

محاسبات کوانتومی از راه رسیدن و اکنون چندین شبهه کامپیوتر کوانتومی در دنیا کار می‌کنند. کامپیوترهای کوانتومی سرفصل جدیدی در دنیای فناوری شدند و به نظر می‌رسد صنعت مراکز داده باید هرچه سریع‌تر با آن‌ها سازگاری و انطباق پیدا کند. آیا با ورود کامپیوترهای کوانتومی مراکز داده از رونق می‌افتند یا به‌طور خاص تهدیدی برای مراکز داده کلوکیشن هستند؟

حل بزرگ‌ترین چالش اینترنت

شاید زیاد درباره محاسبات کوانتومی شنیده باشیم، اما درباره تأثیرات کامپیوترهای کوانتومی بر صنعت مراکز داده کمتر صحبت شده است. برای شروع باید درباره توانایی کامپیوترهای کوانتومی صحبت کنیم که اگر به اندازه کافی قدرتمند باشند، چه کاری می‌توانند انجام بدهند. در کوتاه‌مدت، هدف محاسبات کوانتومی عمومی حل یکی از معضلات اینترنت مدرن است و آن چیزی جز «رمزنگاری» نیست!

«رمزنگاری» یکی از معضلات اینترنت مدرن است و آن چیزی جز رمزنگاری نیست!

بانک‌ها، فروشگاه‌ها و مراکز تجاری بدون رمزنگاری به مشکل برخورد خواهند خورد. تا هنگامی که اطلاعات بانکی حساب‌های ما روی سرورهای بانک‌ها و فروشگاه‌ها هستند، توسط فایروال‌ها محافظت می‌شوند، اما هنگامی که توسط سویچ‌ها و روترهای متصل به اینترنت به حرکت درمی‌آیند و از یک نقطه به نقطه دیگری برای انجام درخواست‌های ما منتقل می‌شوند، نیازمند رمزنگاری هستیم. یکی از راه‌های نشان دادن قدرت محاسبات کوانتومی در همین مسئله رمزنگاری است. اجازه بدهید با یک مثال توانایی کامپیوترهای کوانتومی را در رمزنگاری اطلاعات نشان دهیم.

تصور کنید یک پازل شامل میلیاردها میلیارد قطعه داریم. هنگامی که اطلاعاتی را برای یک بانک از طریق اینترنت ارسال می‌کنیم، یک قطعه جدید به لبه پازل افزوده می‌شود. پازل دو تصویر در بالا و پایین دارد که تصویر بالایی توسط کاربر یا ما و تصویر پایینی توسط بانک ترسیم شده است. کاربر فقط می‌تواند تصویر بالایی و بانک فقط می‌تواند تصویر پایینی را ببیند و هیچ‌یک از این دو نمی‌توانند تصویر دیگری را ببینند.



برای ارسال اطلاعات به بانک، کاربر تصویر خود را تکه‌تکه و درهم می‌کند و توسط یک بسته بی‌نام به نشانی بانک می‌فرستد. اگر در میانه راه فردی این بسته را باز کند، فقط تعدادی قطعه مجزا و درهم می‌بیند و نمی‌تواند این قطعه‌ها را در کنار یکدیگر قرار دهد و تصویر کاربر را بسازد. اما وقتی این بسته به دست بانک می‌رسد، آن‌ها می‌دانند چه تصویری است و می‌توانند قطعه‌های جدا شده و درهم را سریع به هم متصل کنند و تصویر اولیه کاربر روی پازل را بسازند. برای هر فرد ساختن تصویر روی پازل با فناوری‌های موجود هزاران سال به طول می‌انجامد.

چگونه محاسبات کوانتومی می‌تواند بازی را تغییر دهد؟

مثال بالا نمونه کاملی از الگوریتم رمزنگاری کلید عمومی قابل انجام توسط کامپیوترهای کوانتومی است. کامپیوتر کوانتومی A می‌تواند قطعات یک پازل را به هم بریزد و درهم کند، به طوری که ممکن است ساخت تصویر پازل برای کامپیوترهای معمولی یا افراد غیرممکن باشد، اما کامپیوتر کوانتومی B به محض دریافت قطعات پازل بتواند، تصویر مورد نظر را بسازد و از آن رمزگشایی کند.



در واقع، محاسبات کوانتومی قانون مور را زیر سؤال می‌برد. قانون مور به افزایش دو برابری ظرفیت‌های محاسباتی در هر دو سال اشاره دارد، اما در کامپیوترهای کوانتومی با افزایش یک بیت کوانتوم، قدرت محاسباتی به صورت نمایی رشد می‌کند. در کامپیوترهای معمولی یا ترانزیستوری، یک رابطه لگاریتمی میان پیچیدگی سیستم و ظرفیت‌های محاسباتی وجود دارد. هرچه ترانزیستورها کوچک‌تر می‌شوند، تأثیرات محاسباتی کوانتومی آن‌ها کمتر و کمتر می‌شود. پس، به نظر جالب می‌آید که یک قانون ساده فیزیک دارد به‌طور هم‌زمان کامپیوترهای کوانتومی را قدرتمندتر و کامپیوترهای معمولی را ضعیف‌تر می‌کند.

به این نکته نیز باید اشاره کرد کامپیوترهای کوانتومی با این قدرت فزاینده‌ای که دارند، می‌توانند به تهدیدی بزرگ برای امنیت ملی کشورها و دولت‌ها تبدیل شوند. تصور کنید یکی از این کامپیوترهای کوانتومی به‌دست یک گروه هکری شرور بیفتد، بدون شک قدرتمندترین افراد روی زمین خواهند شد، زیرا توانایی رمزگشایی هر اطلاعاتی را دارند.

اکنون ما کجا هستیم؟

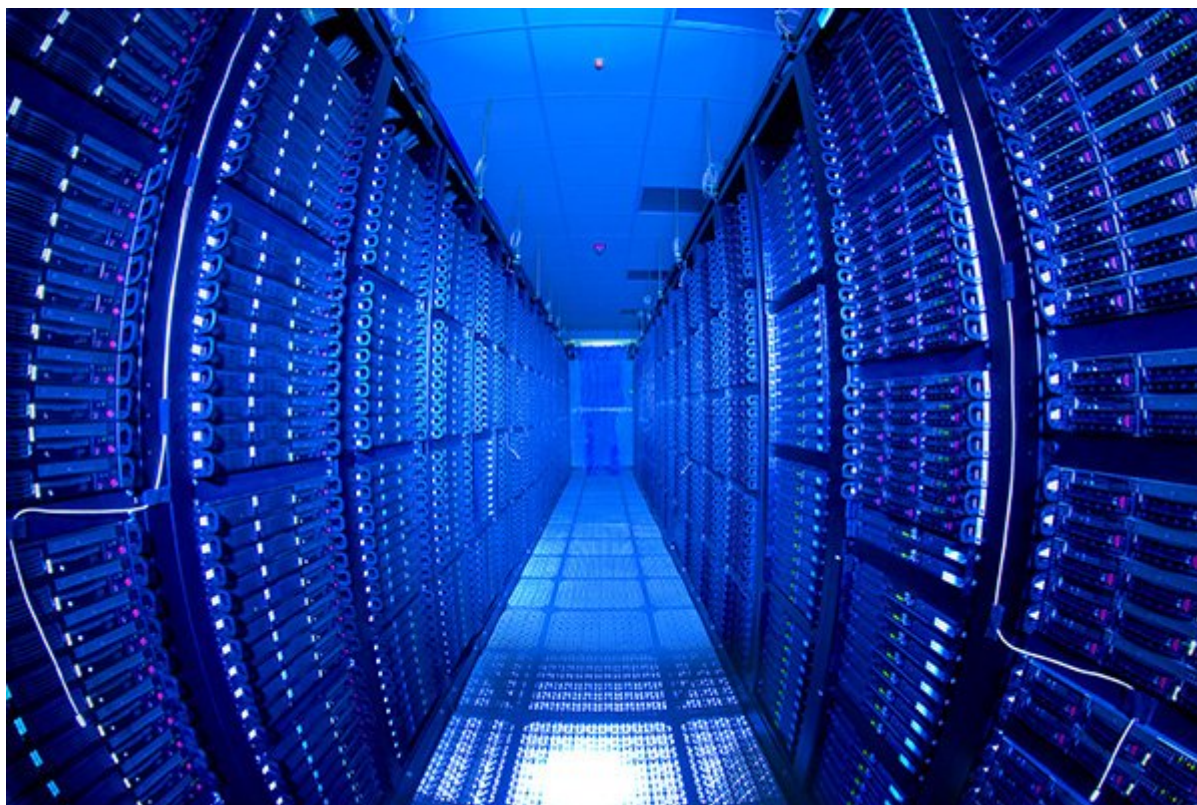
هنوز هیچ شرکتی در جهان نتوانسته است یک کامپیوتر کوانتومی عمومی با قدرتی بسازد که در بالا اشاره کردیم. اخیراً شرکتی به نام D-Wave یک کامپیوتر کوانتومی تجاری ساخته است که البته با ابهام‌ها و سؤال‌هایی روبه‌رو است. به نظر می‌رسد کامپیوتر D-Wave به‌طور کامل بر اساس محاسبات کوانتومی نباشد. کارشناسان اعتقاد دارند D-Wave یک کامپیوتر کوانتومی است، ولی هنوز جای بحث دارد و با یک کامپیوتر صددرصد کوانتومی تشریح شده در چند سال اخیر فاصله دارد. به‌علاوه، نوع مشکلات و چالش‌هایی که کامپیوترهای کوانتومی امروزی مانند D-Wave حل می‌کنند، از نوع چالش‌های رمزنگاری نیست. D-Wave از پردازش‌هایی به نام quantum annealing بهره می‌برد که برای ارائه راهکارهای بسیار سریع بهینه‌سازی مشکلات استفاده می‌شود و برای برخی برنامه‌های کاربردی خاص مناسب است، ولی به‌طور عمومی قابل استفاده نیست.



در حال حاضر، کامپیوتر کوانتومی D-Wave قدرتمندی خود را تنها از آرایه‌ای محاسباتی کسب کرده است که هرکس می‌تواند در گاراژ خانه‌اش آن را بسازد. البته سازندگان D-Wave برای این کامپیوتر نزدیک به ۱۴ میلیون دلار هزینه کرده‌اند. در واقع، D-Wave را نمی‌توان یک کامپیوتر کوانتومی نامید و ما هنوز راه بسیار طولانی برای رسیدن به یک کامپیوتر کوانتومی با قابلیت رمزنگاری کوانتومی داریم. تنها راهکار مقابله با رمزنگاری کوانتومی، خود رمزنگاری کوانتومی است. به محض اینکه اولین کامپیوتر کوانتومی واقعی در جهان ساخته شود، نیاز داریم که به سرعت یک میلیون کامپیوتر کوانتومی دیگر ساخته شود تا برای مقابله با همان اولین کامپیوتر کوانتومی به کار گرفته شوند. بنابراین، به نظر نمی‌رسد در سال جاری یا یک سال بعد شاهد یک کامپیوتر کوانتومی با قابلیت رمزنگاری کوانتومی باشیم و فناوری‌های موجود نمی‌توانند چنین جهش بزرگی داشته باشند، اما دنیای فناوری و اقتصاد در این مسیر حرکت می‌کند و تاریخچه فناوری در جهان نشان می‌دهد به زودی کامپیوتر کوانتومی واقعی ساخته خواهد شد.

کوانتوم کولوکیشن

با توضیحات بالا، به راحتی می‌توان نتیجه گرفت که محاسبات کوانتومی به این زودی‌ها (چند سال آینده) نمی‌تواند جایگزین زیرساخت‌های مراکز داده شود. شاید بتوان پیش‌بینی کرد، محاسبات کوانتومی در ده سال آینده بتواند به یکی از بازیگران اصلی دنیای مخابرات و ارتباطات، زیرساخت‌های محاسباتی و مراکز داده تبدیل شود و جولانگاه تاخت و تاز پیدا کند و در آن صورت، به یک فرصت بزرگ برای ارائه‌دهنده‌گان سرویس‌های مراکز داده کولوکیشن (اجاره فضا) تبدیل شود.



اگر رمزنگاری کوانتومی و رمزگشایی کوانتومی به یک واقعیت عینی تبدیل شوند، می‌توان گفت مراکز داده کولوکیشن ارزش بیشتری خواهند یافت. زیرا تنها ارائه‌دهندگان کولوکیشن می‌توانند هزینه‌های دستگاه‌های رمزنگاری کوانتومی را پرداخت کنند. مشتریان می‌توانند در یک فضای کولوکیشن از این دستگاه‌ها بهره ببرند، در حالی که مراکز داده عمومی دیگر از رونق خواهند افتاد. کامپیوترهای کوانتومی به زیرساخت‌های به‌مراتب بیشتر از رک‌های سنتی مناسب نصب سرورها نیاز دارند. برای دستیابی به عملکرد واقعی یک کامپیوتر کوانتومی، باید دمای فضای استقرار این کامپیوتر نزدیک به صفر درجه باشد و در یک محیط کاملاً ایزوله و الکتریسیته قرار بگیرد. فراهم کردن چنین فضایی نه آسان و نه ارزان است، اما ارائه‌دهندگان مراکز داده کولوکیشن در یک موقعیت مناسب هستند تا امکانات مورد نیاز کامپیوترهای کوانتومی مانند امنیت، سیستم‌های افزودنی، منابع انرژی مؤثر، سیستم‌های خنک‌کنندگی و اتصالات را تأمین کنند. کامپیوترهای کوانتومی به سیستم‌های دیگری مانند مایع نیتروژن و قفس‌های فرادی نیز نیازمند خواهند بود که تأمین آن‌ها برای کولوکیشن‌ها زیاد سخت نیست.

کولوکیشن مراکز داده کوانتومی نیازمند زیرساخت‌هایی مشابه مراکز داده فعلی نیستند، اما نیازمند قابلیت اعتماد، اتصال‌گرایی، امنیت و کارآمدی هستند که مهم‌تر از قبل خواهند بود. کامپیوترهای کوانتومی به این زودی تهدیدی برای مراکز داده کولوکیشن نیستند، اما شاید در چند دهه بعد بتوانند این مراکز داده را تکامل ببخشند و رونق بیشتری بدهند.

می‌توان نتیجه گرفت محاسبات کوانتومی در راه است و مراکز داده کوانتومی نیازمند زیرساخت‌هایی مشابه مراکز داده فعلی نیستند، اما نیازمند قابلیت اعتماد، اتصال‌گرایی، امنیت و کارآمدی هستند که مهم‌تر از قبل خواهند بود. کامپیوترهای کوانتومی به این زودی تهدیدی برای مراکز داده کولوکیشن نیستند، اما شاید در چند دهه بعد بتوانند این مراکز داده را تکامل ببخشند و رونق بیشتری بدهند.

منبع:
دیتاستریست
تاریخ انتشار:
06 اردیبهشت 1396

نشانی منبع:

<https://www.shabakeh-mag.com/cover-story/7522/%D8%A2%DB%8C%D8%A7-%D9%85%D8%AD%D8%A7%D8%B3%D8%A8%D8%A7%D8%AA-%DA%A9%D9%88%D8%A7%D9%86%D8%AA%D9%88%D9%85%DB%8C-%D8%B5%D9%86%D8%B9%D8%AA-%D9%85%D8%B1%D8%A7%DA%A9%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87-%D8%B1%D8%A7-%D9%86%D8%A7%D8%A8%D9%88%D8%AF-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D8%AF%D8%9F>