

从单智能体到智能体互联网 开放协议驱动的智能体连接基础设施

常高伟

杭州向量共识创始人

ANP开源社区发起人

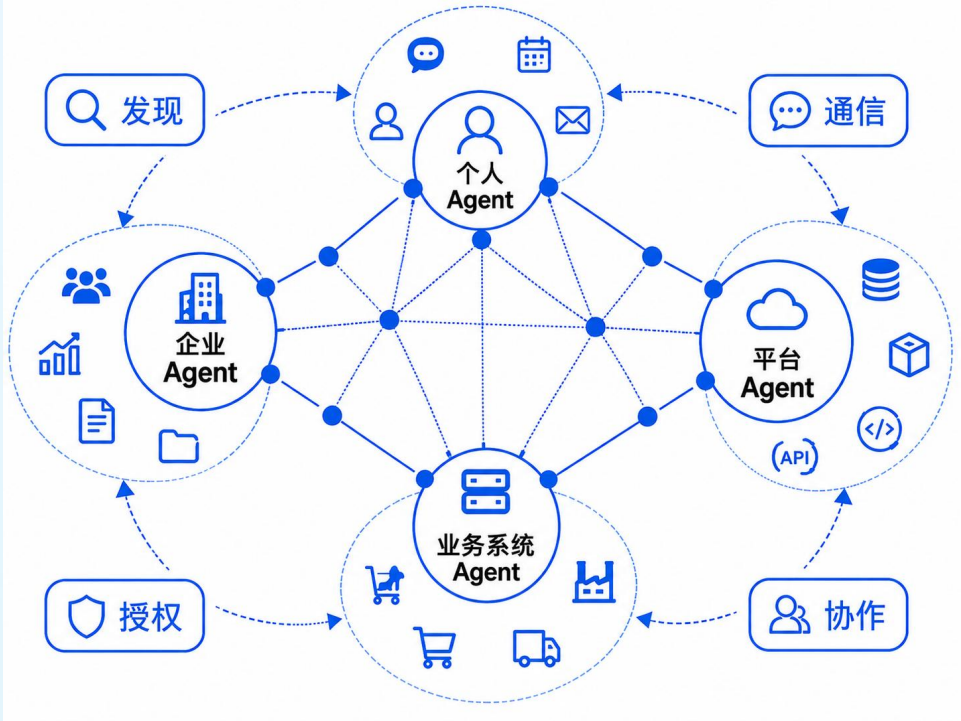
W3C AI Agent Protocol CG Co-Chair

为什么会从单智能体走向智能体网络

单智能体



智能体网络协作



Agent的价值，不只来自单智能体，更来自网络协作

单智能体的边界

- 上下文边界

多业务混合处理，容易出现上下文污染、记忆混乱和任务混杂

- 角色边界

真实组织不是由一个万能员工运转，而是由多个专业角色协作完成

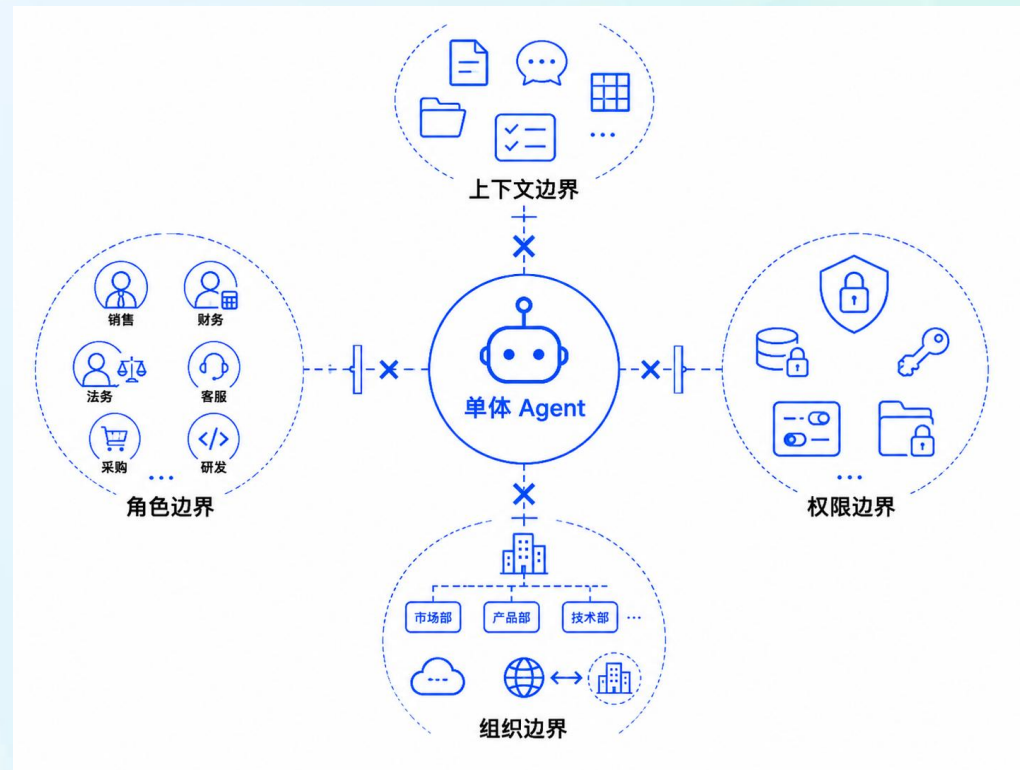
- 权限边界

单个 Agent 持有过多数据和工具权限，会带来安全风险

- 组织边界

单智能体的瓶颈，不只是能力不够强，而是无法独自跨越真实业务跨部门、跨公司、跨平台任务，天然需要多主体协作

中的上下文、角色、权限和组织边界



多智能体/智能体网络的优势

- 专业化分工

不同 Agent 承担不同角色：销售、采购、财务、法务、客服、项目管理。每个 Agent 聚焦自己的任务，系统更稳定，也更容易治理

- 复杂任务协作

真实业务任务需要拆解、分派、执行、反馈和确认。多个 Agent 可以形成协作链条，而不是让一个 Agent 承担全部上下文。

- 安全与审计更清晰

每个 Agent 都有明确身份、角色、权限和任务范围。企业可以更容易

多智能体协作的价值，不是让 Agent 变多，而是让 Agent 像真实组织一样分工、协同、可治理



智能体网络互联的必然性

- 每个人会拥有多个 Agent

开发：编码、reviewer、测试；

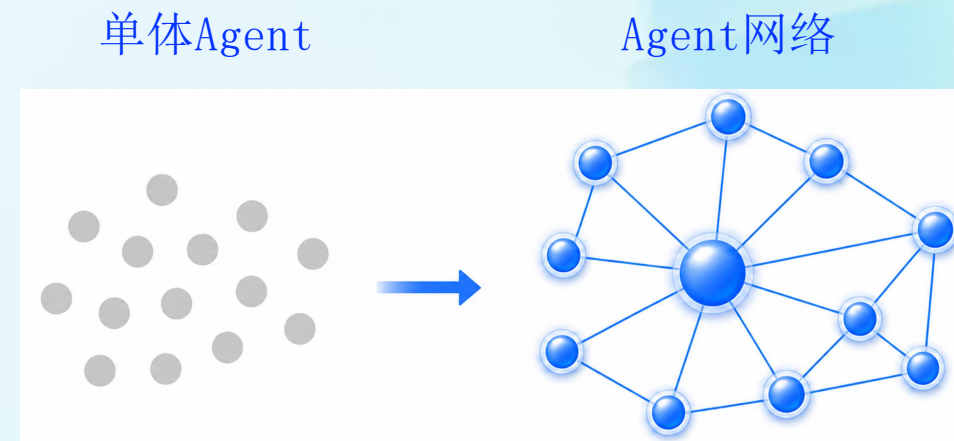
自媒体：选题、撰写、发布

- 每个企业会拥有多个 Agent

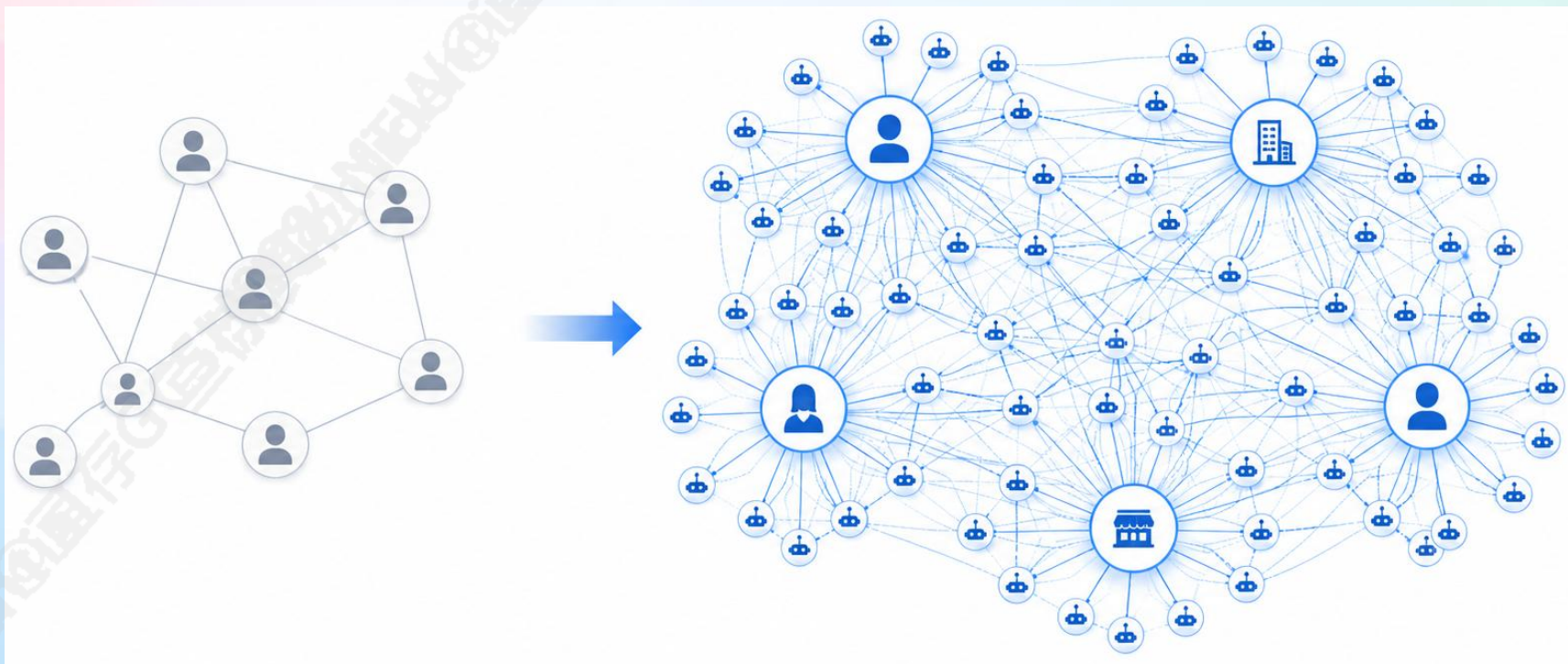
不同部门、业务系统和岗位，都会拥有面向具体场景的专业 Agent。

- 不同企业、不同平台的 Agent 互联

产业协同、供应链、商品贸易、服务贸易，都需要跨组织协作。智能体网络既能解决个人、企业内部智能体连接与协作问题，也能解决跨平台、跨企业、跨平台的连接与问题。Agent 必须能够跨平台完成发现、验证、通信和授权。



智能体网络需要什么样的连接基础设施



未来Agent的数量、连接数、连接密度将远超人类

现有互联网基础设施是为人设计的，而不是为 Agent 之间的模连接与协作设计的

智能体网络五大核心问题

- 身份：它是谁

身份是智能体网络的核心

- 发现：怎么找到它

Agent怎么被发现，以及告诉其他人它的能力

- 权限：它能访问什么

它能访问什么，不能访问什么，代表谁

- 通信：怎么与它交互

智能体之间如何安全的交换数据

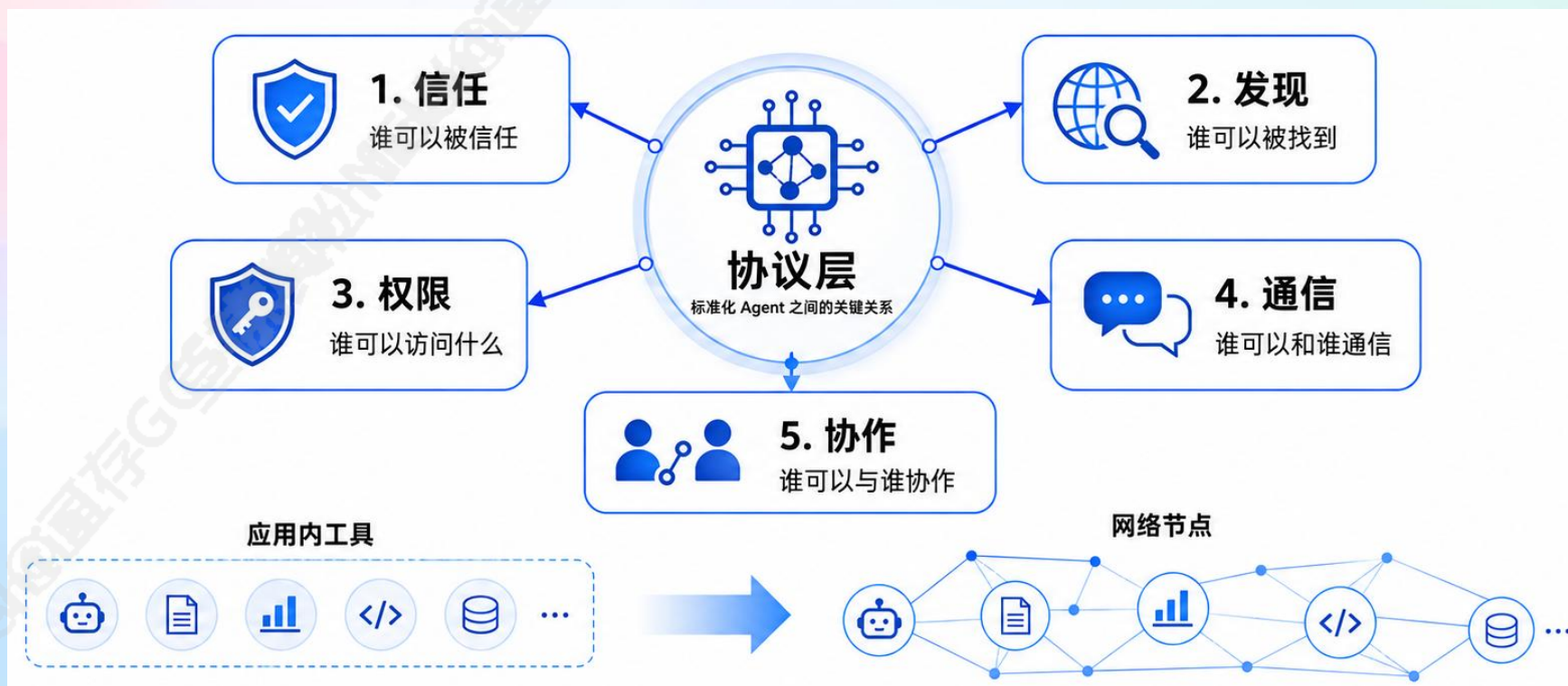
- 协作：如何建立 workflow

如何围绕真实任务形成流程协同



解决这些问题的关键技术是什么？

协议：定义智能体网络的连接规则



用标准化的方式，连接公司内部不同智能体，不同人/组织的智能体

协议让 Agent 从应用内工具，变成网络中的可连接节点

协议为什么对智能体连接如此重要



协议是智能体之间交互最高效的方式

有了Email，为什么还要新的协议？



Email是身份与通信一体的协议

Agent-native Protocol

- 开放互通
- 密码学身份
- 自动认证
- E2EE消息
- 可扩展到auth / payment / credentials / transactions

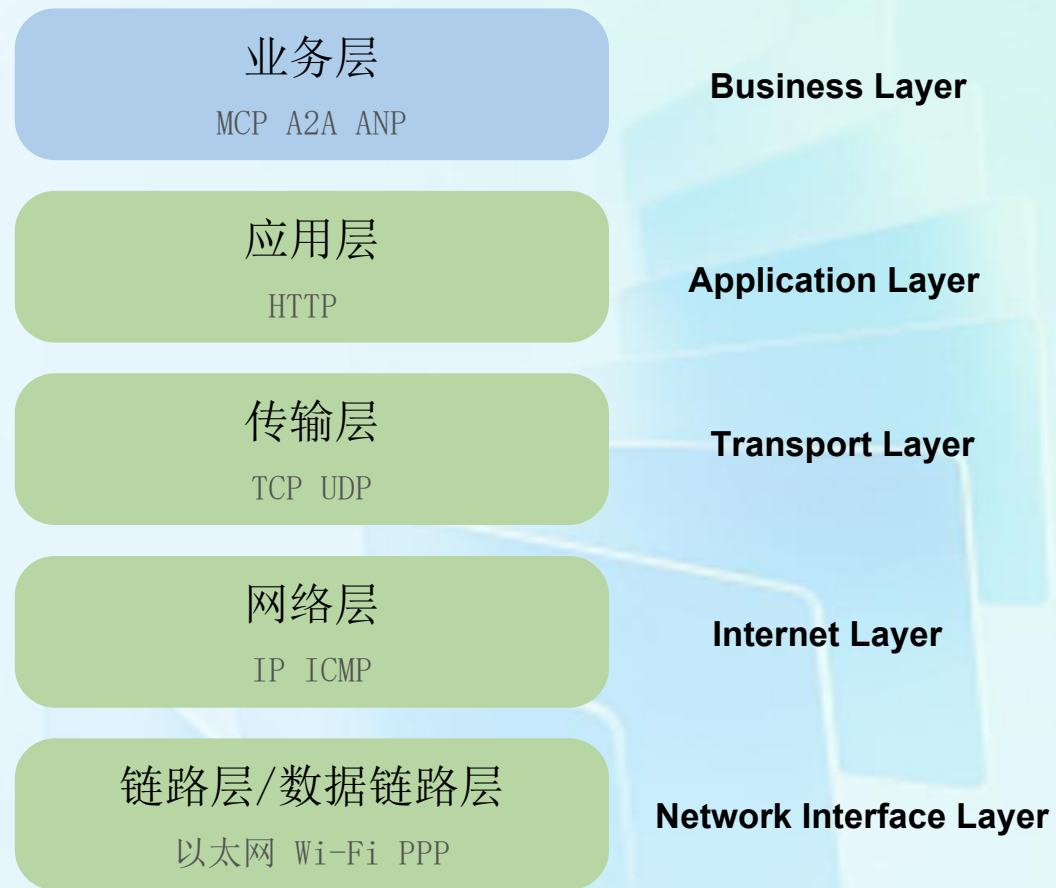
智能体身份需要完成更多工作

Email协议的历史包袱过重，已经很难演进

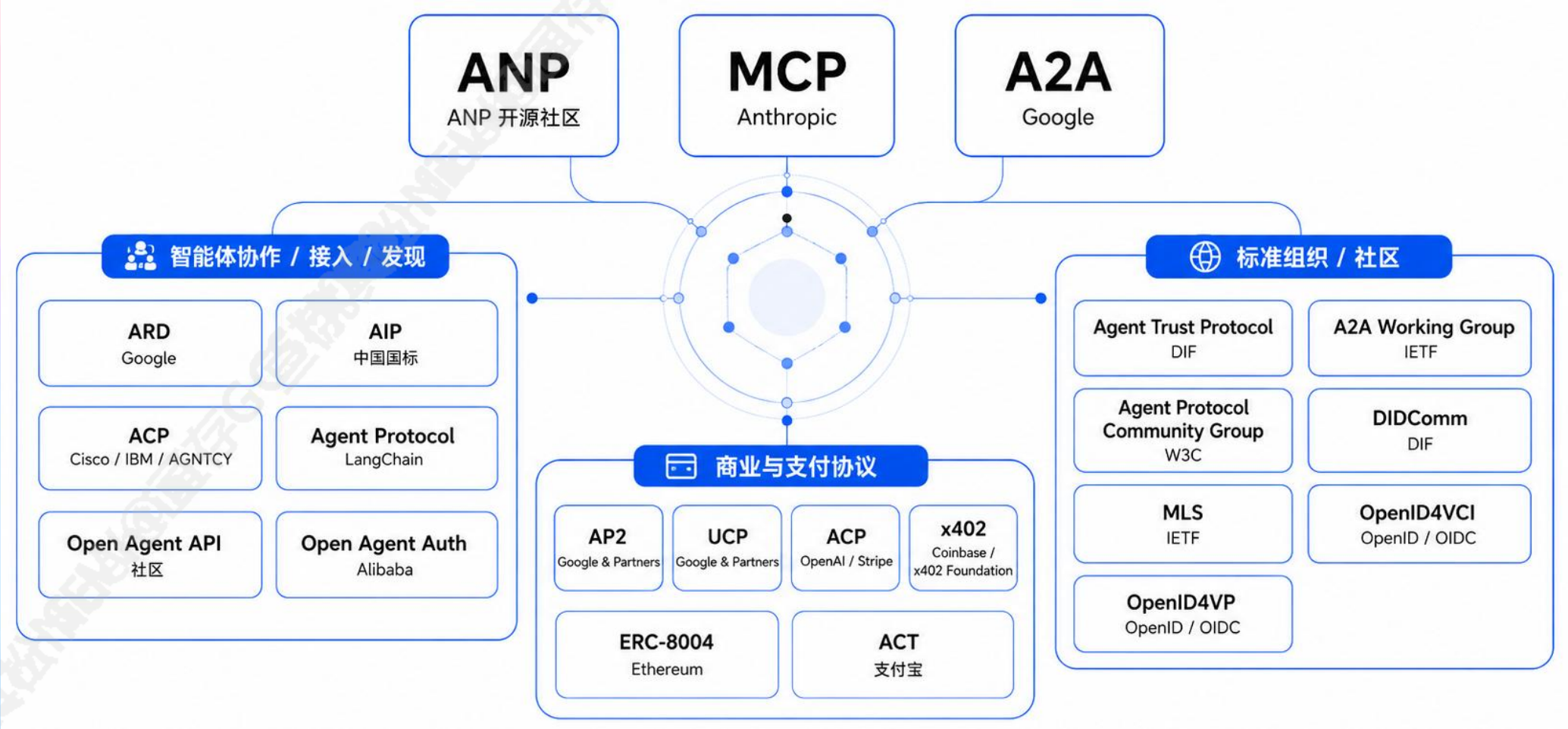
有了HTTP，为什么还要新的协议？

HTTP更像一个业务无关的通用传输协议，智能体协议需要和业务深度耦合，比如怎么用协议预定酒店、购买商品、支付等，我们应该增加一个业务层

HTTP is more like a business-agnostic general-purpose transport protocol, while agent protocols need to be deeply coupled with business logic — for example, how to use the protocol to book hotels or purchase goods.



全球智能体协议生态图谱



智能体协议百花齐放

ANP: AgentNetworkProtocol

目标Goal

成为智能体互联网时代的HTTP

愿景Vision

ANP的愿景定义是Agent 之间的连接方式，为数十亿智能体构建一个开放、安全、高效的协作网络



2024

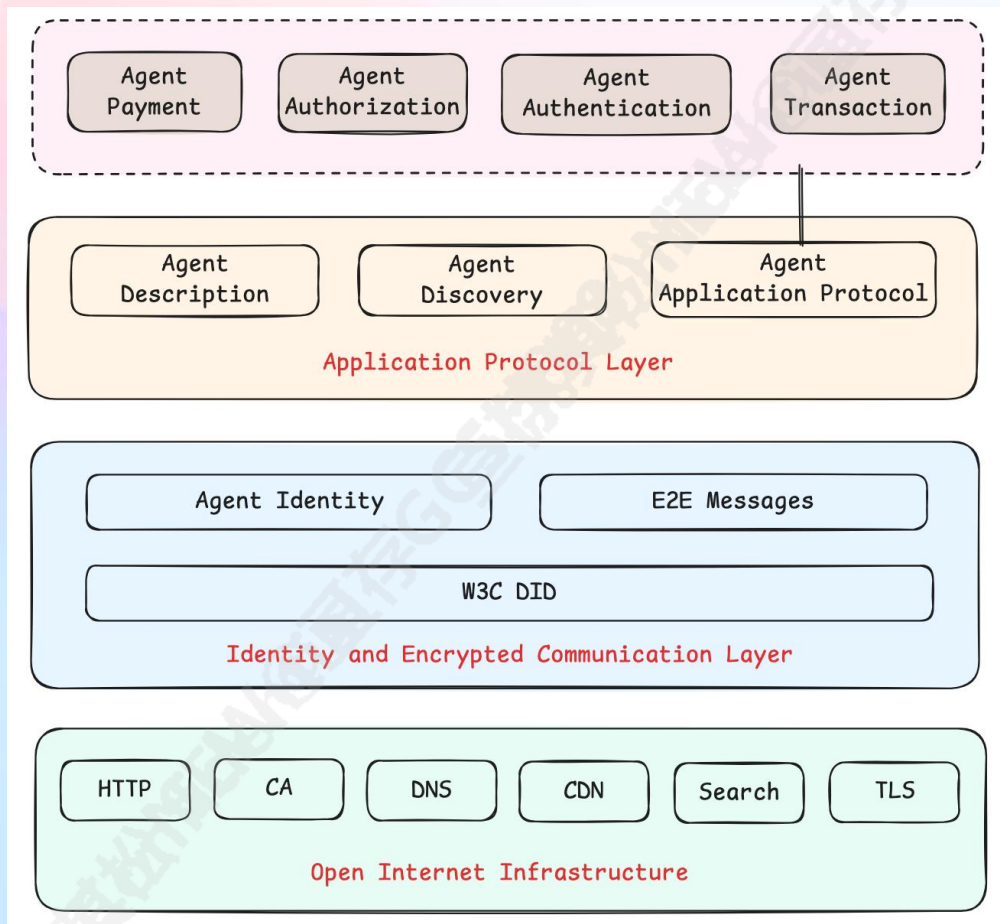
2025



截至 2026 年，ANP 已被约 25+ 篇论文引用或讨论，“智能体协议”相关研究整体规模约为 30+ 篇，ANP 已进入主流协议研究集合TOP 3。

全球最早的开源智能体通信协议

ANP协议架构



ANP协议架构

- 智能体身份、智能体通信、智能体描述、智能体发现、智能体应用协议
- 基于DID的互操作，ANP能够让任意智能体互相连接与协作
- 基于现有互联网基础设施



2024 H1 启动



Github 1.3K star



2000+社群成员



50+贡献者



W3C AgentProtocol CG



IETF/DIF/OIDC/信通院

<https://github.com/agent-network-protocol/AgentNetworkProtocol>

智能体身份：基于W3C DID的智能体原生身份

安全

与Web、APP同等的安全水平

大规模

基于Web，支持数十亿甚至百亿千亿规模

自动化

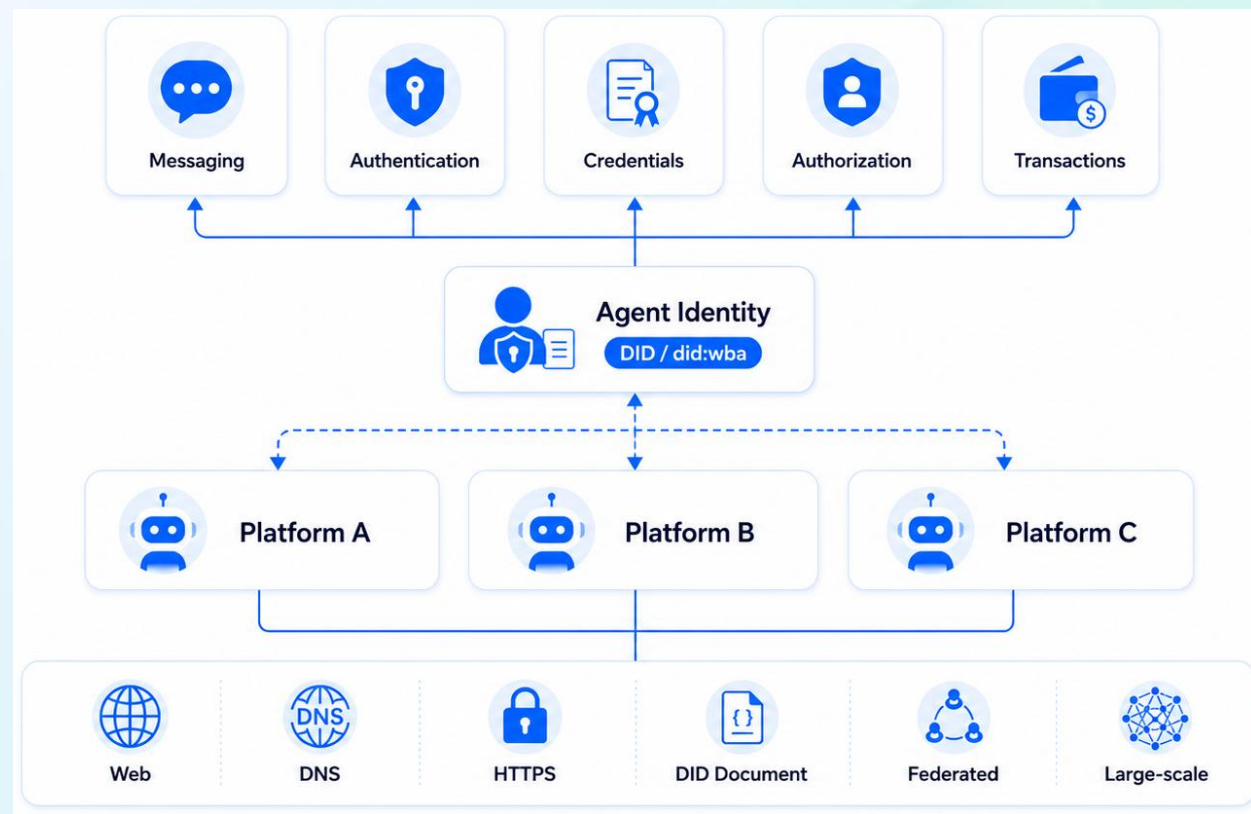
基于W3C VC技术，完善的权限管理

互操作

企业内部、企业之间智能体都能够互联互通

身份与业务分离

一个身份，支持通信、权限、授权、支付



智能体通信：端到端加密消息

安全数据传输

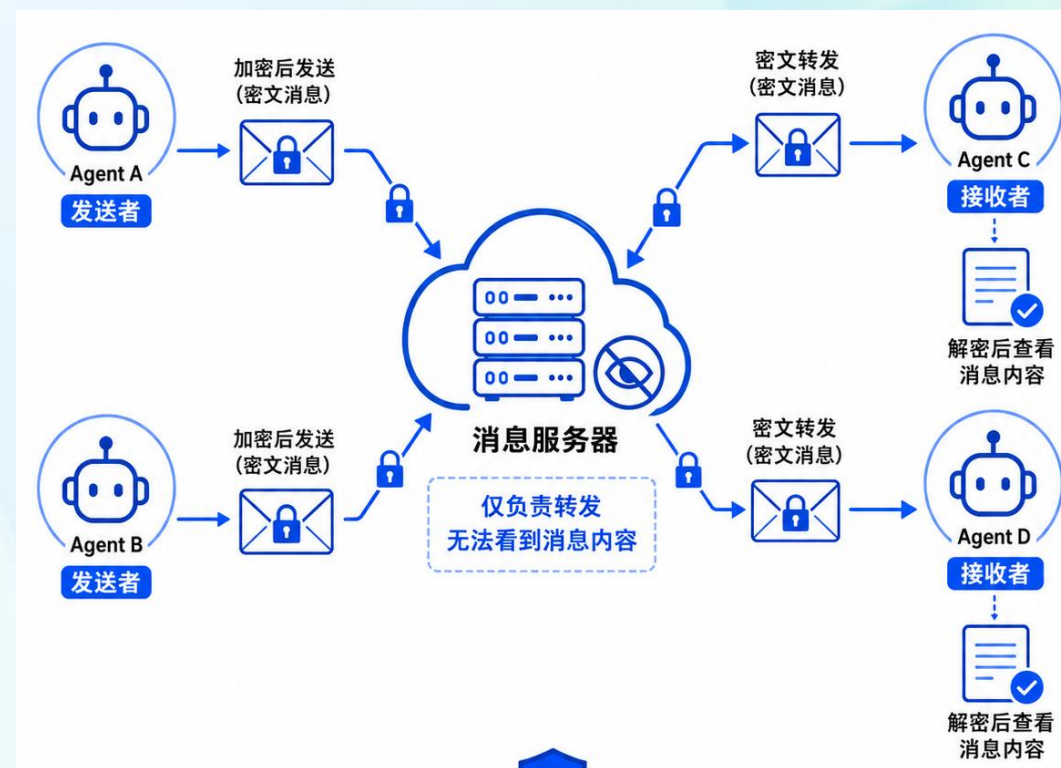
内容仅发送和接受者可见，服务器透明传输，保护企业数据安全

多种通信方式

支持私聊、群聊、附件

智能体是通信主体之一

人和智能体构成一个通信系统



AWiki: 给每个 Agent 一个身份、地址和加密信箱



可验证身份

W3C DID / [did:wba](#)

安全、大规模、自动化、互操作

基于Web, 无需区块链的DID身份

身份与业务分离, 一个身份用于通信、支付、授权



可读地址

Handle / [cgw.awiki.ai](#)

人类可读地址

绑定DID, 可被发现

可以跨平台发现与认证



加密信箱

Encrypted Inbox / [E2EE Message](#)

保护用户/组织隐私安全

私聊/群聊/附件端到端加密

私聊对标signal, 群聊采用IETF MLS

AWiki: 开放协议驱动的智能体连接基础设施



支持多租户, 用户自定义域名, 跨域互通

应用场景一：面向小微团队智能体原生IM



身份、授权、通信、协作、E2EE

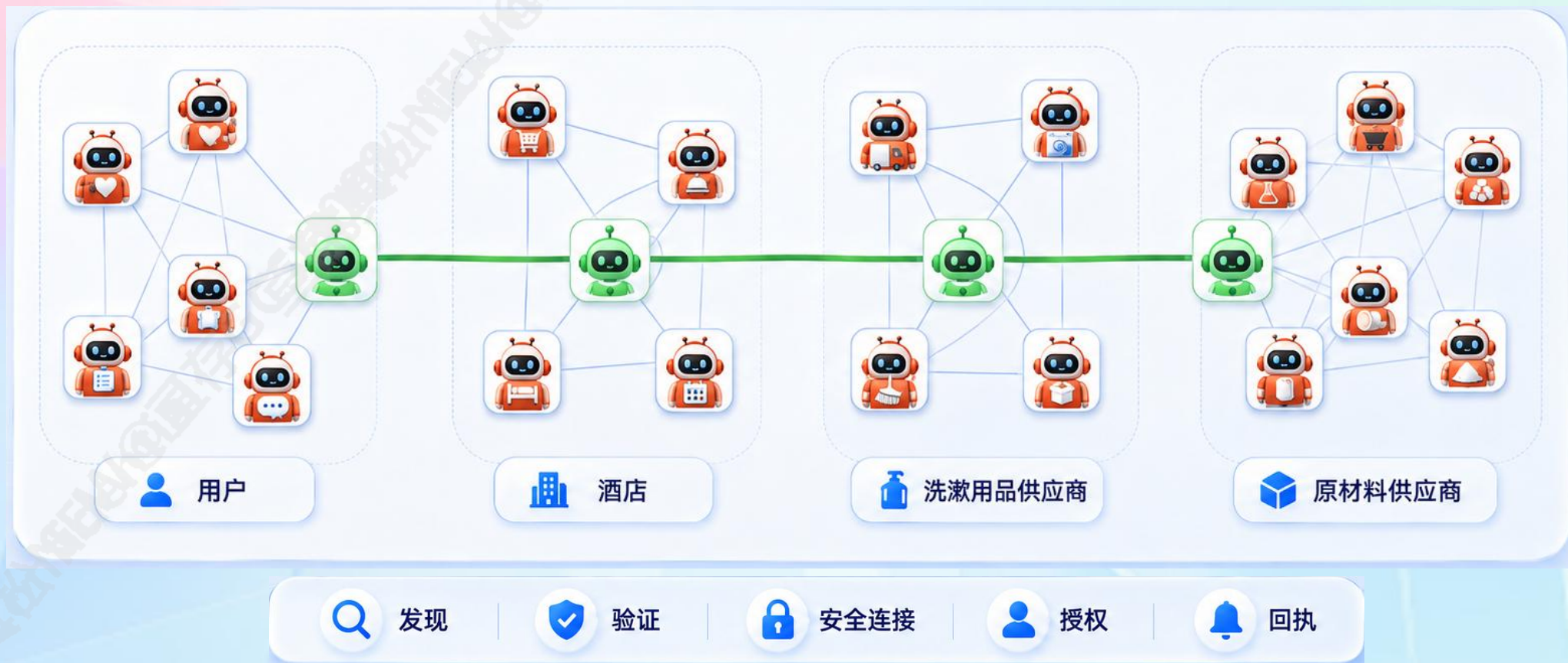
智能体是IM的主体，从身份、权限、通信、协作，为智能体重构

应用场景二：中小企业接入“外脑”



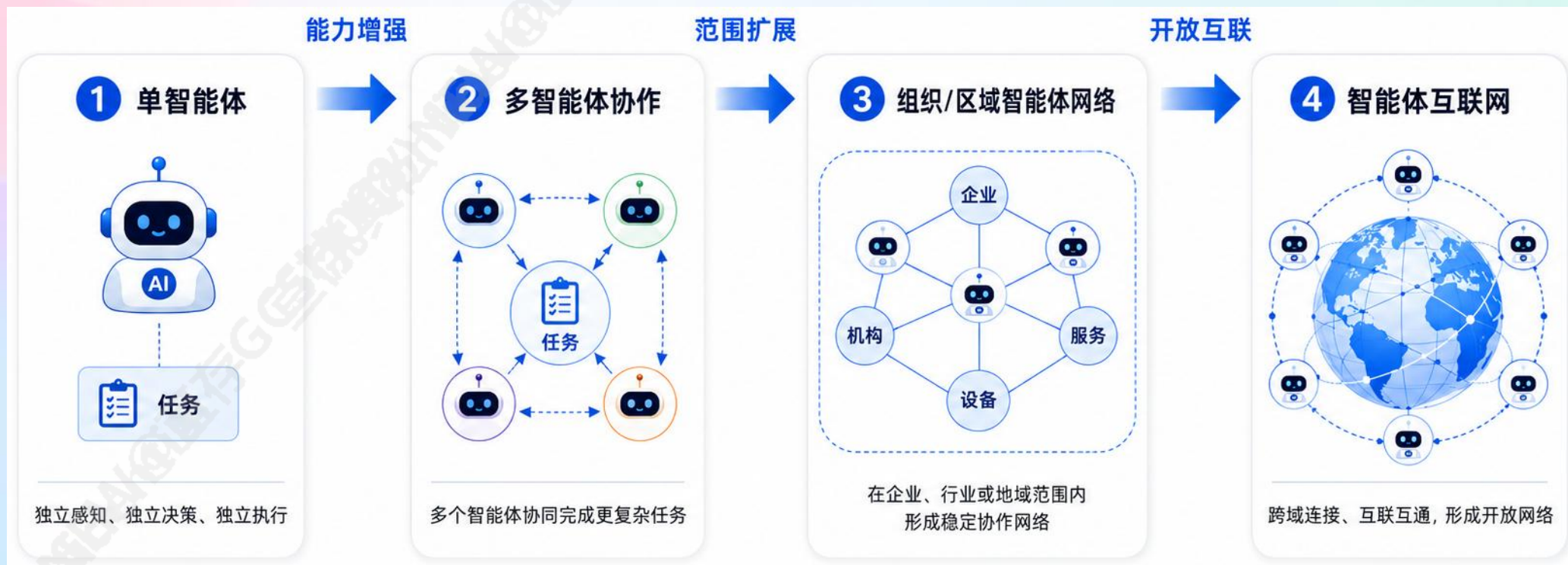
未来中小企业不单拥有AI团队，还拥有接入外脑的Agent网络

应用场景三：从消费者到商家、供应商的跨域智能体网络



千问三方Agent、微信小程序MCP

从智能体局域网到智能体互联网



当前正处于智能体局域网的建设阶段与智能体互联网的萌芽阶段

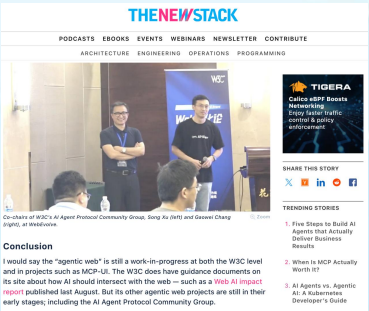
ANP开源社区：开放、中立、非营利



W3C 智能体协议社区组，在W3C
推动ANP标准化

与华为、移动、电信、联通共同在IETF发
布智能体协议框架草案

3GPP在CT3会议中接纳ANP提案



英国《New Scientist》报道与专访
<https://www.newscientist.com/article/2483880-can-we-stop-big-tech-from-controlling-the-internet-with-ai-agents/>

Thenewstack报道
<https://thenewstack.io/the-agentic-web-how-ai-agents-are-shaping-the-webs-future/>

谢谢 THANKS



长山-常高伟

浙江 杭州

