تاثیر چالش برانگیز کامپیوتر های کوانتومی روی آینده‌ی رمزارزها

چندی پیش خبری مبنی بر این که کمپانی بزرگ گوگل تکنولوژی کامپیوترهای کوانتومی خویش را راه اندازی کرده است، فضای کریپتو را ملتهب کرد و موجب ایجاد رعب و وحشت قابل توجهی در میان اعضای جامعه کریپتو گشت.

چراکه یکی از **کاربردهای اساسی کامپیوترهای کوانتومی**، از بین بردن سختی معادلات ریاضی است؛ معادلاتی که در حال حاضر زیربنای اصلی بسیاری از رمزارزهای موجود محسوب می‌شوند و در این مدت زمانی که از انتشار این خبر سپری شده است، بسیاری از صاحب نظران بازار رمزارزها پیش‌بینی‌های عجیبی در ارتباط با افول ارزهای دیجیتالی (به ویژه بیت کوین) منتشر کرده‌اند و همین مسئله سبب شده تا توجه کاربران دنیای رمزارزها بیش از پیش به سمت این موضوع جلب شده و سوالاتی نظیر این که کامپیوترهای کوانتومی چیست؟ آیا کامپیوترهای کوانتومی می‌توانند بلاک چین بیت کوین را از بین ببرند و سوالاتی از این دست ذهن آن‌ها را به خود مشغول سازد.

به طور کلی گفته شده است که کامپیوترهای کوانتومی و رمزارزها با یکدیگر سازگار نیستند و احتمالا تا کنون این جمله را بارها از زبان برخی از صاحب نظران این حوزه شنیده باشید؛ اما چرایی این ناسازگاری را می‌دانید؟!

با توجه به اهمیت بررسی **تاثیر کامپیوترهای کوانتومی بر آینده رمزارزها**، ما در این مقاله از کیف پول من قصد داریم تا به صورت دقیق به بررسی تاثیر کامپیوترهای کوانتومی بر آینده رمزارزها بپردازیم؛ پس تا انتهای این مقاله با ما همراه باشید.

مروری اجمالی بر ماهیت کامپیوترهای کوانتومی

پیش از آن که به بحث تاثیر کامپیوترهای کوانتومی بر آینده رمزارزها بپردازیم، لازم است تا مروری بر خود **مفهوم کامپیوترهای کوانتومی** داشته باشیم تا با دید روشن‌تری با مطالبی که در ادامه به آن‌ها خواهیم پرداخت، ارتباط برقرار کنید.

کامپیوترهای کوانتومی در واقع جهشی در فناوری کامپیوترهای دیجیتالی محسوب می‌شوند و آن‌ها را به شکلی طراحی می‌کنند تا به راحتی از پس حل کردن بزرگ‌ترین و پیچیده‌ترین مسائل و معادلات ریاضی برآیند، مسائلی که شاید امروزه ابر کامپیوترها نیز قادر به حل کردن آن‌ها نباشند!

به طور کلی **کامپیوترهای کوانتومی** (Quantum Computer) به دستگاه‌های قدرتمندی اطلاق می‌شوند که از قوانین اختصاصی مکانیک کوانتوم پیروی می‌نمایند. برای این که مفهوم کامپیوترهای کوانتومی روشن‌تر گردد، بهتر است به بررسی نحوه عملکرد این دستگاه‌های ویژه بپردازیم:

نحوه عملکرد کامپیوترهای کوانتومی

کامپیوترهای کوانتومی در واقع از ادغام تکنولوژی‌های بسیار پیشرفته به وجود آمده‌اند و دارای قدرت محاسباتی بسیار منحصربه‌فردی هستند. برخی از افراد که چندان آشنایی با کامپیوترهای کوانتومی ندارند، تصور می‌کنند که اندازه چنین دستگاه‌هایی بسیار غول پیکر هستند؛ اما جالب است بدانید که چنین تصوری درست نبوده و **بزرگترین کامپیوترهای کوامنتومی** به اندازه یک یخچال خانگی فضا اشغال می‌کنند.

کامپیوترهای کوانتومی قادر هستند که به صورت همزمان اعداد 0 و 1 و حتی اعدادی که مابین این دو وجود دارند را پردازش و ذخیره نمایند و این در حالی است که کامپیوترهای دیجیتالی در حالت روشن و خاموش بودن ترانزیستور، فقط توان پردازش و همچنین ذخیره 0 و 1 را دارند.

تاثیر کامپیوترهای کوانتومی بر روی بلاک چین ارزهای دیجیتالی

زیربنای بلاک چین بر روی مسائل پیچیده ریاضی بنا نهاده شده است و به منظور ایجاد و اضافه شدن بلاک جدید لازم است که ماینرها به کمک دستگاه های استخراج و ماینینگ خویش به حل این معادلات پیچیده بپردازند و در واقع با این عمل خویش از امنیت شبکه بلاک چین حمایت می‌کنند و در ازای آن، بیت کوین یا به طور کلی رمزارز بومی **شبکه بلاک چین** مورد نظر را دریافت می‌دارند و با توجه به قدرت بسیار بالای کامپیوترهای کوانتومی در حل مسائل ریاضی، می‌توان گفت که چنین تجزیه و تحلیل هایی از سوی کامپیوترهای کوانتومی بلاشک بر روی آینده بلاک چین‌ها نیز تاثیر می‌گذارد.

امروزه با توسعه فناوری کامپیوترهای کوانتومی بسیاری از افراد چنین تحلیل می‌کنند که شبکه های بلاک چینی با خطرات جدی تری مواجه شده است و جالب است بدانید که چنین خطری فقط مختص شبکه بلاک چینی بیت کوین نبوده و سایر شبکه ها را نیز تحت تاثیر قرار خواهد داد و به خوبی در روزهای اخیر شاهد تضعیف قدرت بلاک چین ها در مقابل کامپیوترهای کوانتومی بوده‌ایم.

براساس مقاله‌ای که به وسیله مرکز کوانتوم روسیه منتشر شده است، وابستگی به تابع ها و عملگرهای ریاضی یک طرفه را می‌توان عامل اصلی به خطر افتادن **تکنولوژی بلاک چین** و امنیت آن معرفی کرد؛ چراکه کامپیوترهای کوانتومی به راحتی می‌توانند این توابع را محاسبه و حل کنند، کاری که باید با دشواری و صرف زمان زیاد انجام شود تا **امنیت بلاک چین** ها حفظ شود! و در چنین شرایطی احتمال جعل بلاک ها و امضاهای دیجیتالی افزایش می‌یابد.

مطلب پیشنهادی : امنیت بلاک چین چگونه است؟

عدم توانایی کامپیوترهای کوانتومی در از بین بردن بلاک چین

در ادامه کشمکش های رخ داده در جریان توسعه فناوری کامپیوترهای کوانتومی و تاثیر آن بر **آینده بلاک چین**، محققان بلاک چینی نیوزلندی به این ادعا که کامپیوترهای کوانتومی قادر هستند امنیت بلاک چین را از بین ببرد، واکنش نشان داده و چنین ادعایی را مطرح کردند که می‌توان از توابع رمزنگاری ویژه برای جلوگیری از این کار کمک گرفت و براساس تحقیق مرکز کوانتوم روسیه امکان این که توابعی ایجاد شود که **آنتی کوانتوم** (مقاوم در برابر کوانتوم) باشد کاملا وجود دارد.

موضوع دیگری که در این زمینه باید به آن توجه داشته باشید، از این قرار است که هرچند تب گفتگو در زمینه تکنولوژی کامپیوترهای کوانتومی بسیار بالا گرفته است؛ اما واقعیت امر این است که پیاده‌سازی این تکنولوژی در سطح فراگیر زمان قابل توجهی را می‌طلبد و ناگفته نماند که فناوری بلاک چین نیز یک فناوری نوپا محسوب می‌شود و مسلما این فناوری نوظهور نیز تدابیر خوبی را در ارتباط با ایجاد توابع مقاوم در برابر کوانتوم را خواهد اندیشید.

به عنوان مثال در سال 2017 تیمی از اندیشمندان مرکز کوانتومی روسیه موفق به توسعه شبکه بلاک چینی شدند که دارای مقاومت کافی در برابر تهدیدات کامپیوترهای کوانتومی بود. به گفته این محققان روشی که آن‌ها برای **تامین امنیت شبکه بلاک چین** از آن کمک گرفتند ترکیب رمزنگاری پساکوانتومی QKD بود.

در این روش منحصر به فرد، کلیدهای رمزنگاری شبکه با استفاده از پرتوهای لیزری منتقل می‌شوند و به منظور ارتقا سطح موفقیت این فرآیند از خواص کوانتومی فوتون‌ها کمک گرفته‌اند. در این حرکت جالب، به هنگام تلاش یک کامپیوتر کوانتومی برای هک یا رهگیری کلیدهای مربوط به تراکنش، عمل جاسوسی و خرابکارانه این کامپیوتر موجب ایجاد تغییراتی در ویژگی‌های کلید کوانتومی QKD شده و آن را به صورت کامل از حیز انتفاع ساقط می‌کند.

تاثیر کامپیوترهای کوانتومی بر روی ارزهای دیجیتالی

براساس تحقیقات موجود ارتباط چندان خوبی در میان کامپیوترهای کوانتومی و ارزهای دیجیتالی وجود ندارد و پیشرفت های کامپیوترهای کوانتومی از پیشرفت دنیای رمزارزها پیشی گرفته است و احتمالا به همین علت باشد که بسیاری از فعالان این حوزه در برابر چنین کامپیوترهایی چندان اعتماد به نفس کافی از خود نشان نمی‌دهند و خود را در طرف شکست خورده بازی تصور می‌کنند.

این مسئله که براساس گزارشات، امکان شکستن رمزهای تائید شده فضای ارز دیجیتال به وسیله این کامپیوترها وجود دارد نیز نگرانی آن‌ها را بیش از پیش تقویت نموده؛ اما واقعیت امر این است که در حال حاضر این کامپیوترهای کوانتومی توان عبور از استانداردهای ارز دیجیتال رمزنگاری شده را ندارند و این موضوع فقط احتمالی است که در آینده ممکن است رخ بدهد!

البته هرچند این مسئله فقط یک پیش‌بینی نسبت به آینده محسوب می‌شود؛ اما باید آن را بسیار جدی گرفت و علت این امر را نیز در این مطلب که با چنین شکستنی این کامپیوترها قادر خواهند بود گذشته این بازار را نیز تغییر داده و تحت تاثیر قرار دهند، جستجو کرد.

مطلب پیشنهادی : آموزش ثبت نام در متاورس

در صورتی که کامپیوترهای کوانتومی بتوانند به فضای ارزهای دیجیتالی نفوذ نمایند، به راحتی قادر خواهند بود که به تراکنشات و همچنین معاملات خصوصی سابق اعضای جامعه نیز حمله نمایند که چنین امری مسلما تاثیرات بسیار مخربی بر روی استانداردهای ارزهای دیجیتالی، توانایی ماینرها و همچنین حق پخش تراکنشات

خواهد گذاشت و طبیعتا با آسیب دیدن امضاهای دیجیتالی شبکه‌ای همچون اتریوم نیز در معرض خطر قرار گرفته و محافظت از کلیدهای خصوصی بسیار سخت و دشوارتر خواهد شد.

اما مسئله‌ای که باید به آن توجه کنید این است که حتی پس از دسترسی کامپیوترهای کوانتومی به رمزارزها نیز این ارزهای دیجیتالی همچنان به فعالیت و حیات خویش ادامه خواهند داد و شاید فقط مدتی طول بکشد تا بیت کوین و سایر ارزها دیجیتالی با چنین شرایطی وفق پیدا کنند.

ولی باری به هر جهت رمزارزها در این برهه زمانی نیز از حرکت نخواهند ایستاد و به همین منظور امروزه به صورت پیوسته آزمایش‌های متنوعی بر روی افزایش استاندارد رمزارزها صورت می‌گیرد. ناگفته نماند که امروزه استفاده از کیف پول‌های سخت افزاری نیز بسیار رونق گرفته است و در واقع استفاده از چنین کیف پول‌هایی می‌تواند موجب ارتقا سطح امنیت کلیدهای خصوصی باشد.

مهم‌ترین تاثیر کامپیوترهای کوانتومی بر روی آینده رمزارزها

با توجه به ادعاهایی که در ماه های اخیر در ارتباط با فراگیر شدن تکنولوژی کامپیوترهای کوانتومی به گوش می‌رسد، ما در این مقاله از کیف پول من تلاش نمودیم تا با بررسی دقیق نحوه **تاثیر کامپیوترهای کوانتومی بر روی آینده رمزارزها** ابهامات موجود در این زمینه را در حد توان شفاف‌سازی کنیم.

همان طور که در مطالب فوق مشاهده کردید، کامپیوترهای کوانتومی با توجه به قدرت پردازش بالای خویش در عرض چند ثانیه می‌توانند به راحتی پیچیده‌ترین مسائل و معادلات ریاضی که پایه و اساس ایجاد بلاک جدید در بلاک چین‌ها هستند و موجب حفظ امنیت آن‌ها می‌شوند را حل نمایند و به همین علت به یکی از کابوس‌های اصلی اعضای جامعه کریپتوکارنسی تبدیل شده‌اند. جالب است بدانید به راحتی و با قدرت بالا می توان اقدام به ساخت بازی در بلاک چین کرد.

بسیاری از تحلیل‌گران بازار رمزارزها کامپیوترهای کوانتومی را در جبهه مقابل ارزهای دیجیتالی قرار می‌دهند که علت چنین امری را می‌توان در قدرت این کامپیوترها در شکستن رمزنگاری‌های موجود آن جستجو کرد که به شدت امنیت شبکه‌های بلاک چینی را تضعیف می‌نمایند؛ چراکه براساس نتایج تحقیقات به عمل آمده در این حوزه با از بین رفتن استانداردهای رمزارزی، کلیدهای خصوصی نیز به خطر می‌افتند.

البته از سوی دیگر محققان و اندیشمندان حوزه کریپتوکارنسی نیز راه‌حل‌هایی را برای این مسائل پیش‌بینی کرده‌اند و براساس اعلام نظر آن ها امکان ایجاد توابع مقاوم در برابر کامپیوترهای کوانتومی وجود دارد. ناگفته نماند که اگر در ارتباط با نحوه تاثیر کامپیوترهای کوانتومی سوالی دارید که در این مقاله از وب‌سایت کیف پول من، به آن اشاره نشده است، می‌توانید سوال خود را در بخش نظرات مطرح کنید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.