عنوان مقاله: چرا امنیت بلاک چین ها حائز اهمیت است؟

نویسنده مقاله: تیم فنی نیک‌آموز

تاریخ انتشار: ۱۷ دی ۱۴۰۱

منبع: https://nikamooz.com/blockchain-security

امنیت بلاک چین یکی از مهم‌ترین نکاتی است که در چنین فناوری وجود دارد. سرمایه‌گذاران زیادی در سراسر جهان برای خرید بیت‌کوین و سایر ارزهای رمزگذاری شده تلاش می‌کنند؛ اما این افراد تنها به وعده‌های وسوسه برانگیز آن توجه کرده و با خطرات آن آشنا نیستند. موفقیت بیت‌کوین باعث شد تا شرکت‌های زیادی برای رسیدن به موفقیت به سمت معامله آن حرکت کنند.

اما در این مسیر نباید دزدها و هکرها را نادیده گرفت. امروزه نقاط ضعفی نیز در فناوری بلاک چین وجود داشته که هکرها از آن سوءاستفاده می‌کنند .ازاین‌رو برای آشنایی بیشتر با مبحث امنیت بلاک چین ما قصد داریم تا در این مطلب در خصوص نحوه محافظت از دارایی‌های دیجیتال بیشتر صحبت کنیم.

امنیت بلاک چین

بیت‌کوین فعالیت خودش را در سال ۲۰۰۹ آغاز کرد. این توکن یک ارز دیجیتال غیرمتمرکز است. به بیان دیگر، بیت‌کوین توسط هیچ مدیر، گروه، دولت و یا نهاد دیگری نظارت و یا تنظیم نمی‌شود. تراکنش‌های همتا به همتا باعث رشد این ارز دیجیتال شد و آن را به یک چشم‌اندازی مناسب برای شرکت‌ها و سازمان‌های مختلف بدل کرد. اما آیا امنیت بلاک چین و بیت‌کوین نیز به‌خوبی برنامه‌ریزی‌شده است.

بلاک چین‌های رمزنگاری، دفتر کل عمومی هستند که تمامی تراکنش‌ها را در یک شبکه بلاک چین ثبت و تأیید می‌کنند. همه افراد می‌توانند تراکنش‌ها، آدرس‌های مستعار درگیر و میزان انتقال را مشاهده کنند. بااین‌وجود برای امنیت بلاک چین، این دفاتر عمومی به هرکسی اجازه دسترسی به آن‌ها و یا ارسال و تغییر در ورودی‌ها را نمی‌دهد. جهت افزایش امنیت بلاک چین، این کار به‌صورت خودکار توسط اسکریپت‌ها، برنامه‌نویسی‌ها و یک فرایند اعتبارسنجی خودکار انجام می‌شود.

امنیت بلاک چین چگونه تأمین می‌شود؟

امنیت بلاک چین از طریق تکنیک‌های رمزنگاری و مکانیسم‌های اجماع انجام می‌پذیرد. بلاک چین‌ها از رمزگذاری برای قفل‌کردن اطلاعات تراکنش‌ها و گنجاندن داده‌های بلوک قبلی در بلوک‌های بعدی استفاده می‌کنند. کل دفتر بلاک چین از طریق همین داده‌های رمزگذاری شده به هم متصل هستند. هر بلوک جدید ایجاد شده، می‌تواند امنیت بلاک چین را افزایش دهد.

ازاین‌رو یک بلاک چین موجود را نمی‌توان به معنای سنتی هک‌کردن، هک کرد .این بدان معناست که نمی‌توان به واردکردن کدهای مخرب به زنجیره و یا اعمال تغییرات به شبکه نفوذ کرد و امنیت بلاک چین را مورد هدف قرار داد.

در چه جاهایی امنیت بلاک چین به خطر می‌افتد؟

مالکیت ارزهای دیجیتال به‌صورت یک توکن یا رشته‌ای طولانی از اعداد رمزگذاری شده در یک بلاک چین گره‌خورده است. به هر توکن یک کلید خصوصی اختصاص داده می‌شود که توسط مالک و یا متولی تعیین شده او، نگهداری می‌شود .دقیقاً در همین نقطه است که امنیت بلاک چین می‌تواند به خطر بیفتد .درصورتی‌که رمز و شماره شما هک شود، امکان دزدیدن و یا سرقت‌کردن آن وجود دارد.

- **هک کیف پول**

رمزگذاری موجب می‌شود تا کلیدهای خصوصی و نحوه ذخیره‌سازی آن‌ها در ارزهای رمز پایه و بلاک چین تضعیف شود. یک کلید خصوصی از نظر تئوری می‌تواند هک شود و امنیت بلاک چین را به خطر بیندازد. بااین‌حال این کلید یک عدد رمزگذاری شده با عدد ۱ به همراه ۷۵ صفر به دنبال آن است! ازاین‌رو قرن‌ها طول می‌کشد تا فناوری کنونی آن را هک کرد. جایی که امنیت بلاک چین به خطر می‌افتد زمانی است که فردی به کیف پول شما که محل ذخیره‌سازی کلیدهای خصوصی است، دسترسی پیدا می‌کند.

امروزه کیف پول‌ها روی نرم‌افزاهای مختلف در تلفن‌ها و یا رایانه‌ها وجود دارند. همچنین می‌توان آن‌ها را در دستگاه‌هایی مانند درایورها و یا usb ها ذخیره کرد. این کیف پول‌ها به‌صورت گرم (متصل به اینترنت) و سرد (نامتصل به اینترنت) هستند. اگر می‌خواهید امنیت بلاک چین خود را ارتقا دهید، بهتر است تمام تلاش خود را به کار برده تا کیف پول شما به دست افراد سودجو نیفتد.

- **هک‌های تبادل**

امنیت بلاک چین هم با کیف پول‌ها و هم با تبادل‌ها به خطر می‌افتد. مهم نیست که افراد و یا صرافی‌های مختلف در خصوص نحوه نگهداری و یا امنیت بلاک چین چه می‌گویند. این موارد می‌توانند امنیت بلاک چین را به خطر انداخته و به‌عنوان نقطه‌ضعف شناسایی می‌شوند. به‌صورت معمول صرافی‌ها برای نقدینگی، کلیدهای خصوصی و یا ارزهای دیجیتال مشتریان را ذخیره می‌کنند.

همین امر باعث می‌شود که آن‌ها هدفی جذاب برای هکرها باشند. سارقان با دسترسی پیداکردن به تبادل‌های صرافی‌ها، می‌توانند کلیدهای خصوصی مشتریان را هک کرده و امنیت بلاک چین را به خطر بیندازند؛ ازاین‌رو اگر کلیدهای خصوصی خود را در یک صرافی ذخیره نکنید، دسترسی به آن‌ها امکان‌پذیر نبوده و امنیت بلاک چین افزایش پیدا می‌کند.

چگونه ارز دیجیتال خود را ایمن کنید

برای جلوگیری از دزدیده‌شدن ارزهای دیجیتال خود و افزایش امنیت بلاک چین می‌توانید چند قدم ساده بردارید. مهم‌ترین فاکتور این است که بدانید کلیدهای شما چگونه ذخیره می‌شوند و چگونه دیگران می‌توانند به آن‌ها دسترسی

پیدا کنند. کیف پول‌های داغ، آن‌هایی که به اینترنت یا دستگاه‌های دیگر متصل هستند، کمترین امنیت را دارند. هرگز نباید کلیدهای خود را روی دستگاهی که همیشه به اینترنت متصل است، نگه دارید. این کار امنیت بلاک چین را به خطر می‌اندازد.

برای اینکه امنیت بلاک چین را ارتقا دهید نیازی به استفاده از کیف پول‌های تبلیغاتی و یا صرافی‌های نامعتبر نیست. می‌توانید کلیدهای خصوصی خود را روی درایورهای usb نگه داری کنید. بااین‌وجود مراقب باشید که درایور خود را به چه دستگاهی وصل می‌کنید. به‌صورت کلی هیچ راه صددرصدی برای ارتقا امنیت بلاک چین و جلوگیری از هک آن وجود ندارد. بااین‌وجود با رعایت برخی نکات ساده، می‌توانید خودتان را از چنگال هکرها و دزدیده‌شدن اطلاعات نجات دهید.

نتیجه‌گیری

بحث امنیت بلاک چین یکی از مهم‌ترین بحث‌هایی است که در زمان ورود به این بازار باید به آن توجه کنید. بسیاری افراد امنیت بلاک چین را نادیده گرفته و به همین دلیل ضررهای جبران‌ناپذیری را متقبل شدند. تمامی تراکنش‌ها و معاملات انجام شده در بلاک چین در بلوک‌های ذخیره شده و در یک دفتر کل نگهداری می‌شوند. برای دسترسی به ارزهای دیجیتال، کلیدهای خصوصی با رمزهای بسیار پیچیده وجود دارد که هک آن‌ها غیرممکن است.امنیت بلاک چین در زمانی به خطر می‌افتد که شما نتوانید به‌خوبی از کلیدهای خصوصی خود مراقبت کنید. بهتر است از کیف پول‌های سرد استفاده کرده و اطلاعات خود را در اختیار هیچ کسی قرار ندهید. به همین سادگی می‌توانید امنیت بلاک چین را ارتقا داده و خطر هک‌شدن را کم کنید.