پرایوسی کوین چیست و چگونه کار می‌کند؟

با این که امنیت و ناشناخته بودن یکی از اصلی‌ترین اهداف ارزهای دیجیتال است، اما این ارزها را می‌توان با راه‌های مختلفی شناسایی کرد. این امر به دلیل شفافیت بالای ارزهای دیجیتال آسان‌تر نیز می‌شود. **پرایوسی کوین**ها دسته‌ای ارزهای دیجیتال بحث برانگیز هستند که برای مقابله با این عامل به وجود آمده‌اند.

در حال حاضر، این دسته از ارزهای دیجیتال بیشترین امنیت را دارند و به همین خاطر برخی سازمان‌ها و دولت‌ها با این ارزها بیشترین مخالفت را می‌کنند. این نوع از ارزها از چند مکانیزم مختلف برای مخفی نگه داشتن هویت خریداران و فروشندگان استفاده می‌نمایند تا بیشترین امنیت را برای آنها داشته باشند. **ارزهای دیجیتال حریم خصوصی** یا **پرایوسی کوین** به عنوان یکی از جدیدترین و جذاب‌ترین نوع ارزهای دیجیتال، موضوع بحث این مقاله از مجموعه کیف پول من خواهد بود.

پرایوسی کوین چیست؟

پرایوسی کوین یا کوین حریم شخصی (**خصوصی**) نوع جدیدی از ارز دیجیتال هستند که بر خصوصی بودن معاملات اصرار دارند. در دنیای ارزهای دیجیتال، رمزارزهایی مانند بیت کوین و اتریوم بر **ناشناس ماندن** و **امنیت بیشتر** به وجود آمده‌اند.

با این که هدف همه ارزهای دیجیتال امنیت بیشتر و ناشناس ماندن کاربران است، اما همچنان اطلاعات خاصی از کاربران را در دسترس عموم قرار می‌دهند. چرا که هدف دیگر ارزهای دیجیتال، شفافیت تبادلات است. به این دلیل زمانی که شما تراکنشی را انجام می‌دهید. مقدار ارز مبادله شده و آدرس فرد ارسال کننده و دریافت کننده مشخص می‌شود.

همه افراد می‌توانند به این نوع از اطلاعات در دنیای ارزهای دیجیتال دسترسی داشته باشند. این مورد می‌تواند حریم خصوصی و اطلاعات کاربران را فاش کند. به همین خاطر می‌توان گفت که انتقال ارز در دنیای ارز دیجیتال دارای حریم خصوصی زیادی نیست.

مطلب پیشنهادی : کلود ماینینگ چیست؟

پرایوسی کوین دسته‌ای از ارزهای دیجیتال هستند که به دلیل اهمیت زیاد به حریم خصوصی کاربران، این اطلاعات را برای همه فاش نمی‌کنند. در حقیقت، دو نوع پرایوسی کوین وجود دارد. دسته اول ارزهایی هستند که به صورت پیش فرض تمامی اطلاعات تراکنش را مخفی می‌کنند.

یعنی هیچ اطلاعاتی از شما هنگام خرید و فروش ارزهای دیجیتال فاش نمی‌شود. دسته دوم پرایوسی کوین‌ها ارزهای دیجیتالی هستند که کاربر خود فاش شدن اطلاعات را انتخاب می‌کند.

یعنی شما می‌توانید انتخاب کنید که اطلاعات تراکنش در دسترس عموم قرار بگیرد یا نه. **ارز دیجیتال مونرو** در دسته اول و **رمزارز زی کش** در دسته دوم پرایوسی کوین‌ها قرار می‌گیرند. به دلیل این که اطلاعاتی مانند آدرس گیرنده، آدرس فرستنده و مبلغ تراکنش در اختیار عموم قرار نمی‌گیرد، نمی‌توان فرستنده و گیرنده ارزهای دیجیتال پرایوسی کوین را شناسایی کرد.

پرایوسی کوین‌ها باعث ایجاد اختلافات در دنیای ارزهای دیجیتال شده‌اند. عده‌ای متعقدند که این نوع از ارزها امنیت زیادی را به وجود می‌آورند در حالی که دسته دیگر به سو استفاده از این نوع ارزها اشاره می‌کنند.

نحوه کار پرایوسی کوین

شاید مخفی نگه داشتن دو طرف معامله در دنیای ارزهای دیجیتال پس از آشنایی با **مکانیزم‌های بلاک چین** کار سختی به نظر برسد، اما روش‌های مختلفی به وجود آمده‌اند که به وسیله آن می‌توان اطلاعات تراکنش‌ها را مخفی نگه داشت.

پرایوسی کوین‌ها از مکانیزم‌های مختلفی برای دستیابی به اهداف خود استفاده می‌کنند که راه‌های زیر عمده‌ترین روش برای ایجاد پرایوسی کوین هستند:

- آدرس‌های مخفی
- امضاهای حلقه‌ای یا رینگ
- تراکنش‌های حلقه‌ای محرمانه
- روش اثبات دانش صفر ZK-SNARKs
- روش ضدگلوله‌ها
- روش ادغام ارزهای دیجیتال

برای آشنایی با نحوه عملکرد هر یک از این روش‌ها با ما همراه شوید.

روش آدرس‌های مخفی یا Stealth Addresses

آدرس‌های مخفی از بهترین و ابتدایی‌ترین روش‌های برای **عملکرد پرایوسی کوین‌ها** هستند. در ارزهای دیجیتال معمولی مانند بیت کوین و اتریوم، هر کاربر دارای یک **کلید عمومی و خصوصی** است. در این حالت از **کلید خصوصی** می‌توان برای دسترسی به کلید عمومی استفاده کرد و کلید عمومی نشان‌گر یک فرد و تراکنش‌های وی است. اما در دنیا ارزهای دیجیتالی مانند مونرو که از روش آدرس‌های مخفی استفاده می‌کنند، هر فرد دارای دو کلید خصوصی و دو کلید عمومی است.

مطلب پیشنهادی : آموزش پیدا کردن آدرس کیف پول ارز دیجیتال

در انتقال ارز دیجیتال مونرو، برای هر تراکنش یک کلید عمومی یک بار مصرف و فعلی تولید می‌شود. کلید عمومی موقت و یک بار مصرف می‌تواند هویت فرد گیرنده و فرستنده را مخفی کند. در این روش، فرد فرستنده کلید عمومی فرد به همراه یک شماره را دریافت می‌کند که تنها در اختیار فرستنده و گیرنده قرار داده شده‌اند. با استفاده از این دو، یک کلید عمومی یک بار مصرف تولید می‌شود.

پس از ارسال مبلغ، فرد گیرنده از طریق کلید خصوصی خود می‌تواند به مبلغ دسترسی پیدا کند. برای فروش یا خرید بیت کوین به صورت ناشناس، صرافی کیف پول من به صورت کامل از شما پشتیبانی می کند تا بتوانید خرید بیت کوین به صورت مخفیانه بپردازید.

کلید خصوصی گیرنده راه شناسایی و دریافت ارز دیجیتال است. در این حالت، فرد گیرند با استفاده از کلید خصوصی خود، کلید عمومی یک بار مصرفی مانند کلید عمومی تحویل داده شده به گیرنده را ایجاد می‌کند تا ارزهای خود را صاحب شود.

امضاهای حلقه‌ای یا Ring Signatures

زمانی که تراکنشی در ارزهایی مانند **بیت کوین** انجام می‌شود، **کلید خصوصی** و **کلید عمومی** را امضا می‌کند. بدین وسیله می‌توان با کلید خصوصی به کلید عمومی دسترسی پیدا کرد. در پرایوسی کوین‌ها برای این که هویت اصلی فرد گیرنده و فرستنده ناشناس بماند، از امضاهای حلقه‌ای استفاده می‌شود. هنگامی که تراکنشی انجام می‌شود، خود شبکه به صورت اتوماتیک گروهی از امضا کننده‌ها را وارد کار می‌کند. این گروه از امضا کننده‌ها، امضاهای حلقه‌ای را به وجود می‌آورند.

گروه امضا کنندگان مجموعه‌ای از تراکنش‌ها را ایجاد می‌کنند که تنها یکی از آنها اصیل و واقعی است. یعنی تنها یکی از خروجی‌های تراکنش که ورودی جدید را ایجاد کرده‌اند ورودی واقعی است. در این حالت نمی‌توان تشخیص داد که کدام یک از ورودی‌ها واقعی بوده و تراکنش اصلی محسوب می‌شود. قابل ذکر است که ارز دیجیتال مونرو نیز از این روش استفاده می‌کند.

تراکنش‌های حلقه‌ای محرمانه یا Ring Confidential Transactions

تراکنش‌های محرمانه حلقه‌ای نوع دیگری از مکانیزم‌های پرایوسی کوین‌ها برای مخفی نگه داشتن هویت کاربران است. این روش شباهت زیادی به امضاهای حلقه‌ای دارد و در حقیقت برای تکمیل این مکانیزم طراحی شده است.

این روش نیز توسط ارز دیجیتال مونرو استفاده شده و می‌تواند مقدار ارزهای دیجیتال مونرو تراکنش شده را مخفی نگه دارد. در دو روش قبلی، تنها اطلاعات کاربران مخفی می‌شد و بقیه می‌توانستند مقدار مونرو منتقل شده را مشاهده کنند. در صورتی که با تراکنش‌های محرمانه حلقه‌ای افراد نمی‌توانند مقدار تراکنش بقیه را بدانند.

در این روش از **کلید خصوصی نمایش** (**Private View Key**) و کلید عمومی فرستنده استفاده می‌شود تا کاربر فرستنده مبلغ تراکنش را با گیرند به صورت کریپتوگرافی به اشتراک بگذارد. در دنیای بلاک چین برای انتقال ارزهای دیجیتال باید به شبکه ثابت کنید که هر تراکنش یکتا است.

یعنی نباید یک تراکنش دو بار انجام شود. به دلیل این که در این روش مقدار ارزهای دیجیتال منتقل شده مخفی باقی مانده، شبکه از یک روش به نام Commitments Pedersen یا تهدات پدرسن استفاده می‌کند. این روش از اثبات دانش صفر الهام گرفته است.

ZK-SNARKs

دانش صفر در انتقال ارزهای پرایوسی کوین کاربرد زیادی دارد. روش ZK-SNARKs نیز به کمک اثبات دانش صفر به وجود آمده است. عبارت ZK-SNARKs **مخفف شده Zero Knowledge-Succinct non-interactive argument of knowledge** است.

مانند تعهدات پدرسون، این روش نیز راهی برای جلوگیری از تکرار تراکنش‌ها بوده و در شبکه زی کش استفاده می‌شود. همان‌طور که گفتیم، تعهدات پدرسون در شبکه ارز دیجیتال مونرو مورد استفاده قرار می‌گیرند.

ترکیب کوین یا Coin Mixing

ترکیب کوین یا سکه یکی از روش‌های مناسب برای مخفی نگه داشتن هویت کاربران است. در این روش نیاز نیست ارزهای دیجیتال مختلف با هم ترکیب شوند. در عوض، هنگام ارسال یک ارز دیجیتالی که از این روش استفاده می‌کند، شبکه یک مستر نود را انتخاب می‌کند.

مطلب پیشنهادی : بررسی درامد تریدر های ارز دیجیتال

این مستر نود انتخاب شده نباید اخیرا فرایند ترکیب کوین را انجام داده باشد. مستر نود منتخب می‌تواند با در دست داشتن مقدار انتقالی، به مستر نودهای دیگر اطلاع می‌دهد تا آنها مقدار تراکشن شما را به چند بخش دیگر تقسیم کنند.

هر مستر نود وظیفه انتقال مقداری از ارز دیجیتال را بر عهده می‌گیرند. هر مستر نود با یک آدرس تصادفی ارزهای دیجیتال را به گیرنده ارسال می‌کند. در حال حاضر ارزهای دیجیتال و کیف پول‌های دیجیتال زیادی از این روش استفاده نمی‌کنند.

روش ضد گلوله یا Bullet Proof

روش بولت پروف یا ضد گلوله دیگر اقدام امنیتی شبکه مونرو برای محافظت از هویت کاربران است. بولت پروف نیز از اثبات دانش صفر استفاده می‌کند. بولت پروف در حقیقت جایگزین یکی دیگر از مکانیزم‌های شبکه مونرو است که به دلیل اشغال فضای بیشتری برای داده‌های زیاد با بولت پروف جایگزین شد. بولت پروف امنیت بیشتری نسبت به روش قبلی دارد، چرا که از یک رمز عبور مشخص و واحد برای شناسایی تراکنش‌ها استفاده نمی‌کند. از طرف دیگر، روش بولت پروف باعث افزایش سرعت شبکه می‌شود.

منبع : https://www.binance.com/en/blog/fiat/what-you-need-to-know-about-privacy-coins-421499824684903655