



آیا زندگی آنالوگ است یا دیجیتال؟ ما در عصر دیجیتال زندگی می‌کنیم؛ بنابراین، ممکن است جواب به نظر مشخص باشد. اما دوباره فکر کنید. دنیای واقعی دیجیتال نیست، کوانتوم است. کامپیوترهای پیشرفته دیجیتال هستند، زیرا دنیای آنالوگ درون‌اتمی چنان پیچیده است که به راحتی نمی‌توان آن را فهمید. در فناوری کامپیوترهای کوانتومی صفر و یک‌ها به شکل بیت‌های کوانتومی یا کیوبیت ایجاد می‌شوند و بسته‌های داده با کابل‌های نوری کوانتومی جایگزین شده‌اند. کامپیوترهای کوانتومی بسیار قدرتمندتر از ماشین‌های فعلی خواهند بود و این می‌تواند به معنای ظهور یک فناوری جدید باشد: اینترنت کوانتومی.

این مطلب یکی از مجموعه مقاله‌های پرونده ویژه «**کامپیوترهای کوانتومی**» است که در شماره ۱۸۹ ماهنامه شبکه منتشر شد. برای دانلود این پرونده ویژه می‌توانید [اینجا](#) کلیک کنید.

به نظر می‌رسد این رؤیا چندان بلندپروازانه و دور از دسترس هم نباشد. D-Wave Systems که در کانادا پایه‌ریزی شده اولین تولیدکننده کامپیوتر کوانتومی است. در حال حاضر، چهار سیستم D-Wave 2X موجود است که مهم‌ترین آن سیستمی است که توسط ناسا نگهداری می‌شود و برای همکاری بین آزمایشگاه هوش مصنوعی کوانتومی ناسا و گوگل در نظر گرفته شده است.

**مطلب پیشنهادی**



تهدیدی جدی یا فرصتی گران‌بها؟  
آیا محاسبات کوانتومی صنعت مراکز داده را نابود می‌کند؟

یکی دیگر از اقدامات انجام گرفته که راه را بیشتر برای اینترنت کوانتومی هموار می‌کند، از جانب شرکت آی‌بی‌ام است که اولین پلتفرم محاسبات کوانتومی جهان را در مرکز تحقیقاتی واتسون این شرکت توسعه داده است و از ماه می 2016 در IBM Cloud در حال استفاده است. هرچند سرعت پردازش کوانتومی این سیستم تنها 5 کیوبیت است، اما قرار است قدرت این کامپیوتر تا 50 کیوبیت افزایش پیدا کند، قدرتی که آی‌بی‌ام تصور می‌کند بیشتر از تمام 500 ابر کامپیوتر برتر حال حاضر جهان خواهد بود. آرویند کریشنا معاون مدیرکل و مدیر مرکز تحقیقات آی‌بی‌ام می‌گوید: «محاسبات کوانتومی در حال به واقعیت پیوستن هستند و قدرت پردازشی آن به مراتب فراتر از کامپیوترهای

امروزی خواهد بود. حالا زمان آن رسیده است تا فناوری جدید کلاود کوانتومی و در پی آن اینترنت کوانتومی متولد شود.»

## اینترنت کوانتومی چگونه کار خواهد کرد؟

در ظاهر انجام چنین کاری خیلی ساده به نظر می‌رسد. شما یک شبکه کوانتومی ایجاد خواهید کرد که از اتصال کامپیوترهای کوانتومی به یکدیگر به وجود آمده است. بعد آن‌ها را در کلاود در دسترس قرار خواهید داد. اما نحوه انتقال داده و حفظ امنیت آن از جمله مهم‌ترین چالش‌های پیش روی شبکه‌های کوانتومی است. شبکه‌های کوانتومی برای انتقال اطلاعات بین نودهای کوانتومی از فوتون‌ها (ذرات واحد نور) استفاده می‌کنند. سخنران ارشد بخش اتمی، مولکولی و فیزیک نوری دانشگاه ساسکس انگلستان دکتر ماتیاس کلر توضیح می‌دهد: «یک شبکه کوانتومی اصولاً شبیه به شبکه‌های فیبر نوری کلاسیک کار خواهد کرد، اما به جای استفاده از سیگنال‌های نوری قوی، این سیگنال به وسیله یک فوتون واحد حمل خواهد شد.»

به نظر می‌رسد اینترنت کوانتومی از ترکیبی از توپولوژی‌های مختلف شبکه شامل توپولوژی درختی و زنجیره‌ای تشکیل شود و انواع مختلفی از نودهای حافظه کوانتومی مثل اتم‌های خنثی و یون‌های به دام افتاده را به یکدیگر لینک کند.

## انتقال داده‌های کوانتومی

کدگذاری اطلاعات درون فوتون‌های واحد نقاط ضعف خاص خود را دارد، زیرا حالات کوانتومی بسیار شکننده هستند. اگر تنها یک فوتون از بین برود، تمام داده کوانتومی از بین خواهد رفت. مشکل اصلی رابط بین کیوبیت و فوتون (اطلاعات و نحوه حمل و نقل آن) است، موضوعی که گروه تحقیقاتی دکتر کلر مشغول کار روی آن هستند.

اینترنت کوانتومی با استفاده از فوتون‌ها برای انتقال اطلاعات بین نودهای کوانتومی امکان‌پذیر خواهد بود. این فناوری می‌تواند امنیت و سرعت انتقال داده‌ها را به طرز چشمگیری افزایش دهد.

با به دام انداختن یون‌های اتمی به عنوان کیوبیت‌ها در حفره‌های نوری (که از دو آینه تشکیل شده‌اند) و تحریک آن‌ها به وسیله یون‌های لیزری، این یون‌ها تنها نور را در جهت آینه منتقل می‌کنند. کلر می‌گوید: «ما از این اثر پورسل برای انتقال اطلاعات کوانتومی از یون به فوتون استفاده می‌کنیم. با توجه به انتقال متناهی از آینه، فوتون به بیرون نشت می‌کند و برای انتقال می‌تواند درون فیبر نوری قرار گیرد.» به این طریق، داده آماده ارسال می‌شود و گیرنده برای استخراج آن این روند را معکوس می‌کند. کلر می‌گوید: «در حال حاضر این موفق‌ترین سیستم شناخته شده برای محاسبات کوانتومی است.»

## رمزنگاری کوانتومی

اگرچه انتظار می‌رود کامپیوترهای کوانتومی بتوانند اینترنت فعلی را برای مدتی متحول کنند، اما با در اختیار داشتن چنین کامپیوترهای پیشرفته‌ای، تکنیک‌های رمزگذاری قدیمی که توسط کامپیوترهای معمولی استفاده می‌شود، بی‌فایده خواهند شد و ظرف چند ثانیه می‌توان آنها را رمزگشایی کرد. مدیرعامل شرکت Post-Quantum اندرسن چنگ با کمک همکارانش الگوریتم‌های رمزنگاری را توسعه داده که برای حفظ امنیت در مقابل حملات یک کامپیوتر کوانتومی در نظر گرفته شده است. او می‌گوید: «کامپیوترهای کوانتومی قادر خواهند بود به اکثر پروتکل‌های کدگذاری حال حاضر نفوذ کنند. این امر سبب خواهد شد اینترنتی که ما می‌شناسیم به کلی غیر قابل استفاده شود.» در دنیای فراکوانتومی، بزهکاران و هکرها خود را با حملات فیشینگ و تضعیف دستگاه برای دسترسی به سیستم‌ها و اطلاعات به زحمت نخواهند انداخت.

چنگ می‌گوید: «مجرمان اینترنتی با در اختیار داشتن قدرت کامپیوترهای کوانتومی می‌توانند یک بولدوزر را به در خانه شما بیاورند و به طرز وحشیانه به قفل در خانه شما حمله کنند. در اینجا دیگر اضافه کردن قفل‌های بیشتر به در، کمکی به شما نخواهد کرد و هیچ کاری از شما ساخته نیست. چنین پیامدهایی اعتمادی که به کانال‌های ارتباطی و خدمات نگهداری داده داریم، را نابود خواهد کرد.»

چنگ معتقد است ما به شدت به یک سیستم احراز هویت امن کوانتومی به عنوان بخشی از اینترنت آینده نیاز داریم تا بدانیم با چه کسی در ارتباط هستیم و خود این کانال ارتباطی نیز از امنیت کافی برخوردار است.

## آیا اینترنت کوانتومی عملی خواهد شد؟

بله، اما نباید انتظار داشت کامپیوترهای معمولی از صحنه حذف شوند. کلر می‌گوید: «به احتمال زیاد در آینده یک شبکه کوانتومی، یک شبکه دوگانه متشکل از کانال‌های کلاسیک و کوانتومی خواهد بود.» از کامپیوترهای کوانتومی با توجه به اندازه و قیمتشان اصولاً در محاسبات ابری استفاده خواهد شد و به‌نظر می‌رسد بتوانیم برای انجام کارهای خاص با استفاده از کامپیوترهای معمولی به این ماشین‌های پیچیده و پرسرعت متصل شویم. این نوع از شبکه‌ها علاوه بر توانایی محاسبات سنگین و پیچیده قادر خواهند بود تا با ایجاد بستری امن ارتباطی اطلاعات را به‌صورت ایمن منتقل کنند.

تنها کسانی که یک یخچال با قابلیت رسیدن به درجه صفر مطلق را در اختیار دارند می‌توانند به داشتن یک کامپیوتر کوانتومی در خانه فکر کنند (کامپیوترهای کوانتومی برای اینکه بتوانند به‌طور دقیق کار کنند باید سرد نگه داشته شوند)، اما می‌توان به محاسبات کوانتومی به‌عنوان بخشی از کلاود فکر کرد و بخشی از ماهیت اینترنت قابل دسترس برای همگان به‌شکل کوانتومی تبدیل خواهد شد.

بعد از معرفی قانون طلایی مور و رسیدن به محدودیت‌های پیش روی صنعت ترانزیستورها، حالا وقت آن رسیده است تا به استقبال محاسبات کوانتومی با قدرت نامحدود و در پی آن اینترنت کوانتومی برویم، اما برای فایق آمدن به چالش بزرگ رمزنگاری لازم است این اینترنت کاملاً از نو ابداع شود.

## تاریخ انتشار:

16 اردیبهشت 1396

## نشانی منبع:

<https://www.shabakeh-mag.com/cover-story/7711/%DA%A7%D9%88%D9%86%D9%87-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%DA%A9%D9%88%D8%A7%D9%86%D8%AA%D9%88%D9%85%DB%8C%E2%80%8E-%D8%A8%D8%B3%D8%A7%D8%B2%DB%8C%D9%85%D8%9F>