کلید شخصی و عمومی چیست و چه تفاوتی با هم دارند؟

کلید عمومی (Public Key)

همان طور که در مطالب مقدماتی فوق به این نکته اشاره شد، کلید شخصی و عمومی است که امکان ارسال و دریافت رمزارزها را برای کاربران دنیای کریپتوکارنسی فراهم آورده است و در این بین، نقش کلید عمومی در ارسال ارز دیجیتال از یک فرد به فرد دیگر ظاهر می‌گردد، کلید عمومی در واقع به یک کد رمزنگاری شده اطلاق می‌شود که با کلید شخصی (خصوصی) جفت می‌شود.

این کلید به صورت عمومی از سوی افراد دیگر نیز قابل مشاهده بوده و دیگران به راحتی قادر به مشاهده آدرس کلید عمومی شما هستند و می‌توانند به این آدرس ارز دیجیتال ارسال نمایند. به بیان ساده‌تر، کلید عمومی به منزله شماره حساب بانکی شما در دنیای کریپتوکارنسی محسوب می‌گردد و به همین علت کلیه افراد دنیای ارز دیجیتال قادر خواهند بود این کلید عمومی را در اختیار دیگران قرار دهند.

مطلب پیشنهادی : چگونه کلید خصوصی کیف پول ارز دیجیتال خود را پیدا کنیم؟

شاید با مطالعه مطالب فوق این سوال ذهن‌تان را به خود به مشغول سازد که نحوه رمزنگاری کلید عمومی به چه صورت انجام می‌گیرد؟ در پاسخ به این سوال باید بگوییم که رمزنگاری کلید عمومی که با نام اختصاری PKC از آن یاد می‌شود، روشی برای تائید اعتبار و همچنین درستی اطلاعات است و مهم‌ترین کاربرد آن را می‌توان در توانایی این شیوه در رمزگذاری و همچنین رمزگشایی پیام‌ها مشاهده کرد.

در رمزنگاری کلید عمومی از تکنیک‌های ویژه ریاضیات کمک گرفته شده است و آن را می‌توان یکی از اصلی‌ترین فناوری‌هایی دانست که نقش کلیدی ویژه‌ای را در گسترش جهان شمولی دنیای کریپتوکارنسی ایفا کرده است. وجود رمزارزها به وجود این

رمزنگاری کلید عمومی گره خورده و بدون وجود چنین شیوه رمزنگاری عملا وجود ارزهای دیجیتالی به یک فرض محال تبدیل می‌شد.

کلید شخصی (Private Key)

برای این که راحت‌تر بتوانید با ماهیت کلیدهای شخصی ارتباط برقرار کنید در ادامه تمثیل بالا که کلید عمومی را به شماره حساب بانکی تشبیه کردیم در این بخش از مقاله «آشنایی با کلید شخصی و عمومی» باید بگوییم که کلید شخصی به مشابه رمز کارت‌های اعتباری بانکی است و طبیعتا نبایستی آن را در اختیار هیچ فرد دیگری قرار دهید؛ چراکه اگر فردی از این کلید شخصی شما مطلع باشد به راحتی می‌تواند کلیه ارزهای دیجیتالی شما را در اختیار و سلطه خویش قرار دهد.

در دنیای رمزارزها، این کلید شخصی است که این امکان را برای شما فراهم می‌آورد تا مالکیت ارزهای رمزنگاری شده ارسال شده به حساب‌تان را در اختیار داشته باشید و در صورت تمایل آن‌ها را خرج کنید. کلیدهای شخصی را از لحاظ شکلی به چهار دسته تقسیم می‌شوند:

1. کد متشکل از 256 کاراکتر
2. کد 64 رقمی
3. کد RQ
4. رمز عبور

توصیه کارشناسان ما در مجموعه کیف پول من به شما این است که حتما کلید خصوصی و شخصی را به خاطر دلایل امنیتی، به صورت طولانی انتخاب کنید. شما می‌توانید با کلید شخصی خود یک کلید عمومی بسازید؛ اما این مسئله سبب نمی‌شود که فردی بتواند با استفاده از کلید عمومی مورد استفاده شما، کلید شخصی‌تان را حدس بزند و علت این امر را باید در طولانی بودن کلید شخصی جستجو کرد.

احتمالا به همین علت باشد که از رمزنگاری با کمک کلید عمومی، به عنوان **رمزنگاری غیرمتقارن** (Asymmetric Encryption) یاد می‌شود؛ چراکه در این شیوه رمزنگاری منحصرا مسیر استفاده از کلید شخصی به منظور تولید عمومی باز بوده و برعکس آن، یعنی استفاده از کلید عمومی برای تولید کلید شخصی محال و غیرممکن است.

ناگفته نماند که کلید شخصی هر فرد در کیف پول ارز دیجیتال قرار دارد و حال اگر ارزهای دیجیتالی خویش را در حساب کاربری خود در یک صرافی خرید و فروش ارز دیجیتال نگه‌داری می‌کنید، این مسئله به منزله آن است که مسئولیت کلید شخصی کیف پول خود را به این صرافی واگذار کرده‌اید.

به بیان ساده‌تر، در این حالت شما به صرافی مورد نظر خود اعتماد کرده‌اید تا از جانب شما، تراکنشات را انجام دهد. در صورتی که تمایلی به این که صرافی کنترل کلید شخصی شما را در اختیار داشته باشد، ندارید؛ باید ارزهای دیجیتالی خود را به کیف پول مستقل خویش منتقل نمایید.

آشنایی با رمزنگاری غیرمتقارن به زبان ساده

در **رمزنگاری غیرمتقارن** در واقع از **دو کلید مجزا** و در عین حال مرتبط به هم استفاده می‌شود که این دو کلید همان **کلید شخصی** و **عمومی** است.

برای درک راحت این مفهوم به این مثال توجه کنید: تصور کنید که شما رئیس یک نهاد جاسوسی هستید و باید سازوکاری را برای ماموران خویش ایجاد نمایید تا به صورت کاملا امن، اطلاعات ارسالی از سوی این افراد را دریافت کنید. در چنین شرایطی، مسلما شما نیاز به برقراری یک ارتباط دو طرفه نخواهید داشت؛ چراکه ماموران شما قبلا تمام آنچه را که باید می‌دانستند را در اختیار دارند.

مطلب پیشنهادی : رمزنگاری در ارز دیجیتال

بنابراین، قصد شما منحصرا از ایجاد چنین سازوکاری دریافت گزارشات تهیه شده به وسیله این ماموران خواهد بود. در رمزنگاری غیرمتقارن نیز دقیقا ما با چنین جریانی مواجه هستیم و این **شیوه رمزنگاری** این امکان را برای شما فراهم می‌آورد تا با کمک کلید شخصی، اطلاعات ارسال شده به وسیله ماموران خویش را دریافت و رمزگشایی نمایید.

تفاوت کلید شخصی و عمومی

احتمالا با مطالعه مطالب فوق تا حدودی مرزبندی میان دو **مفهوم کلید شخصی و عمومی** در ذهن‌تان شکل گرفته باشد و متوجه تفاوت و تمایز این دو مفهوم با یکدیگر شده باشید؛ اما جالب است بدانید که که این دو کلید هدف یکسانی را دنبال می‌کنند و آن هدف این است که با کمک آن‌ها این اطمینان در خاطر کاربران دنیای کریپتوکارنسی شکل می‌گیرد که واقعا یک معامله معین از جانب فردی که آن را امضا کرده است تائید شده و این معامله جعلی نیست!

با وجود چنین اشتراکی در هدف، این دو کلید از جهات مختلف با یکدیگر تفاوت‌هایی دارند که در ادامه به بررسی تفصیلی این تفاوت‌ها می‌پردازیم:

الگوریتم و مکانیسم متفاوت

گفته شد که در رمزگذاری ما به دو کلید جداگانه نیاز داریم، کلید شخصی منحصرا در اختیار مالک آن قرار دارد و این در حالی است که کلید عمومی را می‌توان در اختیار هر فردی قرار داد. در واقع افراد با کمک کلید عمومی ارزهای دیجیتالی را به شما ارسال می‌کنند و شما نیز با کمک کلید شخصی خویش به رمزگشایی اطلاعات و ارزهای دیجیتالی ارسال شده می‌پردازید.

عملکرد و کارایی

در مقایسه سرعت عملکرد کلید شخصی و عمومی باید گفت که کلید شخصی دارای عملکردی بسیار سریع‌تر از کلید عمومی است و علت این امر را می‌توان در این نکته جستجو کرد که در کلید شخصی ما با یک کلید سروکار داریم و این در حالی است که در کلید عمومی، دو کلید مورد نیاز است.

تفاوت در سطح دسترسی و حریم خصوصی

تفاوت دیگری که میان کلید شخصی و عمومی وجود دارد به لحاظ حریم خصوصی است؛ چراکه کلید شخصی حتما باید به صورت مخفی نگهداری شود و به غیر از صاحب کیف پول، در اختیار هیچ فرد دیگری قرار نگیرد. ناگفته نماند در صورتی که کلید خصوصی گم شود، عملا امکان بازگردانی آن وجود ندارد و پرونده رمزنگاری شده شما غیرقابل استفاده خواهد شد!

اصولا با توجه به این که حفظ و نگهداری این کلید در ظاهر کمی دشوار به نظر می‌رسد، بهتر است از یک دستگاه ذخیره‌سازی آفلاین برای این منظور کمک بگیرید. در طرف مقابل، کلید عمومی قرار دارد که از قابلیت در دسترس عموم قرار گرفتن برخوردار است.

کلید شخصی و عمومی؛ نگهبان امنیتی تراکنش‌های رمزارزی

همان طور که در مطالب بالا مشاهده کردید، کلید شخصی و عمومی در واقع همان فناوری است که این امکان را برای کاربران دنیای کریپتوکارنسی فراهم کرده است که به راحتی و به صورت کاملا امن به ارسال و دریافت بیت کوین رایگان و سایر ارزهای رمزنگاری شده بپردازند؛ اما جالب است بدانید که این دو کلید با وجود دارا بودن هدف یکسان، دارای عملکردهای متفاوتی هستند و به بیان بهتر مکمل همدیگر محسوب می‌شوند.

به این مثال توجه کنید؛ اگر فردی قصد دارد تعدادی بیت کوین به شما ارسال کند در قدم اول باید با استفاده از کلید عمومی آن را رمزگذاری کرده و سپس ارسال نماید. در طرف مقابل شما برای آن که بتوانید به این بیت کوین‌های دریافتی دسترسی داشته باشید، باید از کلید خصوصی برای رمزگشایی کمک بگیرید.

ناگفته نماند که اگر در ارتباط با کلید شخصی و عمومی و همچنین تفاوت آن‌ها سوالی دارید که در این مقاله از کیف پول من به آن اشاره‌ای نشده است، می‌توانید سوال خود را در بخش نظرات مطرح کنید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.