

Điện toán lượng tử: hiện tại và tương lai

Trần Doãn Huân, Viện Công nghệ Georgia, Atlanta, Hoa Kỳ
Vũ Ngọc Tước, Đại học Bách khoa Hà Nội, Hà Nội, Việt Nam

Công nghệ lượng tử đang trở thành trọng tâm chiến lược của nhiều quốc gia, tạo nên một cuộc cạnh tranh toàn cầu. Sáng kiến “Khởi nguyên lượng tử” (Quantum Genesis Initiative) của Hoa Kỳ được công bố tháng 6 năm 2026 với mục tiêu chế tạo một máy tính lượng tử kháng lỗi và có giá trị khoa học thực tiễn vào năm 2028. Trung Quốc, Anh, Nhật Bản, Canada, Úc, Đức, Pháp, Nga, Israel, và Singapore đều có những chương trình đường dài và tham vọng. Với hàng ngàn công ty hoạt động trên lĩnh vực này, chừng vài chục công ty tập trung vào việc chế tạo máy tính, và một số nguyên mẫu máy tính lượng tử ban đầu đã được trình làng. Trong lĩnh vực bảo mật, năm 2025, Trung Quốc công bố mục tiêu tạo ra bộ tiêu chuẩn Mật mã hậu lượng tử (PQC) riêng biệt, độc lập và không dựa trên các tiêu chuẩn của NIST (Hoa Kỳ) hay ETSI (Châu Âu)¹.

Viễn cảnh về một cuộc “Cách mạng lượng tử” sẽ đến, tiếp nối những gì công nghệ bán dẫn và trí tuệ nhân tạo đã mang lại cho nhân loại, là đặc biệt lôi cuốn. Tuy nhiên, vì nhiều lý do dễ hiểu, đã có những cường điệu và hiểu lầm khi nói về lĩnh vực “thời thượng” này.² Trong bối cảnh cuộc đua lượng tử toàn cầu đầy biến động, việc thực hiện đánh giá rủi ro chiến lược thông qua thái độ khách quan và duy lý là rất cần thiết. Đây là bộ lọc then chốt để bóc tách giá trị khoa học thực chứng khỏi các làn sóng cường điệu, từ đó đảm bảo hiệu quả tối ưu và tránh những sai lầm hệ thống trong phân bổ nguồn lực quốc gia và doanh nghiệp. Bài viết nhỏ này, với những giới hạn của nó, hướng về một cách nhìn như vậy đối với điện toán lượng tử, một trong ba trụ cột của công nghệ lượng tử.

Thế giới lượng tử kỳ lạ

Thế giới lượng tử kỳ lạ, nhưng không mới. Năm 2025 đánh dấu 100 năm ra đời của cơ học lượng tử, một lĩnh vực vật lý nghiên cứu bản thể của vật chất ở cấp độ nguyên tử. Trong thế giới mà kích thước và khoảng cách được đo bằng vài nanomet (1 phần tỷ của một mét) và nhỏ hơn, những viên gạch cơ bản như nguyên tử và điện tử hành xử không theo trực giác thông thường của chúng ta, và, chính bằng cách đó, mang lại những hiệu ứng và công dụng chưa từng có. Chúng vừa là sóng, vừa là hạt (wave-particle duality), chúng có thể đồng thời ở nhiều trạng thái khác nhau (quantum superposition), chúng có thể “rối vào nhau”³ theo cách chỉ có ở thế giới kỳ lạ này (quantum entanglement), và không cho phép chúng ta biết “tất cả mọi thông tin” về chúng (uncertainty principles). Cơ học lượng tử được mô tả bằng một hệ thống toán học tuyệt đẹp và được giảng dạy trong trường đại học ở mọi nơi trên thế giới qua nhiều thế hệ.

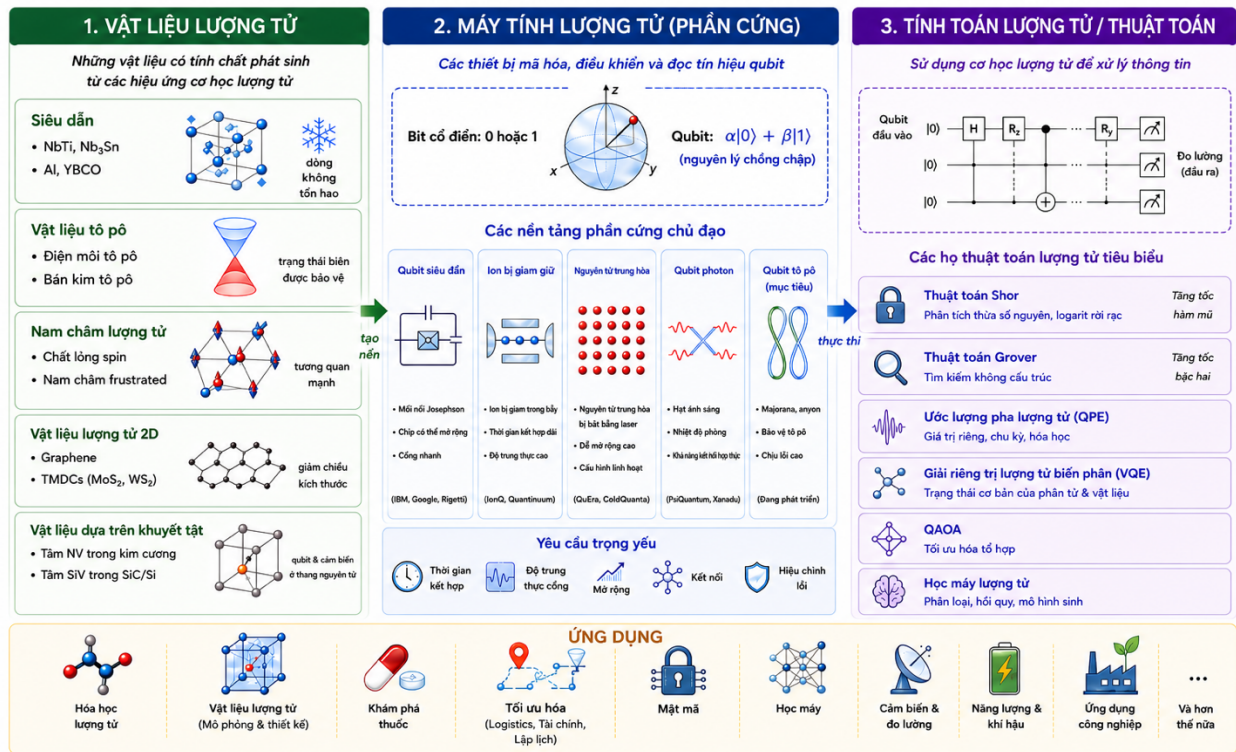
Cuộc cách mạng mà chúng ta đang nói tới cũng không phải lần đầu tiên vật lý lượng tử tạo nên bước nhảy công nghệ. Theo nghĩa đó, cuộc cách mạng lượng tử lần thứ nhất bắt đầu từ khoảng những năm 1940, mang lại vật liệu bán dẫn, transistor, mạch tích hợp, liên lạc vệ tinh và định vị

¹ *Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC)*, https://www.niccs.org.cn/niccs/home/content/1937426388645056512/content_1937426388645056512.html

² *Quantum computing has a hype problem*, <https://www.technologyreview.com/2022/03/28/1048355/quantum-computing-has-a-hype-problem>; *Quantum computer researcher warns that the industry is full of ridiculous hype*, <https://futurism.com/the-byte/quantum-computers-ridiculous-hype>; *Oxford scientist says greedy physicists have overhyped quantum computing*, <https://thenextweb.com/news/oxford-scientist-says-greedy-physicists-overhyped-quantum-computing>; *Disentangling the facts from the hype of quantum computing*, <https://spectrum.ieee.org/ieec-quantum-week>, vv.

³ Quantum entanglement thường được dịch ra tiếng Việt bằng rối lượng tử, vướng víu lượng tử, hay liên đới lượng tử, và có lẽ chúng ta vẫn chưa có một cách dịch tối ưu.

toàn cầu, laser, pin quang điện, kỹ thuật chụp cộng hưởng từ, và vô vàn công nghệ khác đã định hình cuộc sống hiện đại. Chuyển sang *cuộc cách mạng lượng tử lần thứ hai*, chồng chập lượng tử (quantum superposition), giao thoa lượng tử (quantum interference), và rối lượng tử (quantum entanglement), các hiệu ứng mang bản chất lượng tử thuần túy và sâu sắc, đóng vai trò trung tâm. Một vài kỳ vọng nổi bật bao gồm *điện toán lượng tử*, *viễn thông lượng tử*, *cảm biến lượng tử*, *mật mã lượng tử*, và nhiều nữa. Khái niệm hai cuộc cách mạng lượng tử được đưa ra bởi Jonathan Dowling và Gerard Milburn năm 2002⁴ và bởi Alain Aspect năm 2004.⁵ *Cách nhìn này là đủ rộng, mang tính kế thừa, và hợp lý để nói về công nghệ lượng tử.*



Hình 1. Phác thảo sơ bộ về hệ sinh thái điện toán lượng tử. Một cách gián lược, vật liệu lượng tử nhắm tới các vật liệu/thiết bị mà tính chất của chúng mang đặc tính lượng tử điển hình, có thể dùng để chế tạo máy tính lượng tử. Với thuật toán và tính toán lượng tử, vật lý lượng tử được dùng để xử lý thông tin. Ứng dụng của điện toán lượng tử có thể bao gồm thiết kế vật liệu và thuốc, mật mã lượng tử, vv.

Bài viết này tập trung vào điện toán lượng tử, lĩnh vực mang theo nó cả một hệ sinh thái khoa học đỉnh cao, đa dạng, và đang phát triển mạnh mẽ. Trong một cách phân loại đơn giản (Hình 1), hệ này bao gồm vật liệu lượng tử, máy tính lượng tử, và các thuật toán và phương pháp tính toán lượng tử.⁶ Nghiên cứu về vật liệu lượng tử là chủ đề quan trọng của vật lý và khoa học vật liệu trong khi các nhà toán học, vật lý, và khoa học máy tính làm việc với thuật toán và tính toán lượng tử.⁷ *Chế tạo một máy tính lượng tử đủ mạnh cho các vấn đề thực tiễn và có khả năng kháng lỗi là*

⁴ J. Dowling, G. Milburn, *Quantum Technology: The Second Quantum Revolution*, <https://arxiv.org/abs/quant-ph/0206091>.

⁵ J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*, Cambridge University Press, 2004.

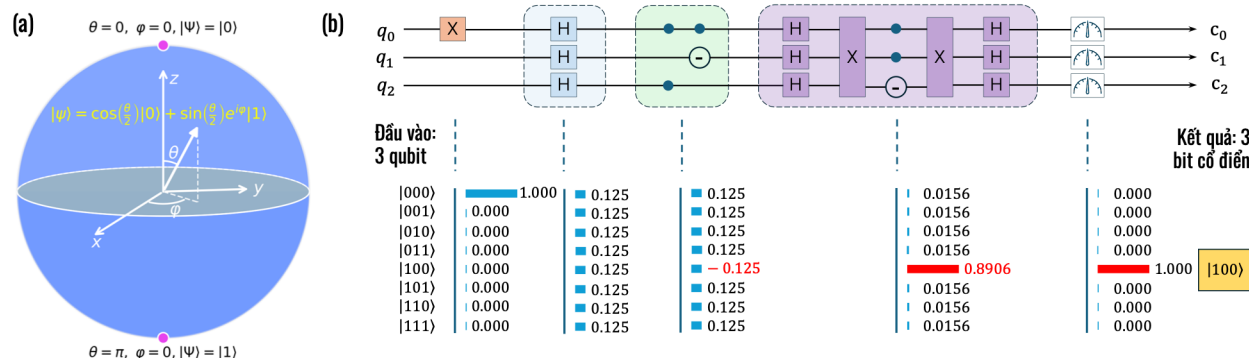
⁶ Cách phân loại này không nhất thiết là đầy đủ và hợp lý nhất, và chỉ được dùng cho mục đích của bài này.

⁷ Các phương pháp như density functional theory (DFT) hay quantum Monte Carlo không nằm trong phân loại này.

thách thức lớn cho các nhà công nghệ, vật lý, khoa học vật liệu, khoa học máy tính, và, ở tầm cao này, là cả các nhà quản lý và làm chính sách. Chúng ta dường như vẫn cách mục tiêu này một khoảng thời gian, và năm 2028 có thể sẽ là một thời điểm thú vị, như nhắc đến ở phần đầu. Trong khi chờ đợi, thì những nguyên mẫu đã được công bố vẫn còn rất sơ khai và chưa giải được những bài toán thực tiễn mà máy tính thông thường đã làm được.

Nguồn gốc sức mạnh của máy tính lượng tử

Đến đây, ngôn ngữ của chúng ta cần “lượng tử” hơn một chút. Máy tính cổ điển dùng hai trạng thái nhị phân (0 và 1) của một đơn vị cơ bản (bit) để lưu giữ và xử lý thông tin. Máy tính lượng tử sử dụng “qubit”, mà, theo nguyên lý *chồng chập lượng tử*, có vô số trạng thái khả dĩ. Mỗi một trong số đó là một tổ hợp tuyến tính của $|0\rangle$ và $|1\rangle$ với hai trọng số có bản chất xác suất, gọi là biên độ xác suất. Không gian trạng thái lượng tử của một qubit thường được biểu diễn bởi mặt cầu Bloch (Hình 2a). Với hệ nhiều qubit, không gian trạng thái không đơn giản chỉ gồm tích trực tiếp của những mặt cầu này (cho các qubit độc lập), mà còn gồm một tập hợp lớn hơn các trạng thái phức hợp của các qubit khi chúng “rối vào nhau” (entangled states). Các thuật toán sẽ hoạt động trong không gian trạng thái này, sử dụng, chẳng hạn, giao thoa lượng tử, để lựa chọn lời giải đúng (tối ưu) cho bài toán với *một tốc độ không máy tính cổ điển nào làm được*.



Mặt cầu Bloch các trạng thái lượng tử của một qubit

Minh họa nguyên lý thuật toán Grover

Hình 2. (a) Mặt cầu Bloch, biểu diễn của không gian trạng thái lượng tử của một qubit. Trạng thái cơ sở $|0\rangle$ và $|1\rangle$ nằm ở tọa độ -1 và $+1$ trên trục z . Với mọi giá trị khả dĩ của góc θ và góc phương vị φ , $|\Psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\varphi}|1\rangle$ là một trạng thái khả dĩ, và có thể ở bất kỳ đâu trên mặt cầu. (b) Minh họa nguyên lý thuật toán tìm kiếm lượng tử Grover, bao gồm cổng Pauli-X (NOT) X, Hadamard H, Oracle (xanh nhạt), Diffuser (tím nhạt), và phép đo kết quả đầu ra.

Hình 2(b) minh họa nguyên lý thuật toán tìm kiếm Grover⁸ với 3 qubit. Hệ lượng tử này bắt đầu ở trạng thái cơ sở $|000\rangle$ với biên độ xác suất bằng 1, các biên độ khác bằng 0. Tiếp theo, trạng thái chồng chập lượng tử được khởi tạo, hệ lượng tử tiến hoá theo thời gian trong không gian trạng thái, và toàn bộ $2^3 = 8$ biên độ xác suất được phân bố lại. Với giao thoa lượng tử, biên độ của trạng thái đích $|100\rangle$ được khuếch đại trong khi các biên độ khác giảm. Cuối cùng, phép đo làm hệ lượng tử sụp đổ về trạng thái cổ điển $|100\rangle$, trả lại kết quả cần tìm. Như vậy, *máy không phải lần lượt duyệt qua tất cả các trạng thái, và điểm khác biệt này tạo nên tốc độ vượt trội*.

⁸ L. K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery. pp. 212-219; <https://dl.acm.org/doi/10.1145/237814.237866>

Bức tranh nguyên lý này đẹp, và “có rất nhiều gai”. Thuật toán Grover về lý thuyết mang lại khả năng tăng tốc mạnh mẽ, nhưng thực tế hiệu quả bị giới hạn bởi tốc độ nhập/xuất dữ liệu lượng tử, đặc biệt là khi qRAM, một yếu tố phần cứng hiện vẫn chưa tồn tại ở dạng thương mại⁹. Bên cạnh nhập xuất dữ liệu, thuật toán lượng tử, và nhiều vấn đề khác, chúng ta điếm qua hai thách thức lớn: phần cứng và khả năng “chuyển thể” sang ngôn ngữ lượng tử, tất cả đều ảnh hưởng nghiêm trọng đến bức tranh lý tưởng này.

Phần cứng: qubit, kết hợp lượng tử, và hiệu chỉnh lỗi

Các công nghệ chế tạo qubit bao gồm qubit siêu dẫn (IBM, Google, Rigetti), qubit ion bẫy (Quantinuum, IonQ), qubit nguyên tử trung hòa (Pasqal, QuEra), qubit quang tử (PsiQuantum, Xanadu), qubit tô pô (topological qubits) (Microsoft, đang phát triển), và qubit từ thông siêu dẫn (superconducting flux qubits) trong máy ủ lượng tử (quantum annealer) của D-Wave. Thường thì những qubit này phải hoạt động ở những điều kiện khắt khe như nhiệt độ cực thấp (cỡ âm 200 độ C với qubit siêu dẫn), kết hợp với từ trường rất cao (cỡ 20000 lần từ trường trái đất cho qubit tô pô). Vận hành ổn định những *qubit vật lý* này rất khó vì chúng rất nhạy cảm với môi trường, trong khi những quá trình có bản chất lượng tử như phát xạ tự phát làm tiêu tán năng lượng và cuối cùng, dẫn đến mất kết hợp lượng tử (decoherence) và phát sinh lỗi.

Quá trình hiệu chỉnh lỗi thường cần một số lượng rất lớn qubit vật lý để lưu trữ lượng thông tin mà, về mặt lý thuyết, chỉ cần một qubit. Năm 2025, Google dùng 101 qubit vật lý trên bộ vi xử lý lượng tử (Quantum Processing Unit - QPU) Willow để mã hóa thành công một qubit logic (sau hiệu chỉnh lỗi) khả dụng mà tỷ lệ lỗi giảm khi tăng khoảng cách mã. IBM công bố bộ vi xử lý Heron r3 với 156 qubit vật lý, nhưng sai số của cổng hai qubit (2Q gate) và khả năng tích lũy lỗi của mạch quy mô lớn vẫn là rào cản lớn để đạt được lợi thế lượng tử thực tiễn.¹⁰ QPU Orion-Gamma của Pasqal (Pháp)¹¹ với 140 qubit vật lý nhưng chưa được xác nhận như một qubit sau hiệu chỉnh lỗi. Một trung tâm dữ liệu lượng tử không chỉ bao gồm các máy tính lượng tử hoạt động độc lập mà còn là các cụm bộ xử lý lượng tử (QPU) được kết nối với nhau. Việc xây dựng và vận hành các hệ thống này đặt ra những thách thức kỹ thuật hết sức to lớn.

Khi nói đến một QPU có bao nhiêu qubit vật lý, chúng ta mới nhìn một mặt của vấn đề, và cách nhìn này dễ dẫn đến hiểu lầm. Nói như Giáo sư Sankar Das Sarma, một trong những nhà khoa học lượng tử được kính trọng nhất thế giới từ Đại học Maryland, Hoa Kỳ, trong bài báo “Điện toán lượng tử đang bị cường điệu hoá”¹² năm 2022, thì

Các hệ qubit mà chúng ta đang có là một thành tựu khoa học vô cùng ấn tượng. Tuy nhiên, chúng vẫn chưa đưa chúng ta đến gần hơn một máy tính lượng tử có thể giải quyết những bài toán thực sự có ý nghĩa trong thực tế. Điều này cũng giống như việc cố gắng chế tạo một chiếc điện thoại thông minh hiện đại bằng các đèn điện tử chân không của đầu thế kỷ XX. Bạn có thể ghép 100 đèn điện tử lại với nhau để chứng minh về mặt nguyên lý rằng, nếu một ngày nào đó có thể khiến 10 tỷ đèn hoạt động đồng bộ và ổn định, bạn sẽ tạo nên những điều kỳ diệu. Tuy nhiên, điều còn thiếu chính là bước đột phá tương đương với sự ra đời của mạch tích hợp và bộ xử lý trung tâm, những công nghệ đã mở đường cho điện

⁹ *QRAM: A Survey and Critique*, Quantum 9, 1922 (2025); <https://quantum-journal.org/papers/q-2025-12-02-1922/>

¹⁰ *Towards utility-scale electronic structure with sample-based quantum bootstrap embedding*, Digital Discovery 5, 945-956 (2026); <https://doi.org/10.1039/d5dd00416k>

¹¹ Trang chủ Pasqal: <https://www.pasqal.com/>

¹² *Quantum computing has a hype problem*, <https://www.technologyreview.com/2022/03/28/1048355/quantum-computing-has-a-hype-problem>

thoại thông minh ngày nay. Trên thực tế, nhân loại đã phải mất khoảng 60 năm với vô số thách thức kỹ thuật để đi từ phát minh transistor đến điện thoại thông minh, mà không cần bất kỳ khám phá vật lý mới nào trong suốt quá trình đó.

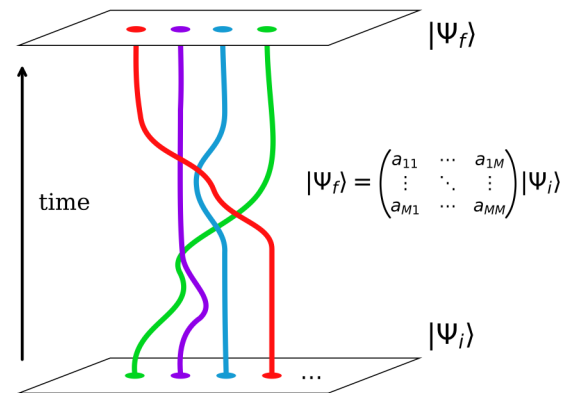
Không phải mọi công nghệ qubit đều nhạy cảm với lỗi như nhau. Một qubit tô pô (topological qubit) gồm một tập hợp các anyon (xem Hình 3), một loại chuẩn hạt không giao hoán có thể xuất hiện trong một số vật liệu bán dẫn hai chiều đặt trong từ trường cực lớn và nhiệt độ cực thấp. Trạng thái lượng tử của qubit này tiến hoá dựa trên thao tác hoán đổi vị trí của từng cặp anyon, về nguyên tắc không nhạy cảm với lỗi. Lý do là vì các thao tác hoán đổi vị trí này tạo nên các đường xoắn trong không thời gian (Hình 3), và giá trị của mỗi chuỗi hoán đổi chỉ phụ thuộc vào số, trình tự, và bản chất của thao tác hoán đổi, tức là vào “tô pô” của các đường không thời gian, mà không chịu ảnh hưởng bởi nhiễu. Ý tưởng này được đề xuất bởi Alexei Kitaev năm 1997¹³ và hiện đang được theo đuổi bởi Microsoft.

Người viết (TDH), sau khi bảo vệ luận án về một cách định lượng rối lượng tử trong một lớp mô hình các anyon¹⁴, hỏi Giáo sư hướng dẫn Thây ước đoán khi nào thì máy tính lượng tử tô pô có thể được chế tạo? Câu trả lời là “50 năm, 100 năm, tôi cũng không biết chắc”. Đã 16 năm kể từ ngày đó, đã có những bước tiến nhất định trong lĩnh vực này, và chúng ta hy vọng những tin tức tốt đẹp trong tương lai.

“Chuyển thể” bài toán sang ngôn ngữ lượng tử

Một thách thức khác là làm cách nào để phát biểu vấn đề cần giải quyết bằng ngôn ngữ lượng tử. Trong bức tranh nguyên lý mô tả ở Hình 2b, thuật toán Grover có đối tượng là một cơ sở dữ liệu. Dù lớn, hệ thống này có thể dễ dàng được biểu diễn bằng một hệ lượng tử gồm N qubit sao cho 2^N lớn hơn kích thước của nó, và sau đó hệ tự tiến hoá trong khuôn khổ thuật toán được thiết lập. Với các vấn đề khác, chuyển thể sang ngôn ngữ lượng tử phức tạp hơn nhiều, và trong giai đoạn hiện tại, việc này quan trọng không kém chính bản thân phần cứng máy tính.

Khoảng năm 2019, người viết (TDH) khảo sát một máy tính (ù) lượng tử (quantum annealer) của hãng D-Wave Quantum Inc. (Canada)¹⁵ cho tính toán và tối ưu hoá năng lượng của một hệ lượng tử. Đây là bài toán cơ bản nhất của thiết kế vật liệu và thiết kế thuốc mà phương pháp phiếm hàm mật độ (DFT) thông thường có thể làm phần nào, dù chậm. Kết luận thu được là, với cấu hình phần cứng khi đó, máy của D-Wave chỉ dùng được cho những mô hình rất đơn giản (chẳng hạn, Ising) của một chuỗi các hạt lượng tử mà mỗi hạt chỉ tương tác với một vài hạt gần nhất. Mức năng lượng của một vật liệu phức tạp hơn nhiều, không thể quy về dạng Ising, và vì thế không thể giải quyết



Hình 3. Tiến hoá của trạng thái lượng tử của một qubit tô pô bằng toán tử hoán đổi vị trí. Ma trận tiến hoá thể hiện trong hình phụ thuộc vào số lượng, trình tự, và bản chất của các hoán đổi, tức là vào “tô pô” của các đường không thời gian, mà không chịu ảnh hưởng của nhiễu.

¹³ A. Kitaev, *Fault-tolerant quantum computation by anyons*, Annals of Physics 303, 2-30 (1997).

¹⁴ *Entanglement and bond fluctuations in random singlet phases*, http://purl.flvc.org/fsu/fd/FSU_migr_etd-1533

¹⁵ Trang chủ: <https://www.dwavequantum.com/>

được. Phù hợp với kết luận này, những công bố khoa học sử dụng D-Wave cho đến năm 2026 cũng vẫn xoay quanh mô hình Ising.¹⁶

Vấn đề này không chỉ máy của D-Wave gặp phải. Năm 2026, các nhà khoa học từ Pasqal công bố một bài báo¹⁷ mô tả kết quả của máy tính lượng tử của công ty, sử dụng QPU Orion-Alpha cho một mô hình Ising. *Đối với các doanh nghiệp khởi nghiệp mà sản phẩm hướng tới người dùng hoạt động khoa học chuyên nghiệp, các bài báo một kênh tiếp cận thị trường đặc thù và đặc biệt quan trọng.* Nói cách khác, chúng ta có thể nhìn vào những bài báo như thế này để thấy kết quả tốt nhất và mới nhất hiện nay.

Kết luận

Công nghệ lượng tử là một lĩnh vực khoa học và công nghệ đỉnh cao, và đang được nghiên cứu rất tích cực trên phạm vi thế giới. Cuộc chạy đua toàn cầu đang tạo ra áp lực “bây giờ hoặc không bao giờ” cho các quốc gia đang phát triển trong việc xây dựng hạ tầng tri thức lượng tử để tránh bị gạt ra khỏi nền tảng an ninh và kinh tế toàn cầu trong thập kỷ tới. Tuy nhiên, việc này nên được thực hiện một cách khách quan, duy lý, và bền vững. Có lẽ một định hướng phù hợp là “tính đường dài và đi từng bước”.

¹⁶ *Phase transitions in a programmable quantum spin glass simulator*, Science 361, 162 (2018), <https://www.science.org/doi/10.1126/science.aat2025>; *Observation of topological phenomena in a programmable lattice of 1,800 qubits*, Nature 560, 456 (2018), <https://www.nature.com/articles/s41586-018-0410-x>; Proposal for Estimating the Energy Gap of the Transverse-Field Ising Hamiltonian Using a D-Wave Quantum Annealer, <https://arxiv.org/abs/2607.21940>

¹⁷ *Identifying hard native instances for the maximum-independent-set problem on neutral-atom quantum processors*, Physical Review Applied 25, 034085 (2026); <https://journals.aps.org/prapplied/abstract/10.1103/8gfv-ll1f>