محاسبات کوانتومی

چگونه کار می‌کند و چرا این فناوری می‌تواند دنیا را تغییر دهد

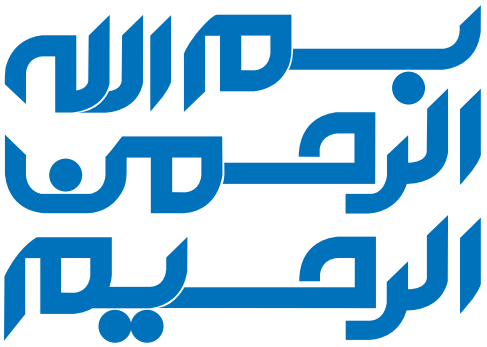
آمیت کاتوالا

کمیل علی‌تقوی

راه کار

WIRED

انتشارات راه پرداخت


بسم الله
الرحمن
الرحيم

سرشناسه: کاتوالا، آمیت. Katwala, Amit
عنوان و نام پدیدآور: محاسبات کوانتومی: چگونه کار می‌کند و چرا این فناوری می‌تواند دنیا را تغییر دهد/ آمیت کاتوالا ؛ [ترجمه] کمیل علی‌تقوی؛ ویراستار ارشد مینا والی.
مشخصات نشر: تهران: راه پرداخت، ۱۴۰۱.
مشخصات ظاهری: ۸۸ص.
شابک: ۹۷۸-۶۲۲-۷۷۰۲-۲۵-۵
وضعیت فهرست نویسی: فیپا
یادداشت: عنوان اصلی: Quantum computing : how it works and how it could change the world.
عنوان دیگر: چگونه کار می‌کند و چرا این فناوری می‌تواند دنیا را تغییر دهد.
موضوع: محاسبات کوانتومی- Quantum computing
شناسه افزوده: علی‌تقوی، کمیل، ۱۳۶۳-، مترجم
شناسه افزوده: Ali Taghavi, Komeil, ۱۹۸٤-
رده بندی کنگره: QA۷۶/۸۸۹
رده بندی دیویی: ۰۰۴/۱
شماره کتابشناسی ملی: ۸۸۹۳۴۵۲
اطلاعات رکورد کتابشناسی: فیپا

محاسبات کوانتومی

چگونه کار می‌کند و چرا این فناوری می‌تواند دنیا را تغییر دهد

آمیت کاتوالا

کمیل علی‌تقوی

راه‌کار

WIRED

عنوان : محاسبات کوانتومی ؛ چگونه کار می کند و چرا این فناوری می تواند دنیا را تغییر دهد
ناشر : راه‌پرداخت
نویسنده: آمیت کاتوالا
مترجم: کمیل علی‌تقوی
ویراستار ارشد : مینا والی
ویراستار محتوایی : قاسم سرافرازی
بازبینی نهایی متن: رضا قربانی
صفحه‌آرا : بهناز سعیدی
ناظر چاپ : قادر شهبازی
نوبت چاپ: اول ۱۴۰۱
شمارگان : ۱۰۰ نسخه
شابک: ۵-۲۵-۷۷۰۲-۶۲۲-۹۷۸
تلفن : ۴۴۴۴۳۹۶۶-۰۲۱
دورنگار: ۸۹۷۸۴۹۰۲
ایمیل : publisher @way2pay.press
وب‌سایت : way2pay.shop
لیتوگرافی: هنر اشکان
چاپ و صحافی: واژه

فروشگاه انتشارات راه‌پرداخت نشانی: تهران، جنت‌آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

@Way2Pay press Way2Pay.press @Way2Pay press

فهرست

مقدمه

سامیت (Summit)، ابررایانه ای بی ام (IBM) در آزمایشگاه ملی اوک ریج (Oak Ridge) در تنسی سه‌برابر یک نهنگ آبی وزن دارد و به‌اندازه دو زمین تنیس است. این ابررایانه ۲۱۹ کیلومتر کابل کشی دارد و در هر ثانیه می‌تواند بیش از سه کوینتیلیون (Quintillion) محاسبه انجام دهد. در ژوئن ۲۰۱۹، برای دومین سال متوالی، سریع‌ترین ابررایانه جهان معرفی شد.

تقریباً همزمان با دریافت این جایزه، رقیب دیگری مخفیانه در حال پیشی گرفتن از سامیت بود، نه سییرا (Sierra) که نزدیک‌ترین رقیبش در ایالات متحده بود و نه فوگاکو (Fugaku) که پروژه‌ای ژاپنی بود و انتظار می‌رفت وقتی در سال ۲۰۲۱ کاملاً آنلاین شود، از سامیت پیشی بگیرد. رقیب جدید و جدی سامیت تراشه‌ای ریز به‌اندازه ناخن انگشت شست بود که در آزمایشگاه تحقیقاتی خصوصی کوچکی نزدیک ساحل سانتا باربارا در کالیفرنیا توانست سامیت را کاملاً بی‌سروصدا شکست بدهد.

این تراشه را که «سیکِمور» (Sycamore) نام دارد، پژوهشگران شرکت گوگل تولید کردند. این تراشه بخش مرکزی رایانه کوانتومی را تشکیل می‌دهد و نوع جدید و کاملاً متفاوتی از دستگاهی است که مطابق قوانین فیزیک کوانتومی کار می‌کند.

رایانه‌های کوانتومی ظرفیت زیادی دارند: آنها می‌توانند سرانجام انقلابی در همه حوزه‌ها، از هوش مصنوعی گرفته تا تولید داروهای جدید، ایجاد کنند. یک رایانه کوانتومی فعال می‌تواند به ساخت مواد جدید قدرتمند کمک کند، مبارزه با تغییرات اقلیمی را قوی‌تر و سریع‌تر پیش ببرد و رمزنگاری را، که اسرارمان را حفظ می‌کند، کاملاً زیرورو کند. طبق گفته مجله دیسکاور (Discover)، در روزهای ابتدایی تحقیقات درباره رایانه‌های کوانتومی: «رایانه کوانتومی ماشین نیست، بلکه می‌تواند یکی از نیروهای طبیعت باشد».

اگر ظرفیت این رایانه‌ها کاملاً محقق شود، صرفاً نسخه‌هایی قدرتمندتر از رایانه‌های موجودمان نخواهند بود، بلکه با روشی کاملاً متفاوت کار خواهند کرد که می‌تواند آنها را قادر سازد کارهایی به‌ظاهر ناممکن انجام دهند. از آنجا که نقاط قوت این رایانه‌ها با ادراک اکثر ما از جهان بسیار فاصله دارد، توضیح دادن آنها بدون توسل به تشبیهات مبهم دشوار است. اما رایانه‌های کوانتومی می‌توانند به‌شکلی مؤثر مجموعه‌ای نوین از توانایی‌ها را بر اساس درک عمیق‌تر و جدیدی از جهان ایجاد کنند که فیزیک‌دانان طی قرن گذشته به وجود آورده‌اند.

مایکل نیلسن (Michael Nielsen)، دانشمند فیزیک کوانتومی و اندی ماتوشاک (Andy Matuschak)، مهندس نرم‌افزار، در تشبیهی می‌نویسند: «تصور کنید در حال شطرنج‌بازی

هستید و قوانین بازی به نفعتان تغییر می‌کند و طیف گسترده‌ای از حرکات را برای رُخ (قلعه) تان امکان‌پذیر می‌کند.» آنها از این تشبیه استفاده کردند تا بتوانند پدیده‌ای را برای مخاطبان معمولی فهم‌پذیر کنند که به‌طرز حیرت‌انگیزی پیچیده است. «این انعطاف‌پذیری بیشتر ممکن است شما را قادر سازد بسیار سریع‌تر رقیبتان را کیش و مات کنید، زیرا خیلی زودتر می‌توانید به موقعیت‌های جدید برسید».

در برخی موارد، رایانه‌های کوانتومی می‌توانند به ما امکان بدهند کارهایی انجام بدهیم که در حال حاضر حتی با قدرت یک میلیون ابررایانه ناممکن‌اند. شور و هیجان موجود در این فضا را باور کنید. در آستانه عصر جدیدی از فناوری قرار داریم که در آن، رایانه‌های کوانتومی به ما کمک می‌کنند مسیرهای سفر را با کارآیی بیشتری انتخاب و شمار بسیار زیادی از داده‌ها را در آزمایش‌های علمی پردازش کنیم. آنها به‌طور بالقوه نحوه تجزیه‌وتحلیل ریسک در بانک‌ها را تغییر می‌دهند، به شیمی‌دانان و زیست‌شناسان اجازه می‌دهند برای توسعه مواد و فرایندهای جدید کارآمدتر شبیه‌سازی‌های دقیقی از جهان طبیعی ایجاد کنند. ویلیام هرلی (William Hurley) (معروف به ورلی)، کارآفرین حوزه فناوری و بنیان‌گذار استرنج‌ورکس (Strangeworks)، تلاش می‌کند رایانش کوانتومی در دسترس همه باشد و می‌گوید: «این پدیده یکی از جهش‌های بسیار بزرگ فناوری در طول تاریخ تاکنون است.»

رایانش در ده سال آینده بیش از صد سال گذشته تغییر خواهد کرد. تا همین اواخر، درمورد اینکه آیا رایانه‌های کوانتومی واقعاً کارایی دارند یا خیر، تردیدهایی وجود داشت. اکنون نیز برخی هنوز شک دارند که آیا نسخه عملی مفید رایانه کوانتومی واقعاً وجود خواهد داشت یا خیر. ساخت رایانه‌های کوانتومی به‌طوری باورنکردنی بسیار دشوار است که نشان‌دهنده چالش‌های بزرگ مهندسی، ساخت و ریاضی است. اما طی بیست سال گذشته، برخی از شرکت‌های بزرگ جهان، مانند گوگل، آمازون، مایکروسافت، ای‌بی‌ام، اینتل برای ساخت دستگاه‌های کوانتومی عملی مفیدی که کارآیی داشته باشند، در رقابت بوده‌اند.

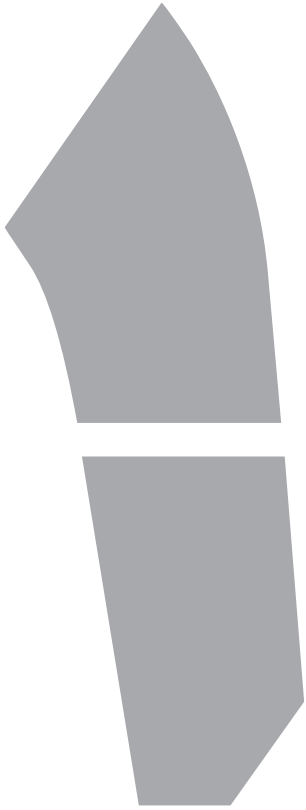
در تابستان ۲۰۱۹، تیمی از پژوهشگران گوگل که تقریباً کل دهه را صرف تلاش برای ساخت رایانه‌های کوانتومی کرده بودند، به نقطه عطفی معروف به «برتری کوانتومی» (Quantum Supremacy) دست یافتند. این اصطلاح که جان پریسکیل (John Preskill) آن را ابداع کرده است، موقعیتی را توصیف می‌کند که در آن، رایانه کوانتومی می‌تواند کاری را انجام دهد که بهترین رایانه کلاسیک جهان هرگز نمی‌تواند انجامش دهد.

این لحظه مهم تاریخی در سیزدهم ژوئن اتفاق افتاد، زمانی که تراشه سیکِمور گوگل در دمایی سردتر از فضای بیرون، مجموعه‌ای از محاسبات پیچیده را فقط در سه دقیقه و بیست ثانیه انجام داد که در ابررایانه سامیت، ده هزار سال طول می‌کشید. لحظه‌ای سرنوشت‌ساز بود. چند ماه بعد، هنگامی که مقاله پژوهشی منتشر شد، پیتر نایت (Peter Knight)، فیزیک‌دان کالج امپریال لندن به نیو ساینتیست (New Scientist) گفت: «دستاوردی فوق‌العاده است. مهندسی آن، بسیار خارق‌العاده است. این اتفاق نشان می‌دهد رایانش کوانتومی واقعاً سخت است، اما ناممکن نیست. قدمی به سوی رؤیایی بزرگ است.»

لحظه‌ای سرنوشت‌ساز رقم خورد: هنگامی که رایانش کوانتومی از نظریه محض به امکانی واقعی تبدیل شد. از زمان اعلان گوگل، دولت‌ها و سرمایه‌گذاران خطرپذیر میلیون‌ها دلار به این حوزه سرازیر کردند. در شرکت گوگل این دستاورد را با اولین پرواز برادران رایت در کیتی هاوک مقایسه می‌کنند که نقطه آغاز صنعت هواپیمایی بود. تونی مگرانت (Tony Megrant)، مهندس سخت‌افزار کوانتومی گوگل که در طراحی و ساخت تراشه سیکِمور همکاری کرده است، می‌گوید: «افرادی هستند که به‌معنای واقعی کلمه فکر می‌کنند کاری که ما انجام دادیم یا انجام مراحل بعدی آن، امکان‌ناپذیر است.» دیگران به‌اندازه کافی قانع نشدند. تا زمان انتشار رسمی این پژوهش، برخی از رقبای گوگل در رقابت کوانتومی، به‌ویژه ای‌بی‌ام، درمورد اینکه آیا تراشه سیکِمور به‌اندازه‌ای که غول جست‌وجو، گوگل، ادعا کرده بود، واقعاً بسیار جلوتر از سامیت بوده است یا نه، تردید داشتند. آنها بر این باور بودند که آنچه گوگل انجام داده بسیار محدود و مشخص‌تر از آن است که بتوان آن را برتری کوانتومی قلمداد کرد.

اما صرف‌نظر از مسائل فنی، برتری کوانتومی، دستاورد فنی عظیمی است و می‌تواند دوره جدیدی از فناوری را رقم بزند: طلوع عصر کوانتومی. رقابت واقعی تازه شروع شده است. مگرانت می‌گوید: «۱۰ سال است که در حال کار روی جنبه سخت‌افزاری این موضوع بوده‌ایم. بنابراین، خط شروع رقابت را همیشه در ذهنم بالای کوه تصور می‌کنم... ما برای شروع رقابت مجبور شدیم از اینجا بلند شویم.»

این کتاب، داستان همین رقابت و روش‌های بی‌شماری را بازگو خواهد کرد که رایانه‌های کوانتومی از طریق آنها می‌توانند دنیای مالی، پزشکی و سیاست را دگرگون کنند. همچنین، این روش‌ها را به‌دقت بررسیده و درباره آنها بحث خواهد کرد و ادراکمان از جهان را بهبود خواهد بخشید. اما ابتدا با اصول اولیه شروع خواهیم کرد.



فصل اول

رایانش کوانتومی چیست؟

تا همین اواخر، همه رایانه‌های جهان، از کُدشکن‌های دهه ۱۹۴۰ که به‌بزرگی یک اتاق بودند گرفته تا ریزپردازنده‌های موجود در تلفن هوشمندتان، اساساً به شیوه‌ای یکسان کار می‌کردند. ابداع تراشه‌های سیلیکونی و نیمه‌هادی، باعث پیشرفتی باورنکردنی شده است، اما اصول اساسی حاکم بر دستگاه‌های دارای فناوری پیشرفته امروزی، دقیقاً همان اصولی‌اند که آلن تورینگ (Alan Turing) و همکارانش در بلتچلی پارک (Bletchley Park) با آنها کار می‌کردند؛ یعنی در مرکز کُدشکنی در بریتانیا که برخی از اولین رایانه‌های کلاسیک را پدید آورد. این اصول، همان‌هایی هستند که هر رایانه‌ای که در این بین به وجود آمده است، از آنها تبعیت می‌کند، تا حدی که حتی رایانه شخصی رومیزی (PC) قدیمی شما نیز از لحاظ نظری می‌تواند هر آنچه ابررایانه سامیت می‌کند انجام دهد (اگر زمان و حافظه کافی به آن بدهید).

این رایانه‌های کلاسیک همگی با استفاده از «بیت» (Bit) کار می‌کنند. بیت‌ها در واقع سوئیچ‌های ریزی‌اند که می‌توانند در موقعیت خاموش باشند که با صفر (۰) نشان داده می‌شود یا در حالت روشن باشند که با یک (۱) نشان داده می‌شود (آنها می‌توانند یکی از سه نوع مختلف، شامل «والوها» (Valves)، «رله‌ها» (Relays) یا «ترانزیستورهای سیلیکونی» (silicon transistor) باشند). آهنگی که پخش می‌کنید، ویدئویی که در یوتیوب مشاهده می‌کنید و اپلیکیشنی که دانلود می‌کنید، در نهایت از ترکیبی از این «۰» و «۱»ها تشکیل می‌شوند.

این ترکیب ۰ و ۱ (سوئیچ‌های روشن و خاموش) با عنوان کد باینری (binary code) شناخته می‌شود. وقتی کارهایی که رایانه‌ها باید انجام می‌دادند، ساده بودند، خوب کار می‌کردند. به‌عنوان نمونه، عدد دو در باینری با رشته ۱۰ نشان داده می‌شود، در حالی که سه برابر یازده و چهار معادل صد است. اما با پیچیده‌تر شدن فرایندهای رایانه‌ای، تعداد بیت‌هایی که برای رمزگذاری این فرایندها نیاز دارید، به‌سرعت رشد می‌کند. برای مثال، پانزده به شکل ۱۱۱۱ است، در حالی که پانصد به شکل ۱۱۱۱۱۰۱۰۰ است.

هر عنصر در آن رشته کد باینری به یک بیت جداگانه احتیاج دارد که به‌معنای سوئیچ فیزیکی جداگانه‌ای است که می‌تواند به‌طور متناوب بین یک (۱) و صفر (۰) تغییر کند. شگفتی‌های تکنولوژیکی عصر رایانه، از طریق پیشرفت‌های چشمگیر در توانایی‌مان در

کوچک‌تر و کارآمدتر کردن این سوئیچ‌ها امکان‌پذیر شده است. بنابراین، می‌توانیم بیت‌های بیشتر و بیشتری را در همان مقدار فضا بگنجانیم.

اما هنوز هم چیزهایی وجود دارند که ما نمی‌توانیم انجام دهیم، حتی با میلیون‌ها تراشه و تریلیون‌ها بیت که در ابررایانه‌ای مانند سامیت با هم کار می‌کنند. بیت‌ها، سیاه و سفیدند. وقتی عوامل، نامشخص یا پیچیده‌اند، برای توصیفشان به بیت‌های خیلی بیشتری احتیاج دارید. این بدین معناست که برخی از مشکلات ظاهراً ساده می‌توانند برای رایانه‌های معمولی به‌طور تصاعدی دشوارتر شوند.

ورلی (Whurley)، کارآفرین حوزه فناوری، می‌گوید: «فرض کنید می‌خواهیم شما را از انگلستان به چهارده شهر در ایالات متحده بفرستیم و مسیر بهینه را پیدا کنیم؛ لپ‌تاپ من می‌تواند این کار را در یک ثانیه انجام دهد. اما اگر با استفاده از الگوریتمی یکسان و لپ‌تاپی مشابه، آن را به ۲۲ شهر افزایش دهیم، حل کردن این مسئله دو هزار سال طول می‌کشد.» این مورد، نمونه‌ای کلاسیک از «مسئله فروشنده دوره‌گرد» است؛ نوعی مسئله که در آن با هر متغیر اضافه‌شده، چالش به‌طور تصاعدی رشد می‌کند.

وسیله‌ای کلاسیک که سعی می‌کند کارآمدترین ترتیب بازدید از شهرها را عرضه کند، باید هر ترکیب ممکن را بررسی کند. بنابراین، برای هر شهری که به سفرتان اضافه می‌کنید، میزان قدرت رایانش مورد نیاز سر به فلک می‌کشد. بین یازده شهر، بیست میلیون مسیر وجود دارد، بین دوازده شهر ۲۴۰ میلیون مسیر و بین پانزده شهر بیش از ۶۵۰ میلیارد مسیر. در مدل‌سازی فعل‌وانفعالات پیچیده مولکول‌ها در صورتی که بخواهیم واکنش‌های شیمیایی را دقیقاً شبیه‌سازی کنیم یا سرعت پخش داروها را بیشتر کنیم، مشکلی مشابه ایجاد می‌شود؛ یعنی با افزودن هر متغیری، چالش بزرگ و بزرگ‌تر می‌شود.

ریچارد فاینمن (Richard Feynman)، فیزیک‌دان آمریکایی، از اولین کسانی بود که این موضوع را درک کرد. فاینمن در محافل دانشگاهی، همانند یک ستاره راک بود؛ او روی بمب اتم کار کرد، برنده جایزه نوبل شد و در زمینه فناوری نانو نوآوری‌های پیشگامانه‌ای کرد. او که موهایی بلند و رفتاری رک و راست داشت، حتی توانست در میان عموم مردم نیز مطرح شود؛ یعنی به چیزی دست یافت که بیشتر اوقات دانشمندان از آن محروم‌اند. در یک نظرسنجی

در سال ۱۹۹۹، او جزو یکی از ده فیزیک‌دان تأثیرگذار قرن بیستم انتخاب شد.

اما مهم‌تر از همه، او شخصیتی پیشرو در مکانیک کوانتوم بود. مکانیک کوانتوم مطالعه چیزهای عجیبی است که در مقیاس واقعاً کوچک در فیزیک رخ می‌دهند. در سال ۱۹۸۱، فاینمن چند سخنرانی کرد، یکی در مؤسسه فناوری کالیفرنیا معروف به کال‌تک (CalTech) در پاسادینا (Pasadena) و دیگری در ام‌آی‌تی (MIT) در بوستون، که آغاز حوزه رایانش کوانتومی بود.

تاریخچه (بسیار) مختصر مکانیک کوانتومی

فیزیک‌دانان طی قرن‌ها جهان را نوعی میز بیلیارد غول‌پیکر می‌دانستند که در آن اتم‌ها در خطوط هندسی مناسب (تعیین شده با سرعت و زاویه برخورد مناسب) با هم برخورد می‌کنند. در طی تمام این سال‌ها نظریه‌های فیزیک‌دانان به کار ریاضی‌دان قرن هفدهم، ایزاک نیوتن، برمی‌گشت؛ یعنی به قوانین حرکت و گرانش نیوتنی.

اما در ابتدای قرن بیستم، فیزیک‌دانان با بررسی دقیق‌تر کارکرد درونی اتم چیزهایی کشف کردند که با درکمان از فیزیک نیوتنی یا ترمودینامیک (نحوه رفتار مواد با تغییر دما) مطابقت نداشت.

در مقیاسی خاص، به نظر می‌رسید قوانین جهان متوقف شده‌اند.

رشته مکانیک کوانتومی برای توصیف رفتار عجیب ذراتی پدید آمد که می‌خواهند یک اتم را تشکیل دهند (جهت یادآوری، اتم‌ها از هسته اغلب شامل پروتون‌ها و نوترون‌ها تشکیل شده‌اند و الکترون‌ها در مدارهایی به دور این هسته‌ها می‌چرخند). فیزیک‌دانان کشف کردند که گاهی اوقات الکترون‌ها مانند جریان‌های پیوسته رفتار می‌کنند و مانند پرتو نوری گسترش می‌یابند. در مواقع دیگر، به نظر می‌رسد آنها به «بسته‌ها» (Packets) یا «کوانتا»ی (Quanta) منفرد تقسیم می‌شوند (ازاین‌رو، «فیزیک کوانتومی» نامیده می‌شود)، که پیوسته نیستند و فقط به مقادیر گسسته محدود می‌شوند؛ مانند خودرویی که فقط با سرعت سی یا چهل مایل در ساعت می‌تواند حرکت کند، نه سرعتی بین این دو عدد، یا آبی که از شیر آب می‌چکد و نه به‌عنوان یک جریان، بلکه فقط به شکل قطره‌هایی رؤیت‌پذیر ظاهر می‌شود. گاهی اوقات این اتفاقات می‌توانند به‌طور همزمان در هر دو

حالت ظاهر شـوند، آن هـم صرفاً در پدیـده‌ای به نـام «برهم‌نهی کوانتومـی» (Quantum Superposition).

نمونه کلاسـیک این مـورد، «آزمایش دو شـکاف» اسـت. تصور کنیـد روبـه‌روی دیواری نازک ایسـتاده‌اید که دو شـکاف عمودی مانند پنجره‌هایـی در آن به وجود آمده‌انـد و دیوار دیگری نیز پشـت آن قرار دارد. حال تصور کنید که یک «تفنگ پینت‌بال» دارید و آن را به سمت دیوار مقابلتان شلیک می‌کنید. دیوار جلوی شما با رنگ پوشانده می‌شود، البته در حالی‌که دیوار پشت آن کاملاً تمیز اسـت، به‌جز دو نوار عمودی رنگی که با دو شکاف دیوار اول مطابقت دارند (این همان بیتی است که اساساً کل رشته فیزیک کوانتومی را یک قرن به پیش رانده است). اما اگر قرار بود این آزمایش را در مقیاسی بسیار کوچک انجام دهیم و به‌جای توپ‌های رنگی، الکترون‌های منفرد را شلیک کنیم، با نتیجه‌ای کاملاً متفاوت مواجه می‌شدیم.

تصویری از آزمایش دو شکاف

حتی اگر الکترون را از طریق یکی از این دو شـکاف شـلیک کرده باشـید، در جایی ظاهراً تصادفی روی دیوار پشتی ظاهر می‌شود، نه لزوماً پشت یکی از دو شکاف. فقط پس از تکرار صدها یا هزاران بار شلیک الگویی شروع به پدیدار شدن می‌کند: نوارهای یک‌درمیان روشن و تاریک مانند بارکد. این الگو یا همان «الگوی تداخل» (Interference Pattern) برای آن ظاهر می‌شود که به نظر می‌رسد الکترون‌ها مادامی که مشاهده یا اندازه‌گیری شوند مانند موج رفتار می‌کنند و در غیاب ناظر یا مشاهده‌گر دوباره مانند ذره رفتار می‌کنند.

هنگامی‌که موج الکتـرون اولیه در «آزمایش دو شـکاف» از دو شـکاف عبـور می‌کند، دو موج کوچک‌تر ایجـاد می‌کند که بعداً یکدیگـر را خنثی و تقویت می‌کنند. گویی دو سـنگ در حوضچه انداخته‌اید و تماشـا می‌کنید که موج‌ها روی هم قرار گرفتـه و یکدیگر را تغییر می‌دهند. اما اینها امواج واقعی مثل امواج روی سـطح آب سـاکن نیسـتند. به‌جای ردیابی حرکت یا رفتار جسمی در طول زمان، این «توابع موج» (Wave Functions)، همان‌طورکه شناخته می‌شوند، تمام موقعیت‌های ممکن یک الکترون و احتمالات متفاوت حضورش را در هـر موقعیتی در یـک لحظه خـاص از زمان توصیـف می‌کنند. هنگامی‌کـه توابع موج

اندازه‌گیری می‌شود، وقتی الکترون به دیواره پشتی برخورد می‌کند، می‌گوییم «تابع موج» به یک برآیند خاص «فرومی‌ریزد»، همچون تاسی که از چرخیدن بازمی‌ایستد. فیزیک‌دانان هنوز توضیحی در مورد چگونگی یا چرایی این رخداد نداده‌اند، یا اینکه آیا تابع موج صرفاً یک پدیده ریاضی است، یا چیزی که در واقع در دنیای واقعی به روشی رؤیت‌پذیر رخ می‌دهد.

یک «نقشه بافتارمند» (Textured Map) را تصور کنید، مانند یکی از آنهایی که ویژگی‌هایی مانند پستی و بلندی رشته‌کوه‌ها و دره‌ها را نشان می‌دهد، هر نقطه روی نقشه دامنه احتمالی را نشان می‌دهد: هرچه زمین بیشتر باشد، احتمال حضور الکترون در آن گستره فضایی بیشتر است. تابع موج در این تشبیه، خود نقشه است، اما نقشه‌ای که می‌تواند مانند موج صدا یا آب پیچ‌وتاب بخورد.

احتمال فرود الکترون در نقطه‌ای خاص بر دیواره پشتی با توجه به نحوه تداخل این دامنه‌های احتمال با یکدیگر تعیین می‌شود. در زندگی عادی، احتمال فقط می‌تواند یک مقدار مثبت باشد: از صفر درصد (غیرممکن) تا صددرصد (قطعی). همان‌طورکه اسکات آرونسون (Scott Aaronson)، بنیان‌گذار و مدیر مرکز اطلاعات کوانتومی دانشگاه تگزاس در آستین، در مقاله‌ای در نیویورک تایمز توضیح می‌دهد: «در سطح کوانتومی(دنیای الکترون‌ها و پروتون‌ها) احتمال می‌تواند مثبت یا منفی یا ترکیبی از هر دو باشد. در حالی‌که وقایع در مقیاس کلاسیک دارای احتمالی بین صفر و یک هستند. در عوض، در سطح کوانتومی، رخدادها دامنه‌های احتمالی دارند که می‌توانند مثبت یا منفی باشند.

این بدین معناست که این دامنه‌های احتمال علاوه بر تقویت همدیگر می‌توانند یکدیگر را خنثی کنند، بنابراین، چنین رویدادی به‌هیچ‌وجه اتفاق نمی‌افتد و این فضای خالی موجود در الگوی بارکدمانند آزمایش دو شکاف را توضیح می‌دهد. آرونسون می‌نویسد: «این پدیده «تداخل کوانتومی» (Quantum Interference) است و زیربنای هرچیز دیگری است که شما در مورد عجیب بودن جهان کوانتومی شنیده‌اید.»

در مقیاس اتم (مقیاسی که همه ما در آن زندگی می‌کنیم) اگر سرعت و جهت اتم را بدانید، می‌توانید پیش‌بینی‌هایی مشخص و نسبتاً دقیق راجع به محل پایان یک اتم یا شیء انجام دهید. اما این الگوهای تداخل کوانتومی به این معناست که مقیاس زیراتمی درجه‌ای

از تصادفی دارد که از آن جدانشدنی است. فقط می‌توان احتمال تقریبی وقوع چیزی را دانست. هرگز به‌طور قطعی نمی‌توان سخن گفت. جهان هستی میز بیلیارد نیست. طبیعت در قلب خود عدم‌قطعیتی را جای داده است که از آن جدایی‌شدنی نیست.

از بیت تا کیوبیت

تا دهه ۱۹۸۰، از رایانه‌های اولیه برای اجرای شبیه‌سازی آب‌وهوا یا واکنش‌های شیمیایی استفاده می‌شد، اما ریچارد فاینمن نقصی را کشف کرد. برای شبیه‌سازی دقیق فیزیک، شیمی یا هرچیز پیچیده و کوچکی، به شبیه‌سازی‌ای نیاز دارید که بتواند از همان قوانین مبتنی بر احتمال مکانیک کوانتومی تبعیت کند. فاینمن در پایان یکی از صحبت‌هایش درباره چالش‌های شبیه‌سازی طبیعت با استفاده از رایانه، مسئله را در بخشی خلاصه کرد که اکنون جزئی از علم رایانش کوانتومی است. او گفت: «طبیعت کلاسیک نیست. لعنتی! اگر می‌خواهید طبیعت را شبیه‌سازی کنید، بهتر است از مکانیک کوانتومی استفاده کنید. تعجب‌آور اینکه این امر مسئله‌ای شگفت‌انگیز است، زیرا خیلی آسان به نظر نمی‌رسد.»

برای مدتی امکان‌پذیر بود که از پرداختن به استدلال فاینمن (دست‌کم از لحاظ عملی) اجتناب کرد، زیرا به نظر می‌رسید رایانه‌های کلاسیک، بسیار سریع در حال پیشرفت‌اند. در سال ۱۹۶۵، گوردون مور (Gordon Moore)، «قانون مور» را فرمول‌بندی کرد، که بیان می‌کند تعداد ترانزیستورهایی که می‌توانند روی یک «مدار مجتمع» (Integrated Circuit) قرار گیرند (و تعداد بیت‌هایی که می‌توانند با آن پردازش شوند) تقریباً هر دو سال، دو برابر می‌شوند. در طی دهه‌ها چنین بود و این همان روندی است که به یک دوره شگفت‌انگیز پیشرفت فناوری کمک کرد. ترانزیستورهای کوچک‌تر و کارآمدتر روی تراشه‌هایی با ساختارهایی به‌طور فزاینده پیچیده‌تر، امکان ساخت رایانه‌هایی با توانایی ذخیره‌سازی بیشتر، حافظه بیشتر، قدرت بیشتر را فراهم می‌کنند. چنین رایانه‌هایی می‌توانند برنامه‌ها و شبیه‌سازی‌هایی حتی قدرتمندتر را اجرا کنند.

اما در طی سال‌های اخیر مشکلات مختلفی به وجود آمده‌اند؛ ترانزیستورها آن‌قدر کوچک شده‌اند که با مشکلاتی روبه‌رو شده‌ایم. مشکل اول «انرژی» است. افزودن ترانزیستورهای بیشتر و بیشتر مصرف برق تراشه‌ها را بیشتر می‌کند. این امر بدین

معناست که مجبوریم هر یک از سوئیچ‌ها را کارآمدتر کنیم، یا برای میزان انرژی بسیار فزاینده مورداستفاده رایانه‌ها چاره‌ای بیندیشیم. مشکل دوم، «گرما» است. اگرچه سازندگان تراشه تمام تلاششان را می‌کنند، روند انجام محاسبات به‌شکلی اجتناب‌ناپذیر گرما تولید می‌کند که این امر به سیستم‌های خنک‌کننده بسیار پیچیده‌تری نیاز دارد.

مشکل سوم خود «فیزیک» است. وقتی به مقیاس کوچک‌تر می‌رسیم قانون مور پا کند می‌کند، زیرا با رسیدن به مقیاس بسیار کوچک دیگر قوانین فیزیک تغییر می‌کنند و مکانیک کوانتومی زمام امور را در دست می‌گیرد. این مسئله به این معناست که ایجاد این نوع از بهبودهای افزایشی که باعث پیشرفت‌های زیادی شده است، دشوارتر است. در سال ۲۰۱۲، پژوهشگران استرالیایی ترانزیستوری تولید کردند که از یک اتم تشکیل شده بود که برای نشان دادن «۱» و «۰»ها، بین دو حالت سوئیچ می‌کرد. امروزه ترانزیستورهایی ساخته می‌شوند که کوچک‌تر از ۲۲ نانومترند (به‌جای مقیاسی برای مقایسه: ضخامت موی انسان حدود هشتاد هزار نانومتر است).

همان‌طورکه تونی مگرانت از گوگل اشاره کرد، سازندگان تراشه چاره‌ای ندارند جز دست‌به‌گریبان شدن با کوانتوم و تلاش برای درک تأثیرات کوانتومی. فیزیک کوانتومی به بخشی اجتناب‌ناپذیر از رایانش تبدیل خواهد شد. مگرانت می‌گوید: «همان‌طورکه حوزه ما (رایانش کوانتومی) تازه در حال شکل‌گیری است، شاهد مقالاتی درباره پایان قانون مور هستیم. چیزها آن‌قدر مینیاتوری و بسیار کوچک شده‌اند که تأثیرات کوانتومی در حال ظاهر شدن هستند. این موضوع برای آنها یک خطاست، در حالی‌که این، چیزی است که ما در حال مهار کردن آن هستیم.»

در سال ۱۹۸۵، دیوید دویچ (David Deutsch)، فیزیک‌دان مستقر در آکسفورد، گامی فراتر از فاینمن برداشت. مانند فاینمن، دویچ تقریباً به جایگاهی افسانه‌ای در دنیای فیزیک کوانتومی دست یافته است. مشهور است که دویچ تقریباً هرگز خارج از خانه‌اش در آکسفورد (جایی‌که او با افکاری درگیر دنیاهای دیگر تا پاسی از شب مشغول کار کردن است) دیده نمی‌شود. بیشتر کارهای او بر فرضیه «چندجهانی» (Multiverse) متمرکز است؛ یعنی بر این ایده که جهان ما فقط یکی از تقریباً بی‌نهایت جهان‌های موازی است که هر آینده محتملی همزمان در یکی از آنها رخ می‌دهد. این فرضیه شامل همه‌چیز می‌شود، از

جهانی که مشابه دنیای ماست تا لحظه‌ای که سکه شما به‌جای شیر، خط می‌آید تا جهانی که در آن شهاب‌سنگ به زمین برخورد نکرده است و دایناسورها به موجوداتی هوشمند تبدیل شده‌اند و حالا ماشین، هواپیما و میکروچیپ‌های خودشان را دارند.

دویچ دریافت رایانه‌ای که از اجزای کوانتومی ساخته شده است می‌تواند بسیار قدرتمندتر از یک شبیه‌ساز فیزیک باشد. به‌جای بیت‌ها که فقط می‌توانند یک یا صفر باشند، این اجزا که در نهایت به بیت‌های کوانتومی (Quantum Bits) یا کیوبیت‌ها (Qubits) معروف شده‌اند – می‌توانند یک، صفر یا در حالت «برهم‌نهی» (Superposition) باشند که «همزمان یک و صفر» هستند.

این فقط توضیحی ساده است، شبیه به توضیحی که معمولاً در مقاله‌های خبری و کتاب‌های علوم عامه‌پسند با آن مواجه می‌شوید. حقیقت کمی پیچیده‌تر است. کیوبیت در حالت برهم‌نهی، از نظر فنی همزمان در هر دو حالت نیست. در عوض، تا حدی احتمال اینکه یک باشد، وجود دارد و همچنین تا حدی احتمال اینکه صفر باشد، که «مشاهده کردن» آن باعث می‌شود به یکی از این دو حالت سقوط کند، همان‌طورکه نتیجه پرتاب سکه را معلوم می‌کنید.

به زبان ساده، می‌توانید کیوبیت‌ها را کره زمین در نظر بگیرید، یک (۱) قطب شمال، صفر (۰) قطب جنوب و حالت برهم‌نهی در نقطه‌ای نامشخص در جایی دیگر روی کره است. می‌توانید سکه را تصور کنید: اگر شیر یک و خط صفر باشد، پس در حالت برهم‌نهی سکه در حال چرخش است: مملو از آینده‌های بالقوه محقق‌نشده.

کیوبیت‌ها می‌توانند اطلاعات بیشتری را با کارآیی بیشتری در مقایسه با بیت‌ها در خود جای دهند. برای توصیف حالت کیوبیت دست‌کم به دو بیت نیاز دارید (۰۰ در کیوبیت، ۰۱ است، ۱۰ در کیوبیت ۱۱ است، و حالت برهم‌نهی ۰۱ یا ۱۰). برای دو کیوبیت به چهار بیت و برای سه کیوبیت به هشت بیت نیاز دارید. برای توصیف حالت سیصد کیوبیت به بیت‌های بیشتری از تمام اتم‌های موجود در جهان شناخته‌شده نیاز دارید. برای نمونه، برای ذخیره اطلاعاتی به‌اندازه ۵۳ کیوبیت در تراشه سیکمور گوگل به ۷۲ میلیارد گیگابایت حافظه رایانه کلاسیک نیاز دارید. تونی مگرانت توضیح می‌دهد: «رشدی نمایی از اعداد است که برای توصیف این سیستم کوانتومی باید دنبال کنید. این امر، همان قدرت تصاعدی است که

درباره رایانش کوانتومی می‌شنوید.»

دویچ دریافت که رایانه‌های ساخته‌شده از کیوبیت به‌جای بیت می‌توانند از عدم‌قطعیت مکانیک کوانتومی به نفع خود استفاده کنند. همچنین دریافت که علاوه بر شبیه‌سازی مؤثرتر طبیعت، ماشینی ساخته‌شده از کیوبیت قادر خواهد بود از عدم‌قطعیت بهتر استفاده کند و مشکلاتی خاص را هزاران یا میلیون‌ها بار سریع‌تر حل کند. به‌جای اینکه شبیه‌ساز هر مسیر مارپیچی را به‌نوبه خود امتحان کند، می‌تواند همزمان به‌صورت موازی هر مسیر را به‌شکلی مؤثر طی کند. کمی شبیه نگه داشتن انگشت در صفحات مجموعه کتاب‌های «ماجراجویی خودت را انتخاب کن» (choose your own adventure) است که عواقب هر تصمیمی را فوراً می‌بینید.

اگر چندین کیوبیت به هم بپیوندند، می‌توان الگوهای تداخلشان را به‌دقت تنظیم کرد تا مسیرهایی که به پاسخ‌های غلط منجر می‌شوند یکدیگر را خنثی کنند، در حالی‌که مسیرهایی منتهی به پاسخ درست یکدیگر را تقویت می‌کنند. نتیجه، افزایش تصاعدی توان رایانش برای انواع خاصی از مشکلات است. به همین علت، برخی بر این باورند که رایانه‌های کوانتومی می‌توانند در ساخت مواد جدید قدرتمند، مبارزه قوی‌تر و سریع‌تر با تغییرات اقلیمی و زیرورو کردن کامل رمزنگاری، از محدودیت‌های رایانه‌های کلاسیک بسیار فراتر بروند.

از لحاظ نظری، ماهیت مکانیک کوانتومی، چالشی اساسی برای رایانش به وجود می‌آورد. برای انجام محاسبات بایستی بتوانید عوامل را اندازه‌گیری و نتایج یافته‌هایتان را به مرحله بعدی معادله منتقل کنید. اما اندازه‌گیری چیزی در حالت برهم‌نهی، آن را از آن حالت خارج می‌کند: به نظر نمی‌رسد فوتون دیگر همزمان در دو مکان باشد؛ گربه شرودینگر (Schrödinger's cat) یا مرده است یا زنده. باید قادر باشید بدون ایجاد مزاحمت برای چرخش سکه، آن را دور خودش بچرخانید.

در واقع، این امر به لطف ویژگی عجیب دیگری از مکانیک کوانتومی به نام «درهم‌تنیدگی» (Entanglement) امکان‌پذیر است. هنگامی‌که دو موج الکترون با یکدیگر در تعامل‌اند، هریک بر دیگری اثری می‌گذارد؛ بدین معنا که این دو موج هرقدر هم از یکدیگر فاصله داشته باشند به‌شکلی جدایی‌ناپذیر به هم پیوند می‌خورند یا «درهم‌تنیده» می‌شوند. حتی اگر

دو ذره میلیاردها مایل از همدیگر دور باشند، اندازه‌گیری یک ذره درهم‌تنیده فوراً حالت ذره دیگر را تغییر می‌دهد؛ تابع موج هر دو ذره به‌طور همزمان فرومی‌ریزد. این پدیده چیزی است که در طی دهه‌ها فیزیک‌دانان را متحیر کرده است. چیزی وجود دارد که این دو ذره را به هم پیوند می‌دهد؛ به این معنا که می‌توان اطلاعات کوانتومی را از یک مکان به مکانی دیگر منتقل کرد بدون اینکه برهم‌نهی اصلی فروبپاشد. درهم‌تنیدگی، مسئله اندازه‌گیری را حل می‌کند؛ بدین معنا که بدون فروپاشی برهم‌نهی می‌توانید اطلاعات را از یک کیوبیت به کیوبیت دیگری منتقل کنید.

بینش دویچ از اهمیتی اساسی برخوردار بود و تا سال ۱۹۹۲ مردم به دنیای رایانش کوانتومی جذب شدند. اما اگر جوزپه کاستانیولی (Giuseppe Castagnoli)، رئیس بخش فناوری اطلاعات در السگ بیلی (Elsag Bailey) یعنی تولیدکننده سیستم‌های کنترل صنعتی که اکنون بخشی از ای‌بی‌بی (ABB) است، نبود، ممکن بود این ایده در حد نظریه باقی بماند. کاستانیولی که در زمان نگارش این کتاب ۷۸ سال دارد و هنوز مقاله‌هایی درمورد رمزنگاری کوانتومی منتشر می‌کند، این‌گونه به یاد می‌آورد: «در آن زمان، مسئول بخش فناوری ارتباطات اطلاعات در السگ بیلی بودم و شخصاً به محاسبات کوانتومی که در مراحل اولیه بود، علاقه داشتم. وقتی دیدم امکان استفاده صنعتی از محاسبات و ارتباطات کوانتومی وجود دارد، به جامعه علمی نزدیک شدم.»

آرتور اکرت (Artur Ekert) به یاد می‌آورد: «کاستانیولی، شرکت خود را متقاعد کرد که به‌جاي حمایت مالی از برخي نمایشگاه‌هاي هنري از مجموعه‌ای از کنفرانس‌ها حمایت کند». آرتور اکرت، استاد فیزیك کوانتومی در دانشگاه آکسفورد و جزو شرکت‌کنندگان اولیه در کارگاه‌هاي سالانه کاستانیولی از سال ۱۹۹۳ تا ۱۹۹۸ در ویلا گوالینو (هتلی در دامنه تپه مشرف به تورین) است. در آنجا دانشگاهیان جوان که اکنون در میان تأثیرگذارترین افراد در رایانش کوانتومی‌اند، با همدیگر ارتباط برقرار کردند و به تبادل‌نظر پرداختند.

در سال ۱۹۹۴، اکرت بر اساس برخی از ایده‌هایی که در ویلا گوالینو به دست آورده بود، در کنفرانس بین‌المللی فیزیک اتمی در بولدر کلرادو سخنرانی کرد. برای اولین‌بار، او محاسبات کوانتومی را به عناصر اصلی سازنده‌شان تقسیم کرد و شباهت‌های آن را با دستگاه‌های کلاسیک نشان داد و انواع سوئیچ‌ها و «دروازه‌های منطقی» (logic Gates) لازم برای ساخت

ماشین کوانتومی را توصیف کرد. دروازه‌های منطقی، کارهایی مانند ترکیب ورودی‌ها از دو بیت و دادن یک جواب را انجام می‌دهند. برای نمونه فقط اگر هر دو دروازه ورودی یک باشند، یک را نشان می‌دهد.

صحبت‌های اکرت تولد رایانش کوانتومی را، در جایگاه صنعتی جدید، رقم زد. او می‌گوید: «این جلسه سبب آغاز ریزش بهمن شد. ناگهان دانشمندان علوم کامپیوتر درمورد الگوریتم‌ها صحبت کردند. فیزیک‌دانان اتمی دریافتند که می‌توانند نقشی داشته باشند. بعداً [مبحث رایانش کوانتومی] شروع به نفوذ در سایر حوزه‌ها کرد، شروع به شتاب گرفتن کرد و به صنعتی تبدیل شد که امروز شاهد آن هستید.»

ولی پیش از اینکه رایانش کوانتومی به صنعت تبدیل شود، دانشمندان مجبور بودند بفهمند که واقعاً چگونه باید کیوبیت بسازند. در دهه ۱۹۹۰، محاسبات کوانتومی هنوز ساختاری کاملاً نظری بود و برای تحقق آن، دانشمندان باید چیزی را پیدا یا ایجاد می‌کردند که به‌اندازه کافی کوچک باشد تا بتواند از قوانین مکانیک کوانتومی تبعیت کند و در عین حال به‌اندازه کافی بزرگ باشد تا بتواند به‌طور قابل اعتمادی کنترل شود. این امر، جست‌وجویی است که درکمان را از فیزیک و علم مواد تا سر حد نهایی ممکن به کار گرفته است.

فصل دوم

ساخت ناممکن

آزمایشگاه کوانتومی گوگل در ساختمانی بژرنگ در شمال سانتا باربارا در کالیفرنیا، در گوشه‌ای قرار دارد که به نظر نمی‌رسد قلب تپنده موفقیت چشمگیر بعدی در فناوری باشد. اما احتمالاً در دهه ۱۹۴۰ نیز می‌توانستید درباره پارک بلتچلی همین حرف را بزنید. داخل ساختمان، ردیف‌هایی از میزهای نامرتب دیده می‌شوند و تخته‌های موج‌سواری از دیوار آویزان‌اند. هنگام ناهار، گروهی از مهندسان در اتاقی به نام ریچارد فاینمن، که نشست‌هایشان را در آن برگزار می‌کنند، نشستندو بازی می‌کنند. تخت و کاسه غذایی هم برای سگ اداره، کیوبیت، در گوشه‌ای قرار دارد.

کار واقعی در آزمایشگاه سخت‌افزار انجام می‌شود که پر است از درهای دولنگه پوشیده‌شده با برچسب‌های شوخی‌های مخصوص آدم‌های خوره فناوری و برای درکشان باید دکتری مکانیک کوانتومی داشته باشید. در داخل، همه‌چیز تمیز و سفید و مرتب است. صدای دستگاه‌ها فضا را پر کرده است و کارکنان انگشت‌شمار این بخش، آرامش و تمرکزی قابل‌احترام دارند. اینجاست که تراشه ۵۳ کیوبیتی گوگل (سیکمور) به برتری کوانتومی دست یافت و آغاز عصر جدیدی در علوم کامپیوتر را رقم زد.

در سال ۱۹۹۴، هنگامی که آرتور اکرت در بولدر سخنرانی کرد، کیوبیت هنوز در حد یک تئوری بود. برای اینکه ایده رایانه‌های کوانتومی به واقعیت تبدیل شود، فیزیک‌دانان باید راهی برای ساخت «کیوبیت» پیدا می‌کردند: سوئیچی واحد که بتواند به‌شکلی قابل‌اعتماد بین یک (۱) و صفر (۰) تغییر کند و همچنین بتواند در حالت برهم‌نهی وجود داشته باشد. لازم بود چیزی به‌اندازه کافی کوچک باشد تا بتواند از قوانین مکانیک کوانتومی پیروی کند، در عین‌حال به‌اندازه کافی هم بزرگ و پایدار باشد تا بتوان با اطمینان کنترلش کرد.

این دو شرط، به‌قدر کافی چالش‌برانگیزند. اما مسئله سومی نیز وجود دارد که مهندسان کوانتومی با آن دست‌به‌گریبان‌اند: «تداخل» (Interference)، نه از جانب کیوبیت‌های دیگر، بلکه از جهان خارج. هنگامی که در مقیاس کوانتومی کار می‌کنید، کوچک‌ترین نویزی می‌تواند کیوبیت را از حالت ظریف برهم‌نهی خارج کند، مانند نسیمی که بر شمع می‌وزد یا سکه‌ای در حال چرخیدن که تعادلش به هم می‌خورد و در این صنعت «ناهمدوسی» (Decoherence) نامیده می‌شود و این معمولاً در کسری از

ثانیه رخ می‌دهد. چتان نایاک (Chetan Nayak)، مدیرکل بخش سخت‌افزار کوانتومی مایکروسافت، می‌گوید: «همزمان تلاش می‌کنید عملکرد داخلی یک رایانه کوانتومی را کاملاً ایزوله کنید، در عین‌حال قادر باشید به آن بگویید چه کاری انجام دهد و پاسخش را بگیرید.»

همه اینها بخشی از یک عمل متعادل ظریف است. هر محاسبه کوانتومی، رقابتی دیوانه‌وار برای انجام هرچه بیشتر عملیات در کسری از ثانیه است، پیش از آنکه کیوبیت از حالت برهم‌نهی خارج و ناهمدوس شود. یان گوتز (Jan Goetz) از استارتاپ فنلاندی آی‌کیوام (IQM)، که در حال توسعه فناوری برای افزایش «سرعت کلاک» (Clock Speed) تراشه‌های کوانتومی و بهبود کارآیی آنها از این لحاظ است، توضیح می‌دهد: «طول عمر اطلاعات کوانتومی بسیار کوتاه است. هرچه پردازنده‌ها را پیچیده‌تر کنید، طول عمر بیشتر کاهش می‌یابد.»

هر روش کنترلی جدیدی که اضافه می‌کنید، تداخل و نویز بیشتری نیز ایجاد می‌کنید. تونی مگرانت می‌گوید: «هر بار که خطی به آن اضافه می‌کنیم، در حقیقت ناهمدوسی اضافه می‌کنیم. در حال آسیب رساندن به دستگاهمان هستیم، اما آیا می‌توانیم به‌نحوی به نتیجه‌ای بهتر دست یابیم؟ چالش‌برانگیزترین مسئله این است که چگونه می‌توانیم به یک سیستم کوانتومی با طول عمری کافی برای کارکردی به‌اندازه کافی طولانی دست یابیم تا بتوانیم کارهایی معنادار انجام دهیم.»

برای همین، بیشتر فضای اتاق را شش دستگاه «زَم‌پا» (Cryostat) در دو ردیف سه‌تایی اشغال کرده‌اند. این دستگاه‌ها سیلندرهای فلزی تودرتویی هستند که هرکدام با یکی از رنگ‌های شرکت گوگل رنگ‌آمیزی شده‌اند، مانند لوستر از سقف آویزان‌اند و از بالا به پایین کمی باریک می‌شوند. آنها طراحی شده‌اند تا تراشه کوانتومی را به‌تدریج با دمایی سردتر از فضای بیرونی خنک کنند و آن را کاملاً از گرما، نویز، لرزش و تداخل الکترومغناطیسی دور نگه دارند. «زَم‌پا»ها به‌تدریج دما را پایین می‌آورند؛ هر سطح آهسته و پیوسته سردتر می‌شود و تقریباً دو روز طول می‌کشد تا تراشه کوانتومی به دمای ۱۰ میلی‌کلوین برسد و تقریباً یک هفته زمان می‌برد تا به دمای اتاق برسد. یو چن (Yu Chen)، دانشمند تحقیقات کوانتومی در گوگل که روی اندازه‌گیری و کالیبراسیون

سیستم‌ها متمرکز است، می‌گوید: «همه‌چیز درمورد چگونگی محافظت از طول عمر سیستم است.»

رایانش با استفاده از لیزر

فناوری گوگل فقط یکی از چندین تلاش گوناگون برای ساخت کیوبیت‌های دارای کارآیی است. صحبت‌های آرتور اکرت باعث شد تحقیقات در جهات مختلف شروع شود. همگی به‌طور موازی، مانند کوهنوردانی که مسیرهای مختلف کوه را طی می‌کنند، پیش می‌روند. ده‌ها رویکرد مختلف وجود دارد که به روزهای نخست رایانش کوانتومی بازمی‌گردند؛ کیوبیت‌ها در پرتوهای لیزر معلق شده‌اند، در الماس گیر افتاده و از مسیر مغناطیسی تجمیعی میلیاردها ذره در دستگاهی که مانند اسکنر ام‌آرآی (MRI) کار می‌کند، بیرون کشیده می‌شوند. بعضی از مسیرها، پیش از سرعت بخشیدن، به سختی شیب شروع ملایم‌تری دارند، در حالی که برخی دیگر، منحنی یادگیری اولیه تندتری دارند، اما نوید می‌دهند که برای رسیدن به هزاران یا میلیون‌ها کیوبیت که در نهایت برای حل مشکلات دنیای واقعی به آنها نیاز خواهیم داشت، آسان‌تر خواهد بود.

نخستین تلاش‌ها، بر تله‌های یونی (Ion Traps) مبتنی بودند، فناوری‌ای که حاصل کارِ به‌خوبی تثبیت‌شده‌ای در زمینه ساعت‌های اتمی بود که در اواسط قرن بیستم توسعه یافت تا به‌وسیله ضربه زدن به مترونوم داخلی یک اتم، زمان‌سنجی فوق‌العاده دقیقی فراهم کند. یون، اتمی دارای بار مثبت یا منفی است (و نه بار خنثی). در رایانش کوانتومی به روش یون به‌دام‌افتاده، کیوبیت‌ها از یون‌هایی منفرد تشکیل می‌شوند که با پالس‌هایی از چراغ‌هایی که برای جابه‌جایی آرام و تدریجی‌شان بین حالت‌های مختلف استفاده می‌شوند و آنها را از حرکت به اطراف بازمی‌دارند، در چاه‌های ریزی نگه داشته می‌شوند، مانند کشتی تفریحی که قایق‌های یدک‌کش آن را ثابت نگه می‌دارند. در تاریخ یکم می ۱۹۹۵، پیتر زولر (Peter Zoller) و ایگناسیو سیراک (Ignacio Cirac) از دانشگاه اینسبروک اتریش که بخشی از جامعه کوانتومی نوظهوری بودند و سالانه در تورین با هم ملاقات می‌کردند، مقاله‌ای منتشر کردند که شرح می‌دهد یون‌ها چگونه می‌توانند

در نقش کیوبیت برای عملیات ساده استفاده شـوند و چگونه حالت‌های یک (۱)، صفر (۰) و برهم‌نهی می‌توانند در حرکت تکان‌دهنده یون، یا سطح انرژی یا «چرخش» یکی از الکترون‌هایی که در مداری به دور آن می‌چرخد، رمزگذاری شوند.

آرتور اکرت نیاز به ساخت نوع خاصی از «دروازه منطقی کوانتومی» (Quantum Logic Gate) را توصیف کرد که با نام «دروازه سی‌نات» (C-NOT Gate) یا (Controlled NOT Gate) شناخته می‌شـود؛ دروازه‌ای دو بیتی که بیت دوم فقط در صورتی که بیت اول در حالتی خاص باشـد، از یک به صفر تبدیل می‌شـود. در رایانه‌های کلاسـیک که شـامل شبکه‌ای پیچیده از دروازه‌های منطقی متشـکل از بیت‌های جداگانه‌اند، می‌توانید هر نوع مـداری را از «دروازه نقیـض یـا» (NOR Gate) و «دروازه نقیـض وَ» (NAND Gate) بسازید. دروازه‌های سی‌نات، معادل کوانتومی‌اند. اکرت گفت: «اگر بتوان به دروازه‌های سی‌نات دست یافت، به این معناست که دانشـمندان علوم کامپیوتر همه آنچه را برای شروع ساخت مدارهای کوانتومی موردنیاز است، در اختیار دارند.»

در سال ۱۹۹۵، فقط یک سال بعد، اعضای تیمی در انستیتوی ملی استاندارد و فناوری (NIST) در بولدر توانستند با استفاده از یون منفرد از عنصر برلیوم، یک دروازه سی‌نات فعال بسـازند. پالس لیزری می‌تواند چرخش الکترون چرخان در مـدار را از بالا به پایین (یا یک به صفر) تغییر دهد، اما فقط در صورتی که یون به روشی خاص (که با یک و نه با صفر مطابقت دارد) ارتعاش کند. آنها دروازه کوانتومی دو کیوبیتی‌ای ایجاد کردند که کار می‌کرد، اما برای سـاخت رایانه‌ای کوانتومی که کار کند، به موارد دیگری بیش از این نیاز داشتند.

تله‌های یونی شـاید در مقایسـه با همه مسـیرهای رو به سـوی بـالای کـوه کوانتومی، نرم‌ترین شیب را داشته باشند، زیرا به هیچ‌یک از فناوری‌های جدید در حال توسعه متکی نیستند. پیتر چاپمن (Peter Chapman)، رئیس و مدیرعامل شرکت یون‌کیو (IonQ)، که با پشتیبانی آمازون مستقر در بالتیمور تلاش می‌کند رایانه کوانتومی مدل یون به‌دام‌افتاده را تجاری کند، گفت: «کار فیزیک به پایان رسیده است. من دوست دارم شوخی کنم که رایانه‌های یون‌کیو عمدتاً ساخته شـده و در بخش‌هایی از آمازون تحویل داده می‌شوند؛ تقریباً آماده برای فروش‌اند.»

استفاده از یون‌ها، علاوه بر معایب، مزایایی نیز دارد. از جنبه مثبت، لازم نیست یون‌ها ساخته شوند، زیرا در طبیعت وجود دارند. چاپمن می‌گوید: «مشکلی در تولید نداریم. مادر طبیعت اتم تولید می‌کند.» این روش مزایای زیادی از نظر میزان محافظت موردنیاز دارد؛ خیلی کمتر احتمال دارد که یون‌های به‌دام‌افتاده، به‌خاطر تداخل محیطی از حالت برهم‌نهی خارج شوند.

از جنبه منفی، در رایانش کوانتومی به روش یون به‌دام‌افتاده، رسیدن به سطح لازم برای دستیابی به رایانه کوانتومی مفید که به صدها یا هزاران کیوبیت نیاز دارد، به علت کوچک بودن یون‌ها دشوار است؛ حتی به‌گفته برخی ناممکن است. چاپمن معتقد است این امر می‌تواند با ایجاد دستگاه‌های کوانتومی کوچک‌تر مجزا و جابه‌جایی اطلاعات بین آنها با استفاده از نور حاصل شود.

رویکرد اولیه دیگری برای رایانش کوانتومی، راه‌حلی کاملاً متفاوت را برای مسئله ناهمدوسی عرضه کرد: به‌جای تلاش برای دور نگه داشتن کیوبیت‌ها از محیط، پذیرفت که برخی کیوبیت‌ها ناگزیر ناهمدوس می‌شوند و مسئله را با استفاده از نیروی خیلی زیاد اعداد حل کرد.

در سال ۲۰۰۱، پژوهشگران آی‌بی‌ام در سن‌خوزه کالیفرنیا، به رهبری آیزاک چونگ (Isaac Chung) توانستند با استفاده از مقدار کمی مایع و آهن‌ربا، رایانه‌ای کوانتومی بسازند که کار می‌کرد. آنها از مولکولی حاوی پنج اتم فلوئور و دو اتم کربن استفاده کردند. هریک از هفت اتم موجود در این مولکول، حالت چرخش خودش را دارد، بنابراین اگر بتوان آن را به‌شکلی کنترل کرد که قابل‌اعتماد باشد، مولکول می‌تواند در نقش رایانه کوانتومی هفت کیوبیتی کار کند.

این امر ناممکن است، اما با گردآوری تریلیون‌ها مولکول در یک مایع، محققان توانستند مولکول‌ها را به‌صورت دسته‌جمعی کنترل و تا حد زیادی همان اثر را ایجاد کنند. آنها با استفاده از دستگاه تشدید مغناطیسی هسته‌ای (شبیه اسکنر ام‌آرآی در بیمارستان) بر مایع نظارت کردند، در حالی‌که با پالس‌های الکترومغناطیسی کنترل‌شده به آن ضربه می‌زدند که مولکول‌های خاصی از نمونه را به حالت مطلوب برساند. اهمیتی نداشت که فقط بخش کوچکی واقعاً وارد این حالت شدند، زیرا سیگنال ترکیبی آنها

هنوز به‌قدری قوی بود که در مقابل نویز تصادفی پس‌زمینه باقی نمونه مقاومت می‌کرد. جان گریبین (John Gribbin) درباره رایانش با گربه‌های کوانتومی توضیح می‌دهد که «در واقع، بازخوانی از رایانه، میانگین تمام مولکول‌ها بود، تعداد زیادی پاسخ صحیح که به‌شکلی مؤثر بر تعداد بسیار کمتری از اشتباهات ناشی از ناهمدوسی و سایر مشکلات غلبه کردند».

اما این رویکرد، به همراه سایر شیوه‌ها، از «نقاط کوانتومی» (Quantum Dots) گرفته تا رایانه‌های ساخته‌شده از الماس، تا حد زیادی موفق نشده‌اند کارشان را ادامه دهند. تله‌های یونی نیز علی‌رغم وعده‌های اولیه، عمدتاً موردپسند نیستند (اگرچه برخی شرکت‌ها، از جمله یون‌کیو، هنوز این روش را دنبال می‌کنند). بنابراین، امروزه بازیگران اصلی این حوزه عمدتاً حول یک گروه از فناوری‌ها، «کیوبیت‌های ابررسانا» (Superconducting Qubits)، گرد هم آمده‌اند.

راه سرد به سوی برتری

اکثر دانشجویان دکتری، صرفاً به‌خاطر اتمام پایان‌نامه‌شان خوشحال می‌شوند. اما پایان‌نامه برایان جوزفسون (Brian Josephson) به او کمک کرد سهمی از جایزه نوبل را به دست آورد.

در سال ۱۹۶۲، دانشجوی ۲۲ ساله کمبریج در حال مطالعه روی «ابررسانایی» (Superconductivity) بود؛ پدیده‌ای که در آن، مقاومت الکتریکی برخی از مواد هنگام سرد شدن در زیر دمایی خاص، به صفر می‌رسد (مقاومت، اندازه‌گیری می‌کند که جریان چقدر آسان می‌تواند از داخل یک ماده عبور کند، مثلاً مس مقاومت کمی دارد و لاستیک، دارای مقاومت بالاست؛ هرچه مقاومت بیشتر باشد، برای ادامه جریان ولتاژ بیشتری نیاز است). جوزفسون در طی پژوهش دریافت که مطابق با قوانین فیزیک کوانتومی، اگر دو ابررسانا را از طریق پیوند ضعیف با ماده دیگری به همدیگر پیوند بدهید، می‌توانید جریانی ایجاد کنید که بدون نیاز به اعمتل ولتاژ بیشتر برای همیشه از آنها عبور کند. این ساختارها که امروزه به‌عنوان «اتصالات جوزفسون» (Josephson Junctions)

شناخته می‌شوند، کاربردهای گسترده‌ای در الکترونیک و رایانش دارند.

اگرچه آنها دستگاه‌های کوانتومی هستند، برای دیدنشان به میکروسکوپ نیازی ندارید، برخی از اتصالات جوزفسون به‌اندازه حلقه ازدواج‌اند، اما اکنون به‌قدر کافی کوچک شده‌اند تا روی تراشه سیلیکونی قرار بگیرند و همچنین دارای ویژگی مفید دیگری به نام «غیرخطی بودن» (Non-linearity) هستند که به آنها امکان می‌دهد فقط به دو حالت انرژی محدود شوند که به‌صورت یک و صفر نشان داده می‌شوند، صرف‌نظر از اینکه چه مقدار انرژی برایشان صرف می‌شود. گریبین می‌نویسد: «آنها می‌توانند به‌جای سوئیچ‌های بسیار حساس سریع استفاده شوند که می‌توانند با استفاده از نور، روشن و خاموش شوند.»

کیوبیت‌های ابررسانا، متشکل از اتصالات جوزفسون، فناوری‌ای عرضه می‌کنند که افزایش مقیاس و مینیاتوری کردن آن از روش تله‌های یونی آسان‌تر است، زیرا با معماری مبتنی بر سیلیکون درون هر رایانه کلاسیک روی کره زمین سازگارتر است. آنچه به شکل فرصتی بی‌خطر در گوگل آغاز شد، در ابتدا بر رویکردهای دیگر متمرکز بود، اما اکنون برای گوگل، غول بزرگ جست‌وجو و رقیب عمده کوانتومی خود، آی‌بی‌ام، در صدر امور است.

سرجیو بویکسو (Sergio Boixo) که در گوگل روی تئوری کوانتومی کار می‌کند و شخصی است که کاری را طراحی کرده که برتری کوانتومی را ثابت کرد، می‌گوید: «هر رویکردی جنبه‌های مثبت و منفی دارد. این رویکرد (کیوبیت‌های ابررسانا) همیشه شبیه‌ترین نظیر به «مدار مجتمع» کلاسیک که زندگی‌مان را تأمین می‌کند، در نظر گرفته شده است. هنگامی که از کاستی‌های خاص همراه با این رویکرد گذر کنیم، می‌توانیم درست مانند رایانش کلاسیک، افزایش مقیاس دهیم. قصد داریم به همه مزایا دست بیابیم. فقط باید بر نکات منفی غلبه کنیم.» مگرانت اضافه می‌کند: «کیوبیت‌های ابررسانا به‌اندازه کافی بزرگ هستند که بتوان آنها را کنترل کرد. سایر سیستم‌ها خطاهای درونی کمتری دارند، اما اگر خیلی کوچک باشند، نمی‌توان مدارها را به‌درستی کنترل کرد.»

گوگل و آی‌بی‌ام، هر دو از پالس‌های میکروویو برای کنترل کیوبیت‌هایشان استفاده می‌کنند و احتمال نسبی حالت صفر یا یک بودنشان را تغییر می‌دهند. اما

رویکردهایشان اندکی متفاوت است. گیدئون لیچفیلد (Gideon Lichfield) در مقاله‌ای که در نشریه مرور فناوری ام‌آی‌تی (MIT Technology Review) منتشر شد، توضیح می‌دهد: «نقص‌های ریز در ساخت، به این معنی است که هیچ دو کیوبیتی به پالس‌هایی با فرکانس یکسان پاسخ نمی‌دهند. دو راه‌حل برای این مسئله وجود دارد: فرکانس پالس‌ها را برای یافتن «نقطه مطلوب» (Sweet Spot) هر کیوبیت تغییر دهید(مانند آنکه کلیدی برتراش را در قفل تکان بدهید تا بالاخره قفل باز شود) یا از میدان‌های مغناطیسی برای «تنظیم» هر کیوبیت در فرکانس مناسب استفاده کنید.»

گوگل از رویکرد دوم استفاده می‌کند و با عبور جریان از سیستم، پژوهشگران می‌توانند آستانه های هر حالت و نقاط قوت اتصال بین کیوبیت‌ها را اصلاح کنند که آنها را قادر می‌سازد «درهم‌تنیده» (Entangled) شوند. کیوبیت‌های گوگل سریع‌تر و دقیق‌ترند، اما شاید در درازمدت به‌اندازه روش ساده‌تر و پایدارتر آی‌بی‌ام در تغییر فرکانس پالس، قابل‌اعتماد نباشند.

ثابت شده است که حل این چالش فنی، فقط نیمی از مشکل را برطرف می‌کند. پدیده‌هایی که کیوبیت‌های ابررسانا بر آنها تکیه می‌کنند فقط در دمای فوق‌العاده کم پدیدار می‌شوند که این مورد فقط یکی از دلایلی است که درست شدنشان را بسیار دشوار می‌کند. مگرانت می‌گوید: «ما بیشتر مشکلاتمان را در این زمینه به‌طور نامتوازن به ابتدای کار اختصاص داده‌ایم؛ یعنی تمام مشکلات در روز اول پدیدار می‌شوند، هنگامی‌که می‌خواهید کیوبیت بسازید. باید بسیار سخت کار کنید تا عملکرد خوبی داشته باشید.»

تراشه ۵۳ کیوبیتی سیکمور گوگل در پایین یکی از «زَم‌پا»های بزرگ در آزمایشگاه قرار دارد، جایی که دما بسیار پایین نگه داشته می‌شود. همانند مدل قبلی آن، بریستلکون (Bristlecone)، سیکمور نیز در دانشگاه کالیفرنیا در سانتا باربارا ساخته شد که مانند بیسکویت اوریو]شامل دو تکه بیسکویت با کِرِم در میان آنها] برای ساخت اتصال شکننده جوزفسون در کنار هم قرار گرفتند. زیر میکروسکوپ، هر کیوبیت شبیه علامت به‌علاوه نقره‌ای ریز است. خطوط نازک به لبه تراشه منتهی می‌شوند: در نهایت، آنها به سیم‌پیچ‌های آبی متصل می‌شوند که سیگنال ضعیف را از کیوبیت به یکی از رَک‌های

ماشین‌های اطراف هر «زَم‌پا» منتقل و تقویت می‌کنند.

سیم‌کشی یکی از دستگاه‌ها دو هفته طول می‌کشد. برای افزایش تعداد کیوبیت، گوگل باید راه‌حلی جدید برای سیم‌کشی پیدا کند که فضایی کمتر اشغال کند یا راهی برای کنترل کیوبیت از داخل دستگاه زَم‌پا بیابد. مگرانت می‌گوید: «اگر بخواهید دما را تا ۱۰ میلی‌کلوین پایین بیاورید و خنک کنید، موارد بسیاری خراب می‌شوند.» مایکروسافت و گوگل هم‌اکنون در حال کار روی تراشه‌های کلاسیکی‌اند که برای کنترل کیوبیت‌ها بدون افزودن تداخل بتوانند در دمای پایین‌تر کار کنند.

هری پاتر و ماجورانای گم‌شده

در طی ده سال گذشته، رقابتی فزاینده در تعداد کیوبیت‌های مدعای شرکت‌های مختلف به وجود آمده است. در سال ۲۰۱۶، گوگل مولکول هیدروژنی را با استفاده از رایانه کوانتومی ۹ بیتی شبیه‌سازی کرد. در سال ۲۰۱۷، اینتل به هفده کیوبیت رسید و آی‌بی‌ام، تراشه پنجاه کیوبیتی ساخت که می‌تواند حالت کوانتومی‌اش را به‌مدت پنجاه میکروثانیه حفظ کند. در سال ۲۰۱۸، گوگل از بریستلکون، پردازنده ۷۲ کیوبیتی‌اش، رونمایی کرد و در سال ۲۰۱۹، آی‌بی‌ام اولین رایانه کوانتومی تجاری بیست کیوبیتی‌اش به نام «IBM Q System One» را با هیاهوی رسانه‌ای راه‌اندازی کرد.

دی-ویو (D-Wave)، شرکتی مستقر در کانادا، همیشه متفاوت بوده است. این شرکت از اواخر دهه ۱۹۹۰ رایانه‌های کوانتومی تجاری خود را می‌فروشد و ادعا می‌کند چندین هزار «کیوبیت انیلینگ» (Annealing Qubit) در دستگاه‌هایش دارد، اما اینها مبنی بر فناوری متفاوتی‌اند که فقط برای حل انواع خاصی از مشکلات مفید است. پیتر چاپمن از شرکت یون‌کیو آن را به تفاوت بین ماشین‌حساب دیجیتالی و رایانه تشبیه می‌کند.

راب یانگ (Rob Young)، مدیر مرکز فناوری کوانتومی دانشگاه لنکستر، برخی از شرکت‌ها را معتبر نبودن نحوه اعلام این پیشرفت‌ها متهم می‌کند. او می‌گوید: «یک سؤال مهم وجود دارد: چگونه یافته‌هایتان را بدون اینکه بیش از حد احساساتی و هیجانی شوید تفسیر کنید.»

هر روز واضح‌تر می‌شود که تعداد کیوبیت‌ها تقریباً به‌اندازه آنچه هیک ریل (Heike Riel)، رئیس بخش علوم و فناوری در مرکز تحقیقات آی‌بی‌ام (IBM Research Europe)، «حجم کوانتومی» (Quantum Volume) می‌نامد، مهم نیست. حجم کوانتومی یعنی اینکه پیش از ناهمدوس شدن کیوبیت‌ها، چه مقدار محاسبات مفید می‌توان انجام داد. حجم کوانتومی ترکیبی از تعداد کیوبیت‌ها، نحوه سیم‌کشی کیوبیت‌ها و میزان دقت و اعتمادپذیری کیوبیت‌هاست. ریل می‌گوید: «البته تعداد کیوبیت‌ها مهم است، اما همه‌چیز نیست. حجم کوانتومی می‌گوید پیش از اینکه خطا نتیجه شما را بپوشاند، چقدر محاسبات مفید می‌توانید با دستگاه انجام دهید.»

با وجود تمام فناوری‌هایی که گوگل برای محافظت از کیوبیت‌هایش در برابر تداخل به کار می‌گیرد، باز هم میزان خطا به‌طرزی حیرت‌انگیز بالاست. کیوبیت‌ها معمولاً به حالت غلط می‌روند یا پیش از آنکه قرار بوده، ناهمدوس می‌شوند. اصلاح این خطاها امکان‌پذیر است، اما برای انجام این کار به کیوبیت بیشتری نیاز است و به کیوبیت‌های بیشتری برای اصلاح آن کیوبیت‌ها.

همچنین بین تعداد «کیوبیت‌های فیزیکی» (Physical Qubits) تراشه کوانتومی و تعداد «کیوبیت‌های منطقی» (Logical Qubits) که «کیوبیت‌های فیزیکی» شما را قادر می‌سازند با آنها کار کنید، تمایزی مهم وجود دارد. برای نمونه، تراشه سیکمور گوگل شاید ۵۳ کیوبیت فیزیکی داشته باشد، اما به سبب نیاز به استفاده از تعدادی از این کیوبیت‌ها برای تصحیح خطا، از نظر فنی معادل رایانه کوانتومی ۵۳ کیوبیتی نیست. پیتر شور (Peter Shor)، نظریه‌پرداز کوانتومی بسیار تأثیرگذار، می‌گوید: «اگر صدها کیوبیت منطقی می‌خواهید، به ده‌ها هزار کیوبیت فیزیکی احتیاج دارید که بسیار از آن فاصله داریم.»

با میزان خطای کنونی، برای اجرای الگوریتم‌هایی که در دنیای واقعی مفید باشند، به هزاران یا میلیون‌ها کیوبیت نیاز است. برای همین است که جان پریسکیل، فیزیک‌دانی که اصطلاح «برتری کوانتومی» را ابداع کرده است، به‌منظور به رسمیت شناختن این واقعیت که فاصله زیادی با دستگاه‌های عملی داریم، این دوره را «کوانتوم مقیاس متوسط نویزی» [Noisy Intermediate Scale Quantum (NISQ)] نامید.

همچنین به همین دلیل است که مایکروسافت متقاعد شده که کیوبیت‌های ابررسانا بن‌بست هستند. چتان نایاک می‌گوید: «ما هیچ روزنه امیدی برای رایانه‌های کوانتومی در مقیاس تجاری نمی‌بینیم که بتواند مشکلات حل‌نشدنی امروز را رفع کند.» در عوض، در مقر وسیع مایکروسافت در ردموند (Redmond) واشنگتن (که آن‌قدر بزرگ است که سریع‌ترین راه رفت‌وآمد بین جلسات استفاده از سرویس اوبر (Uber) است)، پژوهشگران در حال آزمایش روی یک دستگاه زَم‌پا هستند که بسیار شبیه زَم‌پای گوگل است، اما - اگر همه‌چیز طبق برنامه پیش برود - میزبان نوع بسیار متفاوتی از پردازنده کوانتومی خواهد بود. اگر صعود گوگل به کوه کوانتومی را بسیار سخت بدانیم، صعود مایکروسافت به‌طور بالقوه ناممکن است. مایکروسافت به‌جای ساخت کیوبیت‌های ابررسانا، در حال کوشش برای مهار نوع دیگری از کیوبیت‌هاست که به‌عنوان «کیوبیت توپولوژیکی» (Topological Qubit) شناخته می‌شود. تنها مشکل این است که کیوبیت‌های توپولوژیکی ممکن است در واقع وجود نداشته باشند. کریستا سوور (Krysta Svore)، مدیرکل بخش نرم‌افزار کوانتومی مایکروسافت، می‌گوید: «شاید ما به‌جای دو سرعت، در ماراتن هستیم.»

اگر کیوبیت‌های توپولوژیکی ساخته شوند، برای کیوبیت‌های ابررسانا که خارج شدن آنها از حالت برهم‌نهی سخت‌تر است، جایگزینی قوی‌ترند. در نتیجه، به ده برابر کیوبیت کمتر نیاز است. آنها کیوبیت‌هایی مبتنی بر ذره‌ای تئوری به نام «ذره ماجورانا» (Majorana Particle) هستند که حالت کیوبیت را همزمان در چندین مکان کدبندی می‌کند. چتان نایاک این امر را با استفاده از تشبیه هری پاتر توضیح می‌دهد.

نایاک می‌گوید: «شخصیت شرور اصلی داستان، ولدمورت (Voldemort)، روحش را به هفت قطعه به نام هورکراکس (Horcruxe) تقسیم می‌کند و هورکراکس‌ها را در سراسر دنیا گسترش می‌دهد تا نشود او را کشت. کاری که ما با کیوبیت توپولوژیکی‌مان انجام می‌دهیم، گسترش کیوبیت به شش ماجورانا است. اینها هورکراکس‌های ما هستند. اگر در یک محل روی یکی از آنها کاری انجام دهید، در واقع نمی‌توانید ولدمورت را بکشید. کیوبیت هنوز آنجا خواهد بود.»

تنها مشکل این است که دانشمندان هنوز از وجود ذرات ماجورانا کاملاً مطمئن

نیستند. از دهه ۱۹۳۰ درباره آنها نظریه‌پردازی شده است، اما شواهد تجربی، ردنشدنی و خالی از بحث نیستند. با این حال، چتان نایاک و کریستا سوور در گفت‌وگویی در ژانویه ۲۰۲۰، مطمئن حرف می‌زدند. نایاک گفت: «ما در تاریکی بـه دنبالش]دنبال ماجورانا[نیستیم و امیدواریم آن را پیدا کنیم. ما با استفاده از شبیه‌سازی داریم به مسیر درست هدایت می‌شویم.»

اگرچه به نظر می‌رسد هم‌اکنون کیوبیت‌های ابررسانا حرف اول را می‌زنند و دست‌بالا را دارند، هنوز مشخص نیست کدام فناوری از رایانه‌های کوانتومی آینده پشتیبانی خواهد کرد. ورلی می‌گوید: «مـا در دوران رقابت شـرکت ای‌ام‌دی (AMD) در برابر شـرکت اینتل نیستیم. ما در دوران لامپ‌های خلأ در مقابل دروازه‌های مکانیکی کوچکیم. فناوری‌های گوناگون، موفقیت‌هایی چشـمگیر خواهند داشـت، در حالی‌که برخی دیگر دچار رکود می‌شوند و ممکن است پیدا شدن مسیری مشـخص چندین دهه طول بکشد. آنها به در و دیوار می‌خورند و شـاید سـرانجام در برهه‌ای از زمان، به آرزویمان برای دسـتیابی به دستگاهی دارای میلیون‌ها کیوبیت و رایانه کوانتومی با کاربردهای عمومی برسیم.»

به‌عنوان نمونه، توسعه‌های اخیر در رایانش یون به‌دام‌افتاده می‌تواند زمینه‌ساز توسعه دستگاه‌های کوانتومی با هزاران یا میلیون‌ها کیوبیت باشد. در ژوئن سال ۲۰۲۰، کوانتوم یونیورسال (بخشی از دانشگاه ساسکس) اعلام کرد ۳٫۶ میلیون پوند بودجه برای شکل جدیدی از رایانش یونی به‌دام‌افتاده جمع‌آوری کرده است. به نظر می‌رسد قرار است در این رویکرد، بهترین بیت‌های رویکرد ابررسانایی گوگل و آی‌بی‌ام و روش تله یونی یون‌کیو ترکیب شوند.

وینفرد هنسـینگر (Winfried Hensinger)، یکی از بنیان‌گذاران و دانشـمند ارشـد در کوانتوم یونیورسال، اشـاره می‌کند که عامل محدودکننده بزرگ دستگاه گوگل، خود تراشه کوانتومی نیست، بلکه سیستم خنک‌کننده است که با افزایش تعداد کیوبیت‌ها، برای خنک‌کردن منطقه‌ای بزرگ‌تر بایسـتی بزرگ‌تـر و بزرگ‌تر شـود. از آنجا که کوانتوم یونیورسال از فناوری تله یونی استفاده می‌کند، چنین سرمایش زیادی ضروری نیست و راهی هوشمندانه برای حل مشـکل مقیاس‌پذیری (افزایش مقیاس) پیدا کرده است. به‌جـای اسـتفاده از پرتوهـای لیـزر، بـرای پشـتیبانی از میلیون‌هـا کیوبیت در دسـتگاه

کوانتومی به مقیاس کامل، به میلیون‌ها از آنها نیاز است، کوانتوم یونیورسال از میدان‌های الکتریکی برای کنترل کیوبیت استفاده می‌کند. از میکروویو برای جابه‌جایی کیوبیت بین حالت‌های انرژی استفاده می‌شود، اما به‌جای تلاش برای ضربه زدن دقیق به کیوبیت‌های منفرد با پالس‌های میکروویو، فناوری متعلق به یوکیو (UQ) در عوض از میدان‌های الکتریکی استفاده می‌کند تا کیوبیت‌ها را به حالتی تبدیل کند که پذیرای پالس‌های میکروویو جهانی باشند. این بی‌شباهت به نحوه استفاده گوگل از پالس‌های میکروویو برای تنظیم کیوبیت‌های ابررسانا نیست. این شرکت در حال کار روی ایجاد ماژول‌هایی است که بتوانند برای افزایش مقیاس سریع به یکدیگر متصل شوند: برای ارسال پیام از ماژولی به ماژول دیگر، یون مجبور می‌شود از شکافی ریز بین ماژول‌ها عبور کند، مانند عبور انتقال‌دهنده‌های عصبی بین سیناپس‌های مغز.

راه پیش رو هرچه باشد، چهل سال نظریه‌پردازی گذشته و ۲۵ سال پیشرفته‌ترین توسعه‌های سخت‌افزاری زمینه را برای این امر بسیار مهم فراهم کرده است. برتری کوانتومی به این معناست که الگوریتم‌های در حال توسعه می‌توانند آزمایش شوند و بهبود یابند و اینکه رایانش کوانتومی، از پزشکی گرفته تا کنترل ترافیک، می‌تواند آثار کوچکی بر دنیای واقعی داشته باشد، در حالی‌که منتظر می‌مانیم جنبه سخت‌افزاری پیشرفت کند. مگرانت می‌گوید: «برتری کوانتومی، سیگنالی برای ماست که می‌گوید ما وارد دوره کوانتوم مقیاس متوسط نویزی شده‌ایم. اکنون این سیستمِ به‌اندازه کافی بزرگ را داریم و می‌توانیم به‌جای استفاده از لپ‌تاپمان برویم و بازی کنیم.»

فصل سوم

قدرت تصاعدی

در می ۲۰۰۰، مؤسسه ریاضیات کِلِی (Clay Mathematics Institute) در پیتربورو نیوهمپشایر، مجموعه‌ای از هفت مسئله ریاضی به‌ظاهر حل‌نشدنی را ایجاد کرد و به هرکسی که می‌توانست آنها را حل کند، وعده یک میلیون دلار جایزه داد. تا زمان نگارش این کتاب فقط یکی از این «مسائل جایزه هزاره» به نام «حدس پوانکاره» حل شده است. ریاضی‌دان روسی گوشه‌گیری به نام گریگوری پرلمن (Grigori Perelman) این مسئله را حل کرد. البته پرلمن جایزه را نپذیرفت و برای همیشه بازنشسته شد.

مسلماً مهم‌ترین چالشی که این مؤسسه مطرح کرده است، «مسئله پی در مقابل ان‌پی» (P versus NP problem) است. «پی» به تمام مسائل ریاضی اشاره دارد که رایانه‌ها به‌راحتی آنها را در «زمان چندجمله‌ای» (Polynomial Time) حل می‌کنند. این مفهوم برای غیرریاضی‌دان‌ها قدری دشوار است، اما در اصل، به‌معنای هرچیزی است که ابررایانه‌ای مانند سامیت می‌تواند در زمانی معقول از عهده حل کردن آن برآید. از طرف دیگر، «مسائل ان‌پی» مواردی هستند که در یک زمان معقول به‌راحتی حل‌شدنی نیستند، اما در صورتی که پاسخی بالقوه به شما داده شود، بررسی درستی یا نادرستی این راه‌حل آسان است.

یک مثال کلاسیک از مسئله ان‌پی، «فاکتورگیری» (Factoring) است: تجزیه عددی به کوچک‌ترین فاکتورهای اصلی ممکن. بنابراین، برای نمونه، فاکتورهای اصلی ۳۵، پنج و هفت هستند: دو عددی که می‌توان با هم ضرب کرد تا ۳۵ حاصل شود، اما خود آن فاکتورها (پنج و هفت) بر هیچ عدد دیگری تقسیم‌پذیر نیستند. از نظر محاسباتی، یافتن فاکتورهای اصلی دشوار است، زیرا به نظر می‌رسد هیچ الگوی واقعی‌ای وجود ندارد. بنابراین، ابتدا باید همه مضرب‌های دو، سپس مضرب‌های سه و در ادامه باقی را دستی حذف کنید تا فقط اعداد اول باقی بمانند. این کار برای اعداد کوچک ساده است، اما این چالش در اعداد بزرگ به‌طور نمایی بزرگ می‌شود. اما بررسی درستی پاسخ همیشه آسان است: به‌راحتی اعداد اول را در هم ضرب کنید و ببینید آیا نتیجه با عدد اصلی شما مطابقت دارد یا خیر.

بحثی که ریاضی‌دان‌ها سال‌ها درگیر آن بوده‌اند این است که آیا «پی» برابر «ان‌پی» است یا خیر. جایزه یک میلیون دلاری به کسی تعلق می‌گیرد که بتواند ثابت کند قطعاً

هر مسئله‌ای که بررسی آن آسان باشد حل کردنش نیز ساده است و برعکس. اگر پی برابر ان‌پی باشد، به این معنی است که رایانه‌ها می‌توانند تعداد زیادی از مسائل به‌ظاهر حل‌نشدنی را حل کنند، اما هنوز الگوریتمی مناسب پیدا نکرده‌ایم. اگر پی برابر ان‌پی نباشد، به این معنی است که چالش‌های محاسباتی خاصی وجود دارند که شاید همیشه حل‌نشدنی و فراتر از توانمان باقی بمانند. بخشی از جذابیت رایانش کوانتومی این است که برخی از مسائل ان‌پی را به حل شدن در مدت زمانی معقول نزدیک می‌کند، به‌شرط آنکه بتوانیم نوع مناسب الگوریتم را پیدا کنیم.

یکی از سوءتفاهم‌های اصلی در مورد رایانه‌های کوانتومی این است که مردم تصور می‌کنند آنها صرفاً نوعی ابررایانه سریع‌ترند؛ فناوری جدیدی که می‌توانیم آن را برای حل همه مسائلی که امروزه با آنها مواجهیم، به کار بگیریم و هزاران یا میلیون‌ها بار سریع‌تر به پاسخ دست یابیم. متأسفانه مسئله این نیست. آندره روچتو (Andrea Rocchetto)، پژوهشگر رایانش کوانتومی دانشگاه تگزاس در آستین، می‌گوید: «انواع مسائلی که رایانه‌های کوانتومی می‌توانند در آنها از مزیتی برخوردار باشند، مسائل ان‌پی هستند که از مسئله ان‌پی عمومی ساختار بیشتری دارند. این مزیتی است که می‌توانید از آن بهره‌مند شوید تا تعداد مراحل محاسباتی لازم برای حل مسئله را کاهش دهد.»

روچتو می‌گوید: «فاکتورگیری در مرز بین مسائلی است که این‌قدر ساختار دارند که به‌راحتی می‌توان راه‌حلی کارآمد (مسائل پی) برای آنها پیدا کرد و مسائلی که حتی رایانه کوانتومی نیز به‌سختی می‌تواند ساختاری برای آنها پیدا کند.» او می‌گوید: «رایانه‌های کوانتومی به ساختار نیاز دارند. بدون ساختار، هیچ جادویی وجود نخواهد داشت؛ رایانه کوانتومی، نوعی جعبه سیاه نیست که هر مسئله‌ای را به آن بدهید، جوابی به شما بدهد. مسئولیت این امر بر عهده ریاضی‌دانان و دانشمندان علوم کامپیوتر است که الگوریتم‌های هوشمندی را بیابند تا بتوانند ساختار مسائل ان‌پی را کشف و از آن بهره‌برداری کنند تا آنها را در دسترس رایانه‌های کوانتومی قرار دهند. در سال ۱۹۹۴، یکی از پژوهشگران آزمایشگاه‌های بل (Bell Labs) این کار را انجام داد. کشف او می‌تواند نتایج زیادی برای رایانش کوانتومی، رمزنگاری و موارد بسیار دیگری داشته باشد.

ضریب کیفیت

پیتر شـور، ریاضی‌دان، شـاعری آماتور و خالق یکـی از الگوریتم‌های بسـیار تأثیرگذار تاریخ است. در سال ۱۹۹۴، شور در آزمایشگاه‌های بل در بخش تحقیق و توسعه شرکت مخابرات کار می‌کرد و در آنجا در چندین گفت‌وگو در زمینه رمزگذاری کوانتومی شرکت کـرد. او در دانشـگاه، فیزیک کوانتومی خوانـده بود و شـیفته کاربردهای بالقـوه رایانش کوانتومی شد (قبلاً توضیح داده شد)؛ یعنی آنچه ناشی از ویژگی عجیب تداخل کوانتومی بود که مسیرهای مختلف بالقوه‌ای هستند که فوتون برای ایجاد نتیجه نهایی می‌تواند طی کند تا با فوتون دیگری تداخل ایجاد کند. اگرچه رایانه‌های کوانتومی هنوز سال‌ها با تبدیل شدن به واقعیتی فیزیکی فاصله داشتند، شور و دیگران شروع کردند به فکر کردن در مورد الگوریتم‌هایی کـه روی این رایانه‌ها اجرا خواهند شـد و کارهایی کـه این رایانه‌ها انجام خواهند داد.

در ساده‌ترین شـکل، الگوریتم صرفاً مجموعه‌ای از دسـتورالعمل‌ها یا قوانینی است که در عملیات حل مسـئله پیگیری می‌شـود، اما الگوریتم‌های کوانتومـی باید مطابق با خصوصیات منحصربه‌فـرد مکانیک کوانتومی طراحی شـوند. شـور توضیـح می‌دهد: «رایانه‌های کوانتومی از تداخل در الگوریتم‌های اساسی خود استفاده می‌کنند. می‌توانید به فکر محاسبه از طریق انواع مختلف مسـیرهایی باشید که هر کدام مرحله‌ای مرتبط دارد. اگر به‌نوعی بتوانید محاسـبه‌ای ترتیب دهید تا تمام پاسـخ‌های صحیح مرحله‌ای یکسان داشته باشند، احتمال یافتن جواب صحیح بیشتر می‌شود.»

الگوریتم شور این بینش را در جهت ایجاد روشی برای فاکتورگیری اعداد بزرگ به کار می‌برد. از مجوعه‌ای از ترفندهای ریاضی استفاده می‌کند تا عدد مورد نظر را به «موجی» از اعـداد کوچک‌تـر فاکتورگیری‌شـده تبدیل کند کـه در برخـی از توالی‌های ثابـت تکرار می‌شوند. او دریافت که ریتم و فرکانس این موج که با نام دوره تناوب آن شناخته می‌شود، به فاکتورهای عدد اصلی مربوط می‌شود. شور این کار را به «توری پراش» (Diffraction Grating) تشبیه می‌کند که جسمی فیزیکی مانند منشور است و نور را به طول موج‌های مختلف تقسیم می‌کند: پرتوی نور سفید از یک طرف منشور وارد و رنگین‌کمانی از انتهای

دیگر آن پدیدار می‌شود. همه نور یک طول موج خاص در یک نقطه از فضا تقویت می‌شود و طول موج دیگر در نقطه‌ای متفاوت تقویت می‌شود. الگوریتم شور، مانند یک منشور ریاضی عمل می‌کند: اعداد بزرگ، از انتهایی وارد می‌شوند و فاکتورها از انتهای دیگر بیرون می‌آیند.

روش شور برای رایانه‌های کلاسیک کاری سخت و سنگین است، اما مهم‌تر از همه، ساختار آن به‌گونه‌ای است که می‌توان محاسبات مربوطه را همزمان روی یک رایانه کوانتومی انجام داد. روچتو می‌گوید: «این مطلب، اولین مورد اثبات‌پذیر مسئله‌ای است که در آن، یک رایانه کلاسیک نیازمند گسترش تصاعدی منابع است، در صورتی که یک رایانه کوانتومی نیازی به این کار ندارد.» الگوریتم شور می‌تواند به‌طور تصاعدی سریع‌تر از رایانه‌های کلاسیک، از اعداد بزرگ فاکتورگیری کند؛ هرچه عددی بزرگ‌تر باشد، رایانه کوانتومی مزیت بیشتری دارد. این مطلب باعث ایجاد شوک در جامعه کوانتومی شد و به‌خاطر تأثیراتش بر امنیت سایبری، کمک بزرگی به آغاز شکل‌گیری این حوزه کرد که در فصل بعد مفصل به آن خواهیم پرداخت. روچتو می‌گوید: «این همان چیزی است که باعث ایجاد علاقه زیادی در این حوزه شد و چه از لحاظ تئوری چه از نظر تجاری و دفاعی موفقیت بزرگ چشمگیری برای هر دو حوزه تجاری و دفاعی بود.»

به همین ترتیب، کشف موفقیت‌های چشمگیر قدرتمند دشوارتر شده است. اکثر الگوریتم‌های کوانتومی دیگری که تاکنون توسعه یافته‌اند، به‌جای افزایش تصاعدی عرضه‌شده در الگوریتم شور، فقط «تسریع درجه دوم» (Quadratic Speed-up) متوسط‌تری فراهم می‌کنند. روچتو می‌گوید: «تسریع درجه دوم یعنی زمان اجرای الگوریتم کلاسیک را بهبود می‌بخشیم، اما این برای آسان کردن مسئله کافی نیست، هرچند می‌تواند برای سناریوهای دنیای واقعی بسیار مناسب باشد. تشخیص این تسریع‌های درجه دوم دشوارتر است (در عمل، مسئله آزمودن است) اما هنوز هم می‌توانند بسیار مهم باشند. می‌توانند به صرفه‌جویی در هزینه‌های هنگفت شرکت‌ها کمک کنند.»

در سال ۱۹۹۶، یکی دیگر از محققان آزمایشگاه‌های بل، الگوریتمی را ابداع کرد که می‌تواند توضیح دهد چرا به‌ویژه گوگل این‌همه پول برای ساخت رایانه کوانتومی خرج

می‌کند. لو گرور (Lov Grover) نشان داد که می‌توان از رایانه‌های کوانتومی برای سرعت بخشیدن به جست‌وجو در یک پایگاه داده انبوه نامرتب بهره برد. اگر دفترچه تلفن را به رایانه کلاسیک بدهید و از آن بخواهید شماره‌ای خاص را پیدا کند، باید هر ورودی را به‌ترتیب بررسی کند تا شماره درست را بیابد. می‌توانید با استفاده از پردازنده‌های متعدد برای حل مسئله، سرعت جست‌وجو را افزایش دهید. مثلاً یک پردازنده از بالای فهرست شروع کند و دیگری از پایین فهرست. اما میانگین زمان موردنیاز با توجه به اندازه فهرست همچنان به‌سرعت رشد می‌کند.

الگوریتم گرور، روشی را برای جست‌وجوی پایگاه داده با استفاده از قدرت تداخل کوانتومی توصیف می‌کند. با رمزگذاری هریک از موارد موجود در فهرست در حالت برهم‌نهی، می‌توان امواج این موارد را طوری دست‌کاری کرد که پاسخ‌های اشتباه، یکدیگر را لغو و پاسخ‌های درست یکدیگر را تقویت کنند. توصیف جزئیات این روش نیز بسیار پیچیده است، اما نتایج آن بسیار زیاد است. طی چندین مرحله پردازش، صرفاً پاسخ صحیح مشخص می‌شود، به‌طوری که انگار تمام شماره‌های دیگر دفترچه تلفن به‌آرامی ناپدید می‌شوند. گرور نشان داد که اگر رایانه کلاسیک برای یافتن شماره موردنظر در فهرستی با طول یک میلیون ورودی، به‌طور میانگین لازم باشد پانصد هزار مورد را جست‌وجو کند، کامپیوتر کوانتومی با اجرای الگوریتم او فقط باید هزار مورد را جست‌وجو کند. این مورد، در مقایسه با دستگاه‌های کلاسیک تسریع درجه دوم بالاتری فراهم می‌کند. دستگاه کوانتومی فقط باید ریشه مربع تعداد اقلام را جست‌وجو کند؛ یعنی برای یک میلیون مورد، فقط بیست کیوبیت نیاز است.

شور و گرور، با همدیگر رایانه‌های کوانتومی را به دو سلاح قدرتمند مجهز کردند که از نظر تئوری نوید دگرگونی در تمامی حوزه‌ها را، از رمزنگاری گرفته تا امور مالی، می‌دهد. اما در دنیای واقعی، جایی که معادلات و الگوریتم‌های ظریف با واقعیت روبه‌رو می‌شوند، همه‌چیز بسیار پیچیده‌تر می‌شود.

حاشیه خطا

الگوریتم‌های شور و گرور برای رایانه کوانتومی کامل طراحی شده‌اند. اما در اواسط دهه

۱۹۹۰، هنگامی که این الگوریتم‌ها نوشته شدند، چنین چیزی وجود نداشت و هنوز هم وجود ندارد. علی‌رغم ادعای برتری کوانتومی، ما هنوز در دوره «کوانتوم مقیاس متوسط نویزی» هستیم، به این معنا که بهترین دستگاه‌ها هنوز پر از نویز و مستعد خطا هستند و کیوبیت‌های آنها هنوز به حالت نامطلوب تبدیل یا از برهم‌نهی خارج می‌شوند. حتی بهترین رایانه‌های کوانتومی که تا دمای تقریباً ناممکن سرد و پشت محافظ‌ها ایزوله می‌شوند، هنوز هم نرخ خطای بسیار بالایی دارند. مطابق سخنرانی جان پریسکیل در سال ۲۰۱۹، احتمال خطا در هر گیت (Gate) دو کیوبیتی در سیستم کوانتومی با استفاده از بهترین سخت‌افزار موجود کنونی، حدود ۰/۱ درصد است. به‌طور مشابه، احتمال خطا در هر اندازه‌گیری، حدود یک درصد است، که برای هرچیز مفیدی به‌شدت زیاد است. راب یانگ می‌گوید: «تئوری، خیلی جلوتر از آزمایش است. مسئله واقعاً بزرگ این است که اکثریت قریب‌به‌اتفاق الگوریتم‌هایی که امروزه در نظر گرفته می‌شوند، بسیار جلوتر از معیارهای عملکرد سیستم‌های کوانتومی واقعی هستند که شما نمی‌دانید همیشه مفید خواهند بود یا خیر.»

مدت‌ها بود که بسیاری فکر می‌کردند مشکل اصلاح خطا، حل‌نشدنی است: نقصی مهلک در رایانش کوانتومی. برخی از پژوهشگران هنوز این مطلب را باور دارند. گیل کالایی (Gil Kalai)، استاد دانشگاه ییل، در سال ۲۰۱۹ به وایرد (WIRED) گفت: «تجزیه‌وتحلیل من نشان می‌دهد که رایانه‌های کوانتومی پُرنویز چند ده کیوبیتی، میزانی از قدرت محاسباتی ابتدایی را فراهم می‌کنند که به‌کارگیری آنها به‌عنوان عناصر سازنده لازم برای ساخت رایانه‌های کوانتومی در مقیاس وسیع‌تر، به‌سادگی امکان‌پذیر نخواهد بود.»

خطاها برای رایانه‌های کلاسیک نیز مشکل‌سازند، اما سیستم‌های به‌خوبی تثبیت‌شده‌ای برای شناسایی و اصلاح آنها وجود دارند که بر اساس ارسال چندین کپی از همان پیام و مقایسه‌شان از نظر تفاوت‌ها، یا ارسال هر بیت به تعداد دفعات مشخصی عمل می‌کنند. بنابراین، حتی اگر یک یا دوتا از آنها به‌طور تصادفی تغییر وضعیت بدهند، پیام کلی همچنان واضح است. یا از آنچه با عنوان «بیت‌های توازن» (Parity Bits) شناخته می‌شوند برای بررسی اینکه آیا پیام به‌درستی دریافت شده است یا نه، استفاده کنید.

این موضوع در رایانه‌های کوانتومی کارآیی ندارد، زیرا هر یک از این سیستم‌ها شامل اندازه‌گیری بیت‌ها هستند که آنها را از حالت برهم‌نهی خارج می‌کند و منافع مرتبط را از بین می‌برد. کاهش برخی از خطاها صرفاً با صدها یا هزاران بار تکرار هر محاسبه امکان‌پذیر است، کاری که پژوهشگران گوگل در طول آزمایش برتری کوانتومی‌شان انجام داده‌اند؛ اندازه‌گیری‌های تکراری به جدایی سیگنال از نویز کمک می‌کنند. اما کاهش نویز، مشکل را حل نمی‌کند، به‌ویژه هنگامی که می‌کوشید آن را به دستگاه‌های بزرگ‌تر دارای کیوبیت‌های بیشتر، افزایش مقیاس دهید.

با این حال، کار هوشمندانه شور و دیگران ثابت کرد که اگر کیوبیت کافی داشته باشید، تصحیح خطای کوانتومی امکان‌پذیر است. جورج جانسون (George Johnson) در کتاب «میانبری در زمان» (A Shortcut Through Time) توضیح می‌دهد: «برای محافظت در برابر خطاهای متعدد ممکن است لازم باشد هر کیوبیت را با ده‌ها کیوبیت مازاد احاطه کنید و سپس، وقتی خطایی پیدا شد، نگران باشید که خطاهای بیشتری به خود فرایند اصلاح رسوخ خواهند کرد. محافظت در برابر این مسئله، به کیوبیت‌های مازاد بیشتری احتیاج دارد.»

این الگوریتم‌های تصحیح خطا به‌گونه‌ای طراحی شده‌اند که خطا را بدون تأثیرگذاری بر محاسبات اندازه‌گیری کنند؛ آنها از بیت‌های توازن استفاده می‌کنند که بخشی از محاسبات نیستند، اما اگر اشتباهی رخ دهد تحت‌تأثیر آن قرار می‌گیرند. از سیستمی مشابه برای شماره «کارت‌های اعتباری بانک» استفاده می‌شود: پانزده رقم اول شماره روی کارت را بانک و صادرکننده کارت تعیین می‌کند، اما رقم نهایی با وارد کردن پانزده رقم اول به الگوریتمی خاص ساخته می‌شود. این امر به هر نهادی امکان می‌دهد بدون دانستن شماره کارت اصلی، جزئیات کارت فرد را برای بررسی اشتباهات پردازش کند، اما به منابع اضافی (در این حالت، به ارقام اضافی در شماره کارت) نیاز دارد.

شور می‌گوید: «مشکل اصلی در تصحیح خطا این است که اگر بخواهید خطاها را اصلاح کنید و دروازه‌های کوانتومی خیلی دقیقی نداشته باشید، به میزان سربار بسیار زیادی نیاز است. تعداد کیوبیت‌ها و زمان لازم برای اجرای رایانه، هزاران یا ده‌ها هزار برابر خواهد شد.» در حالی که الگوریتم شور روی کاغذ فقط به چند هزار کیوبیت نیاز دارد، در

عمل، هنگام فاکتورگیری برای پرداختن به تصحیح خطا به تعداد بیت خیلی بیشتری نیاز است. طبق گفته بویکسو، شاید یک میلیون کیوبیت فیزیکی یا بیشتر نیاز باشد. «از نظر کاربرد عملی، شما قطعاً به رایانه کوانتومی مقاوم در برابر خطا یا پیشرفت چشمگیری در خود الگوریتم نیاز خواهید داشت». برخی محققان روی الگوریتم‌های تحمل خطایی کار می‌کنند که به‌خاطر نوع نگارششان، به‌طور طبیعی در برابر خطاها مقاوم‌اند. اما حتی این موارد نیز مستلزم پیشرفت‌های گسترده در سخت‌افزار خواهد بود. علی‌رغم دستیابی گوگل به برتری کوانتومی، هنوز در دوران کوانتوم مقیاس متوسط نویزی هستیم و تا دستیابی به رایانه‌های کوانتومی کاربردی فاصله زیادی داریم.

اما این امر، مانع ادامه کار شرکت‌ها نشده است. شرکت‌ها برای به کار بستن برخی از تکنیک‌های رایانش کوانتومی در تمامی حوزه‌ها، از «کاهش ترافیک» گرفته تا «تشخیص سرطان»، در تلاش‌اند.

ترافیک روان

سیاتل شهری است که شرکت‌های بزرگ فناوری (بیگ‌تک‌ها) در حال بلعیدنش هستند. در محوطه بین خانه مایکروسافت در ردموند و اشتهای سیری‌ناپذیر آمازون، این شهر به آشفته‌بازار جرثقیل‌ها و ساخت‌وسازهایی تبدیل شده است که مشکل بسته شدن جاده‌های متعدد را به مشکلات ترافیکی ناشی از محوطه بندر و آب‌وهوای نامساعد افزوده است و حادثه‌ای در یکی از پل‌های متعدد شهر می‌تواند به‌سرعت منجر به ایجاد ترافیکی طولانی شود.

اپلیکیشن‌های نقشه‌برداری که برای تغییر مسیر رانندگان در صورت وجود تأخیرهای احتمالی طراحی شده‌اند، در حقیقت می‌توانند مشکل را بدتر کنند. آنها خودخواه‌اند، وقتی مسیری را درخواست می‌کنید، گوگل مپس (Google Maps)، برای شما سریع‌ترین مسیر را در آن لحظه پیدا می‌کند، بدون اینکه در نظر داشته باشد که سفر شما چگونه ممکن است سفر سایر کاربران را به تأخیر بیندازد یا چگونه استفاده همزمان صدها نفر از همان بخش از جاده به ترافیک منجر خواهد شد. یک سیستم مسیریابی متعادل‌تر، هریک از درخواست مسیرها را با همدیگر بررسی و مسیرهایی را پیشنهاد می‌کند که به

کاهش ترافیک کمک برساند و جریان سریع‌تر و روان‌تر ترافیک را حفظ کند. اما یک مانع عملی وجود دارد: چنین سیستمی به قدرت محاسباتی بالایی نیاز دارد. این امر همان چیزی است که با عنوان «مسئله بهینه‌سازی» (Optimization Problem) شناخته می‌شود. هزاران نوع مختلف از این مسئله وجود دارد، از یافتن بهترین ترتیب توقف‌ها برای راننده تحویل سفارشات گرفته تا فهمیدن اینکه پیش از ارسال، چند بسته پشت کامیون جا می‌گیرند. هر موضوعی که شامل به حداکثر رساندن کارایی یا به حداقل رساندن هزینه‌ها شود، مسئله بهینه‌سازی است که اکنون به‌طور گسترده از طریق آزمون‌وخطا انجام می‌شود.

بیشتر مسائل بهینه‌سازی، از جمله مسئله معروف فروشنده دوره‌گرد، ساختار زیربنایی ندارند که به رایانه‌های کوانتومی اجازه و امکان بدهد که در مقایسه با رایانه‌های کلاسیک مسائل را با سرعت نمایی حل کنند. اما به‌گفته کریستوفر ساووی (Christopher Savoie) از رایانش زاپاتا (Zapata Computing)، رایانه‌های کوانتومی مطمئناً می‌توانند مسائل بهینه‌سازی را بسیار سریع‌تر حل کنند و پاسخ‌هایی واقعاً بهتری پیدا کنند. اگرچه هنوز در دوران «رایانه‌های پیشاکوانتومی» زندگی می‌کنیم، می‌توانیم از الگوریتم‌هایی که برای اجرای آنها در نظر گرفته شده‌اند جهت حل مسائل بهینه‌سازی کوچک‌تر در سخت‌افزارهای کلاسیک موجود استفاده کنیم.

برای مثال، در سال ۲۰۱۸، پژوهشگران کوانتومی مایکروسافت در پروژه‌ای با هدف بهبود جریان ترافیک در سیاتل با شرکت فورد همکاری کردند. آنها یک مدل مجازی از ترافیک در شهر ساختند و شبیه‌سازی‌ای با بیش از پنج هزار وسیله نقلیه اجرا کردند که هرکدام یکی از ده مسیر مختلف را همزمان درخواست می‌کردند. به‌گفته مایکروسافت، به‌کارگیری الگوریتم‌های الهام‌گرفته‌شده از الگوریتم‌های کوانتومی به‌جای مسیریابی خودخواهانه سیستم‌های کنونی، اگر در دنیای واقعی به کار گرفته شوند، کاهش ۷۳ درصدی ازدحام و کاهش هشت درصدی زمان رفت‌وآمد را به دنبال دارد که ذخیره بیش از ۵۵٫۰۰۰ ساعت در سال را برای رانندگان این وسایل نقلیه به ارمغان می‌آورد. بن پورتر (Ben Porter)، مدیر توسعه کسب‌وکار برای عملیات کوانتومی مایکروسافت، می‌گوید: «بهینه‌سازی، مثمرثمرترین حوزه برای تحقیق و بررسی است، زیرا مسائلی پیچیده

وجود دارند که در هر صنعتی به‌وجود می‌آیند. مهم نیست درباره چه صنعتی صحبت می‌کنید، خودرو، هوافضا یا خدمات رفاهی، حوزه‌های غنی برای تحقیق و بررسی وجود دارند.»

خدمات مالی، یکی دیگر از حوزه‌های بالقوه سودآوری است که رایانه‌های کوانتومی می‌توانند در آینده بر آن تأثیر زیادی داشته باشند. سقوط مالی سال ۲۰۰۸ تا حدی ناشی از ناتوانی بانک‌ها و ناظران در تحلیل صحیح ریسک در سیستمی پیچیده بود. پژوهشگرانی که با آی‌بی‌ام کار می‌کنند، الگوریتم‌های کوانتومی‌ای را می‌آزمودند تا دریابند که آیا الگوریتم‌های کوانتومی در اجرای «شبیه‌سازی مونت کارلو» (Monte Carlo Simulation)، روشی معمول برای تجزیه‌وتحلیل ریسک که بیشتر اوقات روزها طول می‌کشد تا میلیون‌ها شبیه‌سازی از سناریویی خاص را انجام دهد، بهتر از الگوریتم‌های کلاسیک هستند یا خیر. استفان ورنر (Stefan Woerner)، ریاضی‌دان آی‌بی‌ام می‌گوید: «رایانه کوانتومی می‌تواند تسریع درجه دومی را فراهم کند که در آن به‌جای چندین میلیون سناریو، فقط به چند هزار سناریو نیاز است تا به همان دقت دست یابیم.» فقط کفایت می‌کند زمان شبیه‌سازی مونت کارلو را از محاسباتی که باید در طی یک شب انجام شوند به محاسباتی تبدیل کرد که تقریباً همزمان انجام شوند. در این صورت، پیامدهای آن برای خریداران و فروشندگان بازار بورس سهام، ملموس است.

اما شاید یکی از کاربردهای بسیار جذاب رایانش کوانتومی در حوزه «یادگیری ماشین» (Machine Learning) باشد. در طی دهه‌ها، الگوریتم‌های رایانه‌های کلاسیک دستی نوشته می‌شدند که با مشقت بسیار زیاد رمزگذارانی همراه بود که مانند آشپزها دستورالعمل‌های دقیق را یادداشت می‌کردند. اما هرچه قدرت رایانش، ارزان‌تر شد، هوش مصنوعی و یادگیری ماشین مهم‌تر شدند. اکنون این بسیار متحمل است که الگوریتم‌های همه‌چیز، از شناسایی چهره گرفته تا ترجمه آنلاین، از طریق آموزش دادن یک برنامه با اهداف عمومی از طریق مجموعه‌ای گسترده از داده‌ها ایجاد شوند. این فناوری‌ها بسیار قدرتمندند و برای نمونه در تشخیص سرطان ریه از طریق اسکن از متخصصان انسانی موفق‌تر عمل می‌کنند. اما آنها فقط به‌اندازه داده‌هایی که در اختیارشان قرار می‌دهید، خوب عمل می‌کنند. اگر اطلاعات کافی در اختیارشان قرار

ندهید یا داده‌ها سوگیری داشته باشند، در نهایت با الگوریتم‌هایی ناقص و جانبدارانه مواجه خواهید شد.

رایانش کوانتومی از طریق فرایندی که با عنوان «مدل‌سازی مولد» (Generative Modelling) شناخته می‌شود، امکان ایجاد داده‌هایی را فراهم می‌کند که در واقع هیچ‌یک از آنها در دنیای واقعی وجود ندارند. مدل‌سازی مولد فرایندی است که پیش از این، رایانه‌های کلاسیک انجام می‌دادند، اما دستگاه‌های کوانتومی می‌توانند آن را سریع‌تر و در مقیاسی بزرگ‌تر انجام دهند. ساووی توضیح می‌دهد: «اگر یک نمونه از صد چیز را داشته باشیم، می‌توانیم از مدل‌سازی مولد برای ایجاد مواردی مشابه استفاده کنیم. از قدرت اضافی رایانه‌های کوانتومی می‌توان برای برون‌یابی مجموعه داده‌های محدود استفاده کرد و به الگوریتم‌های یادگیری ماشین، داده داد. حتی زمانی که داده‌ای نداریم.» ساووی می‌گوید: «بهبود این امر به ما امکان می‌دهد با داده‌های ناچیز کارهایی، از جست‌وجوی سرطان نادر ریه در ام‌آرآی گرفته تا تشخیص چهره هنگامی که تصاویر زیادی از نیم‌رخ چهره دارید، اما از تمام‌رخ تصویری ندارید، انجام دهیم.» ساووی می‌گوید: «این کار مانند ساخت «جعل عمیق» (Deep Fake) است که کاملاً تصویری واقعی است.»

همان‌طور که جعل عمیق نشان داده است، بسته به اینکه چه کسانی از آن استفاده کنند، ابزارهایی مانند هوش مصنوعی و یادگیری ماشین نیز می‌توانند بسیار سودمند یا به‌شدت آسیب‌رسان باشند. رایانه‌های کوانتومی احتمالاً همین تأثیر را خواهند داشت. اگر کار کنند، بی‌شک منافعی برای حوزه‌های زیست‌شناسی، شیمی و فیزیک به همراه خواهند داشت. اما انحصار چنین ماشین‌های قدرتمندی در دست چند شرکت بزرگ یا دولت‌های خاص خطرناک است. برخی نگران‌اند که رایانه‌های کوانتومی سیستم‌های امنیتی را، که از همه‌چیز، بانک گرفته تا اسرار نظامی، محافظت می‌کنند، زیرورو کنند.

هیچ ندیده‌ام هنوز

محاسبات کوانتومی دنیای فناوری را متحول کرده است. اما معنای دقیق آن چیست و پتانسیل واقعی آن چقدر است؟

کتابی که در دست دارید راهنمای شسته‌رفته‌ای است که **آمیت کاتوالا، روزنامه‌نگار نشریه وایرد**، در آن هر چیزی را که باید درباره تحول بعدی در دنیای رایانه‌ها بدانید گفته است. یک رایانه کوانتومی فعال می‌تواند به ساخت مواد جدید قدرتمند کمک کند، مبارزه با تغییرات اقلیمی را قوی‌تر و سریع‌تر کند و رمزنگاری را که اسرارمان را ایمن نگه می‌دارد، کاملاً زیرورو کند. **رایانه‌های کوانتومی** به‌طور مؤثری می‌توانند مجموعه جدیدی از توانایی‌ها را براساس درک جدید و عمیق‌تری از جهان بگشایند که فیزیکدانان طی قرن گذشته ایجاد کرده‌اند. **در آستانه عصر جدیدی از فناوری** قرار داریم که رایانه‌های کوانتومی به ما کمک می‌کنند مسیرهای سفر را با کارآیی بیشتری انتخاب کنیم و میزان بسیار زیادی از داده‌ها را در آزمایش‌های علمی پردازش کنیم. همچنین **این رایانه‌ها نحوه تجزیه‌وتحلیل ریسکِ بانک‌ها را به‌طور بالقوه تغییر می‌دهند.** به شیمی‌دانان‌ها و زیست‌شناسان اجازه می‌دهند شبیه‌سازی‌های دقیقی از جهان طبیعی را به‌منظور توسعه مواد و فرآیندهای جدید کارآمدتر ایجاد کنند.

کاتوالا علم پیچیده پشت تحول کامپیوتری را شرح می‌دهد. همین‌طور **رقابت‌های غول‌های فناوری همچون گوگل، مایکروسافت و شرکت‌هایی مثل تنسنت و علی‌بابا را برای ساخت کامپیوتر کوانتومی بادوام** و مسیرهای متفاوتی را که هرکدام‌شان باید برای از سرگذراندن چالش‌های تکنیکی طی کنند، توصیف کرده است. او کاربرد بالقوه فناوری را در قلمروهایی گوناگون همچون پزشکی، امنیت سایبری و انرژی پاک بررسی می‌کند. کاتوالا به این پرسش اساسی اشاره می‌کند: **چقدر مانده تا کامپیوترهای کوانتومی را واقعیتی متداول تلقی کنیم؟**

WIRED

کتاب محاسبات کوانتومی با حمایت کارخانه نوآوری رسانه راه‌کار منتشر شده و ناشر اصلی آن انتشارات وایرد است

راه‌کار
کارخانه نوآوری رسانه راه‌کار
way2workir

انتشارات راه‌پرداخت
ناشر فناوری و نوآوری
way2pay.press

ISBN 978-622-7702-25-5
9 786227 702255
۹۹ هزار تومان