




Evolution of AI in Programming

Agentic Coding in VS Code...what the duck is happening?

Andrej Karpathy

9.889 post



...

Following

Andrej Karpathy

@karpathy

Building @EurekaLabsAI. Previously Director of AI @ Tesla, founding team @ OpenAI, CS231n/PhD @ Stanford. I like to train large deep neural nets.

Traduci bio


Stanford

karpathy.ai

Iscrizione: aprile 2009

1.040 following

1,5 Mln follower



Seguito da HackerNoon | Learn Any Technology, Elon Musk e altri 3 che segui

Post


Risposte

Highlight

Articoli

Contenuti

Fissato



Andrej Karpathy

@karpathy · 24 gen 2023

The hottest new programming language is English

1.500

8.555

54.154

9 Mln

The Evolution of the IDE - AI Relationship



Copy/Pasted Code

Manual copying from LLM (no integration)



Autocomplete in the IDE

Intelligent real-time suggestions



Chat with Context

Conversation with codebase awareness



Agents

Complex tasks autonomously



Why AI Alone Isn't Enough

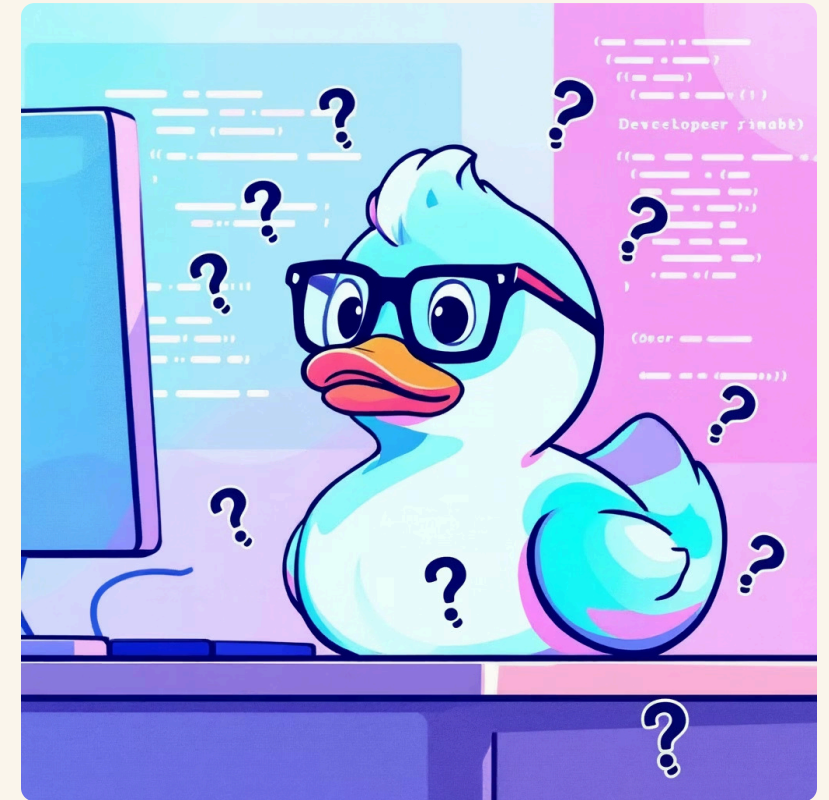
Plausible but Wrong Code - Generates code that looks correct but has hidden bugs

Incomplete or Noisy Context - Lacks full understanding of the codebase

No Real Memory Between Tasks - Can't learn or remember from previous interactions

No Execution or Verification - Doesn't test or validate the code it generates

Loss of Control Risk - Potential to introduce unwanted changes to the codebase



What Are AI Agents?

PERCEPTION & REASONING

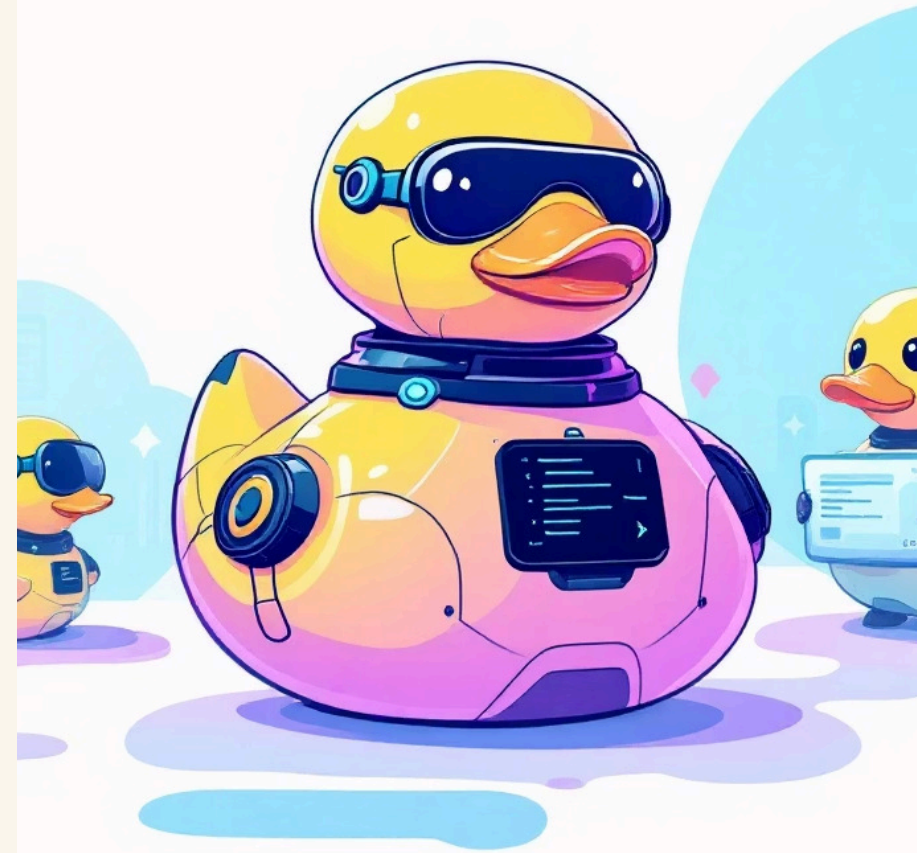
- Plan (planning + reasoning)
- Gather context independently

ACTION

- Read/write files
- Search the web
- Execute commands

ADAPTATION

- Iterate on errors
- Use tools (tooling)





Agentic Programming Workflow



Describe Task

Detailed prompt



Generate Code

Diff view for review



Review

Approve or modify

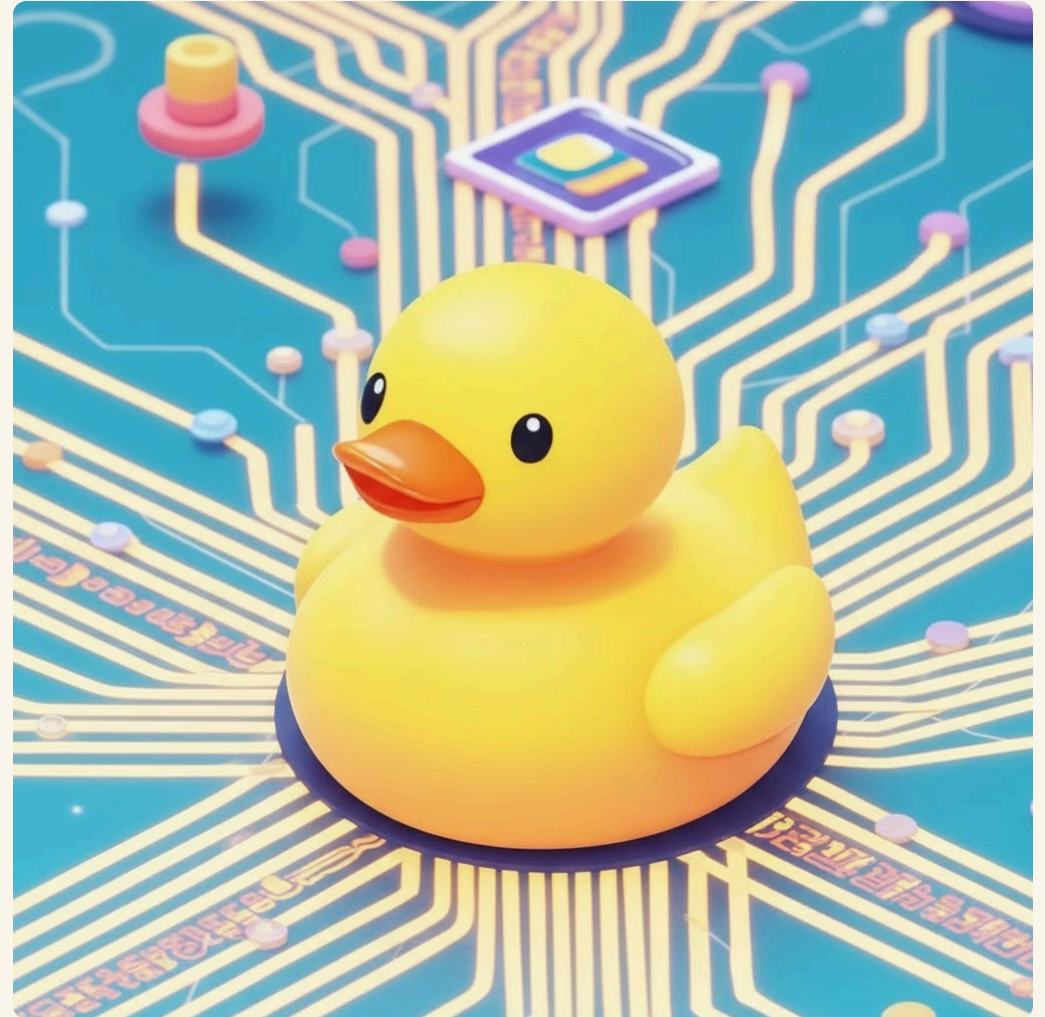


Iterate

Commit and repeat

Model Context Protocol (MCP) Servers

- Definition: MCP servers are standardized interfaces that extend the capabilities of AI agents.
- They allow agents to connect to external tools, data sources, and services.
- They offer a unified way for agents to access resources beyond their built-in functions.
- They enable seamless integration with various platforms and APIs.
- Key Advantage: They allow agents to interact with real-world systems and data.



Custom Agents

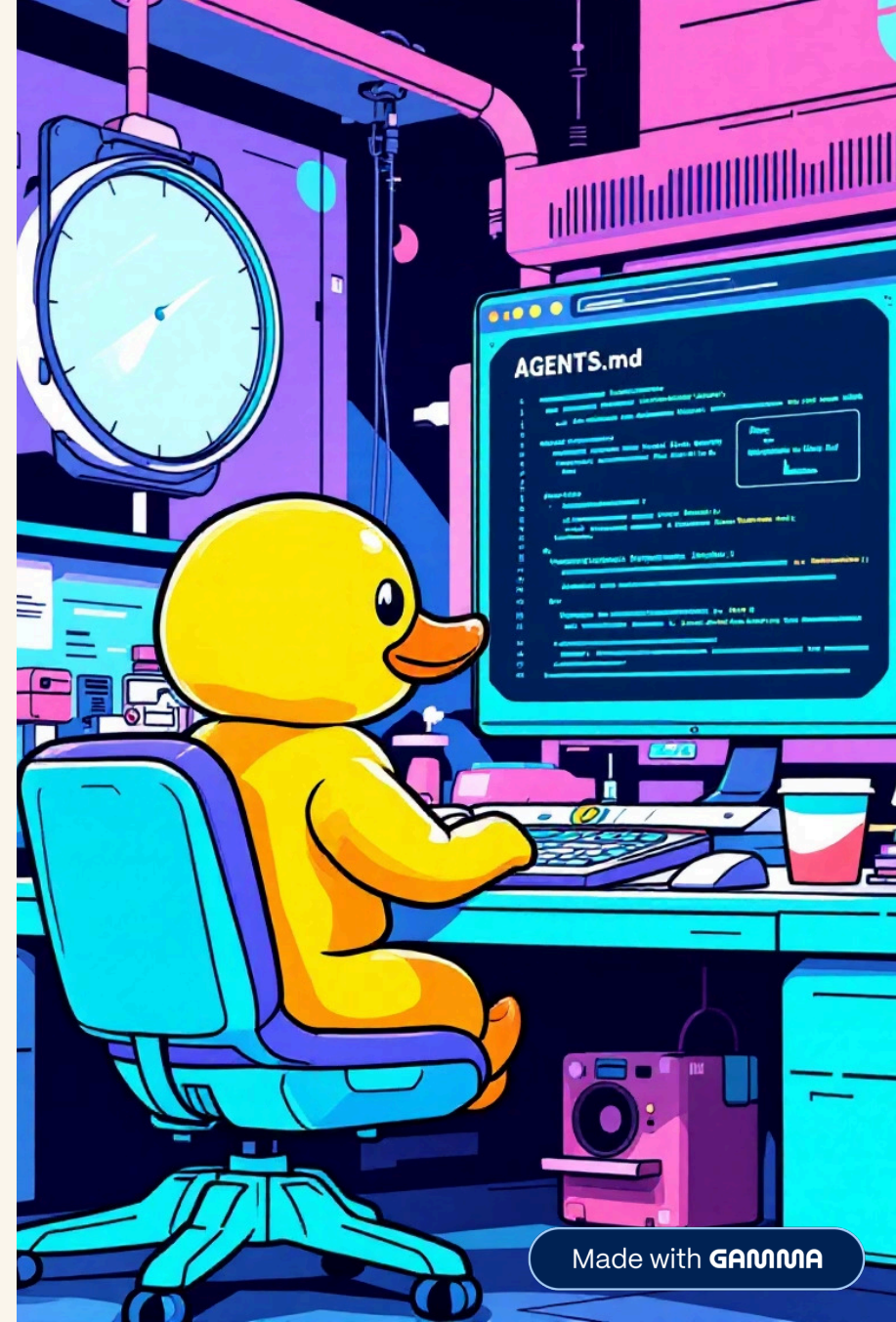
- Custom agents are specialized versions of Copilot designed for specific tasks
- They leverage tools and MCP servers for extended capabilities
- Enable task-specific optimization and domain expertise
- Can be tailored and chained to create powerful workflows



AGENTS.md Files

Introducing **AGENTS.md**, a structured format designed to guide AI coding agents within software projects. It complements traditional **README.md** files by providing essential context and instructions specifically tailored for autonomous coding.

- Provides detailed context and instructions for AI agents.
- Includes crucial build steps and testing procedures.
- Helps keep **README.md** focused on human contributors.
- Supports a wide range of AI coding tools like OpenAI's Codex and Google's Jules.
- An open, adaptable format for universal adoption.



Agent Skills

Agent Skills are collections of instructions and resources designed to enhance AI agent capabilities by providing procedural knowledge and contextual information.

- Package domain-specific knowledge
- Create new capabilities for agents
- Establish repeatable and reliable workflows
- Ensure interoperability with other systems

