



Agentic Web 时代

– Web 与 AI 的技术演进与治理挑战

- 胡春明 W3C

AI 正从“回答者” 变成“行动者”

Web 从“信息空间” 变成“行动空间”



Web 在 Agentic 时代的角色

Web as data source

网页、开放数据RDF, JSON-LD、结构化标记、文档和媒体是 AI 的重要数据来源。

Web as runtime

WebNN、WebGPU、WASM 让 AI 能力进入浏览器和终端侧。

Web as action space

Agent 可以浏览、点击、填表、调用API、连接服务。

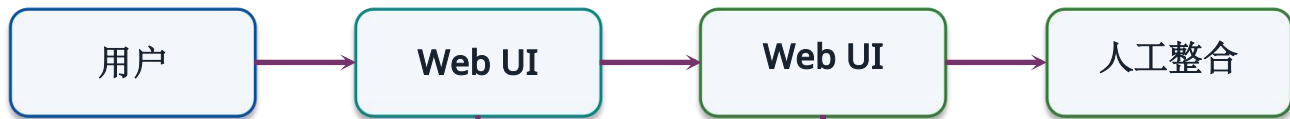
Web 不再只是信息交互平台，也正在成为 AI 的运行环境和行动空间。

问题：当 Web 的主要使用者不再只是人，而还包括 Agent，Web 的基础假设会发生什么变化？

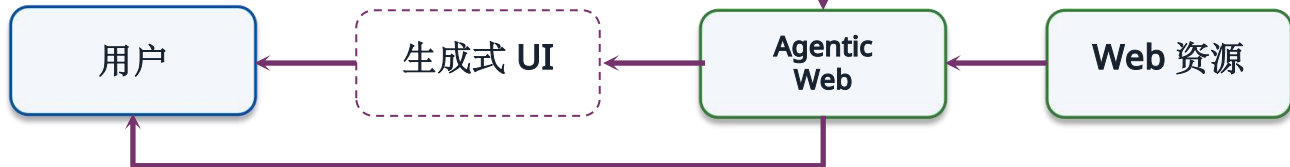


Agent 与 Web 交互

人驱动:



Agent 驱动:



Agent 成为用户与 Web 之间的中间层。



Semantic Web 与无障碍字段为 Agent 提供语义

Semantic Web

Web 的创始人 Tim Berners-Lee 在2001年提出 agent, 后续创造了一系列包括RDF, JSON-LD, OWL 等语义标准。但由于部署成本高, 没有大范围的使用。

ARIA

ARIA 提供的无障碍的语义, 增强了agent 对web 页面的了解, 但是缺依赖于 Web 页面本身的无障碍实施程度。



探索 Agent 可交互的 Web

llm.txt

WebMCP

WebSkills

well-know *

...

- 结构化标注：告诉 Agent 内容是什么。
- 能力声明：告诉 Agent 能做什么。
- 交互意图：告诉 Agent 操作会带来什么后果。

Agent 与 Agent

Model Context Protocol

- Initiated by Anthropic
- "USB-C port for AI"
- Solves M×N integration problem

Agent-to-Agent Protocol

- Contributed to Linux Foundation by Google
- Focuses on cross-vendor interoperability
- Supports task collaboration and negotiation

Agent Network Protocol

- Open-source community effort
- "HTTP of the Agentic Web"
- Use JSON-LD and DID

Agent Connect Protocol

- initiative by Cisco
- Communication layer for autonomous
- Uses RESTful APIs and message passing

Agent Communication Protocol

- Contributed to Linux Foundation by IBM
- Shared language for heterogeneous agents
- Emphasizes peer-to-peer model

Agent Communication Network

- Initiated from Telecommunication industry
- Telecom Operators
- Comm. Core Networking + Trusted Identity

For more information, see:

<https://w3c-cg.github.io/ai-agent-protocol/#protocol-overview>

or: <https://w3c-cg.github.io/webagents/TaskForces/Interoperability/Reports/report-interoperability.html#state-of-web-based-multi-agent-systems>



Agent 的身份与授权



Agent 的身份与授权

- 用户授权主 Agent。
- 主 Agent 调用子 Agent。
- 子 Agent 访问第三方服务。
- 第三方服务看到一次请求，但不知道背后是谁、代表谁、权限是什么。

- 这次访问是人、爬虫，还是被授权的 Agent?
- Agent 是否真的被用户授权?
- 授权范围是什么?
- 如果出错，责任链能否追溯?

DID - 分布式可验证身份

VC - 可验证声明和授权

Oauth - 账号授权

JEP - 因果责任链追溯责任



治理嵌入 Web 架构



Web 生态 Agent 的治理

安全/隐私

- [AI in the Browser](#)
- [Privacy Principles](#)
- Threat modeling CG
- Linked Web Storage - from Tim (Solid)

Web 内容控制

- robot.txt
- AI Preference
- C2PA and W3C AI content disclosure
- [Impact of Machine Learning models on the Web](#)
- [Draft report on AI agents](#)

伦理/规则/无障碍

- [Ethical Principles for Web Machine Learning](#)
- [Web User Agents](#)
- AI and Accessibility

身份/责任/追溯

- Judgement Events Protocol(JEP)
- AIP
- [Web User Agents](#)



开放 Web 的未来



Web & AI 在 W3C

语义和数据

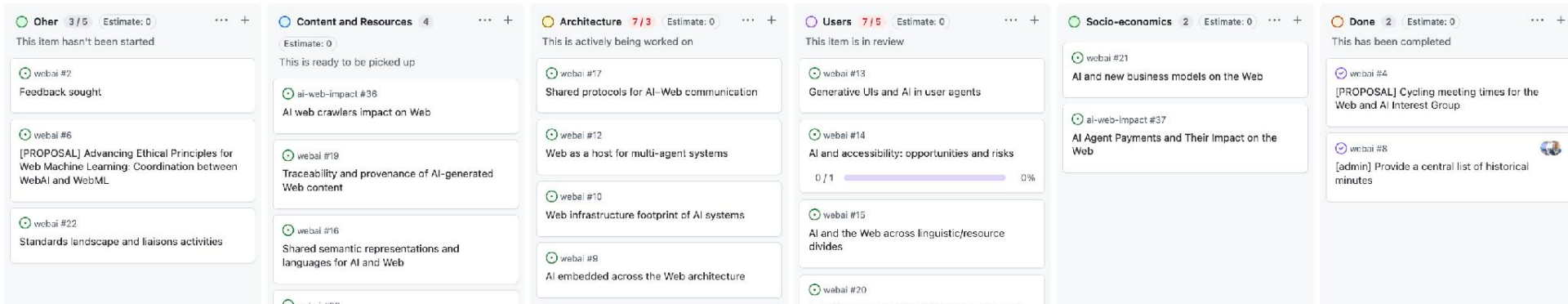
浏览器内 AI 能力

Agent 交互

身份，责任与委托

安全、隐私、无障碍

伦理与开放生态





E-commerce and AI Agent



Workshop: E-commerce for Humans and AI Agents

Jointly organized by W3C and GS1

Hybrid event in Zurich

September 8-9, 2026



Photo by [Growtika](#) on [Unsplash](#)

[Workshop Overview](#)

[Call for Participation](#)

[Participation](#)

[Logistics](#)

[Sponsorship](#)

谢谢聆听，
请多指教！

