AOSF • 智能体开源基金会

智能体 AI 与氛围编程全景

智能体开源基金会为何重要

高层简报 • 2026 年 2 月

执行摘要

两股汇聚的力量——智能体 AI 与氛围编程——正在从根本上重塑软件的编写、审核与部署方式。到 2026 年初，AI 智能体已能自主编写、测试和部署代码。然而，目前尚无任何基金会能够满足 AI 生成开源软件的独特治理需求。

$47–93B
智能体 AI 市场
2030–2032 年

45%
AI 生成代码
存在安全漏洞

60K+
已采用
AGENTS.md

1B+
C/C++ 代码行数
待重写

智能体开源基金会（AOSF）填补了这一空白——为氛围编程时代提供智能体原生的治理机制。AOSF 并非与现有基金会竞争，而是在 AI 代码质量验证、安全保障、溯源追踪和公正模型评估方面形成互补。

01

智能体 AI 全景

重塑软件开发的自主系统

什么是智能体 AI ？

能够自主行动的 AI 系统——追求复杂目标、规划多步骤工作流程，并在无需人工直接干预的情况下与工具及外部系统进行交互。

🎯 目标追求

自主追求复杂目标，设定子目标并迭代优化

🧠 规划与推理

多步骤规划与实时策略调整

🔧 工具使用

与 API 、数据库、代码编辑器及外部系统交互

🔄 自我纠错

从错误和反馈中学习以改进输出

👥 多智能体协作

协调专业智能体团队执行复杂任务

智能体 AI 领域主要参与者

Anthropic

Claude Code ， MCP 协议创建者
Model Context Protocol 标准

Google

A2A 协议， Agent Development Kit
已将 A2A 捐赠给 Linux 基金会

Microsoft

AutoGen 框架， GitHub Copilot
事件驱动的多智能体系统

OpenAI

Codex 、 Operator 、 ChatGPT 智能体
规划与推理能力

Meta

LLaMA 开放模型， CodeLlama
开放权重模型生态系统

开源社区

LangChain 、 CrewAI 、 OpenClaw
社区驱动的智能体框架

智能体协议： MCP 、 A2A 与 AGENTS.md

🔌 MCP

模型上下文协议

由 Anthropic 创建
"USB-C port for AI"

智能体→工具通信

已被 Cursor 、 Windsurf 、
Claude Code 、 AutoGen 等采用

🤝 A2A

智能体间通信协议

由 Google 创建
已捐赠给 Linux 基金会

智能体→智能体通信

不透明执行、能力
发现与任务管理

AGENTS.md

代码仓库约定

由 OpenClaw 推广
草根式采纳

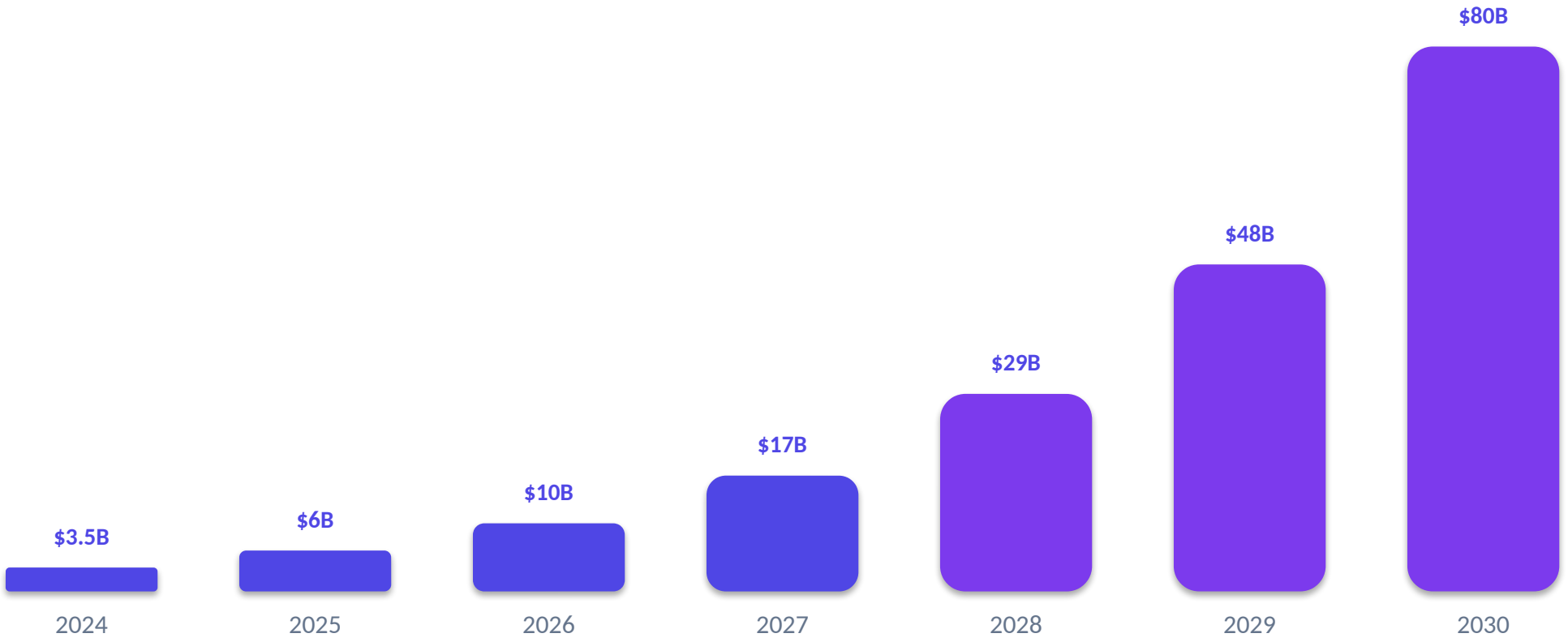
机器可读的代码库
AI 智能体操作指令

60K+ 仓库且持续增长

MCP = 智能体到工具 • A2A = 智能体到智能体 • AGENTS.md = 智能体到代码库

注：并非所有平台都采用这些标准。例如，OpenClaw 使用专有协议（内置工具、基于会话的多智能体、自定义通道插件），并可选 MCP 桥接。这种碎片化使得 AOSF 的中立治理角色对跨平台互操作性更加至关重要。

市场规模与增长



智能体 AI 市场预测 • 年复合增长率 44–47% • 数据来源： MarketsandMarkets 、 Gartner 、 LangChain

02

氛围编程革命

当 AI 编写大部分代码时，一切都将改变

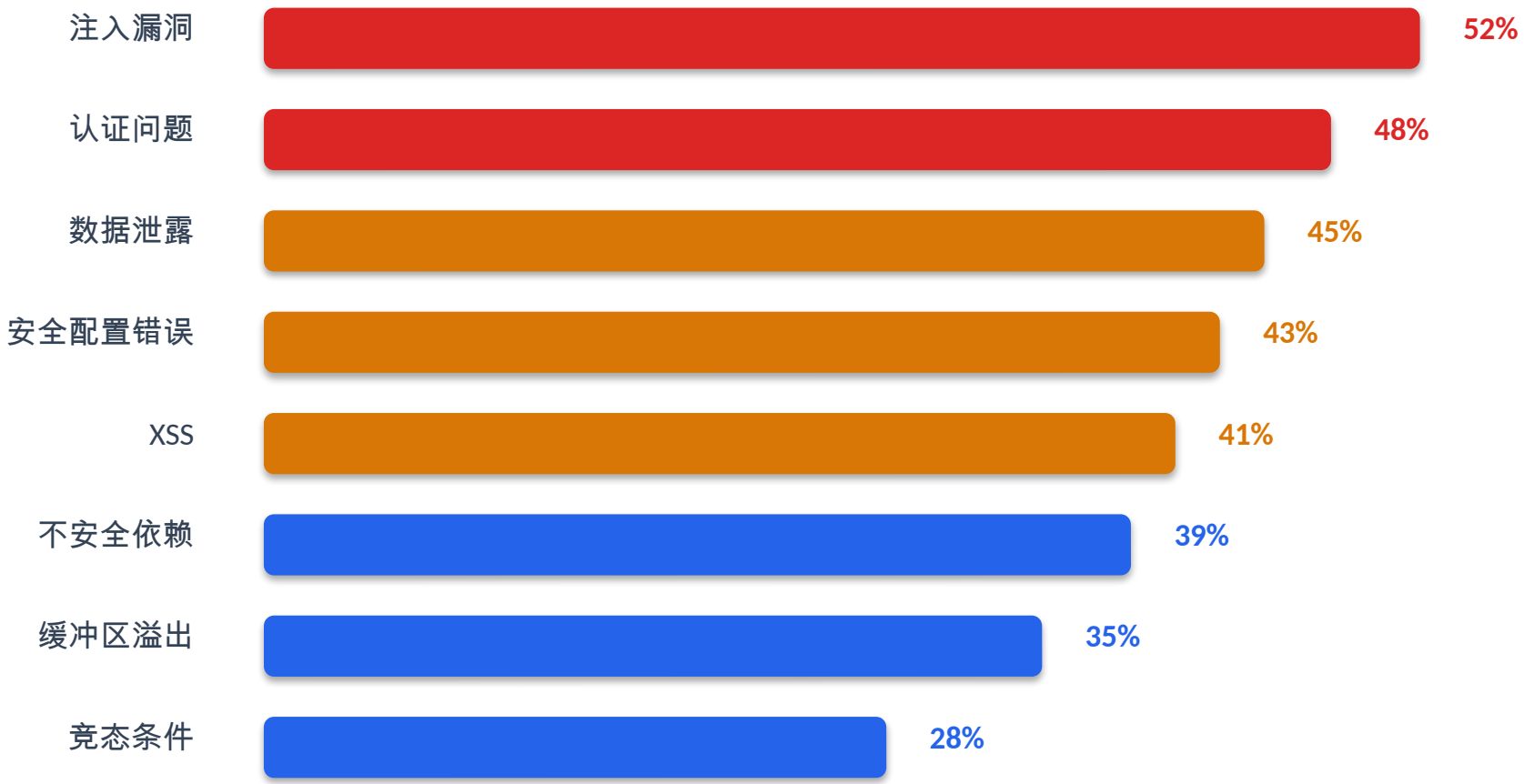
什么是氛围编程？

"There's a new kind of coding I call 'vibe coding', where you fully give in to the vibes, embrace exponentials, and forget that the code even exists."
— Andrej Karpathy ， 2025 年 2 月

- 由 Andrej Karpathy 提出（ 2025 年 2 月 ）—— 2025 年 Collins 词典年度词汇
- 开发者用自然语言描述意图， AI 生成代码
- YC 2025 冬季班 25% 的初创公司代码库中 95% 由 AI 生成
- Google 现有 70% 的代码由 AI 生成（ Sundar Pichai ， 2025 年 10 月 ）
- GitHub Copilot ：平台上 40% 以上的代码由 AI 生成
- 核心工具： Cursor 、 Windsurf 、 Claude Code 、 Replit Agent 、 Bolt 、 Lovable
- 开发者角色从编写代码转变为→审核、指导和验证 AI 输出

安全问题

AI 生成的代码速度快但脆弱，近半数存在安全漏洞。



03

治理空白

现有基金会未覆盖的领域

基金会覆盖范围对比

领域	Linux 基金会	Apache	CNCF	OSI	AOSF
AI 原生项目托管	✗	✗	✗	✗	✓
AI 代码安全扫描	~	✗	~	✗	✓
智能体治理	✗	✗	✗	✗	✓
AI 伦理框架	~	✗	✗	~	✓
内存安全倡议	~	✗	✗	✗	✓
开源模型评估	✗	✗	✗	✗	✓
AI 代码溯源	✗	✗	✗	✗	✓
传统开源治理	✓	✓	✓	✓	✓

AOSF 不与现有基金会竞争——而是填补它们未能覆盖的空白。

04

AOSF 简介

智能体开源基金会

五大核心功能

📦 氛围编程项目仓库

AI 生成开源软件的精选平台
项目按质量分级：实验级→企业级

🦀 Rust 迁移倡议

AI 辅助 C/C++→Rust 翻译转化关键基础设施代码

🤖 智能体原生运营

智能体辅助审核、自动化文档、透明审计追踪 + DAO 混合模式

⚖️ AI 伦理开发标准

署名、许可、人机协同框架面向 AI 生成代码

🏆 CELLO 排行榜

100% 开源 LLM 代码评估。开放模型、开放工具、可复现

协同一体：为 AI 生成开源软件提供全面治理

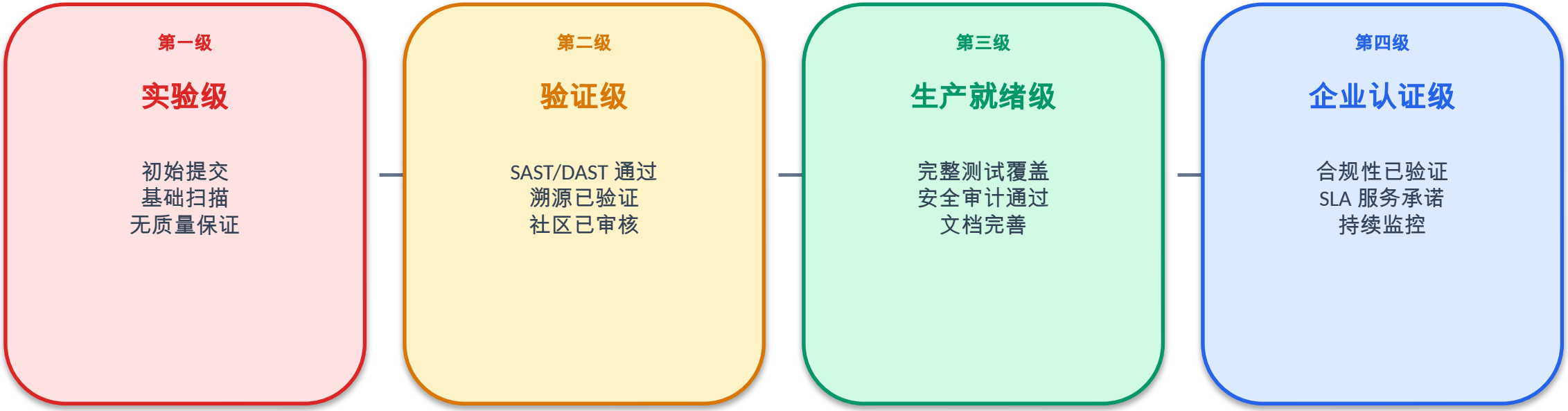
AI 代码溯源标准

对 AI 生成代码的来源、审核状态和质量进行机器可读追踪——这对建立企业信任至关重要。


```
{
  "schema": "aosf-provenance/v1",
  "model_id": "deepseek-coder-v3-236b",
  "human_reviewer": "@chris-dev",
  "security_scan": { "tool": "semgrep", "findings": 0, "passed": true },
  "cello_score": 87.4,
  "quality_tier": "production-ready",
  "license": "Apache-2.0"
}
```

质量分级体系

每个 AOSF 托管的项目都会根据安全性、测试、文档和社区验证逐级递进。



05

参与其中

共同构建开源的未来

如何参与

👷 开发者

构建工具和基础设施：

- 为 CELLO 基准做出贡献
- 构建安全扫描工具
- 参与 Rust 迁移倡议
- 提交 AI 生成的项目
- 审核社区提交

🏢 企业

塑造行业标准：

- 赞助溯源标准
- 加入治理委员会
- 企业认证案例
- 共建伦理框架
- 访问认证项目等级

🔬 研究人员

推进科学研究：

- 评估方法论
- AI 漏洞模式
- 溯源与署名
- 通过工作组发表成果
- 对新开源模型进行基准测试

准备好构建
开源的未来了吗？

加入首个专为 AI 生成代码时代而创建的基金会。
中立治理。开放标准。社区驱动。

github.com/aosf-org

探索 CELLO

AOSF • 智能体开源基金会 • 创立于 2026 年

🤖 由 AI 智能体构建，服务于 AI 生成软件——每一步都有人工监督