زنجیره بلوکی در تعامل یا تقابل با محاسبات کوانتومی

کامپیوترهای کوانتومی چگونه امنیت بیت‌کوین را به چالش می‌کشند؟

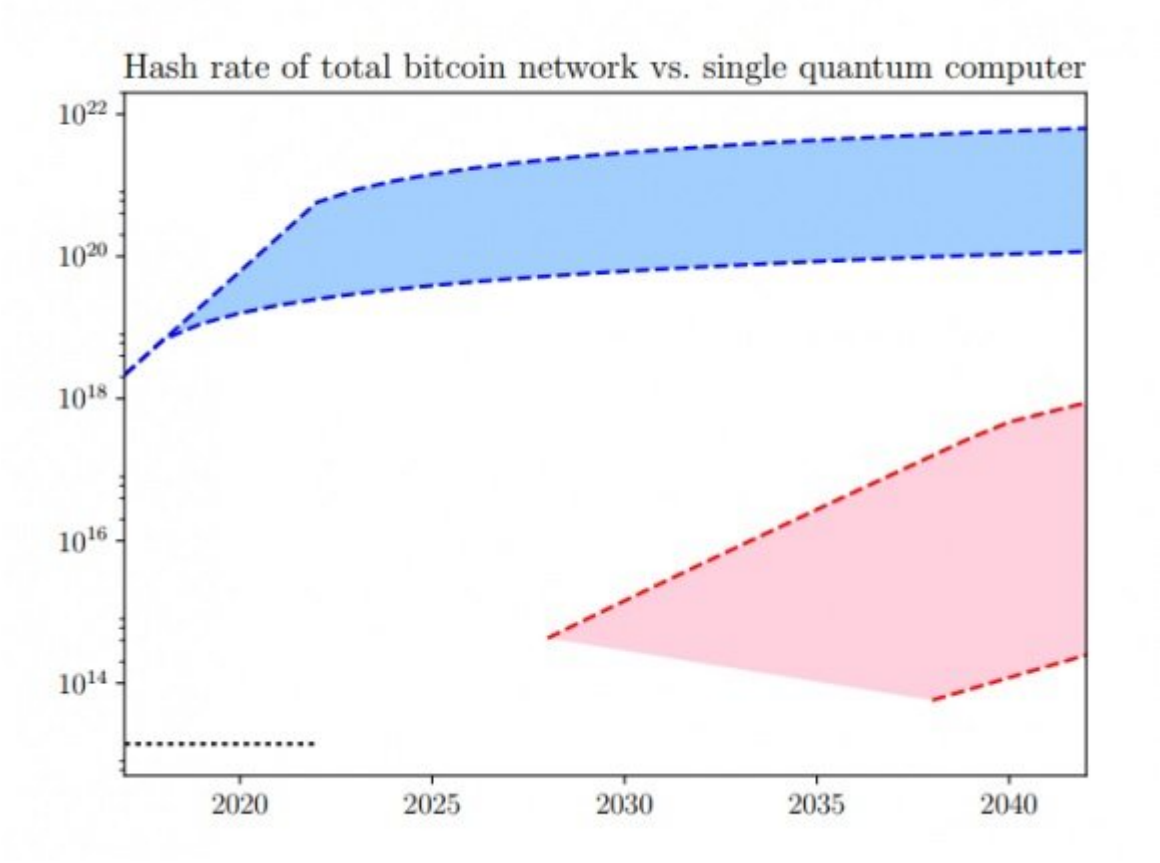
کارشناسان حوزه امنیت بر این باور هستند که توان محاسباتی بسیار بالای کامپیوترهای کوانتومی به این سامانه‌های قدرتمند اجازه می‌دهد تا در ده سال آینده از مکانیزم امنیتی بیت‌کوین به راحتی عبور کنند.

بیت‌کوین همانند طوفانی به سرعت در حال تخسیر جهان ما است. این واحد پول دیجیتالی غیرمتمرکز یک پلتفرم پرداخت ایمن بوده که هر فردی قادر است از آن استفاده کند. این سامانه فارغ از نظارت‌ها یا مداخله‌های دولتی بر پایه یک شبکه باز یکپارچه نظیر به نظیر کار می‌کند. این استقلال عمل که عامل اصلی محبوبیت روزافزون بیت‌کوین است، در نهایت باعث شد تا ارزش این پول مجازی یک شیب تند به خود گیرد. در اوایل سال 2017 میلادی یک بیت‌کوین تنها 1000 دلار ارزش داشت. اما در نوامبر سال 2017 ارزش بیت‌کوین به 7000 دلار افزایش پیدا کرد. در حال حاضر برآورد شده است که بازار کل این ارز مجازی برابر با 150 میلیارد دلار باشد. محبوبیت و ارزش بیت‌کوین متکی بر مکانیزم امنیتی فوق‌العاده بالای آن است.

مطلب پیشنهادی

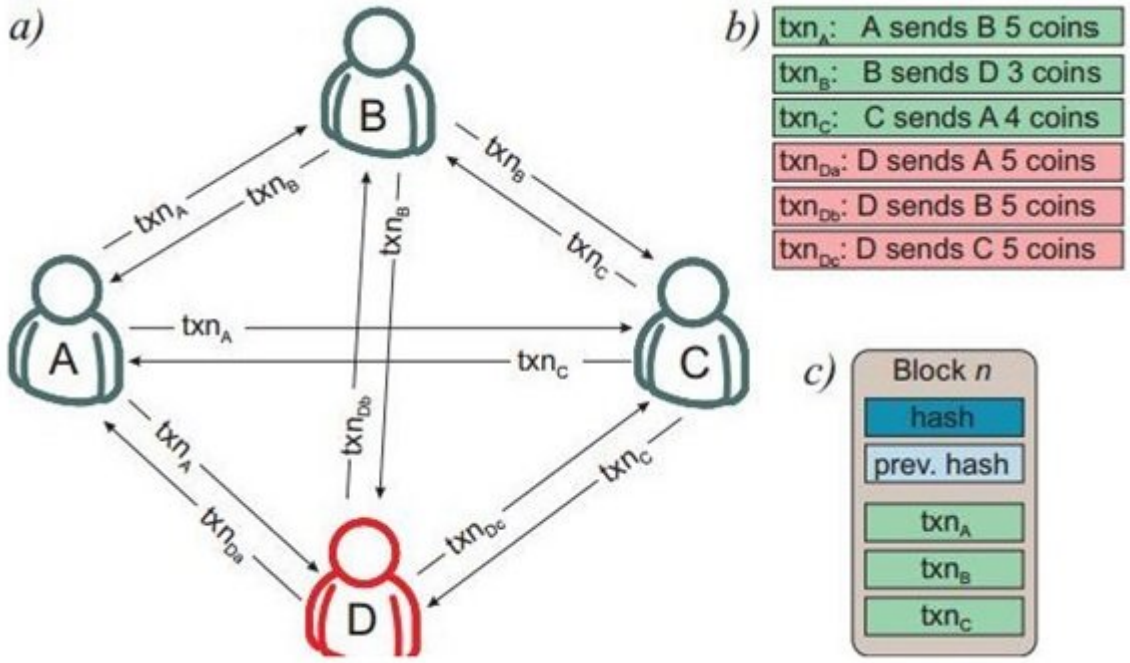
رایگان دانلود کنید: کتاب الکترونیکی همه‌چیز درباره بیت‌کوین

بیت‌کوین دارای دو ویژگی امنیتی مهم است که امکان دزدی یا کپی کردن آن‌ها اگر نگوییم منتفی ساخته‌اند باید بگوییم به حداقل رسانده‌اند. پروتکل‌های رمزنگاری که بیت‌کوین بر پایه آن‌ها کار می‌کند را به سختی می‌توان درهم شکست. به عبارت دیگر، آن‌ها از توابع مختلف ریاضی همچون فاکتورگیری بهره می‌برند که استفاده از آن‌ها ساده بوده اما در مقابل شکستن آن‌ها برای کامپیوتر کلاسیک به سختی امکان‌پذیر است.



دورنمای بیت‌کوین چندان روشن نیست

در حالی که امروزه عبور از سد مکانیزم امنیتی بیت‌کوین برای کامپیوترهای کلاسیک سخت است، اما در مقابل کامپیوترهای کوانتومی به راحتی می‌توانند این مشکل را حل کنند. کامپیوترهایی که در حال حاضر اولین نمونه آن‌ها در حال توسعه است. طراحی اولین کامپیوتر کوانتومی قابل استفاده این پرسش مهم را مطرح می‌کند که بیت‌کوین‌ها چگونه قادر خواهند بود در چند سال آینده در برابر یک حمله کوانتومی از خود دفاع کنند. دیوش اگروال (Divesh Aggarwal) از دانشگاه ملی سنگاپور به همراه چند نفر از همکاران خود پژوهشی در این زمینه انجام داده‌اند تا تهدیداتی که از جانب کامپیوترهای کوانتومی بیت‌کوین‌ها را تهدید می‌کند را شناسایی کنند. آن‌ها بر این باور هستند که تهدید کاملا جدی است.



تهدیدی که در پس‌زمینه قرار دارد

تراکنش‌های بیت‌کوین در یک دفتر توزیع شده ذخیره می‌شوند که تمام معاملات انجام شده در یک دوره زمانی خاص که به‌طور معمول ده دقیقه به طول می‌انجامد را جمع‌آوری می‌کنند. این مجموعه که بلوک نامیده می‌شود شامل یک هش رمزنگاری شده از بلوک قبلی است که خود شامل یک هش رمزنگاری شده‌ای است که بر پایه بلوک قبلی ساخته شده که ترکیب این بلوک‌ها با یکدیگر تشکیل یک زنجیره را می‌دهند. این مکانیزم در اصطلاح تخصصی به نام زنجیره بلوکی شناخته می‌شود. بلوک جدید باید شامل عددی باشد که قطعه داده تصادفی (nonce) نام داشته و یک خاصیت منحصر به فرد دارد.

مطلب پیشنهادی

به سمت ناکجا آباد
چرا استخراج بیت‌کوین از طریق گوشی‌های هوشمند کاری بیهوده است؟

زمانی که این قطعه داده تصادفی هش‌گذاری شده با محتوای بلوک ترکیب می‌شود، باید اولا یک خروجی با ارزش معنی‌دار را تولید کرده و دوما به لحاظ طولی اندازه‌ای کم داشته باشد. اما تولید قطعه داده تصادفی فرآیندی زمان‌بر بوده و تنها راه دستیابی به آن به‌کارگیری یک حمله جست‌وجوی فراگیر است. حمله‌ای که در آن باید شماره‌های مختلف مورد آزمایش قرار گیرد تا یک قطعه داده تصادفی درست پیدا شود. این فرآیند پیدا کردن قطعه داده تصادفی کاوش یا معدن‌کاوی نام دارد. معدن‌کاوی یک فرآیند محاسباتی بسیار سنگین بوده که در عمل این فرآیند میان کامپیوترهای مختلفی که توان محاسباتی بسیار بالا دارند شکسته می‌شود. بلوک در ادامه در دفتر توزیع شده قرار گرفته و زمانی که درست بودن آن مورد تایید قرار گرفت در زنجیره بلوکی قرار می‌گیرد. پس از انجام این‌کار معدن‌کاوان می‌توانند کار روی بلوک بعدی را آغاز کنند. بعضی مواقع دو گروه معدن‌کاوی دو قطعه داده تصادفی مختلف را پیدا کرده و دو بلوک مختلف را تعریف می‌کنند. پروتکل بیت‌کوین اعلام می‌دارد که در این حالت بلوکی که روی آن کار بیشتری انجام شده در زنجیره بلوکی وارد می‌شود و بلوک دیگر از میان می‌رود. این فرآیند در دنیای بیت‌کوین به نام پاشنه آشیل معروف است.

مطلب پیشنهادی

وب‌سایت‌ها از پردازنده سیستم شما برای درآمدزایی استفاده می‌کنند
آیا از پردازنده شما برای استخراج غیرقانونی بیت‌کوین استفاده می‌شود؟ + 5 راه جلوگیری از آن

نقش محاسبات کوانتومی در این زمینه چیست؟

در دنیای بیت‌کوین و داده‌کاوی اگر گروهی بتواند 50 درصد از فرآیند محاسباتی را تحت کنترل خود درآورد، در عمل از سرعت بالاتری نسبت به گروهی که 49 درصد امور را تحت کنترل دارند برخوردار هستند. درست در همین نقطه است که کامپیوترهای کوانتومی به میدان وارد می‌شوند. مالک یک کامپیوتر کوانتومی به راحتی می‌تواند در فرآیند معدن‌کاوی از همتایان خود پیشی بگیرد. اگروال و همکارانش این موضوع را آزمایش کرده و مشاهده کرده‌اند که در شرایط یکسان هیچ شانسی برای افرادی که از کامپیوترهای کلاسیک استفاده می‌کنند وجود ندارد. همچنین سرعت کامپیوترهای کوانتومی و توان سخت‌افزاری آن‌ها در 10 سال آینده به شکل وحشتناکی پیشرفت خواهند کرد. اگروال می‌گوید: «امروزه اکثر معدن‌کاوان بیت‌کوین بر پایه مدارهای مجتمع خاص (ASIC) که از سوی انودیا طراحی شده کار می‌کنند. اما در ده سال آینده سرعت کامپیوترهای کوانتومی به مراتب فراتر از حال حاضر خواهد بود.» اما این تنها سرعت بالای محاسبات کوانتومی نیست که بیت‌کوین را در معرض خطر قرار می‌دهد. تهدید نگران کننده دیگر در ارتباط با ویژگی‌های امنیتی رمزنگاری است. بیت‌کوین بر پایه ریاضیات عمومی و اسکیمای رمزنگاری کلید عمومی (کلید عمومی/خصوصی) کار می‌کند. کامپیوترهای کوانتومی به راحتی می‌توانند با محاسبه کلید عمومی کلید خصوصی را به دست آورده و در عمل از سد مکانیزم رمزگذاری عبور کنند. الگوریتم رمزگذاری منحنی بیضوی که بیت‌کوین بر مبنای آن کار می‌کند تا سال 2027 در معرض تهدید جدی قرار خواهد گرفت، به‌طوری که برخی از کارشناسان فرضیه بلااستفاده بودن آن‌ها را مطرح کرده‌اند.

تاریخ انتشار:
09 فروردین 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/12299/%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1%D9%87%D8%A7%DB%8C-%DA%A9%D9%88%D8%A7%D9%86%D8%AA%D9%88%D9%85%DB%8C-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%A8%DB%8C%D8%AA%E2%80%8C%DA%A9%D9%88%DB%8C%D9%86-%D8%B1%D8%A7-%D8%A8%D9%87-%DA%86%D8%A7%D9%84%D8%B4-%D9%85%DB%8C%E2%80%8C%DA%A9%D8%B4%D9%86%D8%AF%D8%9F