



امضای اشنور یا امضای دیجیتال چیست؟

اثبات مالکیت بر یک چیز همواره نیازمند مدرکی محکم خواهد بود! این را گفتیم تا به این نکته برسیم که، بسیاری از افراد گمان می‌کنند نمی‌توان مالکیت افراد بر ارزشهای دیجیتال را ثابت کرد و به همین دلیل ارزشهای دیجیتال را دارایی واقعی تلقی نمی‌کنند. **امضای اشنور یا همان امضای دیجیتال** ضامن امنیت در دنیای کریپتوکارنسی بوده، اصالت این تراکنش‌ها را مشخص می‌کند و با استفاده از این امضای رمزنگاری شده، مالکیت افراد بر روی دارایی ارز دیجیتال به اثبات می‌رسد. برای آشنایی بیشتر با ویژگی‌های امضای اشنور و نحوه عملکرد آن در ادامه این مقاله از **بلاگ کیف پول من** ما را همراهی کنید تا همه چیز را در مورد این امضای دیجیتال و دلایل اهمیت آن مورد بررسی قرار دهیم.

نحوه عملکرد امضای اشنور (Schnorr signature)

امضای اشنور برای اثبات مالکیت دیجیتال طراحی شده و ضامن اصالت و یکپارچگی تراکنش محسوب می‌شود. این امضاها ضمانت می‌کنند که تراکنش به مقصد مورد نظر ارسال خواهد شد و در طول مسیر دچار دستکاری نخواهد شد. **امضای اشنور** یکی از الگوریتم‌های مهم در ریاضی شمرده می‌شود که در دهه 1990 توسط یک ریاضی‌دان آلمانی با نام کلاوس اشنور (Claus Schnorr) ایجاد شده و در سال 2021 وارد ساختار بیت کوین شد.

جالب است بدانید اشنور این امضا را راه‌حلی برای افزایش امنیت در پیام‌های ارسالی رمزگذاری شده ایجاد کرده بود تا کشورهای جاسوسی قادر به رمزگشایی و دستکاری پیام ارسالی نباشند.

دارا بودن امضای اشنور به این معناست که تراکنش به وسیله یک فرد مشخص فرستاده شده و پیام ارسالی دقیقا همان پیام دریافتی است. همان طور که امضای فیزیکی تاییدکننده هویت فرد محسوب می‌شود، در دنیای دیجیتال هم هر فرد کلیدی منحصر به فرد برای تایید هویت خود دارد.

شاید دوست داشته باشید در مورد کارمزد انتقال ارزها در شبکه های مختلف بدانید

آیا تاکنون برای خود کیف پول ارز دیجیتال ایجاد کرده‌اید؟ اگر کیف پول ارز دیجیتال ایجاد کرده باشید، حتما با کلماتی با عنوان Private key مواجه شده‌اید. این کلمات که نرم افزار پیشنهاد می‌کند حتما آن را در جایی مطمئن یادداشت کرده و هرگز فراموش نکنید، امضای شخصی شما در بلاکچین است. به یاد داشته باشید که نگهداری از این امضا اهمیت بسیار زیادی دارد و هر فرد دیگری با در دست داشتن این امضا می‌تواند مالک تمام دارایی شما باشد.

یک کوین در دنیای کریپتوکارنسی، رشته‌ای از امضاها در دیجیتال است. افراد دارای کوین برای انتقال ارز به کیف پول شخصی دیگر، لازم است یک کد هش شده از امضای دیجیتال خود و کلید عمومی دریافت‌کننده کوین را ثبت کنند؛ بنابراین هر فرد برای انتقال دارایی از امضای اشنور و کلید عمومی استفاده خواهد کرد.

با ایجاد یک کیف پول اشتراکی در هنگام انتقال ارز لازم است تمام یا اکثریت اعضا تراکنش را امضا کنند. هر امضا همچون یک تراکنش مجزا بوده و نیازمند زمانی برای تایید تراکنش و کارمزد خواهد بود؛ از همین رو ایجاد یک تراکنش چند امضایی معمولا گران تمام می‌شود.

اشنور با تفکیک امضاها از تراکنش اصلی و با کاهش حجم تراکنش، منجر به جمع شدن تمام امضاها در یک امضا می‌شود که به آن اجماع کلیدها (Key aggregation) گفته می‌شود. با این کار در هنگام واریز بیت کوین از طرف چند کاربر به یک آدرس مشخص، نیازی به پرداخت کارمزد تراکنش برای هر امضا نخواهد بود. لازم به ذکر است که امضای اشنور منجر به افزایش امنیت تراکنش‌ها و مهار حملات سایبری بلاکچین می‌شود.



سیستم بیت کوین برای اثبات مالکیت کاربران بر مقدار بیت کوین منتقل شده، از امضای دیجیتالی به نام ECDSA استفاده می‌کنند. گفته می‌شود امضای اشنور می‌تواند نمونه پیشرفته‌تر ECDSA شمرده شود؛ چرا که دقیقاً همان کار را در حجم فایل کمتر و حریم خصوصی قوی‌تر انجام می‌دهد. البته امضای ECDSA و امضای اشنور از نظر چکش‌خواری یا همان شکل‌پذیری نیز با هم متفاوت هستند.

مطلب پیشنهادی: بررسی کارمزدها انتقال بیتکوین مهم‌ترین ویژگی‌های امضای اشنور

خلاصه کردن کلیدهای مختلف در یک کد واحد، افزایش امنیت سطح تراکنش‌ها، مقاومت در برابر حمله چکش‌خواری، افزایش میزان ناشناخته بودن تراکنش‌ها و ذخیره امضاها در یک کد هش شده مبهم و غیرقابل ردیابی از جمله مهم‌ترین ویژگی‌های امضای اشنور شمرده می‌شود. در برخی از مواقع تعدادی از افراد توافق می‌کنند که اگر تراکنشی را اکثر مالکان یک کیف پول امضا کنند، به معنای تایید تراکنش از جانب همه باشد؛ با استفاده از امضای اشنور تشخیص این که چه کسی تراکنش را امضا کرده و چه کسی آن را امضا نکرده ممکن نخواهد بود.



امضای اشنور همچون بسیاری از مفاهیم دیگر، مزایا و معیبهی دارد. در ادامه به برخی از مزایای امضای اشنور اشاره خواهیم کرد:

- کاهش 25 درصدی نیاز به فضای ذخیره‌سازی در تراکنش‌های چند امضایی
 - کاهش کارمزد و زمان تایید تراکنش در تراکنش‌های چند امضایی
 - آماده‌سازی بلاکچین ارز بیت کوین برای پذیرش **قراردادهای هوشمند**
 - مقاومت در برابر حمله چکش‌خواری
 - توانایی حفظ شبکه از حمله هکرها
 - افزایش حریم خصوصی با تبدیل تراکنش‌های چند امضایی به تراکنش‌های تک امضایی
 - افزایش مقیاس‌پذیری شبکه
- در کنار تمام مزایایی که برای امضای اشنور نام برده شد، این امضا دارای معایبی نیز است که در ادامه به آن‌ها اشاره خواهیم کرد:
- امکان دستیابی هکر به یک کلید عمومی معتبر و کنترل یک تراکنش چند امضایی
 - پیچیدگی فرایند انتقال ارز به دلیل لزوم نشان دادن اعتبار کلید عمومی توسط هر شرکت کننده در اجرای امضای اشنور

دلایل اهمیت امضای اشنور

افزایش مقیاس‌پذیری و تامین امنیت، از جمله مهم‌ترین مشکلات ارزش‌های دیجیتال شمرده می‌شوند. امضاهای دیجیتال با طراحی هوشمندانه قادر به حفاظت بلاکچین در برابر حملات هکرها و ساده‌تر کردن کار برای توسعه‌دهندگان بلاکچین هستند. جالب است بدانید در آپدیت تپروت برای آماده‌کردن بیت کوین برای آپدیت‌های بعدی، **امضای اشنور (Schnorr signature)** یکی از اجزای مهم و اساسی این آپدیت به شمار می‌رفت.

بهبود آینده بیت کوین در دستان امضای اشنور!

همان‌طور که گفته شد امضای اشنور یکی از مهم‌ترین امضاهای دیجیتال است که بر مبنای الگوریتم اشنور راه‌اندازی شده است. این امضا منجر به افزایش سرعت تراکنش، کاهش حجم تراکنش، ادغام امضاهای چندگانه و نیز افزایش مقیاس‌پذیری **شبکه بیت کوین** شده و از اهمیت بسیار زیادی برخوردار است.

در این مقاله به بررسی امضای اشنور، نحوه عملکرد، مزایا، معایب و دلایل اهمیت این امضای دیجیتال پرداختیم تا شما را با چرایی و چیستی این امضا بیشتر آشنا کنیم. برای خرید انواع ارزش‌های دیجیتال و یا درخواست مشاوره و راهنمایی در حوزه ارزش‌های دیجیتال، از طریق تماس با ما، با کارشناسان متخصص ما در کیف پول من در ارتباط باشید.