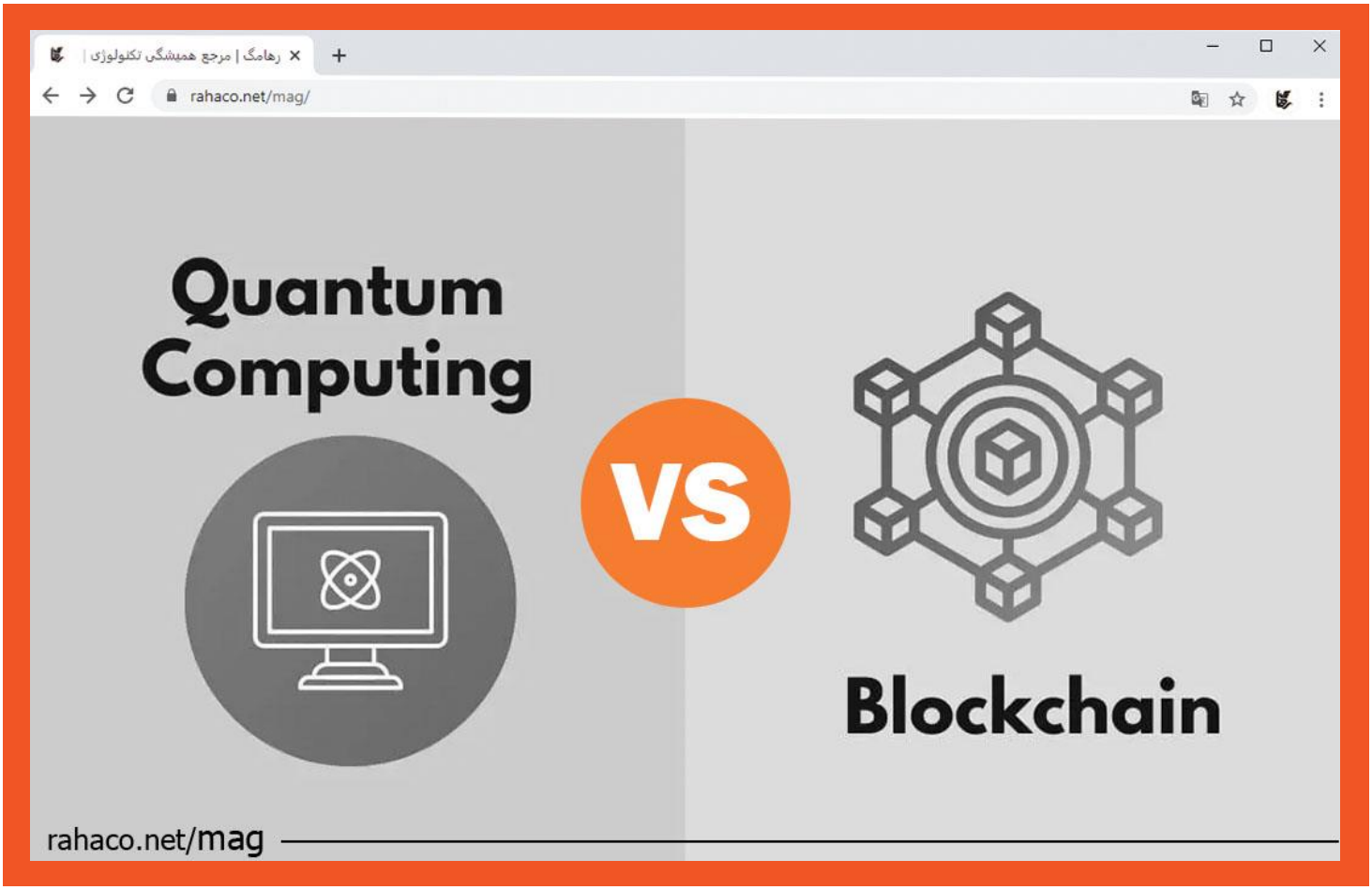
مجله رهاکو

RAHA MAG

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک 12
www.rahaco.net کدپستی1583616414 تلفن :02154521



فهرست

پردازش کوانتومی در مقابل بلاکچین: تاثیرات آن بر بیت کوین

شاید برایتان عجیب باشد که بگوییم پیشرفت تکنولوژی همیشه پیامدهای مثبتی ندارد. همیشه قدرت بیش از حد باعث بروز مشکلات و اختلالات متعددی شده است. احتمالا نام محاسبات کوانتومی به گوشتان خورده باشد اما ندانید که چرا با بلاک چین سازگاری ندارند. دلیل عمده این موضوع این است که قدرت محاسبات کوانتومی به قدری زیاد می‌باشد که حتی می‌تواند رمز ارزهای دیجیتال را بشکند. به دلیل روش جدید و سریع‌تر انجام محاسبات، رایانه‌های کوانتومی می‌توانند برای پیشرفت‌های علمی بسیار مفید باشند. با این حال هنگامی که در دسترس هستند، پتانسیل شکستن رمزنگاری فعلی و تضعیف حفاظت از داده‌های شخصی را دارند. دستیابی به برتری کوانتومی یکی از پیشرفت‌های بسیار مهم است که می‌تواند مسیر تاریخ را تغییر دهد. اما این موضوع چگونه بر بلاک چین تاثیر خواهد گذاشت؟ آیا کریپتو در جنگ محاسبات کوانتومی در مقابل بلاک چین ناپدید خواهد شد؟ در ادامه این مقاله همراه ما باشید تا به توضیحات بیشتری درباره پردازش کوانتومی در مقابل بلاکچین بپردازیم.

پردازش کوانتومی در مقابل بلاکچین؛ تهدیدی برای رمزنگاری

توسعه فناوری محاسبات کوانتومی می‌تواند به رمزنگاری نامتقارن که پایه و اساس بیشتر زیرساخت‌های دیجیتال حکومت‌ها و شرکت‌های چند ملیتی گرفته تا کاربران عادی در معرض خطر قرار دهد. به همین دلیل تعجبی ندارد که این حجم از تحقیقات برای یافتن اقدامات متقابل در برابر این فناوری در دست انجام است. الگوریتم‌های رمزنگاری که قرار است در برابر تهدید محاسبات کوانتومی ایمن باشند، الگوریتم‌های مقاوم در برابر کوانتوم نامیده می‌شوند. اگر الگوریتم‌های رمزنگاری مقاوم در برابر کوانتوم به خطر بیافتند، مانند بلاک چین اسیب خواهند دید. در حال حاضر، تحقیقاتی برای یافتن روش‌های مقابله با شنود در حال انجام است. شنودها در یک مجرای عمومی باز با همان اصول و روش‌هایی که برای کامپیوترهای کوانتومی لازم است قابل شناسایی خواهند بود. با استفاده از این روش، می‌توان فهمید که آیا یک کلید عمومی متقارن قبلا توسط شخص ثالث خوانده و دستکاری شده است یا خیر.

پردازش کوانتومی در مقابل بلاکچین: قدرت کدام فناوری بیشتر است؟

با توجه به گفته‌های ماکر وبر، شکستن رمزنگاری بلاک چین نیاز به یک کامپیوتر کوانتومی با 1.9 میلیارد کیوبیت قدرت پردازشی دارد، که یک رقم بسیار بزرگ است. در حال حاضر، بهترین کامپیوترهای کوانتومی شرکت IBM تنها دارای 127 کیوبیت توان پردازشی هستند. قبلا نیز اشاره شده بود که محاسبات کوانتومی به سرعت وارد دنیای ما نمی‌شوند. با این حال، خطراتی که محاسبات کوانتومی برای فناوری بلاک چین به همراه دارد را نباید نادیده گرفت. بر اساس تحقیقات انجام شده، ممکن است تا 5 سال دیگر به یک کامپیوتر کوانتومی برسیم که بتواند کدهای یک سیستم رمزنگاری شده را بشکند. اما این بدان معنا نیست که کامپیوترهای کوانتومی به طور قطعی قادرند فناوری بلاک چین را بی‌اثر کنند.

پردازش کوانتومی در مقابل بلاکچین؛ ایا پیاده سازی بلاکچین کوانتومی امکان پذیر است؟

دانشمندان در حاضر مشغول بررسی امکان پیاده سازی بلاک چین کوانتومی هستند. این بلاکچین اطلاعات را بر روی ذرات کوانتومی ذخیره می‌کند به این ترتیب اولین بلاک شکل می‌گیرد. به تدریج که اطلاعات بیشتری فراهم شود، اطلاعات جدید در قالب درهم تنیدگی با ذره دوم تلفیق می‌شود. بنابراین ذره‌ی اول از بین می‌رود و اطلاعات بلاک اول با بلاک دوم ترکیب می‌شود. اطلاعات بلاک سوم نیز به همین شیوه به بلاک دوم اضافه شده و ذره‌ی سوم جایگزین ذره‌ی دوم می‌شود. بلاک چین کوانتومی به دلیل امنیت بالایی که دارد دستکاری داده‌های موجود را بلافاصله شناسایی می‌کند. این اصلی‌ترین مزیت درهم تنیدیگی کوانتومی است. اما بلاکچین کوانتومی یک کاربر دیگر هم دارد و آن هم اینکه بلاک‌های اولیه غیر قابل تغییر هستند. در اصل چون فوتون‌های قبلی از بین رفته‌اند، امکان دستکاری آن‌ها وجود ندارد. درهم تنیدینگی در زمان، امنیت به مراتب اهمیت بیشتری نسبت به درهم تنیدینگی در مکان دارد. امروزه بیشتر فناوری‌های لازم برای عملی ساختن بلاکچین کوانتومی به صورت نظری طراحی شده است.

یکی از پیش نیازها برای ساخت بلاکچین کوانتومی وب کوانتومی می‌باشد که هنوز آماده نیست. وب کوانتومی در واقع شبکه‌ای است که اطلاعات کوانتومی را از طریق روترهای کوانتومی جابه‌جا می‌کند، بدون اینکه ویژگی‌های کوانتومی ذرات تغییر کند. البته این شبکه طراحی شده است و احتمالا در چند ماه و یا سال آینده در اروپا، ایالات متحده و چین اجرایی می‌شود. ساخت چنین شبکه‌ای نیازمند کار سنگین مهندسی است و به همین دلیل زمان بر خواهد بود. ایجاد وب کوانتومی می‌تواند راه را برای شکل گیری بلاکچین کوانتومی هموار سازد.

پردازش کوانتومی در مقابل بلاکچین: کامپیوترهای کوانتومی و رمزنگاری

کامپیوترهای کوانتومی و رمزنگاری پیوند تلخ و شیرینی دارند. رمزنگاری کلید عمومی که به نام رمزگذاری نامتقارن نیز شناخته می‌شود، روشی برای رمزگذاری داده‌ها با استفاده از پروتکل‌های رمزنگاری مبتنی بر الگوریتم است. استفاده از دو کلید مجزا، یکی خصوصی و دیگری عمومی ضروری می‌باشد. امنیت رمزنگاری نامتقارن مبتنی بر یک اصل ریاضی است که به عنوان توابع یک طرفه شناخته می‌شود. طبق این اصل کلید عمومی را می‌توان به راحتی از کلید خصوصی مشتق کرد اما برعکس نه.

پیتر شور، ریاضیدان الگوریتم کوانتومی را در سال 1994 منتشر کرد که می‌تواند فرضیه امنیتی رایج‌ترین الگوریتم‌های رمزنگاری نامتقارن را بشکند. این نکته مهمی در جنگ پردازش کوانتومی در مقابل بلاکچین می‌باشد. اگر هکرها دارای یک کامپیوتر کوانتومی بسیار قدرتمند باشند که قادر به انجام رمزگشایی از کلید خصوصی باشد، سیستم‌های رمزنگاری کلید عمومی به خطر می‌افتد.

پردازش کوانتومی در مقابل بلاکچین - آینده این دو فناوری چگونه است؟

محاسبات کوانتومی هنوز راه بسیار زیادی در پیش دارد تا اینکه بتواند تهدید جدی برای فناوری بلاک چین باشد. حوزه محاسبات کوانتومی به نقطه اوج خود رسیده است. محاسبات کوانتومی این پتانسیل را دارد که به حل بسیاری از مهم‌ترین مشکلات علمی و فناوری کمک کند، و فناوری را به گونه‌ای که ما نمی‌توانیم تصور کنیم پیش ببرد. علاوه بر این تا زمانی که

کامپیوترهای کوانتومی به طور گسترده در دسترس قرار گیرند، فناوری بلاک چین به احتمال زیاد برای رسیدگی به موضوع امنیت کوانتومی تکامل یافته است. در حال حاضر ارزهای رمزنگاری شده مانند IOTA (ارز دیجیتال آیوتا) وجود دارند که از فناوری نمودار غیر چرخه جهت دار (DAG) مقاوم در برابر پردازش کوانتومی استفاده می‌کنند. شبکه‌های بلاک چین مانند: پلتفرم QAN از این فناوری استفاده می‌کنند تا به برنامه نویسان اجازه دهند قراردادهای هوشمند، برنامه‌های غیرمتمرکز و دارایی‌های دیجیتالی مقاوم ایجاد کنند.

پردازش کوانتومی در مقابل بلاکچین – کدام فناوری برنده می‌شود؟

توزیع کلید کوانتومی (QKD) از قوانین مکانیک کوانتومی استفاده می‌کند، تا به دو طرف اجازه دهد داده‌های امن را برای تشخیص اینکه آیا شخص ثالثی در حال تلاش برای استراق سمع از مبادله آن‌ها است را تشخیص دهد. استفاده از کلیدهای کوانتومی در ارتباط با شبکه بلاکچین می‌تواند به محافظت در برابر حملات رایانه‌های کلاسیک و کوانتومی کمک کند. تحقیقات آینده در زمینه رمزنگاری کوانتومی در نهایت تغییرات لازم را برای ایجاد امکان توسعه برنامه‌های بلاکچین ایجاد خواهد کرد.

نتیجه گیری

پردازش کوانتومی در مقابل بلاکچین یک تقابل تکنولوژیکی است. پیشرفت‌های قابل توجه در محاسبات کوانتومی ممکن است از نظر تئوری کل بخش ارزهای دیجیتال را از مسیر خارج کند، درست زمانی که فناوری بلاک چین در حال ظهور است. با این حال کد گذاری ضد کوانتومی در حال حاضر توسط کارشناسان رمز ارز در مرحله توسعه است. ارزهای رمزنگاری شده مانند: بیت کوین (BTC) و سایر ارزها بر اساس فناوری بلاک چین توسعه یافته‌اند. رمزگذاری امکان انجام تراکنش‌های مالی را بدون دخالت سایر ذینفعان مانند بانک‌ها و دولت‌ها فراهم می‌کند. کامپیوترهای کوانتومی با افزایش قدرت باور نکردنی خود به این فرآیند، این پتانسیل را دارند که شیوه طراحی محصولات را متحول کنند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک 12 کدپستی1583616414
تلفن :02154521 **www.rahaco.net**