TẠP CHÍ NGHIÊN CỨU
PHẬT HỌC
CƠ QUAN NGÔN LUẬN CỦA TRUNG ƯƠNG GIÁO HỘI PHẬT GIÁO VIỆT NAM
ISSN: 2734-9195

Trí tuệ nhân tạo cần “chính niệm vận hành”

ISSN: 2734-9195 09:30 04/05/2026

Để giảm thiểu rủi ro, “lưới tương tác” phải trở thành một ranh giới an ninh thực sự: kiểm soát ủy quyền, giới hạn quyền lực và duy trì nhật ký hoạt động đầy đủ. Sự tham gia của con người cần được tích hợp sâu vào tầng thực thi.

Để chấm dứt sự lãng phí trong tự động hóa, doanh nghiệp cần triển khai một hạ tầng tương tác có khả năng “điều phục” cách các tác tử AI độc lập vận hành.

Khi trí tuệ nhân tạo cần đến “chính niệm vận hành”

Các tác tử AI hiện đã lan tỏa trong mạng lưới doanh nghiệp, tự suy luận nhiệm vụ và thực thi quyết định với mức độ tự chủ ngày càng cao. Tuy nhiên, khi những “thực thể số” độc lập này cần phối hợp công việc, trao đổi ngữ cảnh hay vận hành xuyên suốt nhiều môi trường đám mây khác nhau, hệ khung tương tác nhanh chóng bộc lộ sự suy yếu.



Con người, thay vì được giải phóng, lại trở thành “chất keo thủ công” kết nối những hệ thống rời rạc, phải quản lý các tích hợp mong manh, trong khi các quy

tắc về phân quyền và chia sẻ dữ liệu vẫn tồn tại một cách ngầm định.

Từ góc nhìn Phật học, đây là biểu hiện của một hệ thống vận hành thiếu **chính niệm** và **giới hạn (giới)**: khi các "tâm hành số hóa" hoạt động mà không có sự điều phục, không có nền tảng quy chiếu rõ ràng, thì sự hỗn loạn là điều tất yếu.

Một startup có tên Band, đặt trụ sở tại Tel Aviv và San Francisco, vừa ra khỏi trạng thái "stealth" (1) với vòng gọi vốn hạt giống trị giá 17 triệu USD nhằm giải quyết chính vấn đề hạ tầng này. Khoản đầu tư hỗ trợ CEO Arick Goomanovsky và CTO Vlad Luzin trong nỗ lực xây dựng một lớp tương tác chuyên biệt cho các hệ thống doanh nghiệp tự trị.

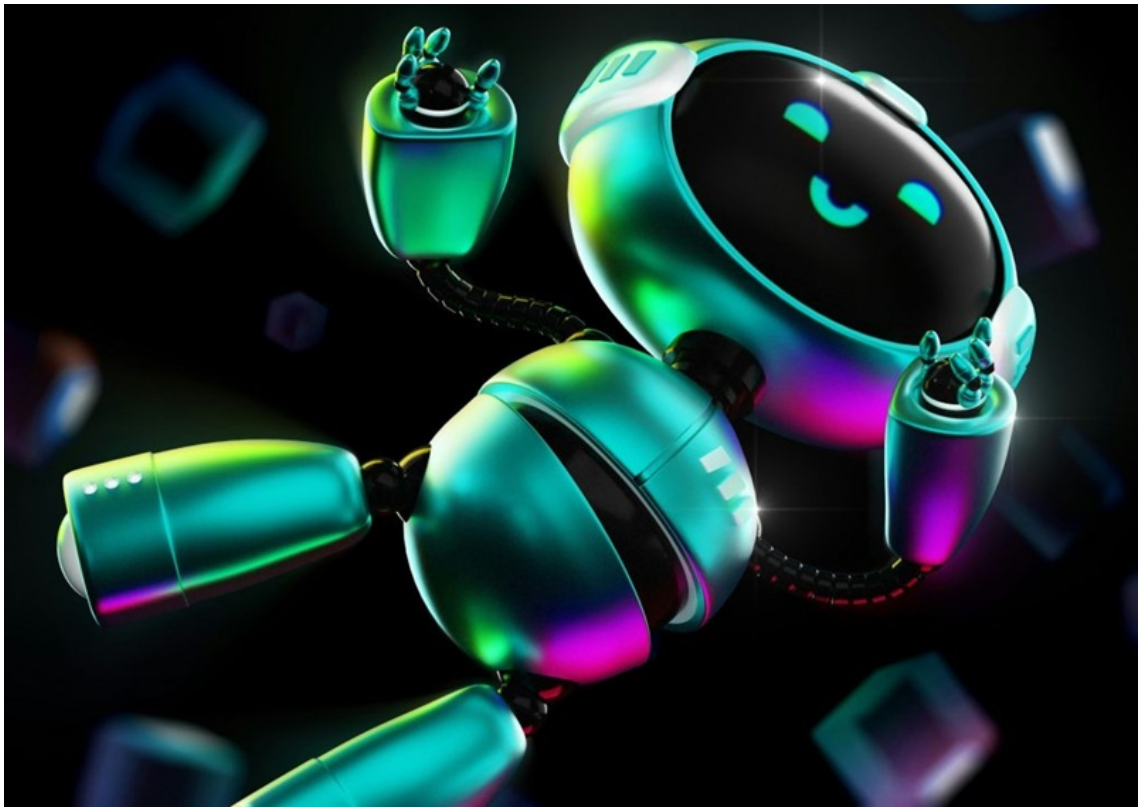
Khái niệm này phản chiếu những bước tiến trước đây của ngành điện toán: khi API cần các cổng chuyên dụng, hay khi microservices (2) đòi hỏi một "service mesh" (3) để vận hành ở quy mô lớn.

Khi các hệ thống phân tán gia tăng dưới sự sở hữu của nhiều nhóm nội bộ khác nhau, việc bổ sung thêm logic nghiệp vụ không thể giải quyết tận gốc sự bất ổn. Thay vào đó, độ tin cậy của tương tác đòi hỏi một lớp hạ tầng riêng biệt.

Ba chuyển dịch cốt lõi của thị trường

Thứ nhất, các tác tử tự trị đã vượt qua giai đoạn thử nghiệm để trở thành những thành phần vận hành thực sự, quản lý pipeline kỹ thuật, xử lý yêu cầu khách hàng và đảm nhiệm các tác vụ **bảo mật**. Việc ứng dụng trong doanh nghiệp không còn là tương lai mà đã là hiện tại.

Vấn đề cấp thiết không còn là "có dùng hay không", mà là: điều gì xảy ra khi các tác tử này phải cộng tác?



→ Nhìn dưới lăng kính Phật học: đây là lúc **“duyên khởi”** trở nên phức tạp. Khi nhiều nhân duyên tương tác mà thiếu một nguyên tắc điều hòa, hệ quả dễ rơi vào rối loạn.

Thứ hai, môi trường vận hành mang tính dị thể hoàn toàn. Các đội kỹ thuật xây dựng công cụ trên nhiều framework (4) khác nhau; các mô hình chạy trên những nền tảng đám mây cạnh tranh, sử dụng giao thức truyền thông khác nhau và phục vụ các chủ thể kinh doanh riêng biệt.

Không có một nhà cung cấp nào kiểm soát toàn bộ **hệ sinh thái**. Sự phân mảnh này không phải là tạm thời mà chính là hình dạng lâu dài của thị trường doanh nghiệp.

Thứ ba, một tầng tiêu chuẩn nền tảng đang dần hình thành. Những sáng kiến như Model Context Protocol (MCP) (5) giúp mô hình truy cập công cụ bên ngoài theo cách thống nhất. Các nỗ lực giao tiếp A2A cũng thiết lập các tham số hội thoại cơ bản.

Tuy nhiên, các giao thức này chỉ định nghĩa “cái bắt tay”, chứ không quản trị môi trường vận hành. Chúng không xử lý định tuyến, phục hồi lỗi, ranh giới quyền hạn, giám sát con người hay quản trị thời gian thực.

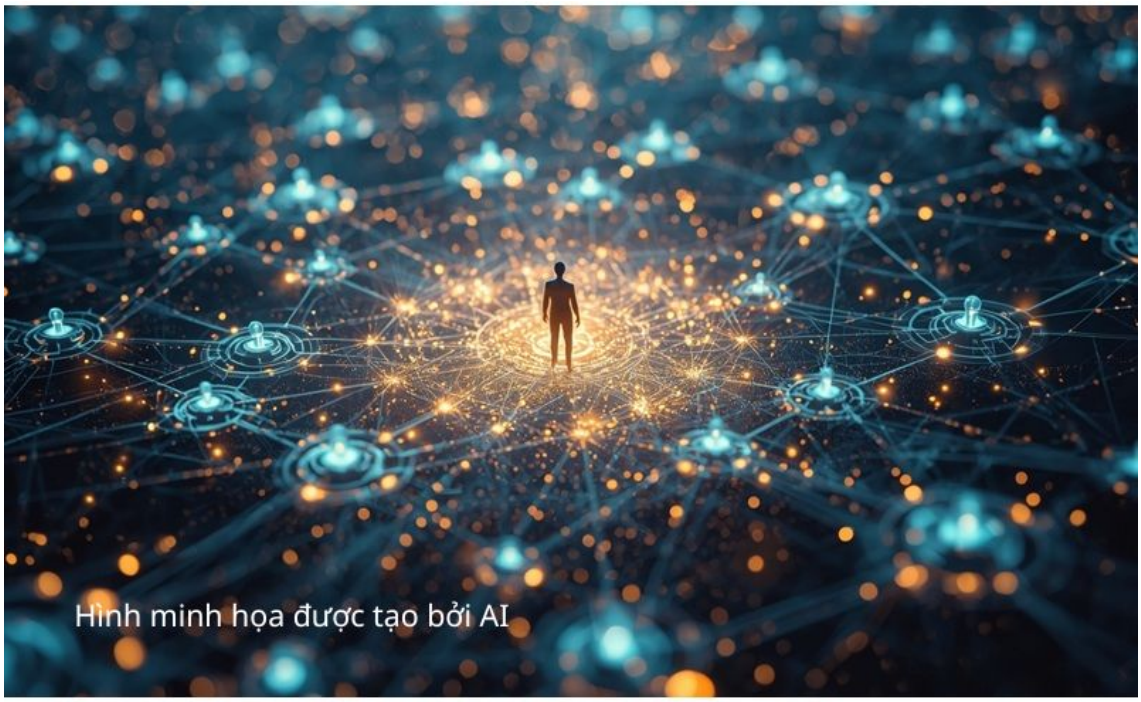
Band hướng đến việc lấp đầy khoảng trống hạ tầng này.

→ Nếu ví von theo giáo lý Phật học: giao thức chỉ là “lời nói”, còn hạ tầng tương tác chính là **giới luật và tăng đoàn**, đảm bảo mọi hành vi diễn ra trong trật tự và trách nhiệm.

Trách nhiệm tài chính của tự động hóa không kiểm soát

Việc triển khai các mô hình độc lập trên nhiều đơn vị kinh doanh tạo ra những thách thức tích hợp chồng chất. Nếu các tích hợp điểm-điểm phải được kết nối thủ công, chi phí bảo trì sẽ bào mòn lợi nhuận và làm chậm tiến độ sản phẩm.

Rủi ro tài chính không chỉ dừng ở chi phí tích hợp.



Khi các tác tử tự động truyền lệnh cho nhau mà không có một “bộ điều phối trung tâm”, chi phí tính toán có thể tăng vọt. Các quy trình suy luận đa tác tử yêu cầu gọi API liên tục tới các mô hình ngôn ngữ lớn đắt đỏ. Một lỗi định tuyến hoặc vòng lặp giữa hai tác tử “hiểu nhầm nhau” có thể tiêu tốn ngân sách đám mây chỉ trong vài giờ.

Các quy trình đa tác tử không được kiểm soát đe dọa tính dự đoán tài chính. Một cuộc “đàm phán tự động” giữa mô hình mua sắm nội bộ và mô hình nhà cung cấp bên ngoài có thể kích hoạt hàng trăm chu kỳ suy luận, khiến chi phí vượt xa giá trị giao dịch.

Do đó, hạ tầng tương tác cần tích hợp các “cầu dao tài chính”, tự động dừng những tương tác vượt ngưỡng ngân sách hoặc tài nguyên.

→ Đây là biểu hiện rất rõ của nguyên lý **tri túc (biết đủ)** trong Phật học: nếu không có giới hạn, mọi hệ thống, dù thông minh cũng sẽ tự đẩy mình vào lãng phí và khổ đau.

Gia cố tầng thực thi đa tác tử

Việc tích hợp các "nút **trí tuệ**" này với hệ thống doanh nghiệp truyền thống đòi hỏi nguồn lực kỹ thuật lớn. Các tổ chức tài chính và y tế vận hành trên những hệ thống dữ liệu nội bộ được bảo vệ nghiêm ngặt, từ mainframe (máy tính chủ) đến ERP (7) tùy biến.

Nếu không có hạ tầng tương tác vững chắc, nguy cơ sai lệch dữ liệu sẽ tăng theo từng bước tự động hóa. Ví dụ: một mô hình thanh toán khởi tạo giao dịch trong khi mô hình tuân thủ đồng thời đánh dấu tài khoản dẫn đến xung đột dữ liệu.

Lớp tương tác chính là nơi ngăn chặn những va chạm này, bằng cách áp đặt giới hạn năng lực và đảm bảo không có tác tử nào tự ý thay đổi hệ thống nguồn.

Các cơ sở dữ liệu vector (6), nơi lưu trữ "ký ức ngữ cảnh" cũng đặt ra thách thức tương tự. Khi dữ liệu phải di chuyển giữa các môi trường riêng biệt, nguy cơ suy giảm chất lượng thông tin xuất hiện nếu mô hình chỉ "hiểu lại" dữ liệu thay vì truy cập bản gốc đã được xác thực.

Ngăn chặn điều này đòi hỏi một "lưới tương tác trung tâm" có khả năng truy vết toàn bộ dòng chảy dữ liệu.

→ Điều này tương tự như việc giữ **chính kiến**: không diễn giải sai lệch, không "nghe qua lời kể", mà phải tiếp cận trực tiếp nguồn chân thực.

Rủi ro "ô nhiễm dữ liệu" còn kéo theo trách nhiệm pháp lý. Nếu một mô hình chăm sóc khách hàng vô tình tiếp nhận dữ liệu tài chính mật từ hệ thống kiểm toán, hậu quả có thể là vi phạm nghiêm trọng quy định.

Do đó, mọi tương tác cần được ghi log mật mã, đảm bảo khả năng truy vết.

Xem lưới giao tiếp như một "biên giới an ninh"

Thiết kế của nền tảng này bác bỏ ý tưởng một mô hình đơn lẻ kiểm soát toàn bộ doanh nghiệp. Thay vào đó, nó hướng đến một tập hợp các tác tử chuyên biệt, mỗi tác tử đảm nhiệm vai trò riêng nhưng phối hợp nhịp nhàng.

Hệ thống hoạt động độc lập với framework (8) và đám mây, tận dụng các công cụ sẵn có trên thị trường.

Band không tập trung vào giai đoạn phát triển, mà vào giai đoạn vận hành, khi mô hình rời "phòng thí nghiệm" để bước vào môi trường doanh nghiệp thực.

Quản trị là cốt lõi của chiến lược này. Một sai lầm phổ biến là xem quản trị như tính năng phụ, chỉ bổ sung sau khi triển khai.

Cách tiếp cận này thất bại khi áp dụng cho các hệ thống tự trị. Nếu quy tắc quyền hạn không rõ ràng và dữ liệu thiếu minh bạch, hệ thống sẽ không thể tạo dựng niềm tin dù về mặt kỹ thuật vẫn hoạt động.

Để giảm thiểu rủi ro, "lưới tương tác" phải trở thành một ranh giới an ninh thực sự: kiểm soát ủy quyền, giới hạn quyền lực và duy trì nhật ký hoạt động đầy đủ.

Sự tham gia của con người cần được tích hợp sâu vào tầng thực thi.

→ Đây chính là tinh thần **"con người làm chủ nghiệp"** trong Phật học: dù tự động hóa đến đâu, trách nhiệm và tỉnh thức vẫn phải quay về nơi con người.

Khi hạ tầng tương tác trở thành hệ "giới luật số"

Cơ chế cộng tác và kiểm soát quản trị phải nằm trên cùng một tầng hạ tầng. Nếu thiếu nền tảng này, việc chuyển từ mô hình đơn lẻ sang hệ sinh thái đa tác tử sẽ bị đình trệ bởi lỗi hệ thống và vi phạm tuân thủ.

Những doanh nghiệp thành công sẽ không chỉ tích lũy các phần mềm ấn tượng, mà sẽ đầu tư mạnh vào hạ tầng tương tác, nền tảng vô hình nhưng quyết định sự bền vững.

Từ góc nhìn Phật học, có thể xem hạ tầng này như một dạng **"giới luật trong thế giới số"**: không phải để hạn chế, mà để bảo vệ, điều hòa và hướng mọi hoạt động về sự ổn định, minh bạch và lợi ích lâu dài.

Tác giả: **Rian Daws**/Chuyển ngữ và biên tập: **Hoa Mạn**

Nguồn: **https://www.artificialintelligence-news.com/news/why-ai-agents-need-interaction-infrastructure/**

***

Chú giải thuật ngữ:

1] Trạng thái "stealth" (stealth mode): Giai đoạn một công ty hoạt động kín, chưa công bố sản phẩm hay chiến lược ra công chúng, nhằm tập trung hoàn thiện nội lực và tránh cạnh tranh sớm.

2] Microservices (kiến trúc vi dịch vụ): Mô hình thiết kế phần mềm chia hệ thống lớn thành nhiều dịch vụ nhỏ, độc lập, mỗi dịch vụ đảm nhiệm một chức năng riêng biệt.

3] Service mesh (lưới dịch vụ): Lớp hạ tầng trung gian điều phối giao tiếp giữa các microservices, đảm bảo an toàn, ổn định và kiểm soát luồng dữ liệu.

4] Quản lý pipeline kỹ thuật (engineering pipeline): Quá trình điều phối và tự động hóa chuỗi các bước kỹ thuật (viết mã, kiểm thử, triển khai...), giúp hệ thống vận hành trơn tru và hiệu quả.

5] Model Context Protocol (MCP): Chuẩn giao thức cho phép các mô hình AI truy cập công cụ, dữ liệu và chia sẻ ngữ cảnh theo một phương thức thống nhất.

6] Dữ liệu vector (vector data): Dạng dữ liệu được biểu diễn bằng các dãy số, giúp AI tìm kiếm và so sánh thông tin theo ngữ nghĩa thay vì chỉ dựa trên từ khóa.

7] ERP: Hệ thống hoạch định nguồn lực doanh nghiệp (ERP): là một hệ thống phần mềm tích hợp các quy trình kinh doanh cốt lõi như tài chính, nhân sự, sản xuất, chuỗi cung ứng và bán hàng vào một nền tảng duy nhất, thống nhất.

8] Framework: Bộ khung phát triển phần mềm tích hợp sẵn cấu trúc và công cụ, giúp xây dựng ứng dụng nhanh, đồng bộ và chuẩn hóa.