حمله فینی (Finney Attack) چیست؟

حمله فینی (Finney Attack) یکی از نخستین حملات بلاکچینی شناخته شده در شبکه بیت کوین است که توسط اولین فردی که بیت کوین را دریافت نمود، کشف شد. حمله فینی یک نوع بسیار ویژه از حملات در حوزه بلاکچین است که بر بیت کوین و هر ارز رمزنگاری شده حاصل از آن تأثیر می گذارد. در این مقاله از مجله آموزشی کیف پول من به شما خواهیم گفت که حمله فینی (Finney Attack) چیست و چگونه کار می کند؟ همچنین در همین مقاله از بلاگ کیف پول من، با راهکارهای جلوگیری از حمله فینی در خدمت شما خواهیم بود. با ما همراه باشید.

حمله فینی (Finney Attack) چیست؟

هال فینی، توسعه دهنده نرم افزار آمریکایی، نخستین دریافت کننده اولین تراکنش بیت کوین بود. او همچنین اولین کسی بود که در جریان راه اندازی اولیه بیت کوین به طور عمومی سخنرانی کرد. به عنوان یک توسعه دهنده نرم افزار، او همچنین امکان انجام یک "طرح هزینه مضاعف" روی بیت کوین را پایه گذاری نمود و این طرح به نام او به «حمله فینی – Finney Hack یا Finney Attack» نامگذاری شد. هک یا حمله فینی نوعی حمله هکی یا هزینه دوگانه است.

بنابراین، وقتی شخصی تراکنش تایید نشده در شبکه را می پذیرد، چه اتفاقی می افتد؟ فینی توضیح داد که یک ماینر می تواند بلوکی ایجاد کند که در آن تراکنش را از یک آدرس (A) به آدرس دیگری (B) وارد کند، جایی که هر دو آدرس متعلق به او هستند. سپس، پرداخت دیگری را با همان ارزها انجام دهد و از آدرس A به آدرس C (که متعلق به کاربر دیگری است) ارسال کند. اگر کاربر مذکور تراکنش را بدون تایید شبکه بپذیرد، مهاجم می تواند بلوکی را که تراکنش اولیه او در آن گنجانده شده، آزاد کند. این امر تراکنش انجام شده با کاربر را باطل نموده و به مهاجم اجازه می دهد تا دو برابر هزینه ایجاد کند.

Finney Attack چگونه انجام می شود؟

همانطور که گفته شد، حمله فینی نوعی حمله بلاکچینی است که به نام خالق آن، هال فینی، یکی از مشارکت کنندگان اولیه بیت کوین، نامگذاری شده است. حمله فینی ممکن است به راحتی مجرمان حوزه سایبری را به خود جذب کند، زیرا به نظر می رسد این روش راهی آسان برای ثروتمند شدن بدون تلاش زیاد و با ناشناس ماندن هویت شان باشد. اما در حقیقت، به سر انجام رساندن این پروسه، اصلاً کار آسانی نبوده و چیزی نیست که هر کسی بتواند آن را انجام دهد. این حمله مخصوص شبکه های بلاکچینی است که از مکانیسم های اجماع اثبات کار (مانند بیت کوین) استفاده می کنند. حمله Finney از تأخیر زمانی بین پخش تراکنش و گنجاندن آن در یک بلوک برای سود بردن از حمله استفاده می کند. در اینجا نحوه عملکرد حمله فینی را شرح داده ایم:

- **مرحله 1 (آماده سازی):** مهاجم ابتدا مقدار قابل توجهی از ارز دیجیتال، معمولاً بیت کوین، به دست می آورد و یک ماینر یا استخر استخراج راه اندازی می کند.
- **مرحله 2 (ارسال وجوه):** مهاجم تراکنشی را برای ارسال ارز دیجیتال خود به گیرنده آغاز می کند. این تراکنش بلافاصله در شبکه پخش نمی شود.
- **مرحله 3 (استخراج یک بلوک):** مهاجم شروع به استخراج یک بلوک جدید به صورت خصوصی می کند، که شامل تراکنش از مرحله 2 است. این فرآیند استخراج خصوصی از شبکه پنهان شده و منتشر نمی شود.
- **مرحله 4 (انتظار برای یک قربانی):** مهاجم منتظر می ماند تا قربانی یک عمل خاص را انجام دهد. به عنوان مثال، قربانی ممکن است خرید بزرگی انجام دهد که نیاز به تأیید در بلاکچین دارد.
- **مرحله 5 (آزاد کردن بلوک):** هنگامی که تراکنش قربانی در شبکه پخش شد و در بلاکچین قرار گرفت، مهاجم بلوک استخراج شده خصوصی خود را که شامل تراکنش مرحله 2 است،

آزاد می کند. این بلوک قبل از اینکه ماینرهای دیگری بتوانند رقابت کنند به بلاکچین اضافه می شود زیرا مهاجم قبلاً آن را به صورت خصوصی استخراج کرده است.

- **مرحله 6 (کسب سود):** تراکنش مهاجم پس از تراکنش قربانی در بلاکچین تأیید می شود، اما قبل از اینکه سایر ماینرها بتوانند بلوک های رقیب را شامل شوند. این به مهاجم اجازه می دهد تا ارز دیجیتال خود را دوبار خرج کند و آن را به آدرس دیگری بفرستد در حالی که هنوز وجوه اصلی را در اختیار دارد.

قربانی که ارز دیجیتال را از تراکنش اولیه مهاجم دریافت کرده، معتقد است تراکنش معتبر و غیرقابل برگشت می باشد. با این حال، پس از اینکه مهاجم بلوک استخراج شده مخفیانه خود را آزاد کرد، تراکنش قربانی معکوس می شود و او وجوه دریافتی خود را از دست می دهد.
موفقیت این حمله تا حد زیادی به قدرت هش ماینر بستگی دارد. این بدان معناست که هرچه قدرت هش ماینر کمتر باشد، احتمال اجرای موفقیت آمیز آن کمتر است. از طرف دیگر، اگر در زمانی که مهاجم در حال یافتن بلوک است تا زمانی که تراکنش برای فروشنده ایجاد شود و فرد آن را بپذیرد بلوک دیگری در شبکه پیدا شود، حمله شکست خواهد خورد. اجرای این نوع حملات به زمان بندی دقیق و صبر زیادی نیاز دارد. چراکه باید منتظر بمانید تا یک بلوک پیدا شود. این پروسه با توجه به تعداد ماینرها و **سختی شبکه بیت کوین** ممکن است زمان زیادی طول بکشد.
حمله فینی بر این واقعیت متکی است که ماینرها بر ترتیب قرار گرفتن تراکنش ها در بلوک ها کنترل داشته و می توانند تراکنش های خود را اولویت بندی کنند. این حملات به طور کلی در مقایسه با سایر انواع حملات بلاکچینی، کمتر کاربرد داشته و حمله سودآوری تلقی نمی شوند. علاوه بر این، با تکامل شبکه های بلاکچین و مکانیسم های امنیتی، پنجره فرصت برای حملات فینی کاهش یافته است.

چگونه می توان از حمله فینی جلوگیری کرد؟

تراکنش های بیت کوین برگشت ناپذیر هستند؛ زیرا بلوک های جدیدی در هر تراکنش ایجاد می شوند و هر بلوک جدید را به عنوان تأییدی برای تراکنش در نظر گرفته می شود. با این حال، برای مبالغ قابل توجه، توصیه می شود که منتظر حداقل 6 تأیید باشید تا مطمئن شوید تراکنش عملاً غیر قابل نفوذ است. با در نظر گرفتن این که حملات فینی نسبت به انواع دیگر حملات کمتر کاربرد دارند، اما همچنان می توانند نگران کننده باشند. به همین خاطر در بخش چند استراتژی برای کاهش احتمال بروز حملات فینی برایتان آورده ایم:

1. **استفاده از تأییدیه های بیشتر:** یکی از مؤثرترین راه ها برای کاهش حملات Finney این است که قبل از در نظر گرفتن یک تراکنش به عنوان تراکنش نهایی، منتظر تعداد بیشتری تأییدیه از سمت بلاکچین باشید. معمولاً در شبکه بیت کوین، برای اطمینان از امنیت تراکنش بایستی منتظر حداقل شش تائید باشید. هرچه تأییدهای بیشتری داشته باشید، تراکنش شما امن تر خواهد بود، زیرا هزینه و دشواری اجرای حمله Finney با هر تأییدیه افزایش می یابد.
2. **پروتکل های پرداخت:** پروتکل های پرداخت یا فناوری هایی مانند شبکه لایتنینگ بیت کوین را برای تراکنش های کوچکتر و سریع تر پیاده سازی کنید. این راه حل های خارج از زنجیره در حالی که برای امنیت خود به بلاکچین تکیه می کنند، می توانند تأییدیه های سریع تری ارائه نموده و خطر حملات Finney را برای تراکنش های روزمره کاهش دهند.

3. **ارزیابی ریسک:** ریسک مربوط به هر معامله را بر اساس ارزش درگیر ارزیابی کنید. برای معاملات کم ارزش، انتظار برای یک یا دو تایید ممکن است کافی باشد. برای تراکنش های با ارزش بالا، یک دوره تأیید طولانی تر توصیه می شود.
4. **سیستم های مانیتورینگ و هشدار:** سیستم های نظارت و هشدار در لحظه را برای شناسایی فعالیت های غیرعادی یا مشکوک در بلاکچین پیاده سازی کنید. این کار می تواند به شناسایی زودهنگام حمله فینی کمک کرده و امکان اقدام فوری را فراهم نماید.
5. **کیف پول های چند امضایی:** از کیف پول های چند امضایی استفاده کنید که برای مجوز دادن به تراکنش به چندین کلید خصوصی نیاز دارند. انجام این کار می تواند یک لایه امنیتی اضافی به دارایی های شما اضافه کرده و حمله فینی را برای مهاجم دشوارتر نماید.
6. **تعویض با کارمزد تراکنش (RBF):** در صورت پشتیبانی بلاکچین، قابلیت RBF را برای تراکنش های خود فعال کنید. RBF به شما امکان می دهد یک تراکنش تایید نشده را با تراکنش جدیدی جایگزین کنید که کارمزد بیشتری می پردازد و این باعث می شود تراکنش اصلی در یک بلوک گنجانده شود.

سخن پایانی

در این بخش از مجله آموزشی کیف پول من، حمله فینی که یکی از نخستین حملات بلاکچینی در شبکه بیت کوین بود را زیر ذره بین قرار داده و آن ها را به زبانی ساده به شما عزیزان توضیح دادیم. امروزه و با توجه به پیشرفت هایی که بلاکچین های مختلف از جمله بیت کوین داشته اند، کمتر شاهد بروز حملاتی مانند هک فینی هستیم. با این وجود، آشنایی با حمله فینی و راهکارهای جلوگیری از آن می تواند امنیت تراکنش های شما را افزایش داده و باعث آسودگی هرچه بیشتر خاطرتان شود. ما در صرافی کیف پول من با در نظر گرفتن تمام تدابیر امنیتی شبکه های بلاکچین و با نظارت بر تمام تراکنش های موجود، به شما این تضمین را می دهیم که تمام خرید و فروش ها و معاملات بیت کوین را بدون هیچ مشکلی به سرانجام برسانید. امیدواریم این مقاله مورد استفاده شما همراهان گرامی کیف پول من قرار گرفته باشد. شایان ذکر است می توانید سوالات، انتقادات و نظرات خود را از طریق بخش دیدگاه ها به سمع و بصر ما و سایر کاربران برسانید.