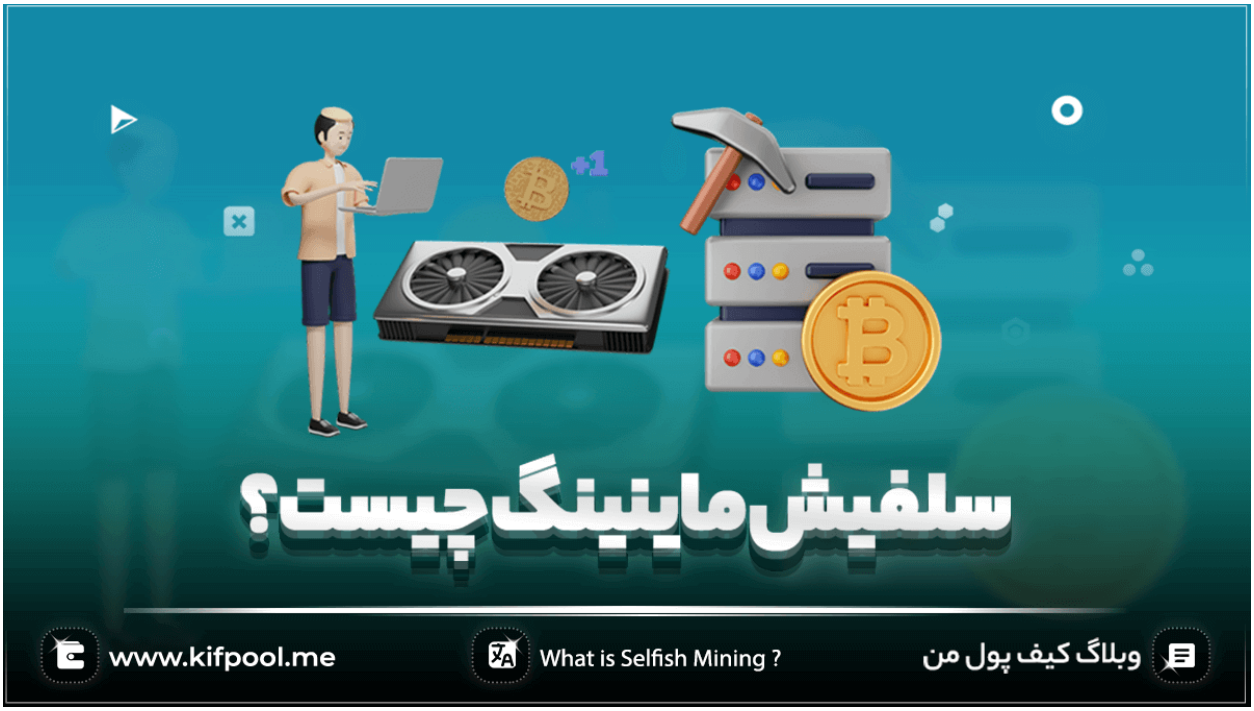


سلفیش ماینینگ چیست؟

سلفیش ماینینگ (Selfish Mining) چیست؟

آیا تا به حال به این موضوع فکر کرده‌اید که چه چیزی ممکن است دنیای امن و غیرمتمرکز رمزارزها را با تهدید مواجه کند؟ یا اینکه واقعاً چه اتفاقی می‌تواند منجر به هک شدن شبکه بلاک‌چین‌های متفاوت مخصوصاً شبکه بیت‌کوین شود؟ در واقع آسیب‌پذیری دنیای رمزارزها تنها از یک روش ممکن است و آن هم **سلفیش ماینینگ** است. سلفیش ماینینگ استراتژی است که در صورت عدم جلوگیری از آن می‌تواند دنیای ارز دیجیتال را از بین ببرد. نکته جالب این است که ماینرها، یعنی دقیقاً همان کسانی که با تایید تراکنش‌های مختلف در سطح بلاک‌چین به امنیت آن کمک می‌کند، باعث ایجاد چنین فرآیندی می‌شوند.

سلفیش ماینینگ امروزه تبدیل به یک مفهوم جالب برای کاربران کریپتوکارنسی شده است و به آنها کمک می‌کند پیش‌زمینه‌ای درباره سازوکار شبکه‌ای که در آن سرمایه‌گذاری می‌کنند داشته باشند و با چشم باز نسبت به حرکات بعدی خود تصمیم بگیرند. با این مقاله از وبلاگ **کیف پول من** همراه باشید اگر دوست دارید درباره مفهوم سلفیش ماینینگ، نحوه کار آن و خطراتی که برای اکوسیستم ارزهای دیجیتال می‌آفرینند اطلاعاتی کسب کنید.

سلفیش ماینینگ؛ تبانی دست‌های پشت پرده برای سود بیشتر

بلاک‌چین‌های مختلف برای اینکه بتوانند در امنیت کامل به حیات خودشان ادامه بدهند نیاز دارند تا یک سری از افراد به‌عنوان ماینرها به‌صورت گروهی همواره در حال تایید تراکنش‌ها باشند و

همچنین با حل معادلات سخت ریاضی، بلوک‌های جدید از کوین‌های یک رمزارز را استخراج کنند. قوانین بلاک‌چین‌های مختلف مخصوصاً بیت‌کوین به این شیوه است که هر ماینر می‌تواند به‌عنوان پاداش کار خود بیت‌کوین دریافت کند و این پاداش بر اساس میزان بلوکی که استخراج کرده است محاسبه می‌شود.
وقتی یک ماینر یک معادله را حل می‌کند و بلوک استخراج شده و به زنجیره او اضافه می‌شود، باید به تمام اعضای آن استخر اطلاع دهد تا دیگران بر روی معادله فعلی زمان صرف نکنند و به سراغ معادله بعدی و استخراج بلوک بعدی بروند. این داستان باور تمام اعضای بازار ارز دیجیتال و ماینرها تا سال 2013 بود تا اینکه دو تن از توسعه‌دهندگان و محققان دنیای کریپتو به نام امین گون سیرر (Emin Gün Sirer) به همراه ایتای ایال (Ittay Eyal) مفهومی تحت عنوان **سلفیش ماینینگ** یا استخراج خودخواهانه را مطرح کردند.

مطلب پیشنهادی : بررسی امینیت شبکه بلاکچین

سلفیش ماینینگ در واقع استراتژی است که در آن یک ماینر یا گروهی از ماینرها تصمیم می‌گیرند با یکدیگر همکاری یا به اصطلاح تبانی کنند تا سود بیشتری کسب کنند. سلفیش ماینینگ در اصل فرآیندی است که در آن یک ماینر بعد از اینکه جواب یک معادله را به دست آورد و توکن مربوط به آن را استخراج کرد، آن را از نودها و ماینرهای دیگر پنهان کند. در این شرایط، ماینر حمله کننده به سمت استخراج بلوک دیگری می‌رود و سعی می‌کند جواب آن معادله را پیدا کند؛ در حالی که دیگر ماینرها هنوز بر روی جواب معادله قبلی انرژی صرف می‌کنند.

سلفیش ماینینگ چگونه کار می‌کند؟

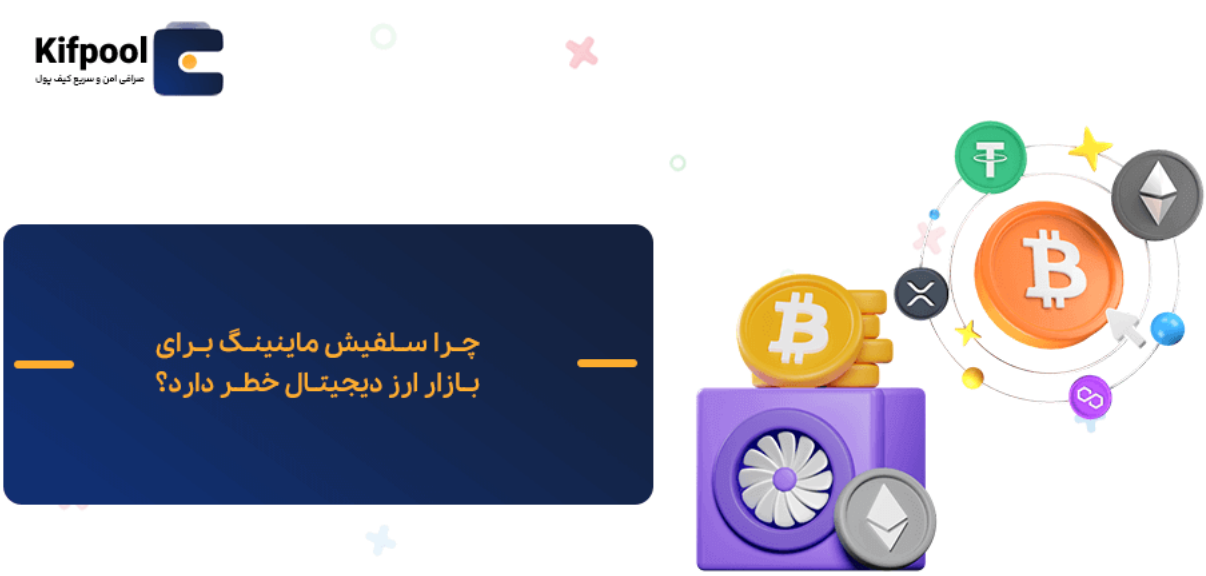
اگر بخواهیم به زبان ساده بگوییم، باید گفت که **سلفیش ماینینگ** در اصل بر اساس فریب‌کاری و بی‌صداقتی ماینرهای حاضر در شبکه به وجود می‌آید. در اکوسیستم ارزهای دیجیتال قانون بر این منوال است که در یک شبکه بلاک‌چین، تمام ماینرها از یک شانس و یک نرخ هش (میزان سرعتی که یک دستگاه ماینینگ برای پیدا کردن جواب معادله دارد) برخوردار باشند؛ به این ترتیب همه ماینرها به‌صورت همزمان بر روی پاسخ یک معادله کار می‌کنند و به محض یافتن جواب و استخراج کوین، به بقیه اعضا اطلاع می‌دهند تا بقیه نیز به سوی معادله بعدی بروند.

علاوه بر این، قانون این است که هر بلوک بعد از استخراج به زنجیره متصل می‌شود و ماینرها باید به آخرین بلوک زنجیره برای ادامه کار متصل شوند. طبق قوانین زنجیره‌ای صحیح است که بیشترین میزان اثبات کار برای آن ثبت شده باشد. حالا در سلفیش ماینینگ کار ماینرها این است که بعد از استخراج یک توکن، آن را از بلاک‌چین عمومی پنهان می‌کنند و با یک فورک جداگانه و مخفی برای مدتی کوتاه، یک بلاکچین شخصی برای خود می‌سازند.

سپس در حالی که ماینرهای دیگر هنوز دارند بر روی جواب معمای فعلی شانس خود را امتحان می‌کنند، ماینر حمله‌کننده به سمت معادله بعدی می‌رود و سعی می‌کند جواب را بیاید. بعد از اینکه جواب پیدا شد، دوباره بلوک بعدی به زنجیره اضافه می‌شود و این کار بعد از استخراج چند توکن ادامه می‌یابد تا اینکه سیستم‌های حاضر در بازار متوجه تفاوت طول زنجیره اصلی و زنجیره‌ای که بر روی آن کار می‌کنند می‌شوند و ناچارند برای تبعیت از قانون، دوباره به زنجیره

طولانی‌تر با اثبات کار بیشتر منتقل شوند. در واقع **سلفیش ماینینگ** باعث می‌شود یک ماینر با دور زدن و فریب دادن بقیه شانس و وقت بیشتری برای پیدا کردن جواب معادله داشته باشد و بقیه اعضای بازار با هدر دادن وقت و انرژی خود بالاخره به بن‌بست می‌رسند و مجبور می‌شوند کارشان را از ادامه زنجیره‌ای ادامه دهند که ماینر حمله کننده آن را ساخته است.

چرا سلفیش ماینینگ برای بازار ارز دیجیتال خطر دارد؟



سازوکار استخراج توکن‌های هر شبکه مخصوصاً شبکه بیت‌کوین به شکلی طراحی شده که ماینرها با رعایت صداقت و درستی و با کمترین کار و صرف کمترین انرژی و وقت، درآمد خوبی به دست آورند؛ ولی وقتی برخی از ماینرها طمع می‌کنند، مسئله می‌تواند برای سلامت اکوسیستم خطرآفرین باشد.

سلفیش ماینینگ باعث می‌شود امنیت بلاک‌چین به خطر بیفتد و از آنجایی که هر ماینر حمله کننده سعی می‌کند برای خود، فورک‌ها و شبکه‌های بلاکچینی جداگانه بسازد، توزیع توکن‌های از غیرمتمرکز بودن به سمت متمرکز بودن گرایش پیدا می‌کند. علاوه بر آن، سلفیش ماینینگ باعث می‌شود وقت، انرژی و همچنین درآمد بسیاری از ماینرها هدر رود و ماینرها تمایلات غیرصادقانه‌ای برای ادامه فعالیت خود پیش بگیرند.

درآمد بیشتر سلفیش ماینینگ باعث می‌شود ماینرهای بیشتری به سمت این حرکت گام بردارند و به‌مرور به جای یک نود، نودهای بیشتری در این مسیر همکار شوند و باعث ایجاد شبکه‌های

بلاک‌چینی فرعی و خصوصی شوند. به این ترتیب، رفته رفته نرخ هش یک استخر نقدینگی و استخراج توکن به حدی بالا می‌رود که باعث می‌شود کنترل اکوسیستم از دست تمام نودهای حاضر در بیاید و به دست گروه خاصی از ماینرها بیفتد. این اتفاق را حمله 51 درصدی می‌گویند.

حمله 51 درصدی چیست؟

حمله 51 درصدی که بر اثر تمایل تعداد زیادی از ماینرها به **سلفیش ماینینگ** در اکوسیستم بلاک‌چین‌های رمزارزها انجام می‌گیرد، تنها راهی است که می‌توان با آن شبکه بیت کوین را هک و نابود کرد. در یک شبکه بلاکچینی نودها سعی می‌کنند معتبرترین بلوک را تشخیص دهند و آن را تایید کنند و تایید یک بلوک تنها بر اثر تایید اکثر ماینرها انجام می‌گیرد؛ به عبارت دیگر تنها وقتی یک بلوک به زنجیره اضافه می‌شود که اکثر نودها آن را تایید کنند.

وقتی یک ماینر یا گروهی از ماینرها با سلفیش ماینینگ یک فورک و بلاکچین شخصی جداگانه می‌سازند، استخرها از هم جدا می‌شوند و همواره استخر بزرگ‌تر به علت وجود ماینرهای بیشتر، قدرت تصمیم بیشتری برای اکوسیستم خواهد داشت. با ادامه یافتن این شرایط، کار به جایی می‌رسد که قدرت ماینرهای حمله‌کننده بر دیگر ماینرها می‌چربد و تعدادشان به‌صورت نامساوی و به نفع سلفیش ماینرها تقسیم می‌شود و حمله 51 درصدی رخ می‌دهد؛ یعنی دیگر اختیار و نظارت بازار به‌صورت غیرمتمرکز در دست همه نودها نیست و توسط گروه خاصی از آن‌ها ماینینگ هدایت می‌شود. البته باید گفت تا به امروز چنین اتفاقی در دنیای رمزارزها رخ نداده است؛ اما وجودش هم خالی از احتمال نیست.

مطلب پیشنهادی: فاد در ارز دیجیتال چیست؟

سلفیش ماینینگ تهدیدی برای اکوسیستم ارزهای دیجیتال است!

سلفیش ماینینگ استراتژی است که طی آن یک ماینر یا گروهی از آن‌ها تصمیم می‌گیرند از راهی فریبکارانه و غیرصادقانه، دیگر نودهای حاضر در شبکه را دور بزنند و از این راه درآمد خود را افزایش دهند. در واقع، در این فرآیند وقتی یک ماینر جواب یک معادله را به دست می‌آورد، بدون اینکه آن را به بقیه اعضا اطلاع دهد، آن را به یک بلاکچین شخصی منتقل می‌کند و باعث ایجاد یک فورک و زنجیره جدید می‌شود؛ در حالی که بقیه ماینرها همچنان در حال حل کردن معادله قبلی هستند. سپس ماینر حمله‌کننده به سمت حل معادلات بعدی می‌رود و با این کار شانس خود را برای دریافت پاداش‌های بیشتر افزایش می‌دهد. ماینرهای دیگر هم به‌ناچار بعد از مدتی به زنجیره اصلی که ماینر حمله‌کننده آن را ایجاد کرده، می‌پیوندند؛ در صورتی که انرژی و وقت خود را هدر داده‌اند. سلفیش ماینینگ می‌تواند اثرات بسیار مخربی بر روی اکوسیستم بگذارد که از میان آنها می‌توان به حمله 51 درصدی اشاره کرد.