OCT 25, 2023

AI Agents and the Future of Software

Why we think the next generation of software will be powered by AI agents.



By Jenny Xiao, Jay Zhao, and Val Gui

Leonis Capital · leoniscap.com/research/ai-agents-and-the-future-of-software/

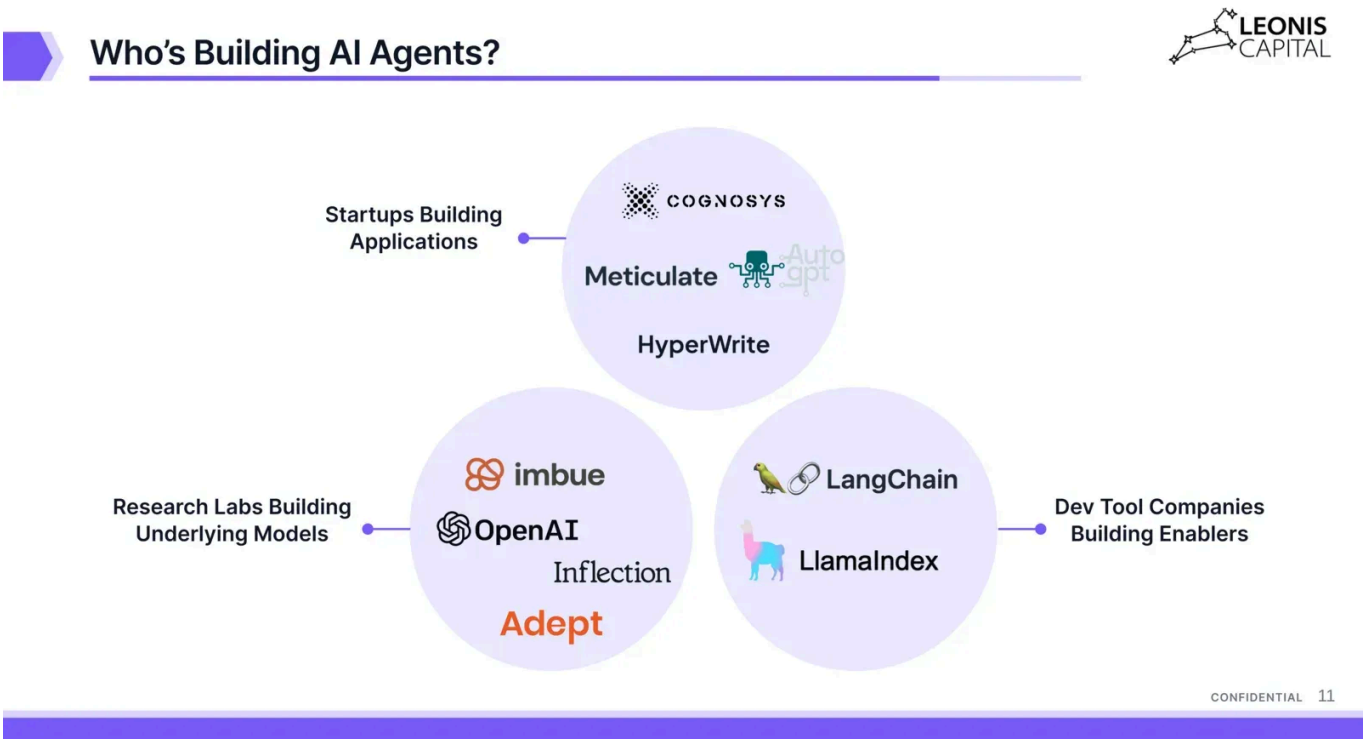


[Full webinar deck available here.]

AI has been a hot topic since 2022, but the rise of AI agents takes this fascination to a new level. At Leonis Capital, we are deeply invested in the future of AI, particularly the evolution of AI agents. In our recent webinar, we explored the latest academic research on AI agents and developed demos to showcase their autonomous capabilities, reasoning skills, and tool integrations. This blog post summarizes our findings on the current state and future potential of AI agents. Despite some limitations in their current capabilities, we are convinced that AI agents will drive the next generation of software, heralding the new age of Software 3.0.

What are AI Agents?

Let's start with the basics. AI agents are advanced systems capable of autonomous action in the real world. Unlike traditional chatbots or co-pilots, AI agents can make decisions, perform tasks, and learn from their environments with minimal human guidance. This autonomy is seen by many as a step toward Artificial General Intelligence (AGI).



The past year has seen significant strides in AI agent development. AutoGPT, an open-source project that went viral in March 2023, showcased AI agents' potential to set goals, devise plans, and execute them autonomously. However, the journey began much earlier. Research labs like OpenAI, Imbue, and Adept have been experimenting with AI agents for years. OpenAI developed reinforcement learning agents for complex games in 2018-2019, while Adept introduced ACT-1, an action-based Transformer model, in 2022.

Despite these advancements, AI agents face significant challenges. They often exhibit instability and inconsistency, struggle with user intent interpretation, and have limited reasoning capabilities. The lack of specialized tools and the potential for real-world harm are also critical concerns. As AI agents gain more capabilities, addressing these issues becomes increasingly important to ensure their safe and effective deployment.

Research Directions and Technological Frontiers

The good news is that many new research directions have emerged to address these current challenges. Here, we summarize three that could meaningfully solve the most apparent limitations in AI agents.

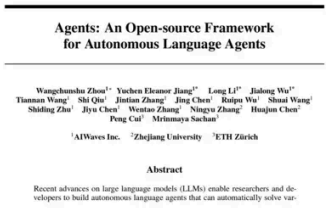
Research Direction 1: Agent Frameworks

Agent frameworks play a crucial role in improving the performance of agents. They decompose complex tasks into manageable subtasks, ensuring consistency and stability. Agent frameworks often contain reasoning structures like React and Reflection that allow models to reflect on their actions, optimizing performance through trial and error. They also incorporate both short-term and long-term memory to enhance the model's ability to recall past interactions and relevant context, leading to more robust and efficient AI systems. Additionally, agent frameworks integrate tools to maximize the potential of AI agents. Tools help agents perform specific tasks more efficiently and accurately, enabling them to tackle diverse challenges and become more versatile in real-world applications.

Research Direction 1: AI Agent Frameworks

LEONIS CAPITAL

- **Academic labs and startups** have both been working on AI agent frameworks.
- Proof-of-concept projects like AutoGPT and BabyAGI only unleash a small portion of LLM agents' capabilities. They rely on **short task descriptions**, which lead to **randomness** across different runs and **inconsistent outcomes**.
- These newer frameworks **support important agent features**, including:
  a. Planning (task decomposition + reflection);
  b. Memory;
  c. Tool usage;
  d. Multi-agent communication;
  e. Fine-grained control.



Agents: An Open-source Framework for Autonomous Language Agents

Wangchunshu Zhou[1*] Yuchen Eleanor Jiang[1*] Long Li[1*] Jialong Wu[1*] Tiannan Wang[1] Shi Qiu[1] Jintian Zhang[1] Jing Chen[1] Ruipu Wu[1] Shuai Wang[1] Shiding Zhu[1] Jiyu Chen[1] Wentao Zhang[1] Ningyu Zhang[2] Huajun Chen[2] Peng Cui[3] Mrinmaya Sachan[3]

[1]AIWaves Inc. [2]Zhejiang University [3]ETH Zürich

Abstract

Recent advances on large language models (LLMs) enable researchers and developers to build autonomous language agents that can automatically solve var-

Table 1: Comparison of Language Agent Frameworks

Framework	Tool Usage	Long-short Term Memory	Multi-Agent	Human-Agent Interaction	Symbolic Control
Transformers Agents	✓	✗	✗	✗	✗
LangChain	✓	✓	✗	✗	✗
Auto-GPT	✓	✗	✗	✗	✗
Gentopia	✓	✗	✗	✗	✗
XLang	✓	✗	✗	✗	✗
Meta-GPT	✓	✗	✓	✗	✗
Camel	✓	✗	✓	✗	✗
AgentVerse	✓	✓	✓	✓	✗
AGENTS	✓	✓	✓	✓	✓

Source: AIWaves, Zhejiang University, and ETH Zurich, "Agents: An Open-Source Framework for Autonomous Language Agents" (Sep 2023).

CONFIDENTIAL 19

Frameworks like Langchain and LlamaIndex have made strides in providing tools for AI agent development. These frameworks simplify the process of initial experimentation, making it easier

for developers to create and test AI agent products. However, they still lack comprehensive support for real-world AI agent deployment, which requires robust stability and performance optimization to handle the complexities and demands of practical applications.

Research Direction 2: Multi-Agent Systems

Imagine a team of specialized agents, each mastering a specific domain, working together to solve problems. This is the vision behind multi-agent systems. Each agent focuses on its niche, and when combined, they deliver more efficient and effective solutions. Collaborative frameworks like AutoGen and insights from Stanford's "Generative Agents" paper exemplify this approach, highlighting the power of AI-agent collaboration. This collaborative approach is poised to surpass the capabilities of a single, generalist model, bringing us closer to more versatile and powerful AI systems.

Research Direction 2: Multi-Agent Systems

LEONIS CAPITAL

- **Renewed interest in academia** in multi-agent systems.
- Key findings:
  a. Multi-agent systems **outperform** uni-agent systems;
  b. Agents can learn to **use other expert AI models**;
  c. **Communication** is key;
  d. Emergent social **behavior**;
  e. Real-world deployment is still difficult.



Figure 1: Generative agents are believable simulacra of human behavior for interactive applications. In this work, we demonstrate generative agents by populating a sandbox environment, reminiscent of The Sims, with twenty-five agents. Users can observe and intervene as agents plan their days, share news, form relationships, and coordinate group activities.

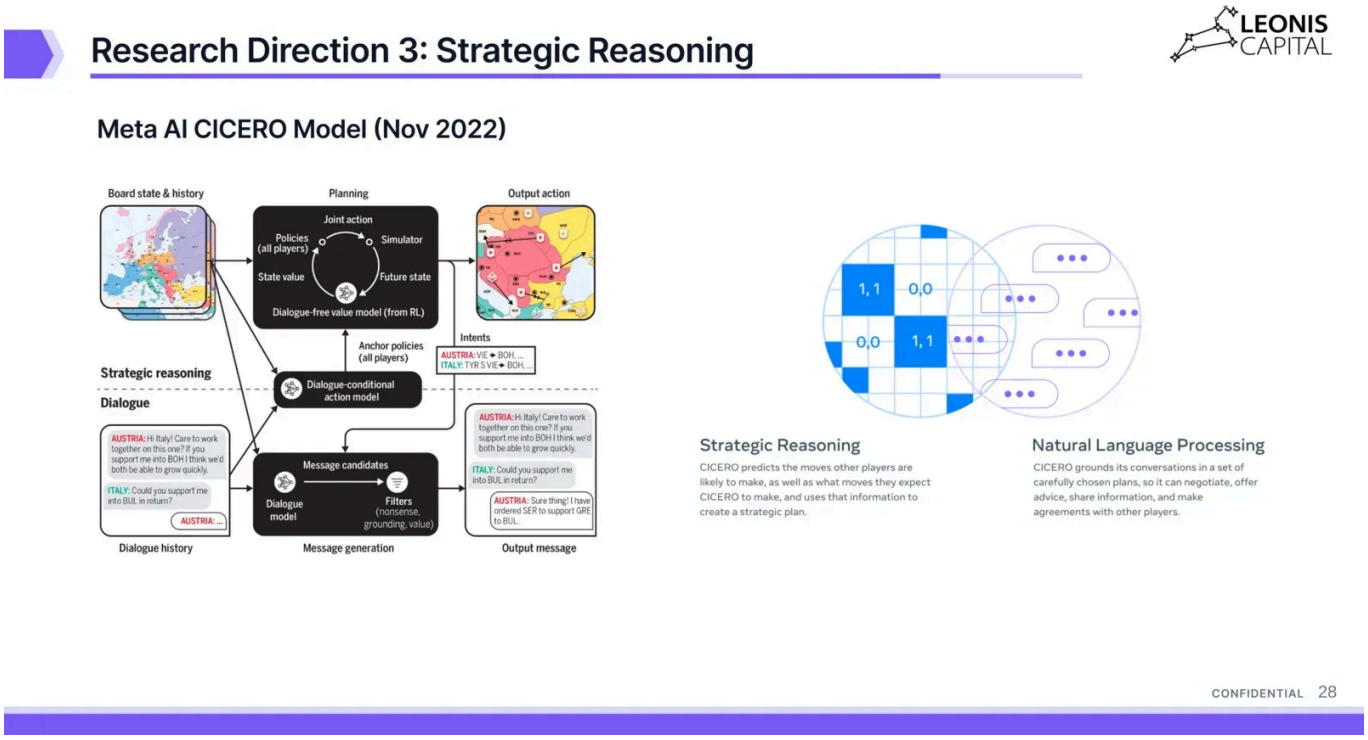
Source: Stanford University and Google, "Generative Agents: Interactive Simulacra of Human Behavior" (Apr 2023).

Research Direction 3: Strategic Reasoning

Strategic reasoning is the secret sauce for developing AI systems that can tackle complex, dynamic environments. It's all about the AI model's ability to think critically and make decisions based on long-term goals and optimization. Techniques like Chain of Thought and Tree of

Thought enable models to break down tasks and explore multiple possibilities, selecting the most optimal solutions. Self-reflection frameworks further enhance the model's ability to evaluate its performance and improve over time. Improvements in strategic reasoning have already enabled AI agents to become top players in strategy games like Diplomacy. This kind of strategic reasoning is vital for AI systems that need to make informed decisions and adapt to changing scenarios.

As we continue to push the boundaries of AI, these research directions offer a glimpse into the future of intelligent agents. The journey is just beginning, and the possibilities are endless.



Four Predictions about the Future of AI Agents

As AI technology continues to advance at a rapid pace, AI agents are poised to revolutionize the way we interact with software and the digital world. Based on current trends and research, we made four key predictions about the future of AI agents:

Prediction 1: Specialized Tools Will Empower Vertical Agents

Specialized tools will become critical for AI agent capabilities. In the near future, building specialized tools for AI will be a crucial aspect of a company's competitive advantage. Just as fine-tuning models and having a robust data moat are important today, giving AI agents access to specialized tools will significantly enhance their capabilities. For instance, allowing an AI agent to utilize an RNA sequencing library would enable it to perform complex, domain-specific tasks that it couldn't accomplish on its own. This trend suggests that companies developing unique, powerful tools for AI agents will have a significant edge in the market.

Prediction 2: Multi-Agent Systems Will Outperform Single-Agent Systems

While generalist models like GPT-4 are incredibly capable, specialized models are likely to outperform them in specific domains. The future of AI agents lies in multi-agent systems, where multiple specialized agents work together to solve complex problems. This approach combines the strengths of various domain-specific models, creating a more efficient and effective system than a single model attempting to master everything. As this technology develops, we can expect to see more sophisticated collaborations between AI agents, each bringing its unique expertise to the table.

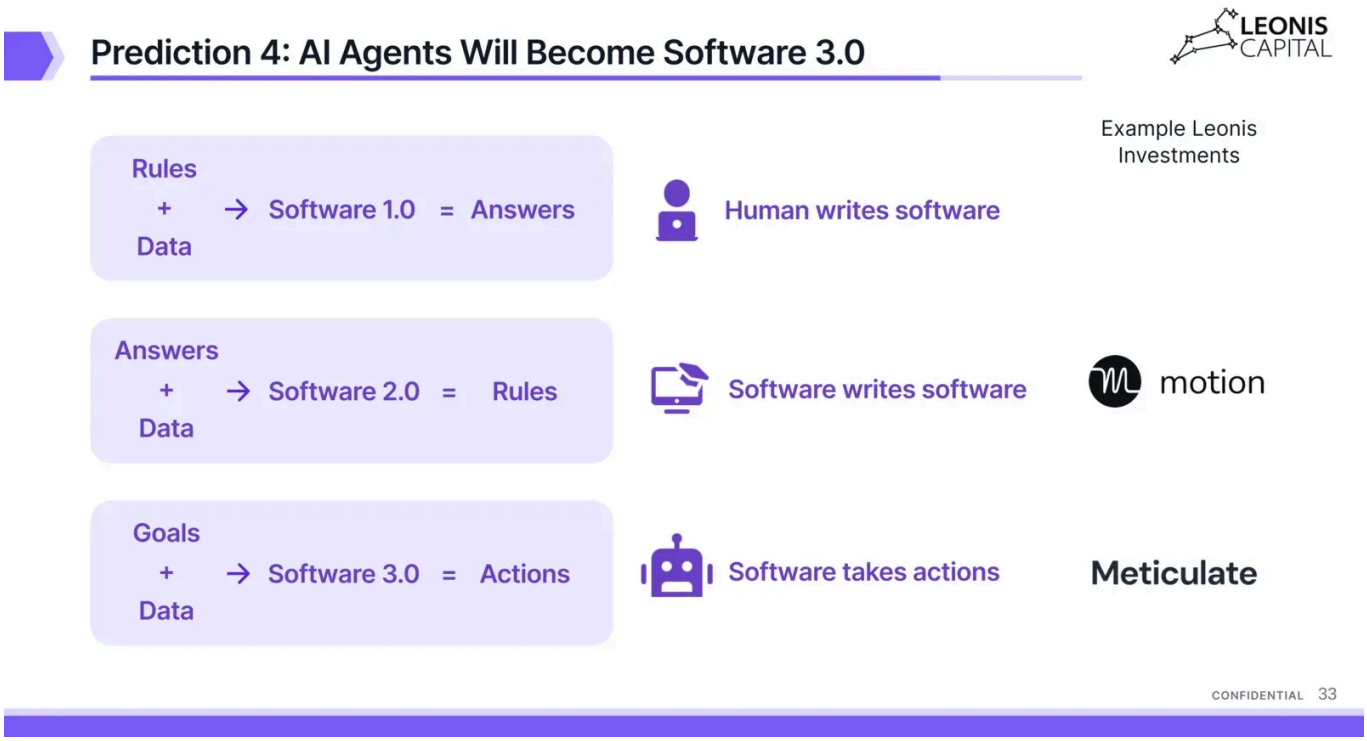
Prediction 3: AI Agent Frameworks Will Become the New Developer Tools

AI agent frameworks are already incorporating cutting-edge research to improve the performance of LLMs. As these agents become more prevalent in real-world applications, areas such as testing, observability, stability, and security will gain paramount importance. The performance and stability requirements for AI agents will be much higher than those for chatbots, given their potential real-world impact. This shift will likely lead to a new generation of development tools specifically designed for creating, testing, and maintaining AI agents, fundamentally changing how software is developed and deployed.

Prediction 4: AI Agents Will Usher in the Era of "Software 3.0”

The evolution of software can be seen in three distinct phases. Software 1.0 refers to traditional, non-AI-powered software with hard-coded rules, like early versions of Yahoo and eBay. Software 2.0 introduced AI-powered systems that can learn and create algorithms based on data, such as recommendation engines used by YouTube and TikTok. Now, we're on the cusp of Software 3.0, where AI agents can take autonomous actions in the real world. This transition is expected to unlock tremendous economic value and revolutionize how software interacts with and impacts our daily lives. As AI agents become more capable of understanding context, making decisions,

and taking actions, we'll see a fundamental shift in how we conceive of and interact with software.



As AI agents evolve to become more sophisticated, specialized, and deeply integrated into our digital infrastructure, we stand on the brink of a technological revolution. These intelligent agents are poised to transform industries, dramatically enhance productivity, and unlock possibilities that we can barely fathom today. The impact of AI agents will likely extend far beyond our current expectations, reshaping how we work, interact with technology, and solve complex problems. At Leonis Capital, we are not just excited about the future of AI agents; we are eager to partner with visionary startups and innovative founders who are pioneering the development of AI agents and pushing the boundaries of what's possible.

The era of AI agents is just beginning, and we believe the most extraordinary innovations are yet to come.