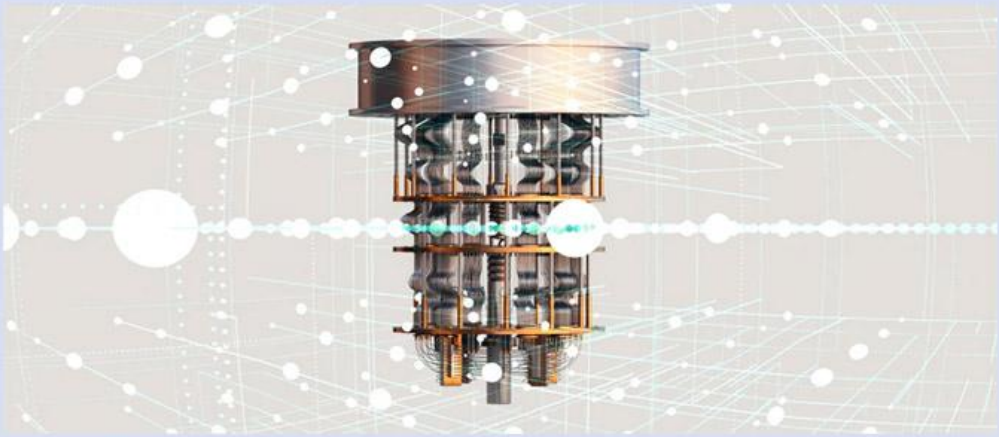


Quantum computing reality check:
What business needs to know now

واقعیت درباره رایانش کوانتومی:
کسب‌وکارها همین حالا چه چیزهایی باید بدانند؟

https://mitsloan.mit.edu

MITSloan MANAGEMENT

مرکز شتابدهی نوآوری

واقعیت درباره رایانش کوانتومی: کسب‌وکارها همین حالا چه چیزهایی باید بدانند؟

(این مقاله نوشته بث استک‌پول در تاریخ ۹ دسامبر ۲۰۲۵ است که در سایت mitsloan.mit.edu منتشر شده است.)

آنچه از این مقاله می‌آموزید:

چهار راهنمای مهم برای پیشبرد رایانش کوانتومی تجاری:
-نیاز به الگوریتم‌های کوانتومی بیشتری را جدی بگیرید.
-رایانش کلاسیک را کنار نگذارید.
-از همین حالا به سمت سامانه‌های رمزنگاری پساکوانتومی حرکت کنید.
-توسعه فناوری تصحیح خطای کوانتومی را سرعت ببخشید.

رایانش کوانتومی در حال حاضر در مرکز توجه قرار گرفته است؛ فعالیت استارتاپ‌ها، نوآوری‌ها و سرمایه‌گذاری‌ها در این حوزه با سرعت زیادی در حال افزایش است.
با این حال، به گفته کارشناسان، رسیدن به رایانه‌های کوانتومی و کاربردهای تجاری‌شده احتمالاً دست‌کم یک دهه دیگر زمان می‌برد. با وجود این، هنوز برای مدیران فناوری و کسب‌وکارها زود نیست که روند تحول این فناوری را به‌دقت دنبال کنند؛ زیرا رایانش کوانتومی در حال حرکت از یک فناوری نوظهور و تا حدی تجربی به سمت یک دارایی راهبردی برای حل دشوارترین مسائل صنعت و جامعه است.
ویلیام الیور، مدیر مرکز مهندسی کوانتوم MIT ، معتقد است رایانش کوانتومی هنوز در مراحل ابتدایی مسیر خود قرار دارد. او یادآوری می‌کند که رایانش کلاسیک تقریباً یک قرن زمان نیاز داشت تا از لامپ‌های خلأ در سال ۱۹۰۶ به تراشه‌های پیشرفته‌ای برسد که امروزه زیرساخت هوش مصنوعی و رایانش با عملکرد بالا را تشکیل می‌دهند.
الیور در سخنرانی خود در برنامه روز مرکز داده MIT توضیح داد که رایانش کوانتومی اکنون در حال عبور از مرحله «کنجکاوی علمی» و تبدیل‌شدن به یک واقعیت فناورانه است؛ بنابراین سازمان‌ها باید از همین حالا وارد این حوزه شوند.
او می‌گوید: «برای اینکه بتوانید در این بازی حضور داشته باشید، باید وارد بازی شوید؛ و زمان ورود به بازی رایانش کوانتومی همین حالاست.»

رایانش کوانتومی چیست؟

رایانش کوانتومی مجموعه‌ای از فناوری‌های حسگری، شبکه‌سازی و پردازش است که می‌توانند محاسباتی را انجام دهند که با فناوری‌های فعلی، یا عملاً بسیار دشوار و پرهزینه‌اند یا حتی امکان انجام آن‌ها وجود ندارد.
البته یک نکته مهم وجود دارد:
رایانه کوانتومی قرار نیست جایگزین رایانه‌های کلاسیک شود.
یک رایانه کوانتومی در صورت رسیدن به مقیاس کامل، برای برخی مسائل مشخص می‌تواند عملکردی بسیار بهتر از رایانه‌های کلاسیک داشته باشد؛ اما این به معنای جایگزین‌شدن رایانش کلاسیک نیست.
چهار نکته مهم برای پیشبرد رایانش کوانتومی
برای ورود جدی به این حوزه، مدیران باید هم ظرفیت‌ها و فرصت‌های رایانش کوانتومی را بشناسند و هم واقعیت‌های فنی و تجاری فعلی آن را درک کنند.

الیور چهار نکته کلیدی را مطرح می‌کند.

۱ .رایانش کلاسیک را کنار نگذارید

با وجود تمام ظرفیت‌هایی که برای رایانش کوانتومی مطرح می‌شود، رایانه‌های کوانتومی جایگزین رایانه‌های متعارف نخواهند شد.

رایانش کوانتومی بیشتر برای مسائل بسیار پیچیده ریاضی مناسب است؛ از جمله:

-تحلیل و شکستن رمزنگاری؛

-محاسبات علمی؛

-علم مواد؛

-شیمی کوانتومی؛

-مسائل بهینه‌سازی.

الیور برای توضیح این موضوع می‌گوید: رایانه‌های کوانتومی بعضی مسائل را بسیار خوب حل می‌کنند، اما قرار نیست جای Microsoft Word را بگیرند.

بنابراین آینده احتمالاً متعلق به ترکیب رایانش کلاسیک و کوانتومی خواهد بود، نه حذف یکی به نفع دیگری.

۲ .به الگوریتم‌های کوانتومی بیشتری نیاز داریم

یکی از موانع اصلی تجاری‌شدن رایانش کوانتومی، کمبود الگوریتم‌های مناسب برای مسائل واقعی کسب‌وکار است.

بسیاری از الگوریتم‌های شناخته‌شده کوانتومی ریشه در پژوهش‌های MIT دارند. یکی از مشهورترین آن‌ها الگوریتم شور (Shor's Algorithm)است که توسط پیتر شور، استاد ریاضیات کاربردی، توسعه داده شد.

الگوریتم شور می‌تواند یک عدد صحیح مرکب بزرگ را به عوامل اول آن تجزیه کند و از این قابلیت می‌توان برای تحلیل برخی سامانه‌های رمزنگاری کلید عمومی مانند RSA استفاده کرد.

اما برای تحقق چیزی که از آن با عنوان برتری کوانتومی تجاری (Commercial Quantum Advantage) یاد می‌شود، به الگوریتم‌های بسیار بیشتری نیاز داریم.

برتری کوانتومی تجاری یعنی:

یک رایانه کوانتومی بتواند یک مسئله واقعی و مرتبط با کسب‌وکار را بهتر از یک رایانه کلاسیک حل کند.

به گفته الیور، هنوز چنین وضعیتی به شکل گسترده محقق نشده است.

او تأکید می‌کند که حتی امروز مسائل زیادی وجود دارند که هنوز مشخص نیست چگونه می‌توان آن‌ها را با رایانه کلاسیک یا حتی رایانه کوانتومی حل کرد.

بنابراین یکی از نیازهای اصلی این حوزه، افراد بیشتری هستند که روی کاربردهای عملی رایانش کوانتومی کار کنند و الگوریتم‌های جدیدی برای آن‌ها توسعه دهند.

۳ .همین حالا رمزنگاری پساکوانتومی را اجرا کنید

یکی از جدی‌ترین نگرانی‌ها درباره آینده رایانش کوانتومی، تأثیر آن بر امنیت سایبری و رمزنگاری است.

رایانش کوانتومی، به‌ویژه با استفاده از الگوریتم شور، در آینده می‌تواند توانایی شکستن برخی سیستم‌های رمزنگاری موجود را داشته باشد.

البته در حال حاضر هنوز یک رایانه کوانتومی با توانایی لازم برای شکستن رمزنگاری‌های رایج در اختیار نداریم.

برای مثال، شکستن رمزنگاری RSA به یک رایانه کوانتومی بسیار بزرگ، مقاوم در برابر خطا و دارای میلیون‌ها کیوبیت (Qubit) نیاز دارد. چنین دستگاهی هنوز فاصله زیادی با واقعیت دارد.

اما این موضوع به این معنا نیست که سازمان‌ها باید منتظر بمانند.

الیور تأکید می‌کند که سازمان‌ها باید از همین امروز مهاجرت به سامانه‌های جدید رمزنگاری پساکوانتومی (Post-Quantum Cryptography)را آغاز کنند؛ سامانه‌هایی که انتظار می‌رود در برابر حملات رایانه‌های کوانتومی آینده مقاوم باشند.

مؤسسه ملی استانداردها و فناوری آمریکا (NIST) نیز استانداردهای جدیدی برای رمزنگاری ارائه کرده است که با هدف مقاومت در برابر حملات احتمالی رایانه‌های کوانتومی آینده طراحی شده‌اند.

این اقدام به ایجاد نوعی امنیت آینده‌نگر (Forward Security) کمک می‌کند.

۴ .توسعه تصحیح خطای کوانتومی را سرعت دهید

یکی از بزرگ‌ترین موانع پیش روی رایانش کوانتومی، قابلیت اطمینان پایین کیوبیت‌ها است.

کیوبیت‌ها برخلاف بیت‌های کلاسیک بسیار حساس و آسیب‌پذیر هستند و پس از تعداد محدودی عملیات ممکن است دچار خطا شوند.

طبق توضیح الیور، کیوبیت‌های امروزی ممکن است پس از حدود ۱۰۰۰ تا ۱۰٬۰۰۰ عملیات دچار خطا شوند.

این میزان پایداری برای رسیدن به کاربردهای تجاری کافی نیست؛ زیرا محاسبات مورد نیاز برای برتری کوانتومی ممکن است به میلیاردها یا حتی تریلیون‌ها عملیات نیاز داشته باشند.

راه‌حل اصلی این مشکل، فناوری تصحیح خطای کوانتومی (Quantum Error Correction) است.

هدف این فناوری افزایش قابلیت اطمینان سیستم‌های کوانتومی و امکان ساخت رایانه‌های کوانتومی بزرگ‌مقیاس است.

در اواخر سال ۲۰۲۴، شرکت Google Quantum AI اعلام کرد که پردازنده Willow به یک نقطه عطف مهم در این زمینه دست یافته است. بر اساس گزارش گوگل،Willow نخستین پردازنده کوانتومی بود که در آن، با افزایش تعداد کیوبیت‌ها، اطلاعات کوانتومی محافظت‌شده در برابر خطا، به شکل نمایی مقاوم‌تر می‌شد.

الیور درباره اهمیت این موضوع می‌گوید: "برای اینکه همه این‌ها امکان‌پذیر شود، به تصحیح خطای کوانتومی نیاز داریم. به گفته او، دستاورد Google در سال گذشته گام مهمی در این مسیر بوده است".

جمع‌بندی برای مدیران کسب‌وکار

پیام اصلی مقاله :

"رایانش کوانتومی هنوز یک فناوری تجاری بالغ نیست؛ اما دیگر صرفاً یک موضوع علمی و آزمایشگاهی نیز محسوب نمی‌شود."

سازمان‌ها لازم نیست همین امروز رایانه کوانتومی خریداری کنند، اما باید از هم‌اکنون برای آینده آن آماده شوند.

چهار اقدام اصلی عبارت‌اند از:

اقدام	اهمیت برای کسب‌وکار
پایش فناوری کوانتومی.....	شناسایی زمان مناسب برای ورود به بازار
توسعه کاربرد و الگوریتم.....	یافتن مسائل واقعی که کوانتوم می‌تواند بهتر حل کند
رمزنگاری پساکوانتومی.....	محافظت از داده‌ها در برابر تهدیدهای آینده
تصحیح خطای کوانتومی.....	یکی از پیش‌شرط‌های اصلی تجاری‌شدن فناوری

در واقع، مزیت رقابتی آینده فقط متعلق به شرکتی نیست که اولین رایانه کوانتومی را داشته باشد؛ بلکه متعلق به سازمانی است که زودتر از دیگران تشخیص دهد کدام مسائل کسب‌وکارش را می‌توان با این فناوری به شکل بهتری حل کرد.

این دقیقاً همان جایی است که رایانش کوانتومی از یک «فناوری نوظهور» به یک موضوع مدیریت فناوری و تصمیم‌گیری راهبردی تبدیل می‌شود.