浙江大學
ZHEJIANG UNIVERSITY

AI大模型与Solid 的可能结合

浙江大学计算机科学与技术学院　陈华钧

2024年01月11日

World Wide Web的起源

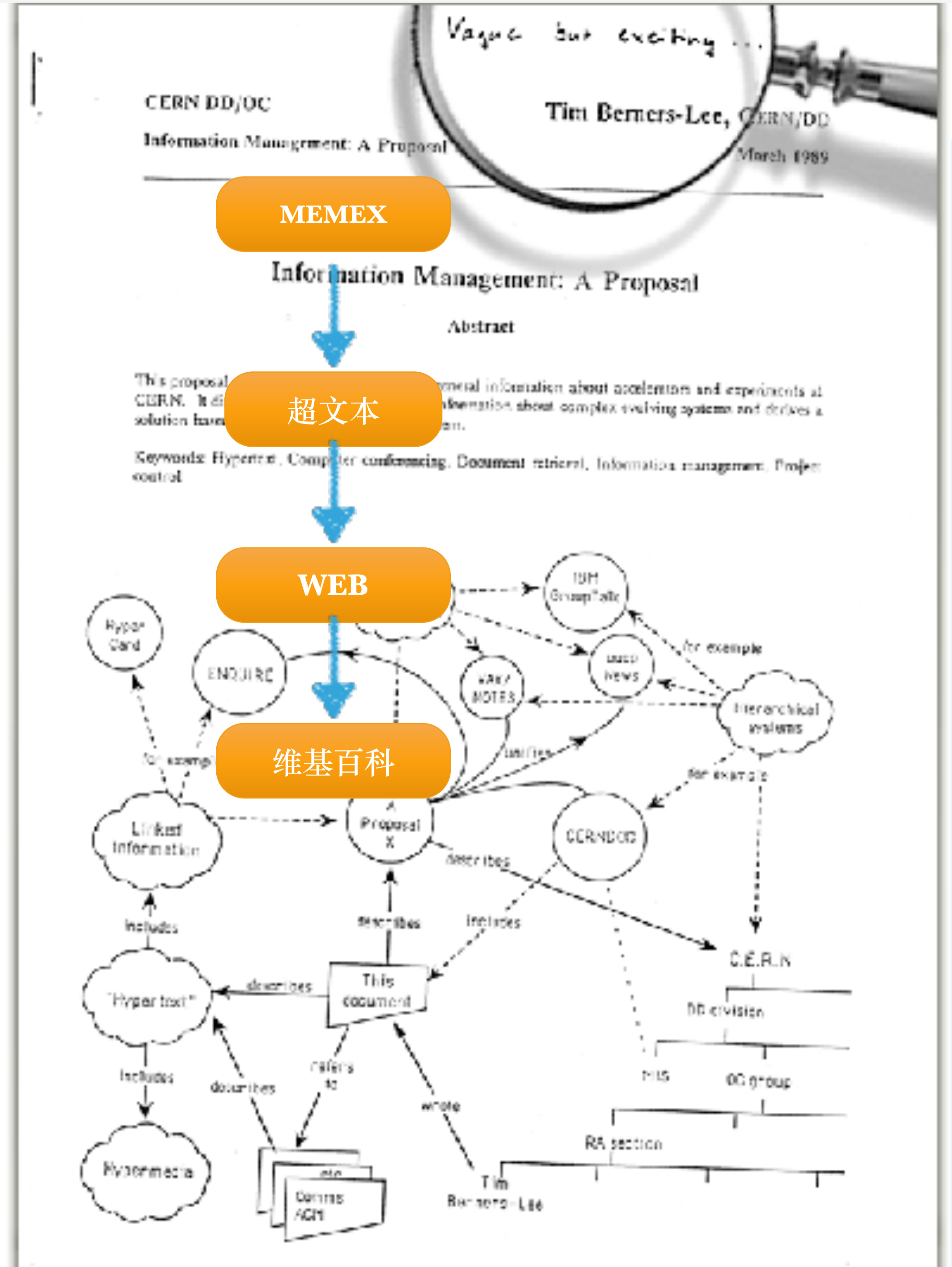
MEMEX - 记忆机器

"Wholly new forms of encyclopedias will appear, ready made with a mesh of associative trails running through them, ready to be dropped into the memex and there amplified"。

As We May Think, The Atlantic,1945

人的记忆偏重关联

Vannevar Bush



Vague but exciting …

CERN DD/OC

Tim Berners-Lee, CERN/DD

Information Management: A Proposal

March 1989

Information Management: A Proposal

Abstract

This proposal … general information about accelerators and experiments at CERN. It di… information about complex evolving systems and derives a solution base… …em.

Keywords: Hypertext, Computer conferencing, Document retrieval, Information management, Project control

万维网是以链接为中心的信息系统

Linked Information System

…This is why a "web" of notes with links between them is far more useful than a fixed hierarchical system. …… Circles and arrows leave one free to describe the interrelationships between things in a way that tables, for example, do not. The system we need is like a diagram of circles and arrows, where circles and arrows can stand for anything.

Information Management: A proposal 1989.

以“链接”为中心的系统，在开放的互联网环境里面更加容易生长和扩展。这一理念逐步被人们实现，并演化发展成为今天的万维网。

SIR TIM BERNERS-LEE

万维网创始人

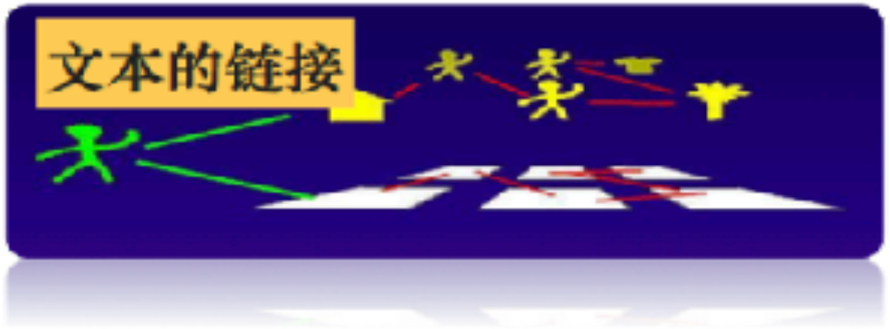
MIT教授

2016年图灵奖获得者

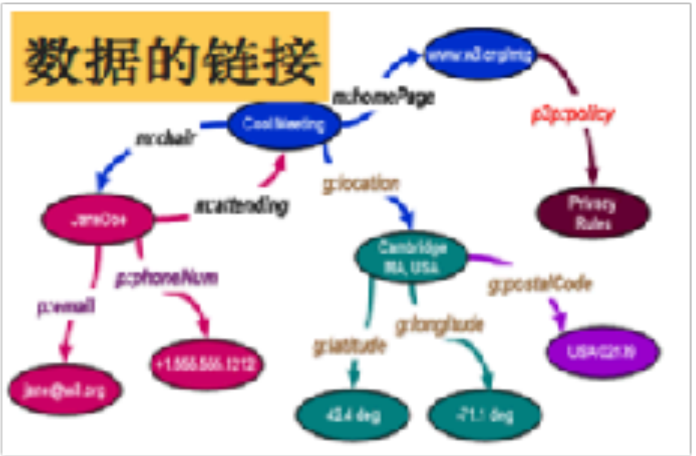
知识图谱溯源：The Semantic Web

"This is a pity, as in fact documents on the web describe real objects and imaginary concepts, and give particular relationships between them but we could not process them at all...

Tim Berners-Lee，Inventor of the Web, @WWW Geneva, 1994



Web of Texts, Web of documents

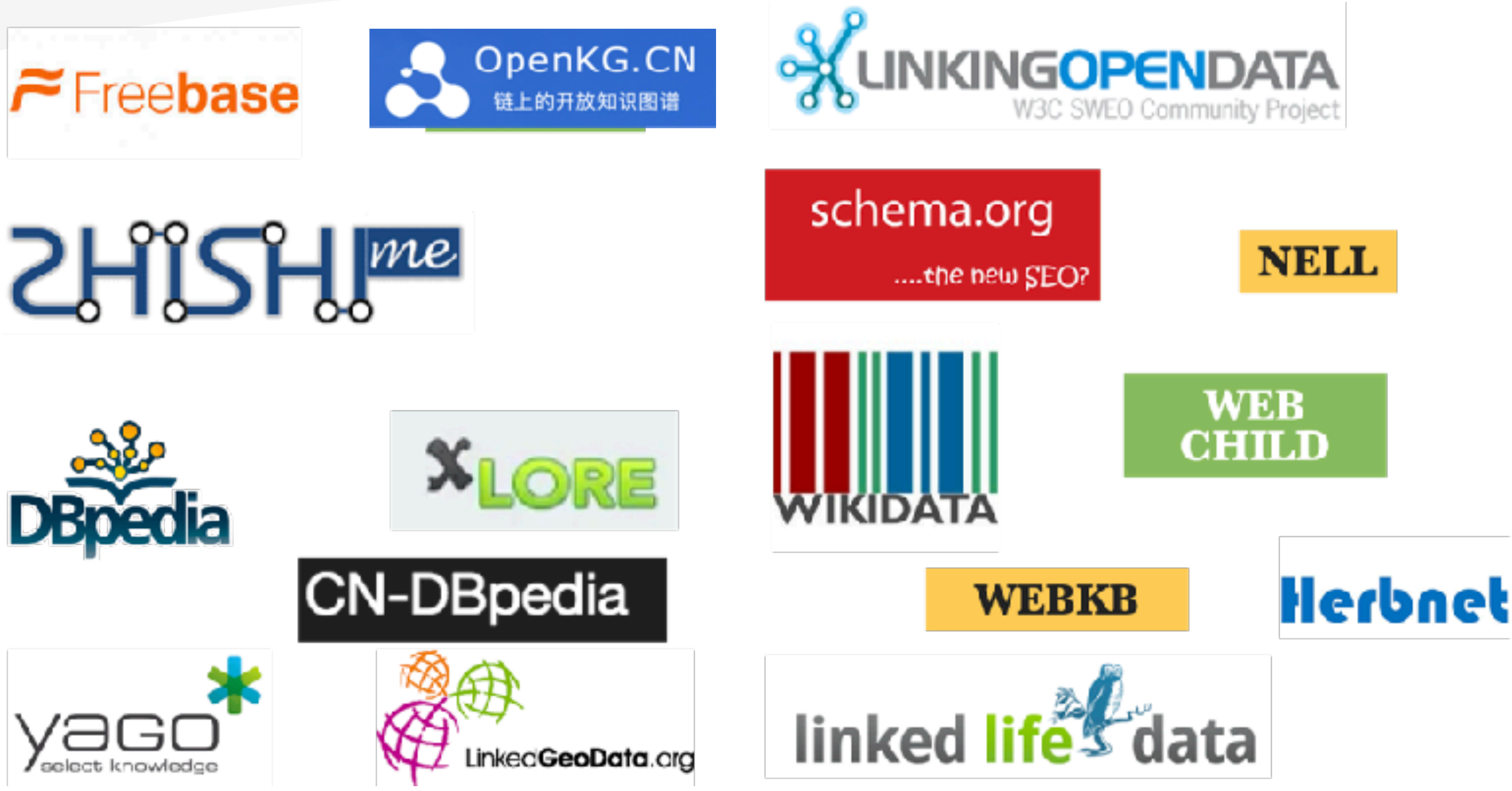


Web of Objects, Web of Data, Web of Things

Linked Data

利用规范化的语义表示（Schema & Ontology）将碎片化的数据关联和融合

各种Linked Data项目

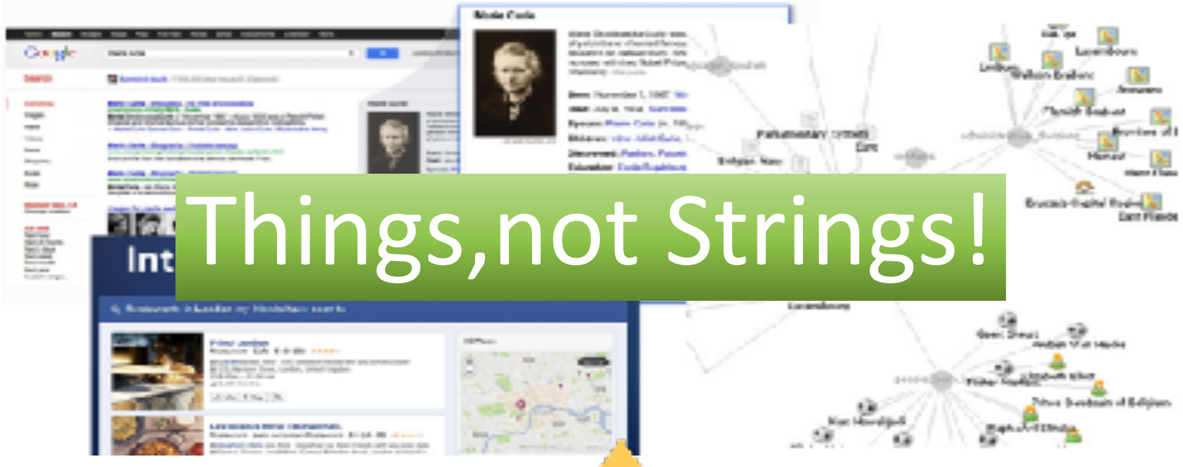


谷歌知识图谱：Things, Not Strings （2012）

网页搜索

↓

语义搜索



WEB OF DOCS

↓

WEB OF DATA

手工众包 ↗ 格式转化 元组抽取 实体融合 ↑ 链接预测 推理补全 ↖ 语义嵌入

Freebase

社区协同构建

WIKIDATA

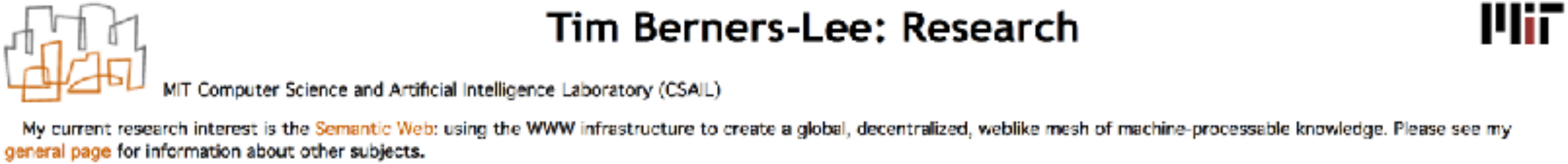
维基众包

schema.org

....the new SEO?

网页嵌入语义数据

被忽略的视角：Decentralization



Tim Berners-Lee: Research

MIT Computer Science and Artificial Intelligence Laboratory (CSAIL)

My current research interest is the Semantic Web: using the WWW infrastructure to create a global, decentralized, weblike mesh of machine-processable knowledge. Please see my general page for information about other subjects.

Using the WWW infrastructure to create a global, decentralized, weblike mesh of machine-processable knowledge.

知识的互联 + 去中心化的架构 + 知识的可信

被忽略的视角：Decentralization

Semantic Web的原始内涵

知识的互联　　数据的规范化描述和强关联——语义

+

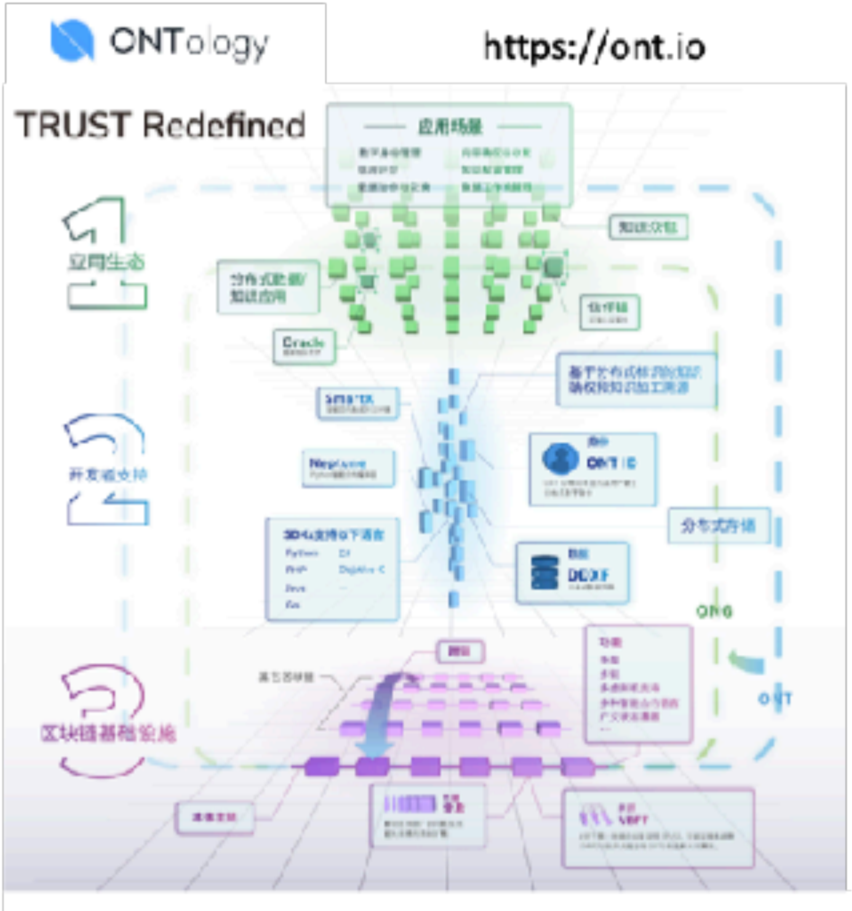
去中心化的架构　　每个人都维护自己的知识库——确权

+

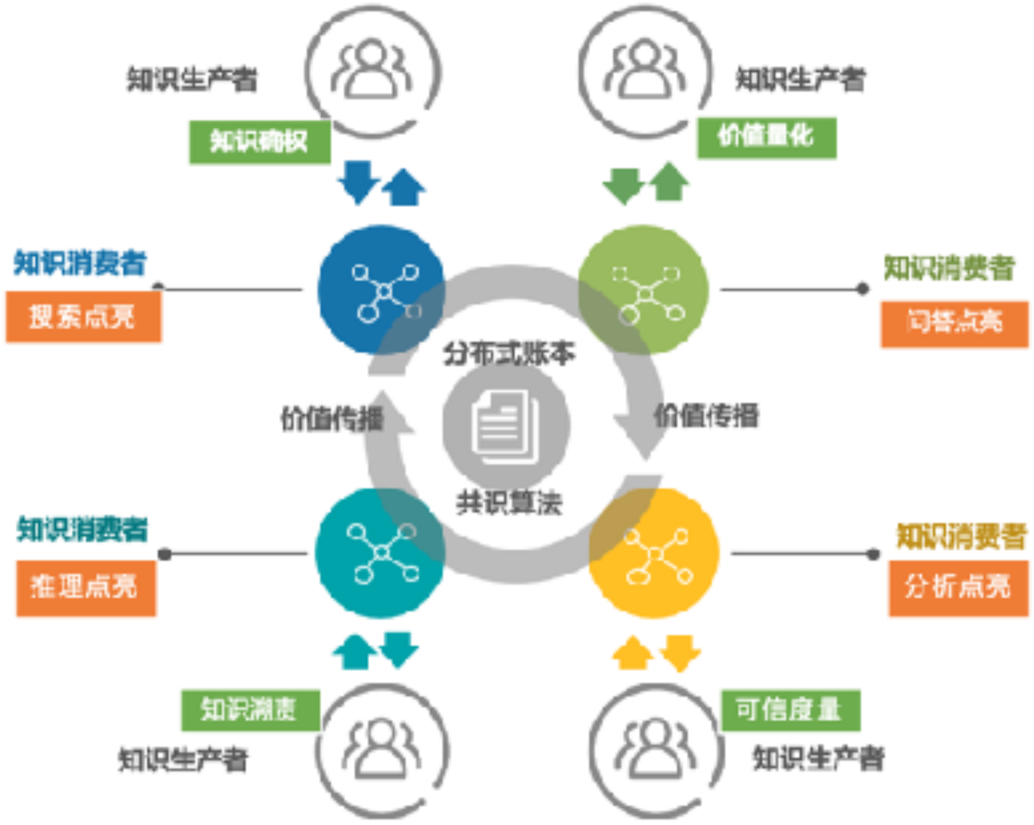
知识的可信　　知识的可信度量和真伪判别——溯源

数据之间有互联和链接的硬需求，但现在还没有能保证数据互联融合所面临的所有权定界、细粒度的价值计算和可信溯源的机制和技术。

OpenKG 区块链



被忽略的视角：Decentralization



SOLID: Social Linked Data

- Any kind of information can be stored in a Solid Pod.
- You control access to the data in your Pod. You decide what data to share and with whom (be it individuals, organizations, and/or applications). Furthermore, you can revoke access at any time.
- To store and access data in your Pod, applications use standard, open, and interoperable data formats and protocols.

SOLID: Social Linked Data

Your Data Revolution: The Future of User Data & the Web.

December 19, 2023

Solid returns to the web’s founding principles of user empowerment. Solid decouples applications, data and identities, and stores user data in a Solid Pod. Applications request access to data stored in Pods, creating fine-grained access control and consent capabilities for using and sharing data.

——Sir Tim

AI and SOLID

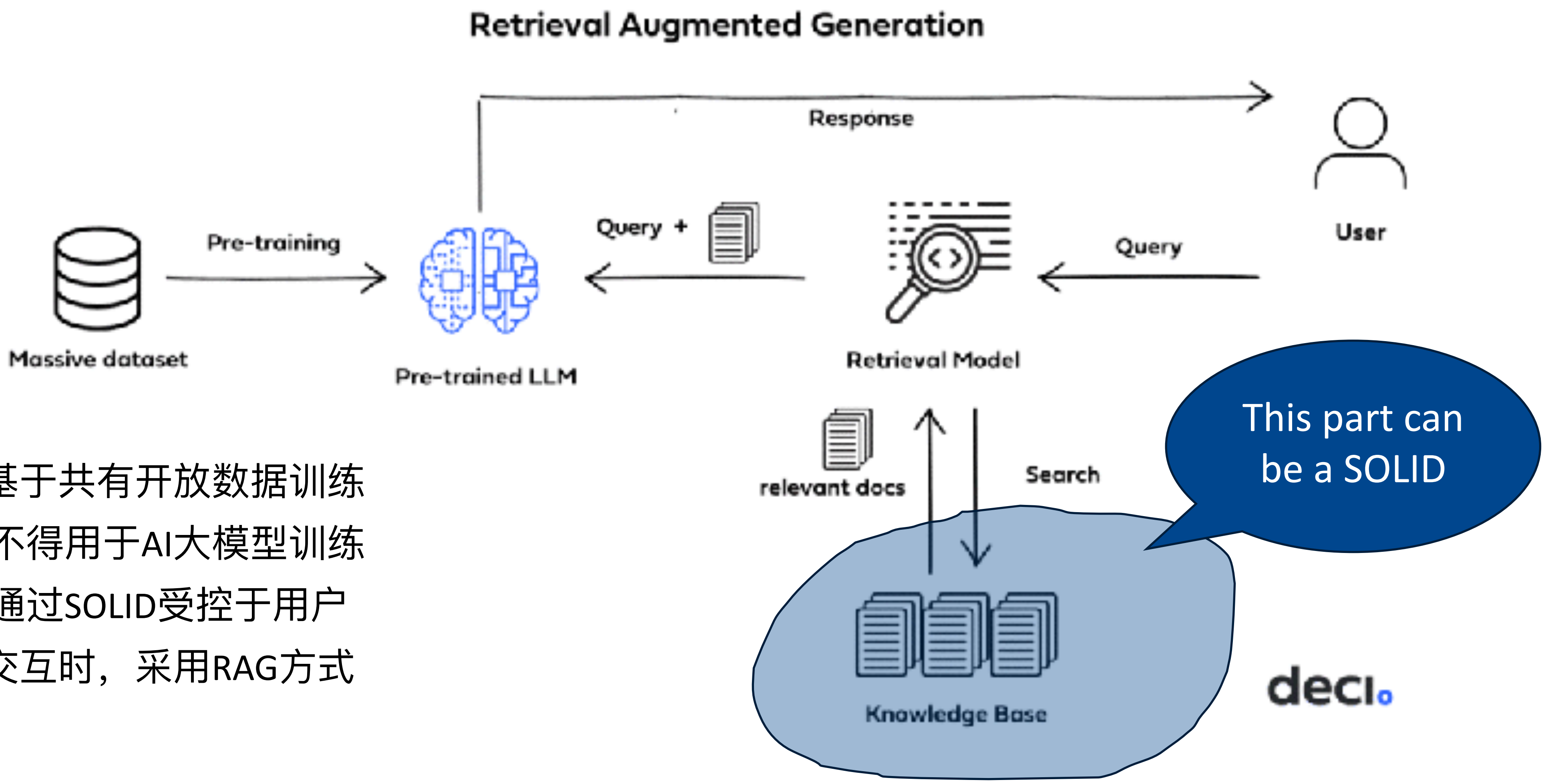
Your Data Revolution: The Future of User Data & the Web.

December 19, 2023

Over the past year, generative AI has taken center stage as every industry aims to capitalize on the new capabilities the technology offers. How do we ensure that AI, like the original web, works for the end user, and not just the entity that built it?

The answer lies in storing data in Pods, where AI can be trained on unique, accurate user data with a user’s consent. Regulation also plays a role: As personal AI technologies become more prevalent, regulators need to ensure that these agents are working with their users’ interests in mind.

AI + SOLID： SOLID + RAG—A Simple Implementation

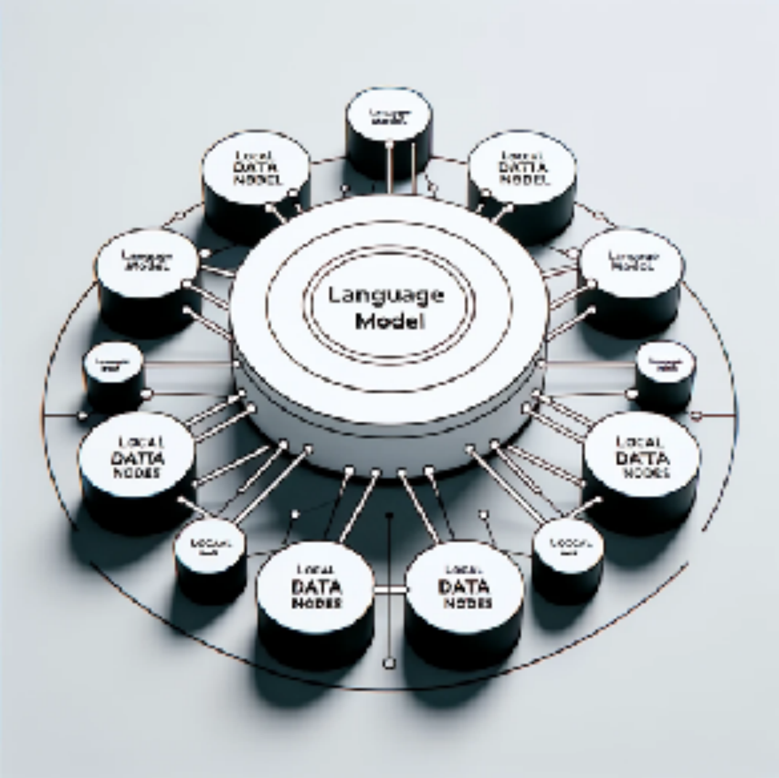


- AI大模型基于共有开放数据训练
- 私有数据不得用于AI大模型训练
- 私有数据通过SOLID受控于用户
- 在需要AI交互时，采用RAG方式

存在问题：

- 在RAG之后，用户私有数据仍然需要提交给中心AI处理

AI + SOLID：Decentralized Large Models



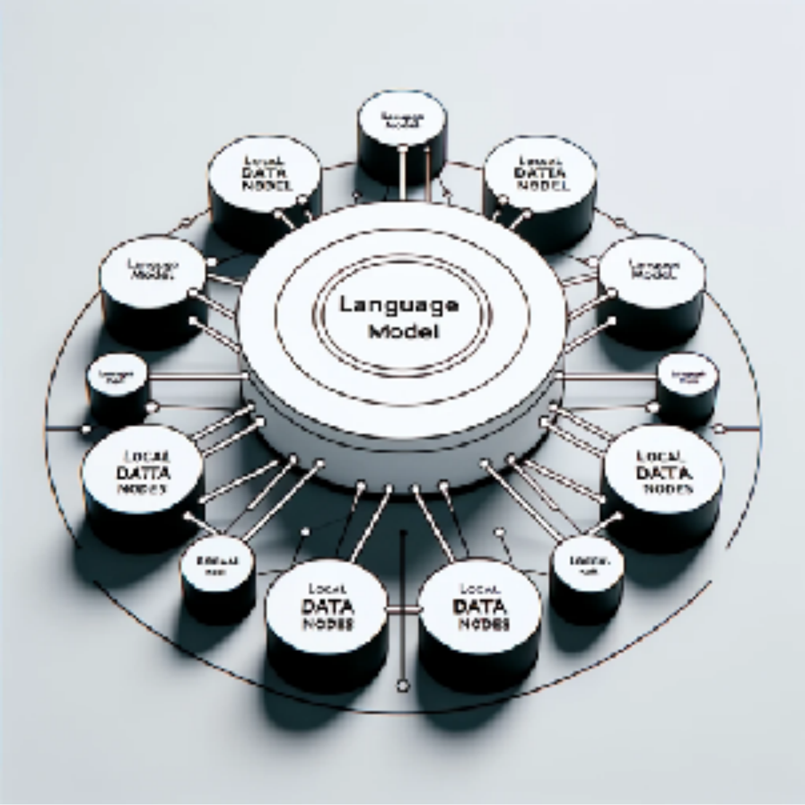
- 未来的AI训练包含：Open Base Model + Private Domain Model
- Open Base Model基于共有开放数据训练
- Private Model基于SOLID控制的数据可以在Base Model上做增强训练，但独立于Open Model在SOLID POD中进行维护和管理
- Private Model也可能是仅依赖于SOLID数据训练的小模型，再与Open Model采用大小模型协同方式进行交互
- 每个Private Model代表一个Agent

存在问题：

- 仍然需要解决Open与Private进行交互协同时的信息隐私问题

A Fully Future: Decentralized Large Model + SOLID

Decentralized Large Models

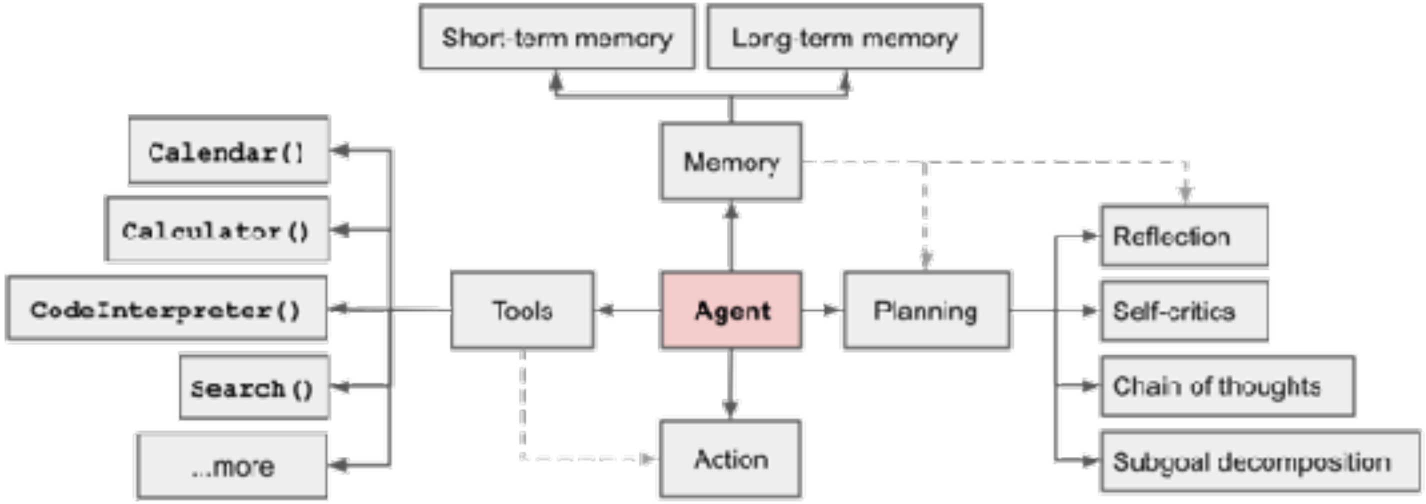


+

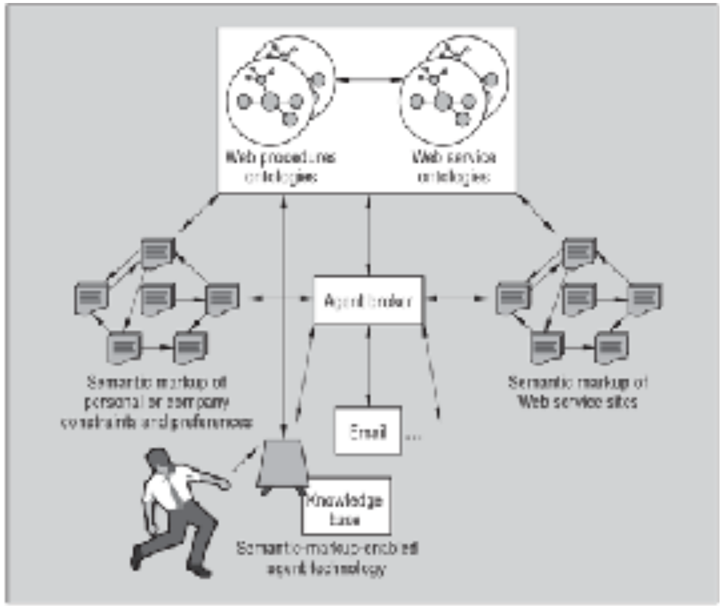
Decentralized Linked Data

SOLID与AI Agents

- 语义网的早期技术都是为Agent设计的，如DAML（DARPA Agent Markup Language，OWL本体语言前身）、KIF（Knowledge Interchange Format）等等。



Knowledge Interchange Format



Web procedures ontologies
Web service ontologies
Agent broker
Semantic markup of personal or company constraints and preferences
Semantic markup of Web service sites
Email
...
Knowledge base
Semantic-markup-enabled agent technology

Planning任务规划：

- Subgoal and decomposition
- Reflection and refinement

Memory记忆：

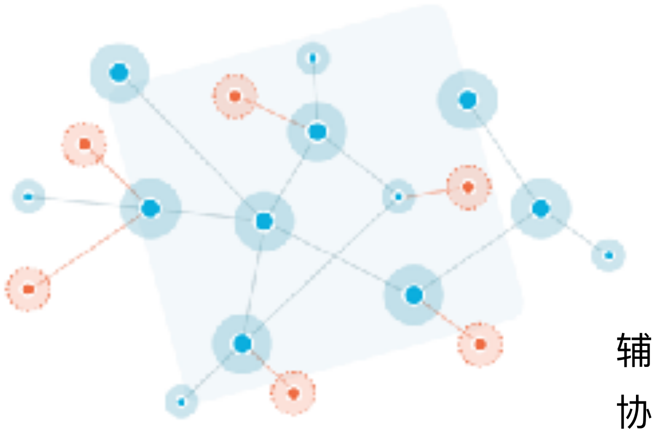
- Short-term memory
- Long-term memory

Tool use工具使用：

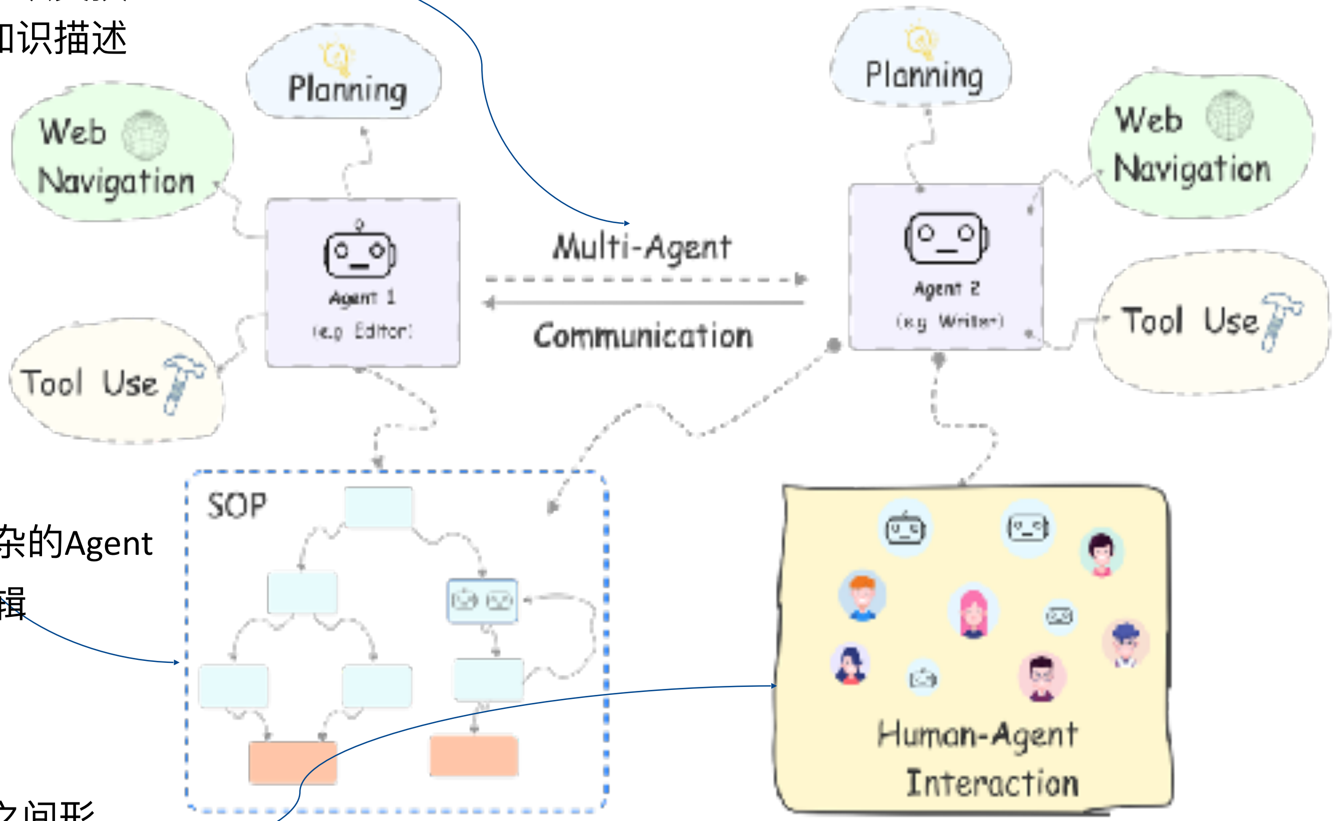
- The agent learns to call external APIs for extra information that is missing from the model weights.

SOLID与AI Agent：Knowledgeable Agents

为智能体之间的知识交换
提供更加精确的知识描述



Agent-centric Knowledge Graphs



辅助大模型生成复杂的Agent
协同流程和协作逻辑

帮助人群和多Agent之间形
成知识社区

谢谢大家！

浙江大学