# IBM开源轻量级智能体框架CUGA，Runway推出四款新模型

中文内部早报 · 5分钟版

## 今日总览

今日AI领域重点关注IBM开源的轻量级智能体框架CUGA，该框架在多个基准测试中表现优异。同时Runway发布了包括Seedance 4K在内的三款新模型，视频生成能力进一步提升。

Agent/Coding板块迎来多项重要进展。IBM开源CUGA框架支持快速构建智能体，Hugging Face将huggingface_hub发布周期缩短至每周。Google ADK与A2A协议展示跨语言多智能体团队构建方案。

模型与多模态方面，Runway推出Seedance 4K、Seedance Mini和Kling 3.0 Turbo三款新模型。字节Seed发布Seed2.1系列，强化通用Agent能力和多模态理解，在多个基准测试中取得优异成绩。

大厂与产业链动态中，Samsung Electronics向全球员工部署ChatGPT Enterprise和Codex。Claude Desktop现已在AWS、Google Cloud和Microsoft Foundry上提供完整体验，支持企业级部署和精细访问控制。

监管安全与研究工具板块，五眼联盟联合警告AI网络威胁将在数月内影响普通用户。Anthropic推出Claude Tag功能，允许在Slack中通过@Claude进行协作，同时GitHub等开源联盟呼吁修改加州AI透明度法案以保护开源发展。

## 头条 今日头条

### 1. IBM开源CUGA轻量级智能体框架

Hugging Face 博客 · 06/23 20:51 · 研究、评测与方法论

IBM开源了CUGA(Configurable Generalist Agent)轻量级智能体框架，处理规划、执行循环、工具调用和状态管理。开发者只需提供工具列表和提示词即可构建CugaAgent，内置计划-执行-反思循环，在AppWorld和WebArena基准上排名第一。

### 2. Claude Code发布v2.1.187版本

Claude Code：GitHub Releases · 06/24 08:00 · 开源项目与开发者工具

Claude Code v2.1.187新增sandbox.credentials设置，可阻止沙箱化命令读取凭证和秘密环境变量。模型选择器支持组织配置的模型限制，修复了多项问题包括resume功能、工作流智能体结构化输出循环、远程MCP工具调用阻塞等。

### 3. Runway推出Seedance 4K等三款新模型

X：Runway (@runwayml) · 06/24 08:00 · 前沿模型与多模态

Runway推出Seedance 4K、Seedance Mini和Kling 3.0 Turbo三款新模型，涵盖不同性能层级需求。这些模型现已正式推出，用户可使用优惠码享受前三个月七折优惠，进一步丰富了Runway的视频生成产品线。

### 4. huggingface_hub 实现每周发布：AI、开源工具、人工审核闭环

Hugging Face 博客 · 06/24 08:00 · 智能体、编程与工作流

Hugging Face将huggingface_hub发布周期从每4-6周缩短至每周，全部由单个GitHub Actions工作流自动完成。流程依赖开源工具和权重模型起草发布说明，保留人类最终审核环节，实现了完整的自动化发布闭环。

### 5. Claude推出智能体身份访问模型

Claude 博客 · 06/24 08:00 · 监管、安全与版权

Claude Tag推出agent identity智能体身份访问模型，让Claude在共享频道中以独立身份工作而非模拟用户。管理员可配置连接器、仓库访问等权限，私有频道拥有独立身份，记忆和访问不跨频道流转。

## 模型 前沿模型与多模态

### 1. 在 Transformers.js 中实验提议的跨源存储 API

Hugging Face 博客 · 06/24 08:00

Transformers.js 在浏览器中运行 AI 模型时，不同来源的 Web 应用会重复下载并缓存相同的模型资源（如 Xenova/whisper-tiny.en）和 Wasm 运行时文件（如 4,733 kB 的 ort-wasm-simd-threaded.asyncify.wasm），即使资源 URL 相同，浏览器因 Network Isolation Key 隔离缓存，单次 demo 就产生 177 MB 冗余下载和存储。Cross-Origin Storage API 是一项早期提案，旨在让跨来源应用共享缓存的模型和运行时资源。目前该 API 尚未在浏览器原生实现，但可通过 Chrome 扩展注入 polyfill 进

### 2. How GPT-5 helped immunologist Derya Unutmaz solve a 3-year-old mystery

OpenAI 新闻 · 06/24 01:00

How GPT-5 helped immunologist Derya Unutmaz solve a 3-year-old mystery。

### 3. Aleph 2.0 已集成到 Figma Weave

Runway 新闻 · 06/22 00:00

Runway 的视频编辑模型 Aleph 2.0 已在 Figma Weave 中上线。设计师可从视频中提取关键帧、重新设计风格并把编辑结果传回 Aleph 2.0 节点，将变化应用到主体出现的每一帧，同时保持其他内容不变。

### 4. Omio 如何构建对话式旅行的未来

OpenAI · 06/24 08:00

Omio 利用 OpenAI 技术打造对话式旅行体验，加速产品开发进程，并推动自身向 AI 原生公司转型。

## 智能体 智能体、编程与工作流

### 1. Google ADK 与 A2A 协议展示跨语言多智能体协作

Google 开发者博客 · 06/22 00:00

Google 开发者博客展示如何用 Agent Development Kit 与 Agent2Agent 协议搭建跨语言多智能体流水线：Python 智能体调用 Gemini 解析合同条款，Go 智能体校验合规性，A2A 通过 Agent Card 做能力发现并用 JSON-RPC 2.0 通信。

### 2. Show HN：Oak - 面向 AI 智能体的 Git 替代方案

Hacker News · 06/23 05:00

Oak 是面向 AI 智能体的开源版本控制系统，服务 Claude Code、Codex、Cursor 等工具。它以分支-会话为基本工作单元，使用内容哈希、分块、diff/merge 和 Blob/Manifest/Commit/Tree 数据模型，支持 SQLite 和 git 后端。

### 3. Grok Build 推出 /goal 模式

xAI 新闻 · 06/22 08:00

xAI 在 Grok Build 中引入 /goal 模式。用户用一行命令设定目标后，agent 会自动规划方案、拆解任务并持续执行，直到目标完成并通过验证；期间用户仍可追加指令和监督任务进展。

### 4. 国内首个高考志愿AI测评出炉，千问多项表现超过资深咨询师

公众号：千问APP（阿里） · 06/24 08:00

友松实验室发布国内首个高考志愿AI能力测评报告，测试千问高考志愿填报Agent四大模块。与53位平均从业4.6年的人类咨询师对照，千问表现更稳定精确：44道事实题全对；模拟10个志愿中6个可录取；100场匿名对比中专家58次倾向千问回答。使用千问辅助后，人类咨询师正确率提升，耗时减少约27%。该Agent基于千问高考志愿大模型和夸克8年高考数据，覆盖约3000所院校、2000多个专业。

## 产业 大厂与产业链

### 1. 我们用免费本地模型对 OpenClaw 仓库进行实时分类

Hugging Face 博客 · 06/22 08:00

Hugging Face 在 OpenClaw 仓库上测试用 Gemma 和 Qwen 等本地模型实时分类 issue 和 PR。他们使用 Pi agent harness 驱动模型，配合 reposhell 只允许读操作防止提示词注入。测试的模型包括 gemma-4-26b-a4b 和 qwen3.6-35b-a3b，经性能优化后均可在本地生成数百 token/s。该方案运行在 NVIDIA GB10（128 GB 统一内存）上，相比每月 200 美元的 ChatGPT Pro 订阅，可实现近乎实时的通知且仅消耗电费。

### 2. Claude Desktop 完整版扩展到 AWS、Google Cloud 和 Microsoft Foundry

Claude 博客 · 06/22 00:00

Anthropic 表示，企业通过 AWS、Google Cloud 和 Microsoft Foundry 使用 Claude Desktop 时，现可获得 Chat、Claude Cowork 和 Claude Code 集成体验。IT 团队可将推理和对话历史保留在自己的云环境，并使用 IAM、Entra ID 或 Okta 等身份体系。

### 3. FastWan-QAD：单卡5090上1.8秒生成5秒视频

X：Sky Computing Lab (@haoailab) · 06/24 08:00

Sky Computing Lab 发布 FastWan-QAD 视频生成模型系列，基于 FastVideo 的量化感知蒸馏（QAD）方案训练。在单张 NVIDIA GeForce RTX 5090 上，端到端生成一段 5 秒 480P 视频仅需 1.8 秒。模型、代码及博客已开源。

### 4. 三星电子向全球员工部署 ChatGPT Enterprise 与 Codex

OpenAI 新闻 · 06/22 07:00

OpenAI 报道，三星电子已在全球范围内向员工部署 ChatGPT Enterprise 和 Codex，这是 OpenAI 规模较大的企业级 AI 落地案例之一。

## 开源 开源项目与开发者工具

### 1. GitHub联合开源联盟呼吁修改加州AI透明度法案以保护开源

GitHub Blog · 06/24 08:00

GitHub 联合 Black Forest Labs、Hugging Face 与 Mozilla Corporation 组成开源联盟，呼吁对加州 AI 透明度法案（SB 942，拟由 SB 1000 修正）进行针对性修改。当前草案要求开发者在下游用户未履行义务时撤销开源许可证，这与开源许可证永久不可撤销的性质冲突。联盟认为该要求非必要，已有直接监管和执法机制，并建议参考欧盟 AI 法案的透明度实践规范，以向下游用户通知最佳实践文档的方式替代撤销条款。GitHub 支持这些修正，以在保持透明度目标的同时兼容开源开发模式。

### 2. 无限制OCR：单次长时域解析

Hacker News · 06/24 08:00

Unlimited OCR 是一个托管在 GitHub 的项目，实现单次长时域解析（One-Shot Long-Horizon Parsing），旨在一次性处理长时间跨度的 OCR 任务。

## 监管 监管、安全与版权

### 1. Anthropic 推出 Claude Tag：在 Slack 中通过 @Claude 协作

Anthropic：Newsroom · 06/24 08:00

Anthropic 推出 Claude Tag，一种在 Slack 频道中通过 @Claude 委托任务的新协作方式。Claude 可记住频道上下文，支持多用户交互，经授权后可自动学习其他频道和数据源。开启“环境”行为后，能主动更新未解决的线程或任务。支持异步工作，可自主推进项目数小时或数天。即日起面向 Claude Enterprise 和 Team 客户提供 beta 版。管理员可精细控制工具和渠道访问权限、设置 token 消耗限额，并查看所有操作日志。

### 2. OpenAI 发布 Daybreak 安全工具

OpenAI · 06/22 18:00

OpenAI 推出 Daybreak 系列安全工具，包括 Codex Security 和 GPT-5.5-Cyber，面向组织的大规模漏洞发现、验证和修补流程。

### 3. 五眼联盟警告：AI网络威胁数月内将影响普通用户

Artificial Intelligence News · 06/24 08:00

2026年6月22日，五眼联盟（美、英、加、澳、新）网络安全部门联合警告，即将到来的AI模型（如OpenAI的GPT-5.5-Cyber、Anthropic的Mythos）将降低编写复杂攻击代码的门槛。自动化智能体可全天候扫描互联网漏洞，大幅缩短安全窗口期。AI驱动的超个性化钓鱼诈骗已在亚太蔓延，印度2026年初勒索软件事件激增165%。五眼联盟建议企业部署自动化防御AI，个人用户开启多因素认证、删除闲置账户。

## 研究 研究、评测与方法论

### 1. Seed2.1 正式发布，深入 AI 生产力

字节 Seed：Research Feed（网页内嵌数据） · 06/24 08:00

字节Seed发布Seed2.1系列，面向真实生产力场景的智能体，强化通用Agent能力、代码工程交付与多模态理解。Seed2.1 Pro在GDPval基准获最高分，Agents' Last Exam位列参评模型第一梯队；MobileWorld手机GUI任务最高分，CreativeWork多环境任务表现突出。多模态在CharXiv-RQ等多项基准取得SOTA。代码能力上，Seed2.1 Pro在NL2Repo-Bench表现良好，开发者评测相比Claude Opus 4.6获59.1%胜率。模型已在豆包、TRAE上线，API通过火山方舟提供。

### 2. 能力强但粗心：计算机使用智能体是否遵循情境完整性?

HuggingFace Daily Papers（社区热门论文） · 06/22 08:00

AgentCIBench评估计算机使用智能体（CUA）是否遵循情境完整性。它针对三种常见失败模式：视觉共置（智能体拉取任务目标旁边被禁止的项目）、任务模糊性过度分享（在提示不明确时泄露个人状态）以及收件人错配（向不适当的收件人发送内容）。对15个前沿CUA的评测显示平均泄漏率67.9%，其中11个在超过50%的场景中泄漏，这些失败在端到端任务中同样存在。AgentCIBench已发布，旨在推动开发更安全的计算机使用智能体。

### 3. PP-OCRv6 登陆 Hugging Face，支持 50 种语言 OCR

Hugging Face 博客 · 06/22 21:18

PP-OCRv6 是 PaddleOCR 新一代通用 OCR 模型族，提供 tiny、small 和 medium 三档参数规模。small 和 medium 支持 50 种语言，官方基准显示 medium 在检测和识别准确率上较上一代 server 模型继续提升。