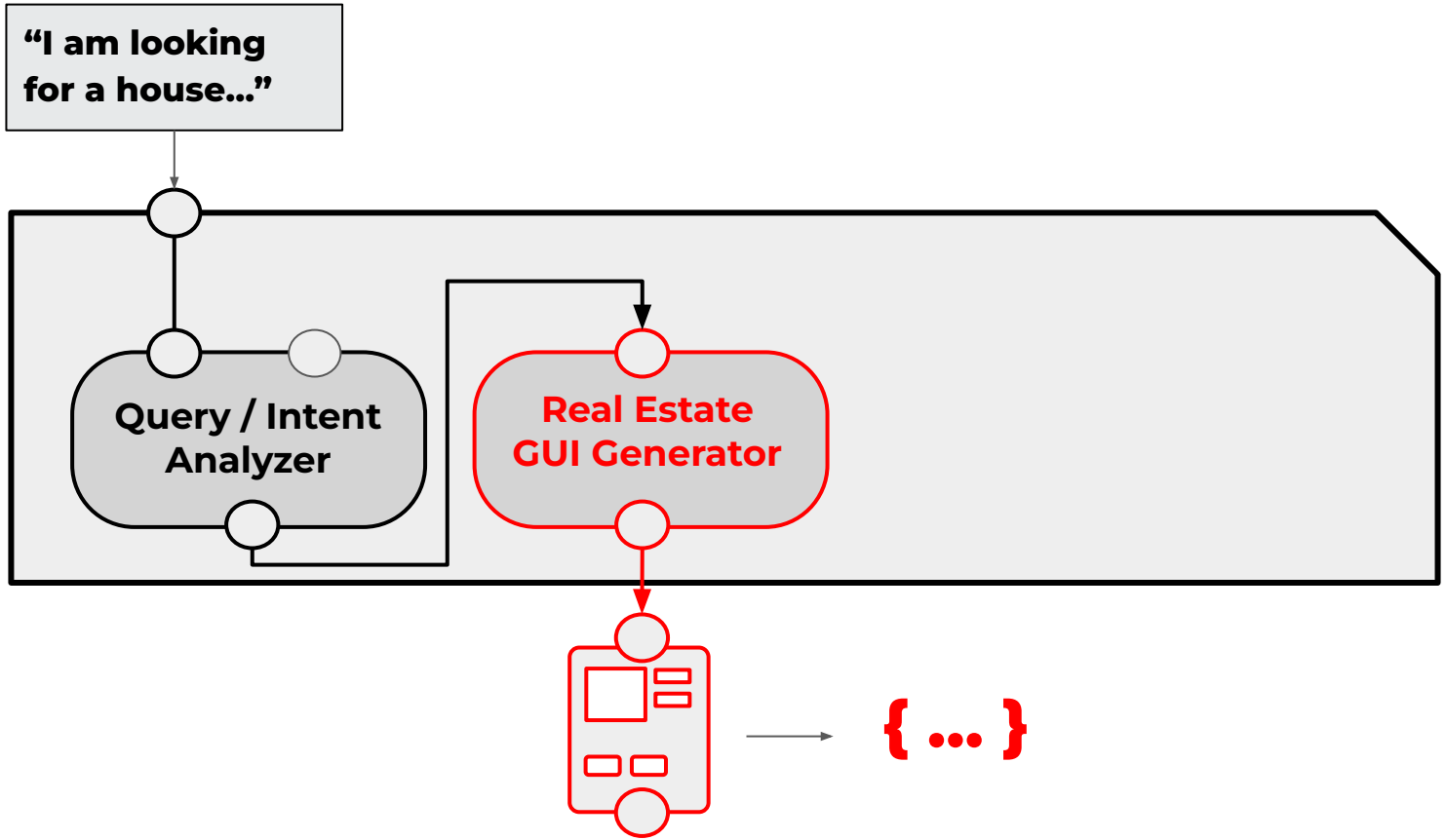
Planner Agent



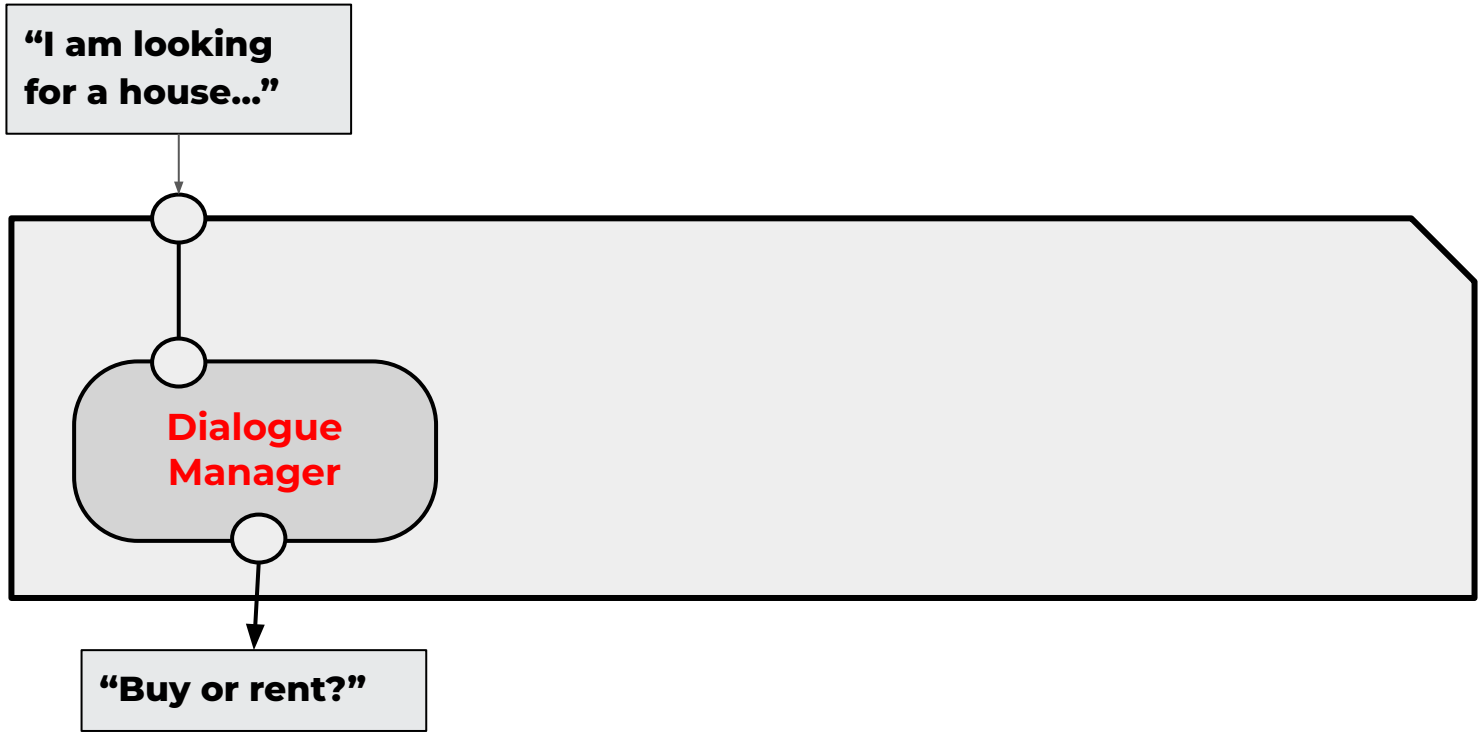
Incremental Planner



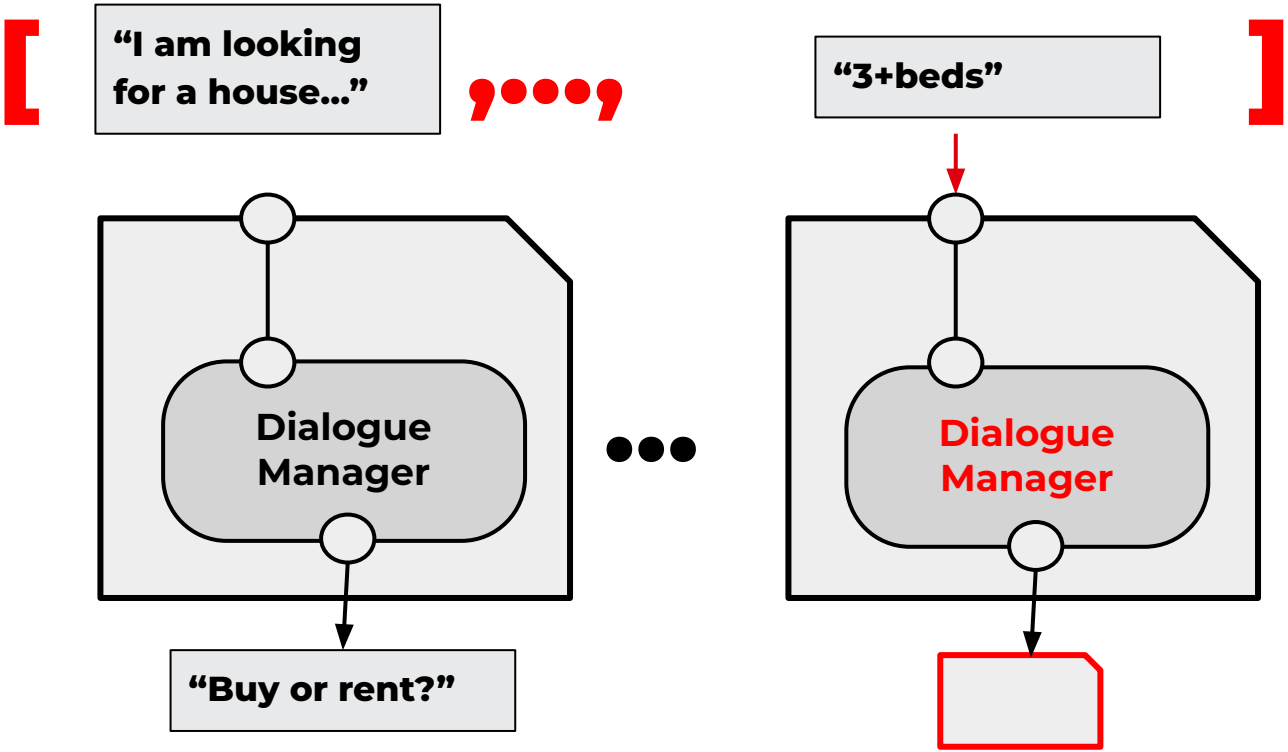
Control thru GUI



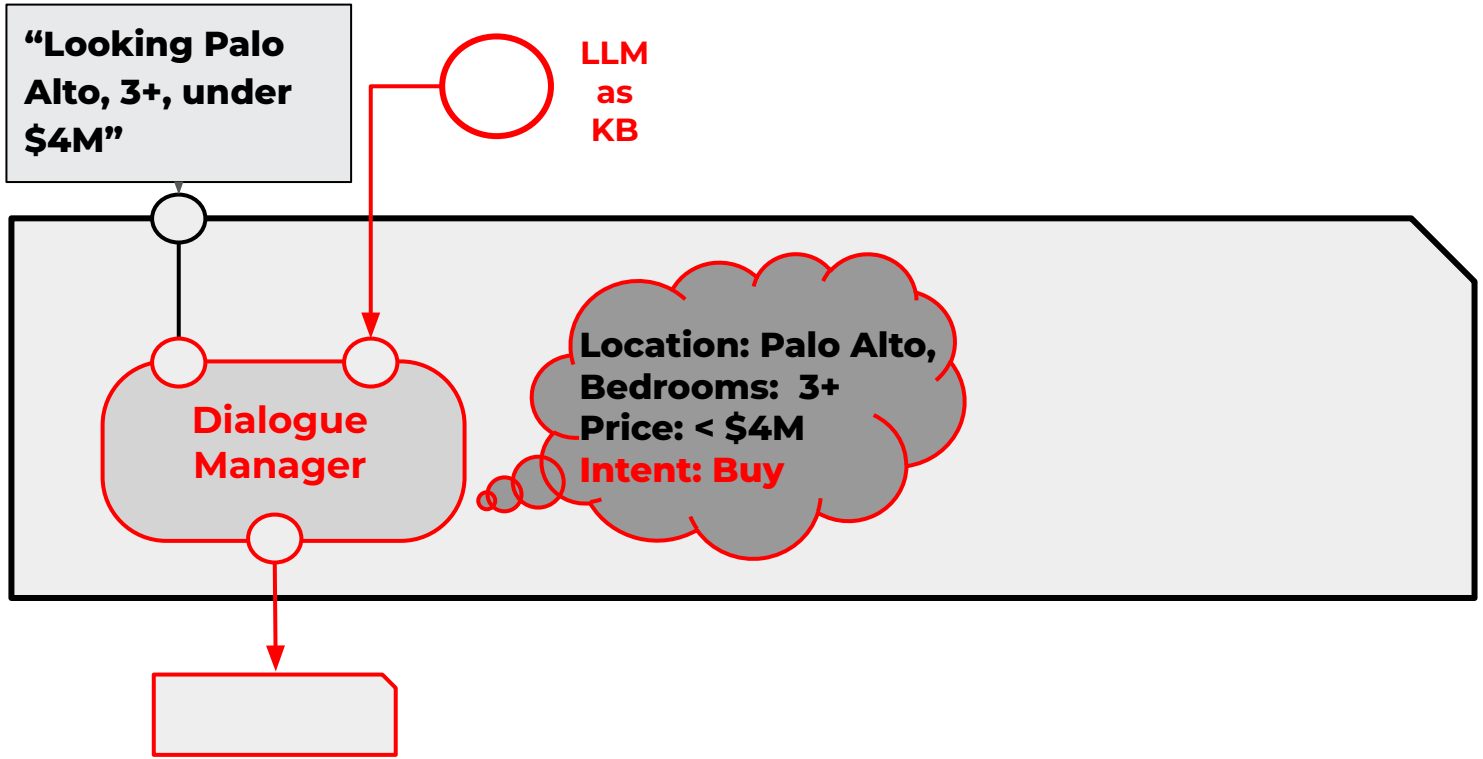
Control thru Dialogue Manager



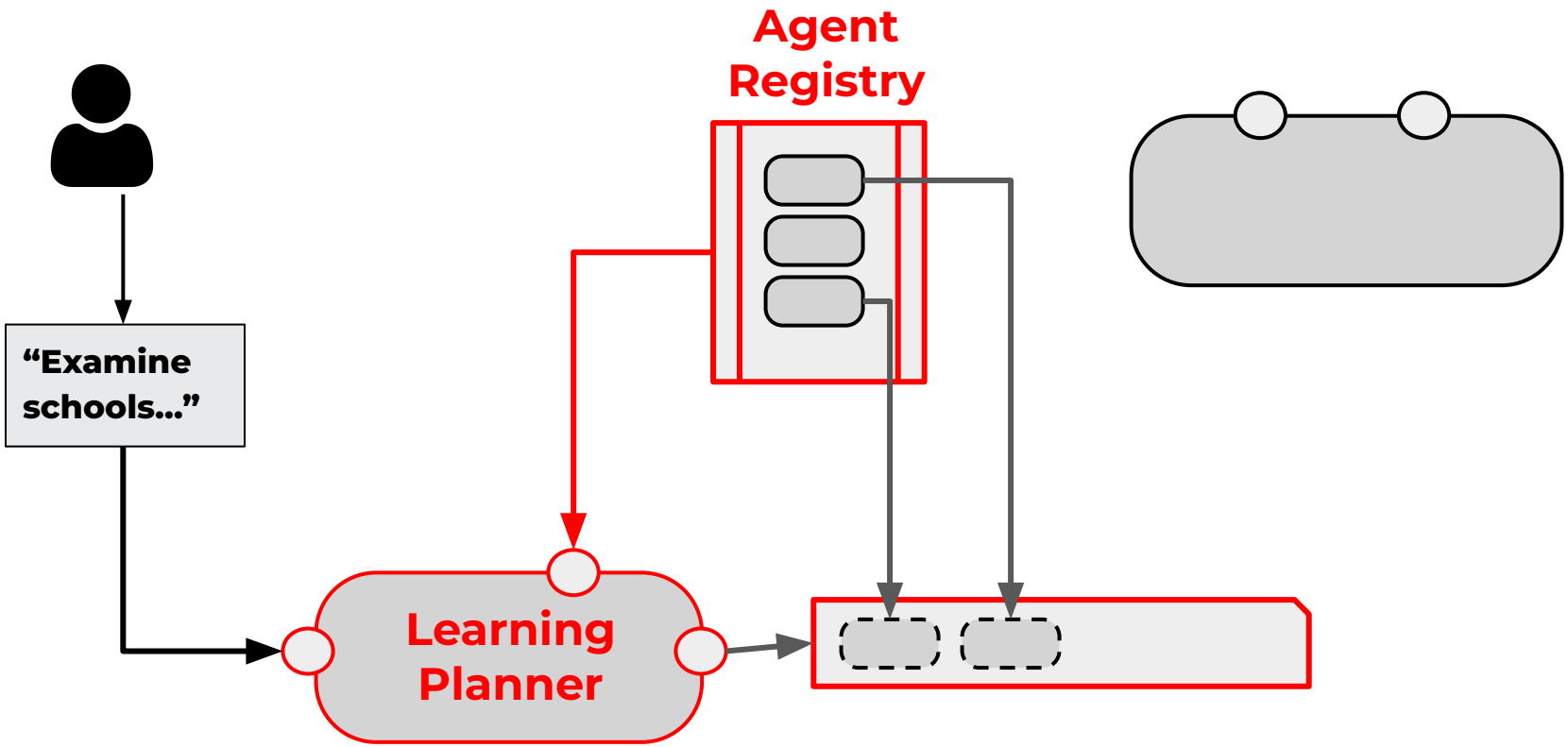
Control thru Dialogue Manager



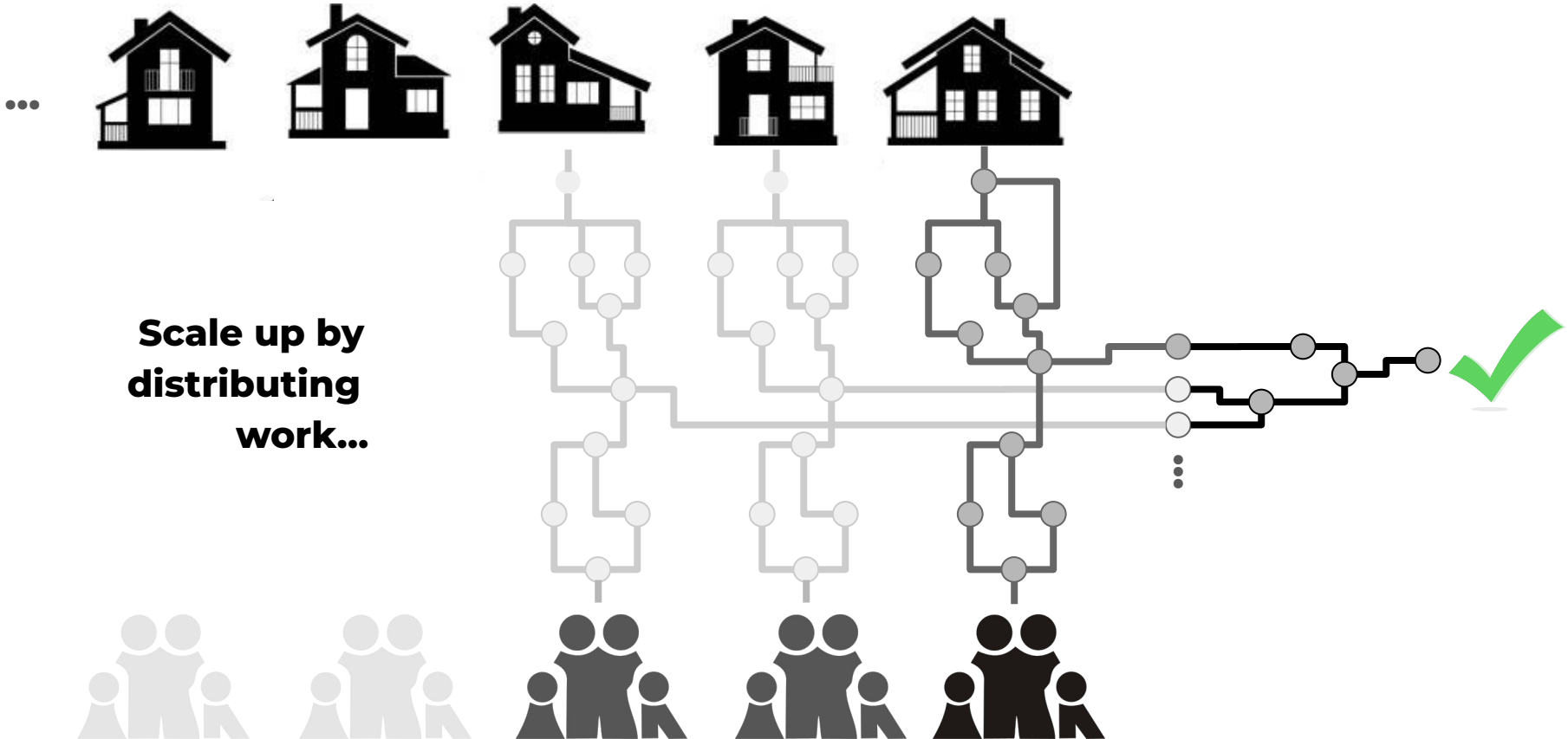
Control thru Dialogue Manager: LLM as KB



Learning Planners

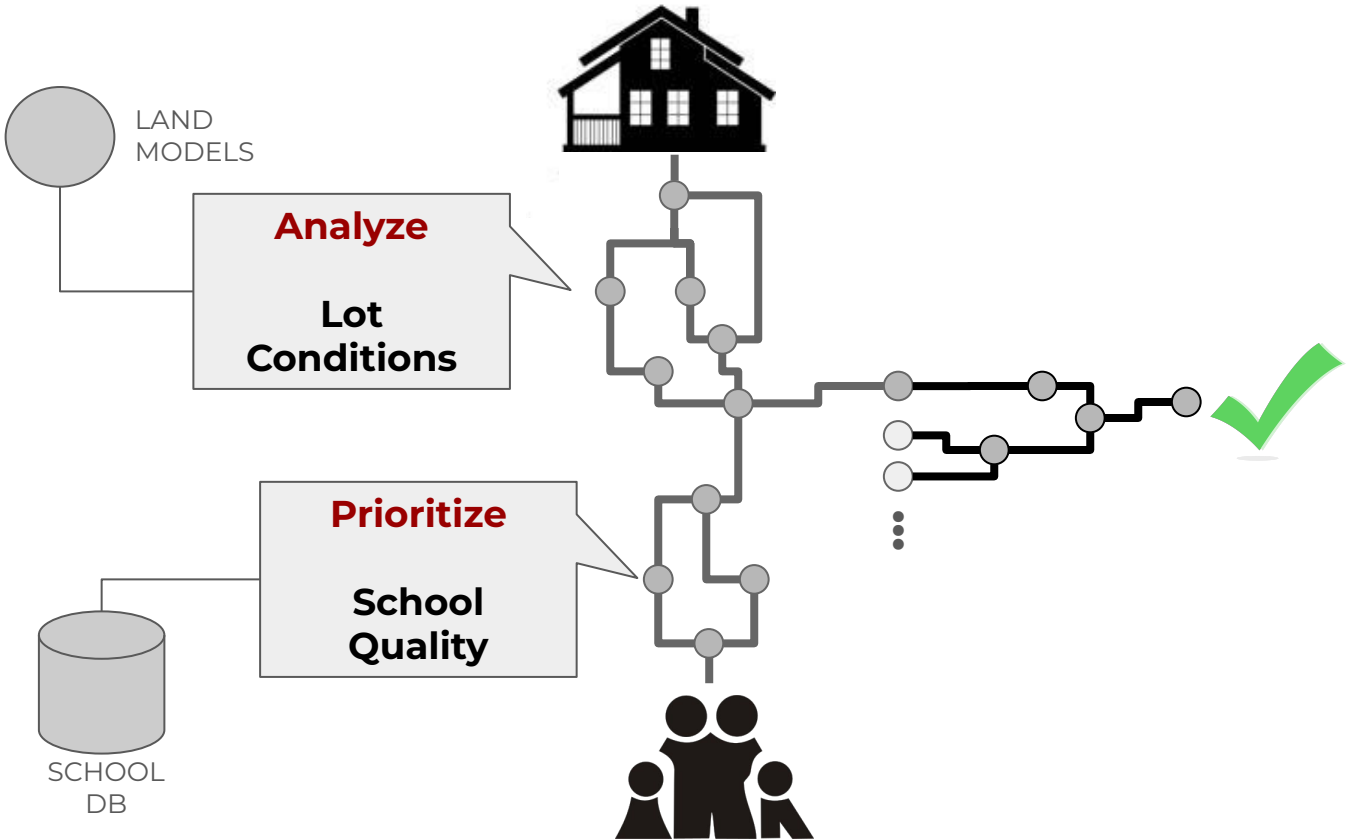


Complex Plans: Distribute Data

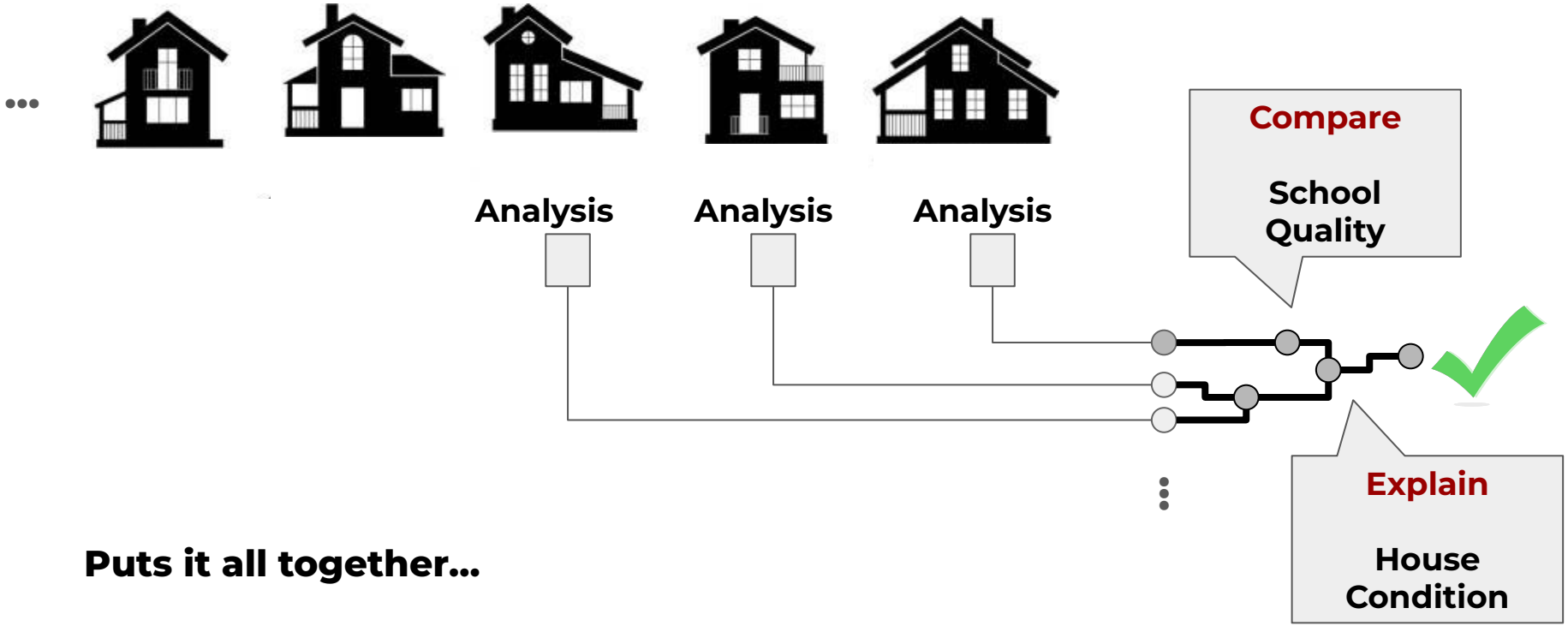


Complex Plans: Distribute Tasks

Examine each property in depth, specific to each house



Complex Plans: Aggregate



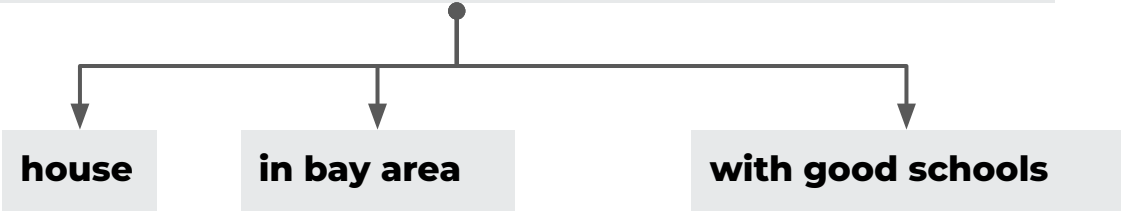
Puts it all together…

Data Planning

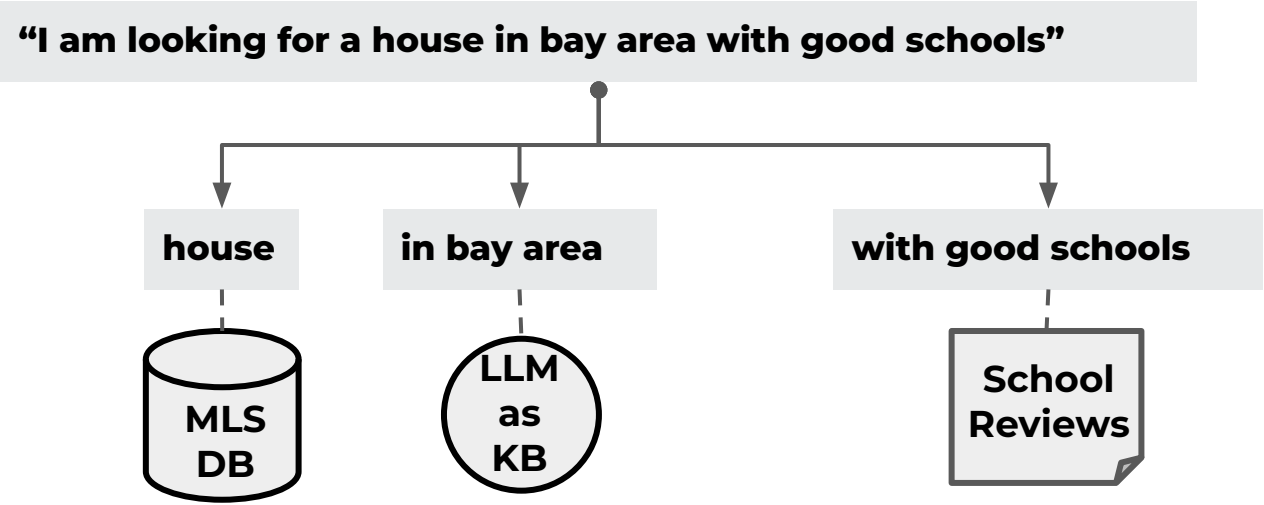
“I am looking for a house in bay area with good schools”

Data Planning

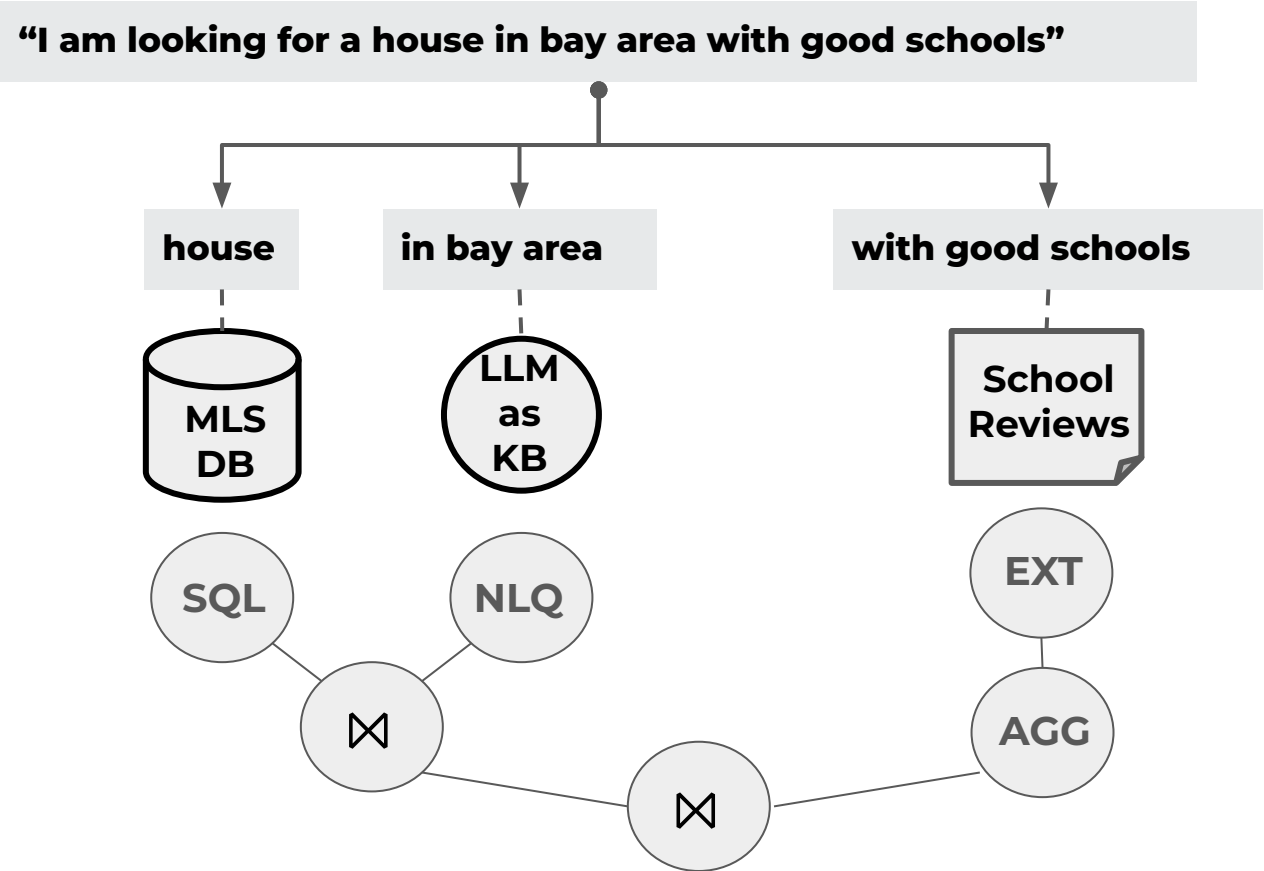
“I am looking for a house in bay area with good schools”



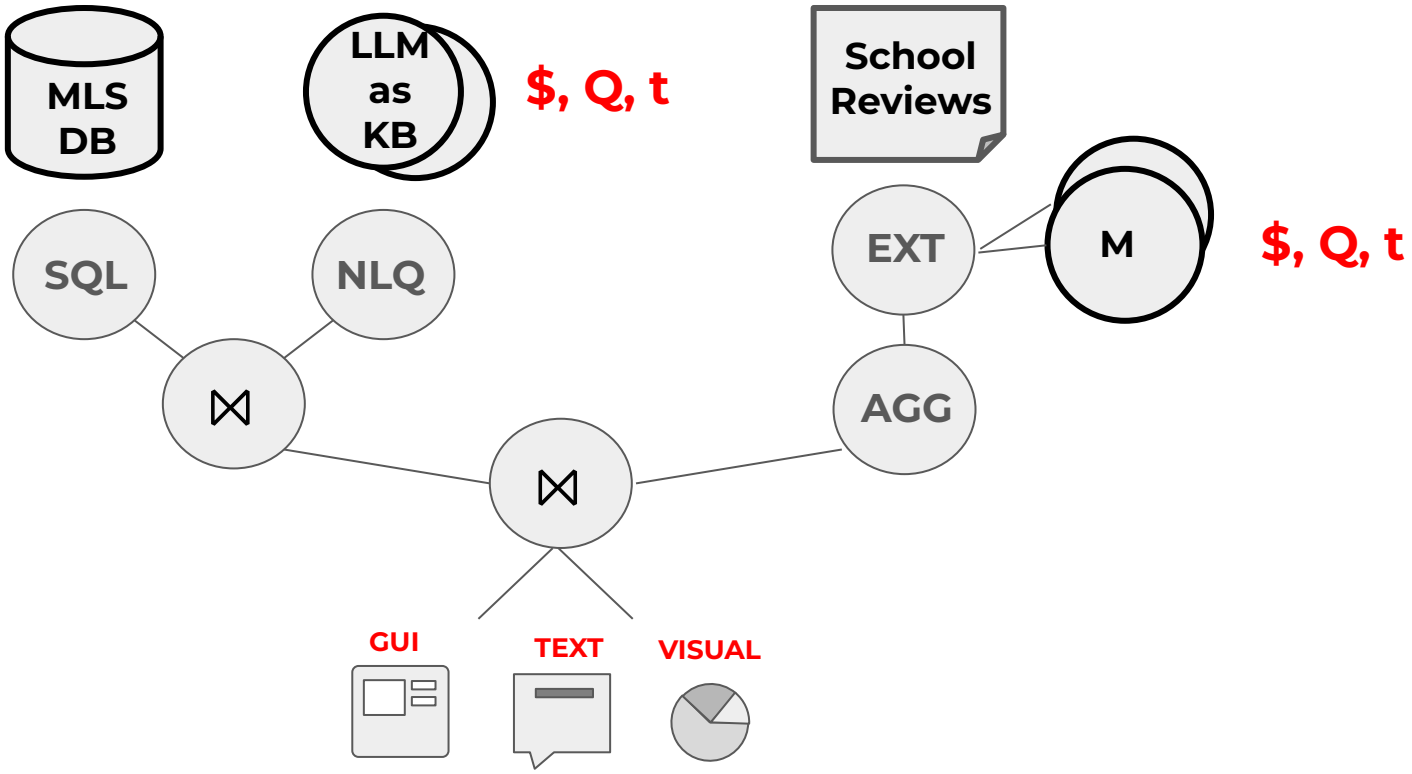
Data Planning



Data Planning



Data Plan Optimization

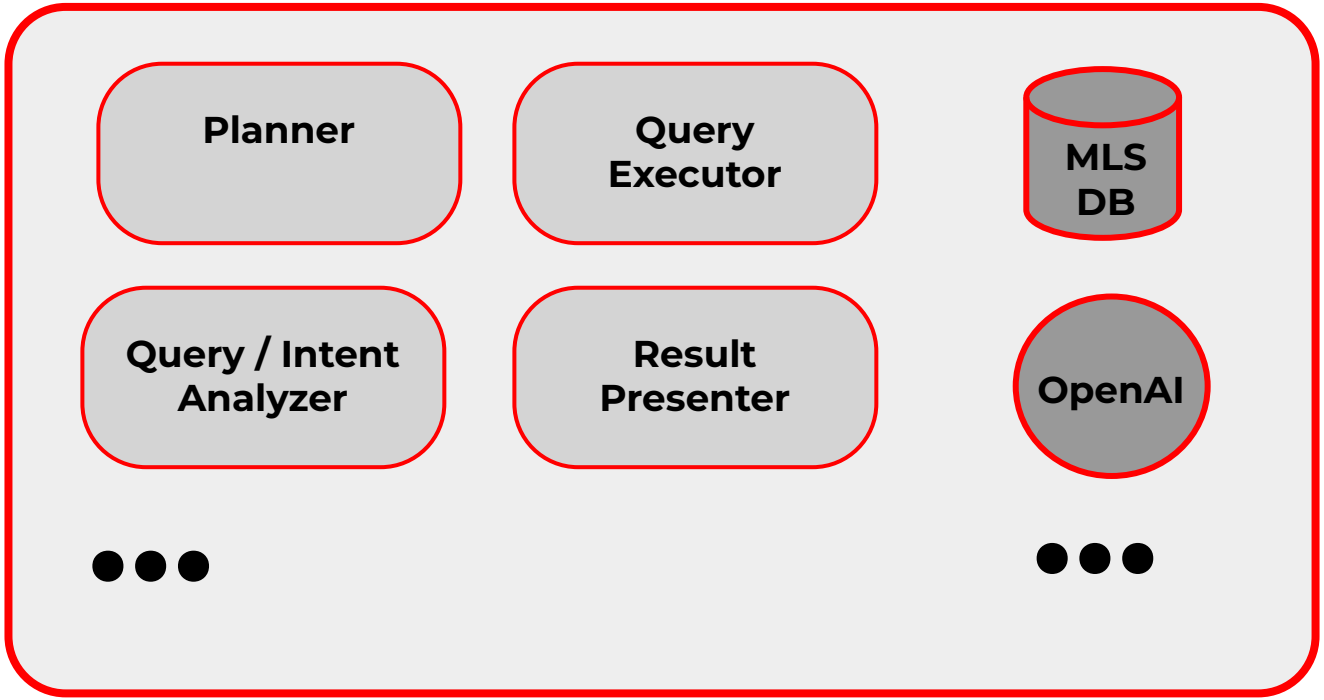


Contextual, Incremental Queries

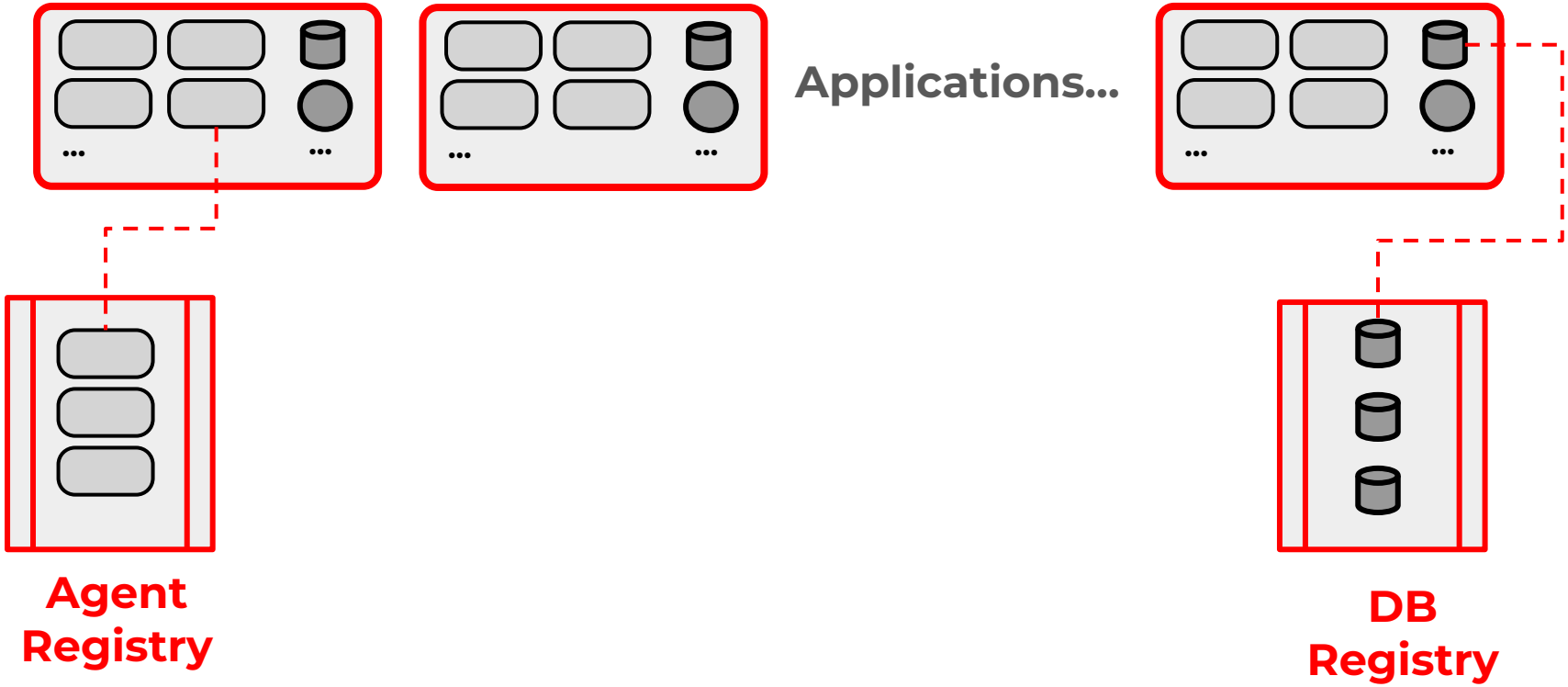
“How about San Francisco?”

“How is the access to highways?”

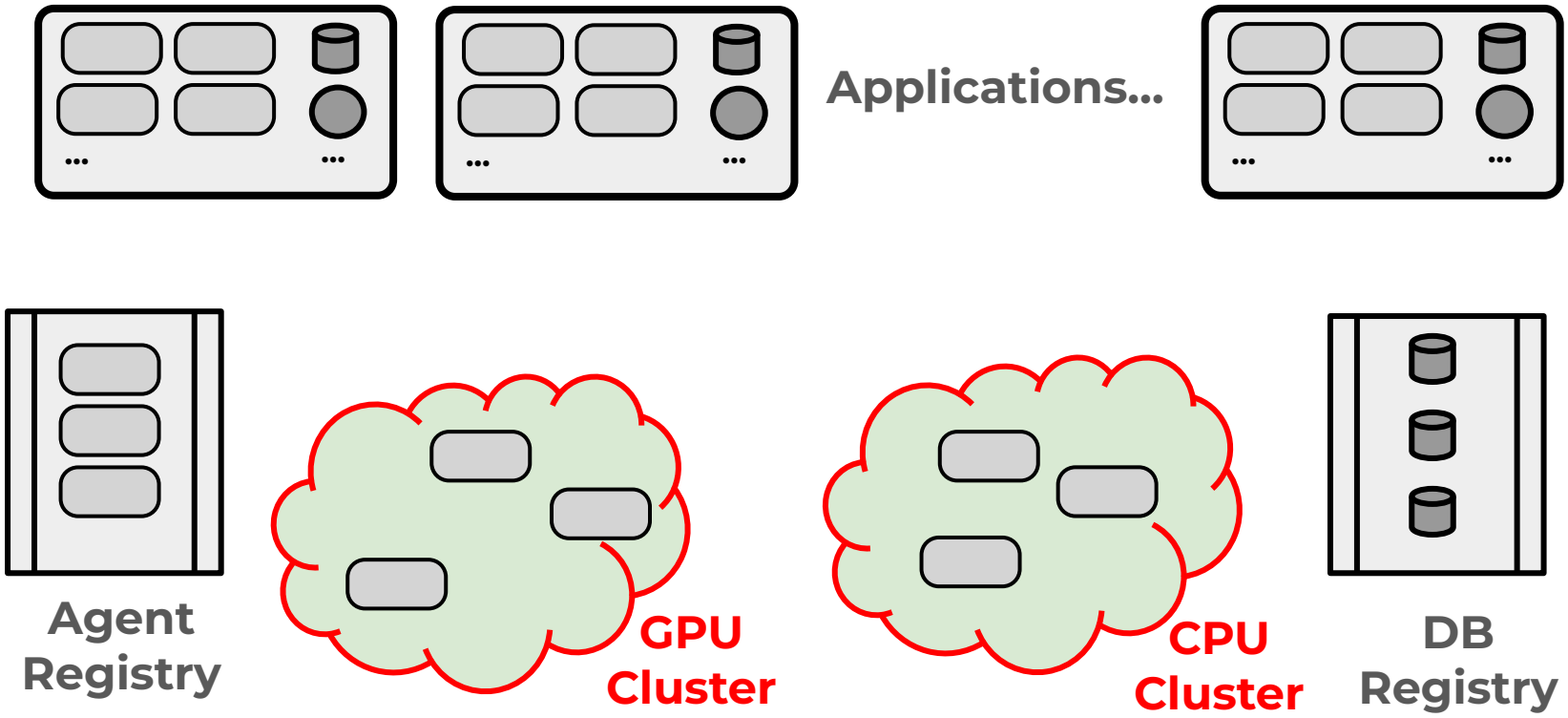
Application



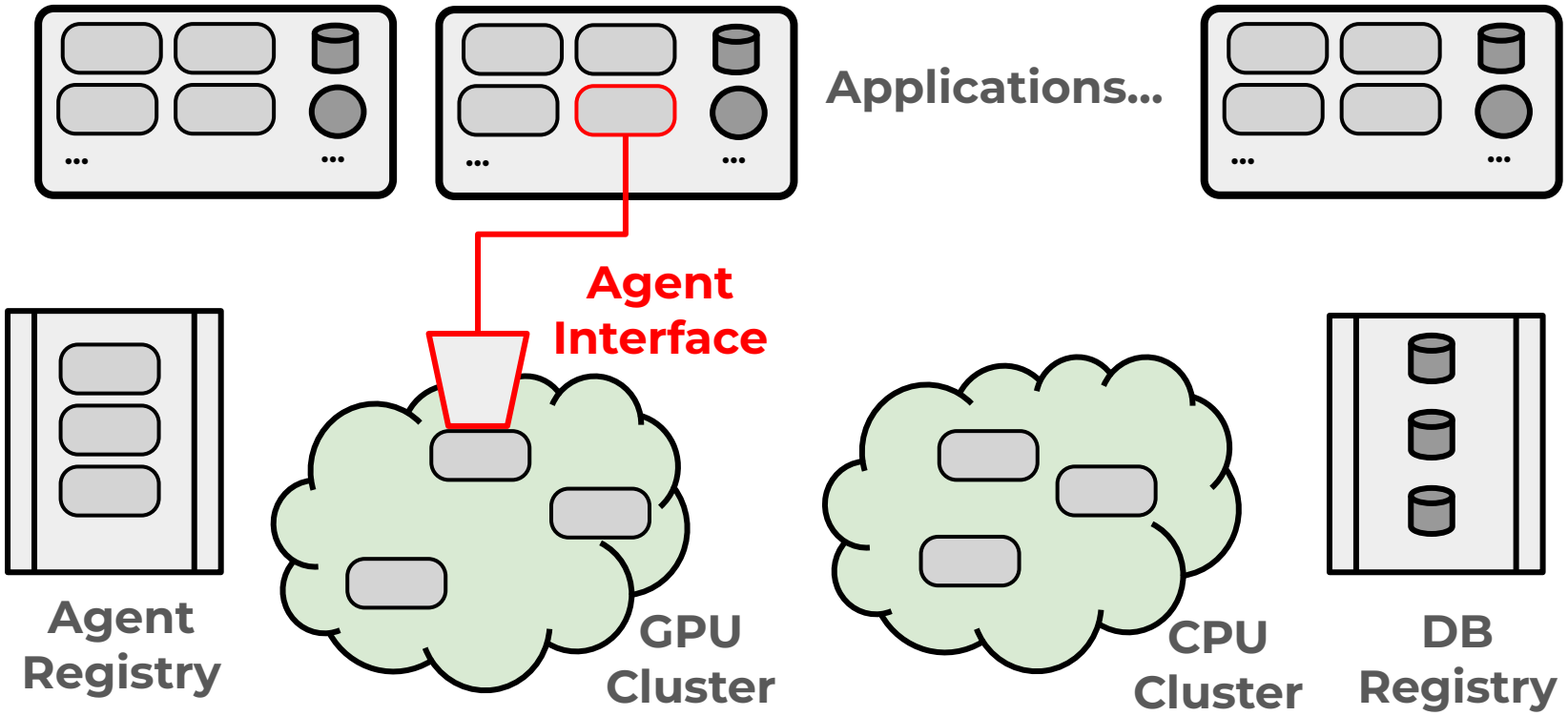
Infrastructure: Discovery



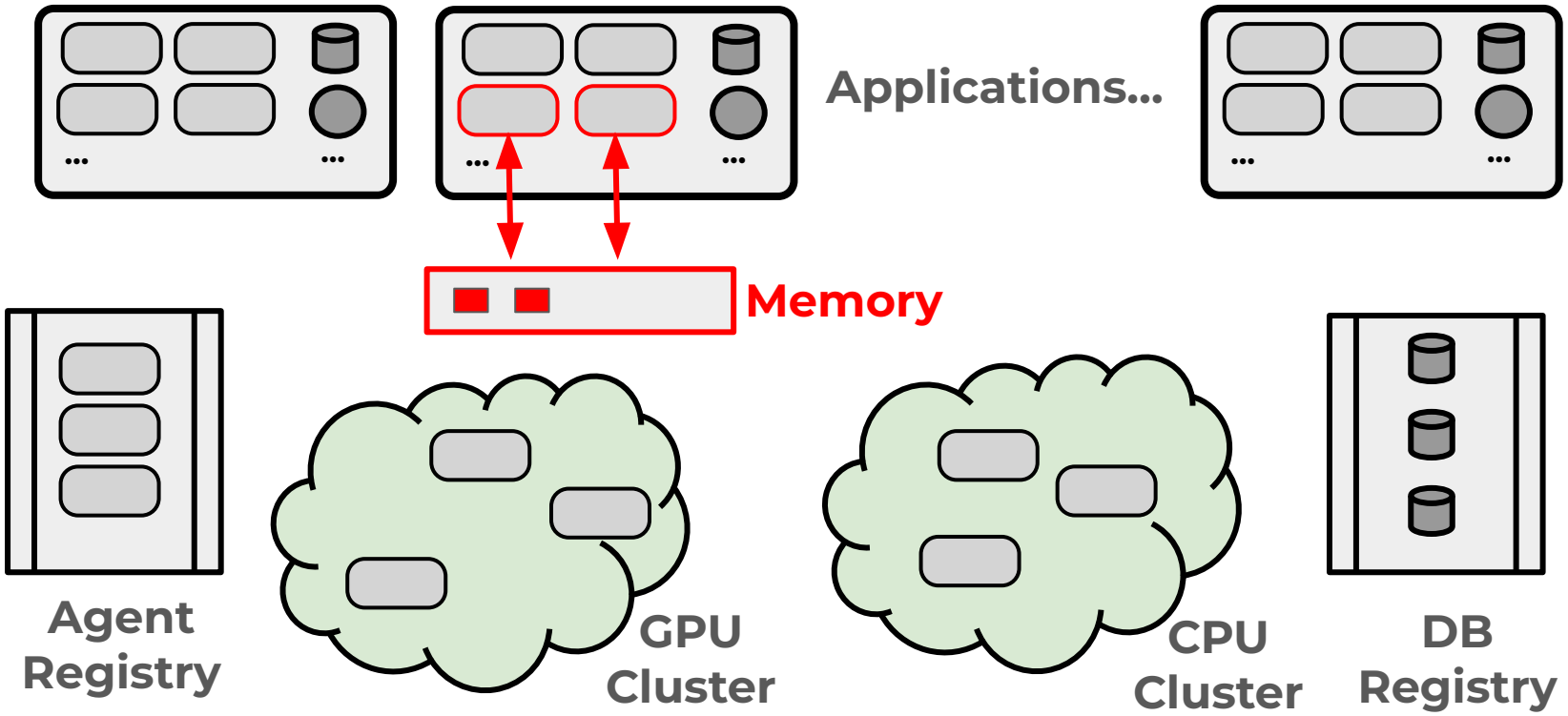
Infrastructure: Runtimes, Scalability



Infrastructure: Interfaces, Async



Infrastructure: Memory, Communication



Research

Data Management

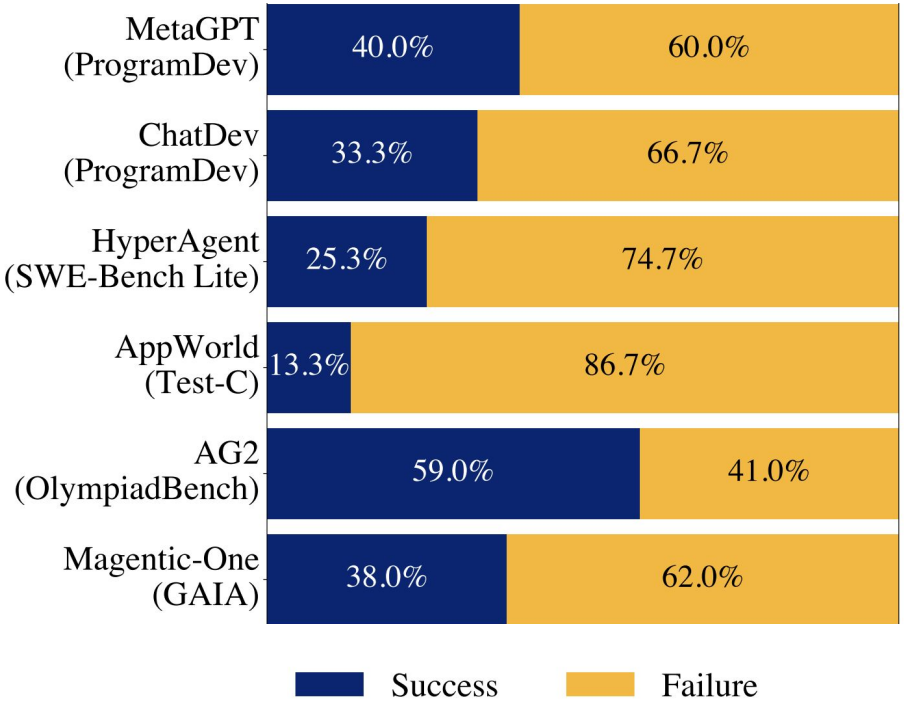
Systems

Programming Languages

AI

HCI

A lot of room for improvement...



Opportunities in Data Management

- Multimodality
  - Parametric Models as Data Source
- Query Understanding, Breakdown
  - (Data) Source Aware, Out of Domain
  - Data Planners
- Operators (multiple modalities)
- Algebra (beyond Relational, Closure, Approximate)
- Optimization (multi-objectives)
- Benchmarks (Multimodal, Conversational, Optimization, ...)

Opportunities in Systems

- Distributed Systems, Architectures
- Communication
  - Data, Control
  - Agent to Agent, Agent to API
- Logging, Monitoring
  - Multi-Perspective
- Optimization
  - Memory, Data

Opportunities in Programming Languages

- Agentic Programming Models
  - Distributed
  - Asynchronous, Synchronous
  - Approximate
- Dynamic Logic
- Context, Memory
- Function Invocation:
  - On-demand Matching
  - Approximate Signatures

Opportunities in AI

- Learning:
  - Agent, Tool, Functions,
  - Scope Granularity
  - Multi-model / Compute
- Planners
  - Continuous, Iterative, Dynamic
  - Evaluation, Benchmarks, Simulations
  - Learning, Error Propagation
- Personal Models

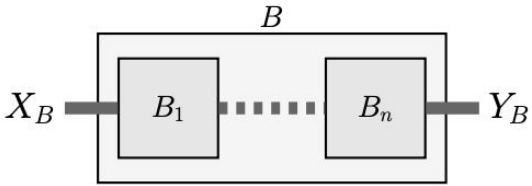
Opportunities in HCI

- Design Practice: Agentic Applications
  - Beyond Professionals
  - Personalization
  - Online - Offline
  - Mixed initiative, Co-operation
- Theories: Context as Affordance, Plan Representation/Interaction
- Agentic in GUI, VIS: Mixed Modality
- Agentic Collaboration Patterns

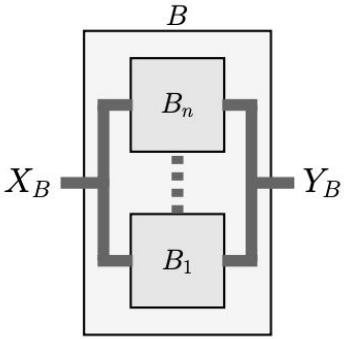
Opportunities in AI Product

- Beyond A/B Testing
  - Personalization
  - Path-based Testing
  - Scenario-driven Testing
- New KPIs
  - Quality, Engagement

Theory: Reasoning in Multi-Agent Systems

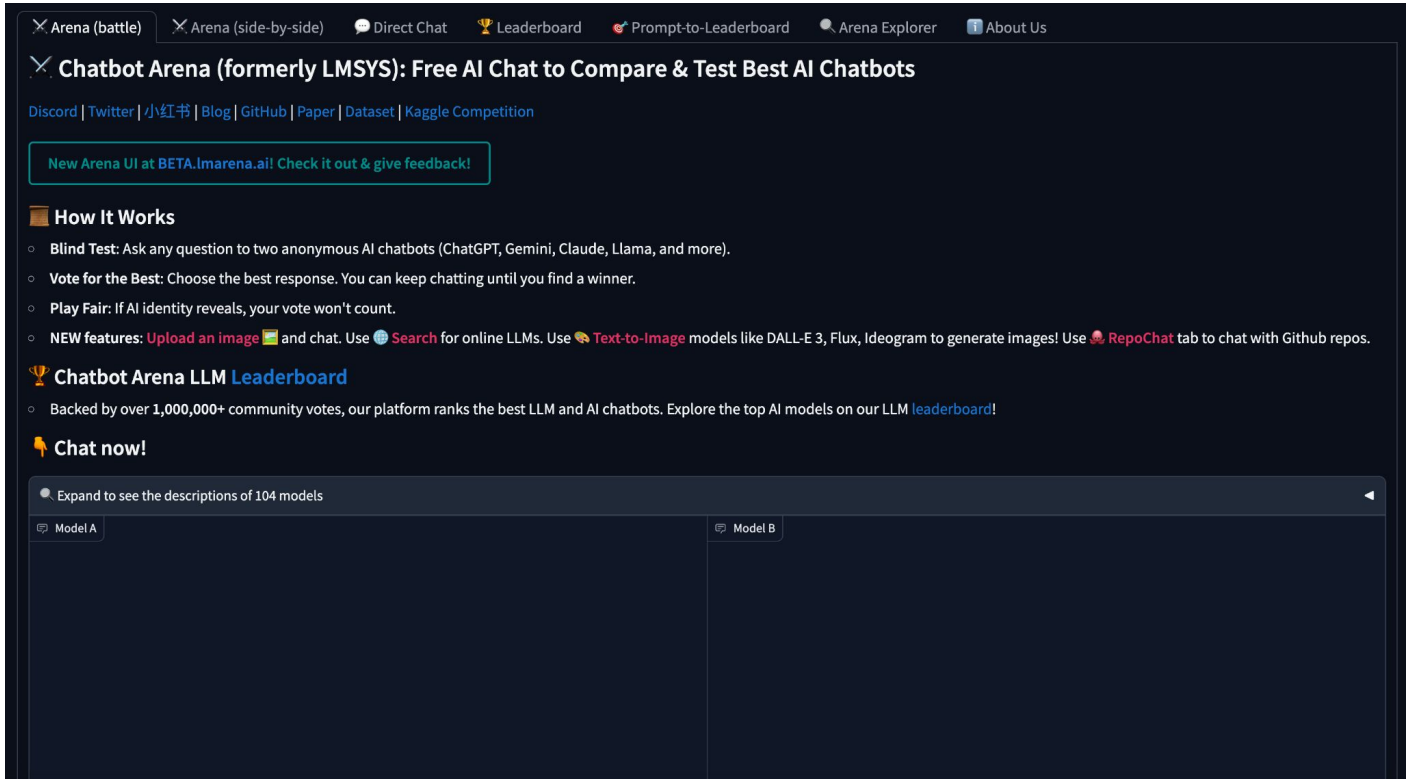


$$RC_T(B,C) = \frac{F_{\text{seq}}(RC_{T_1}(B_1,C_1),...,RC_{T_n}(B_n,C_n))}{max_{\hat{B}_{i=1,2,...,N}} I(Y_B;\hat{B}_i^{PT_i},X_B|C)}$$

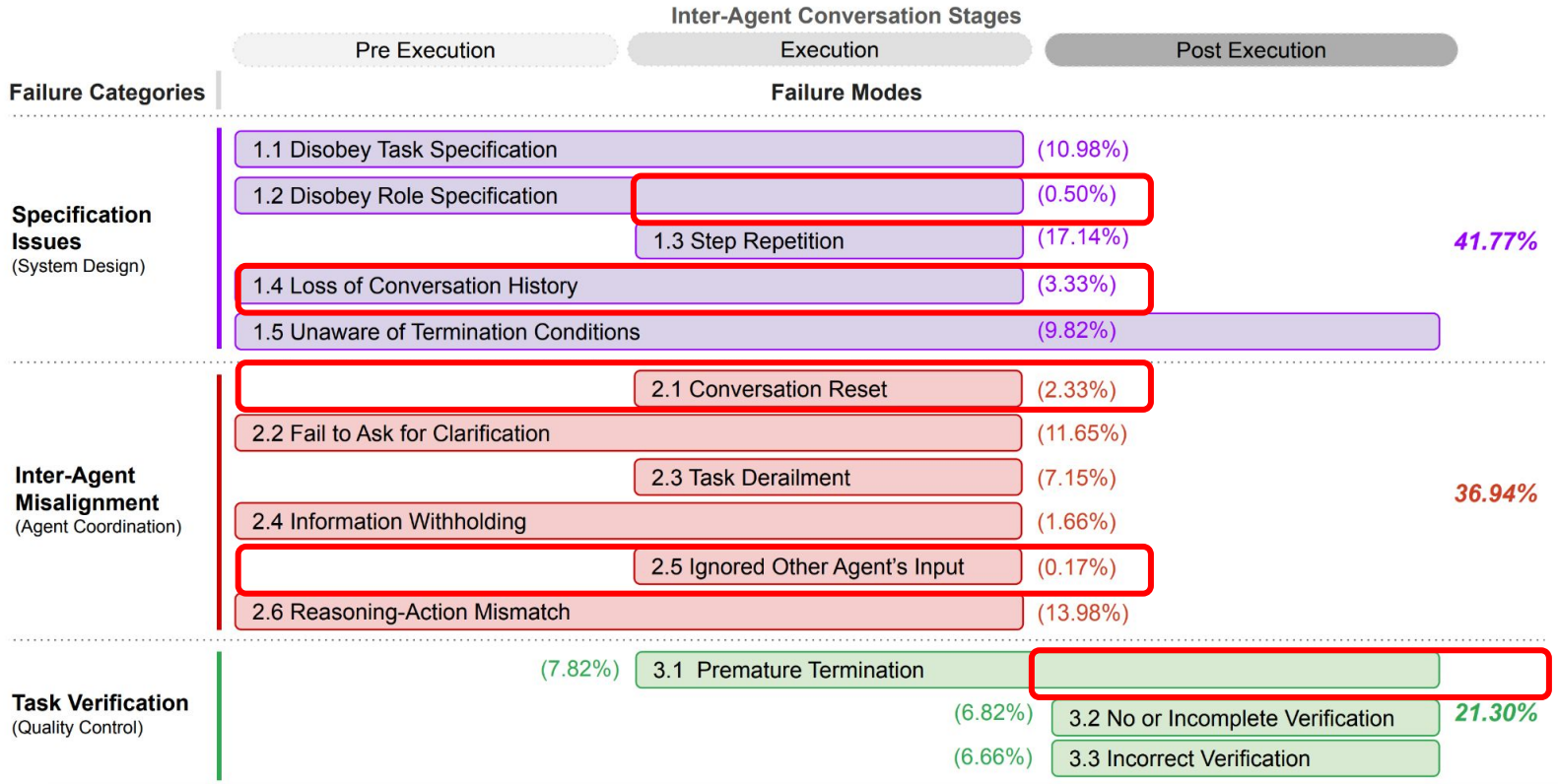


$$RC_T(B,C) = \frac{F_{\text{parallel}}(RC_{T_1}(B_1,C_1),...,RC_{T_n}(B_n,C_n))}{max_{\hat{B}_{i=1,2,...,N}} I(Y_B;\hat{B}_i^{PT_i},X_B|C)}$$

Benchmark: LLM Evaluation in the “wild”



Evaluation: Why Do Multi-Agent LLM Systems Fail?



Conclusion

progress in agentic ...

requires **cross-disciplinary** work

both from **theory and practical** aspects

with new **benchmarks**, new **metrics**

... but also experimental **frameworks**,

to **build and play** with.