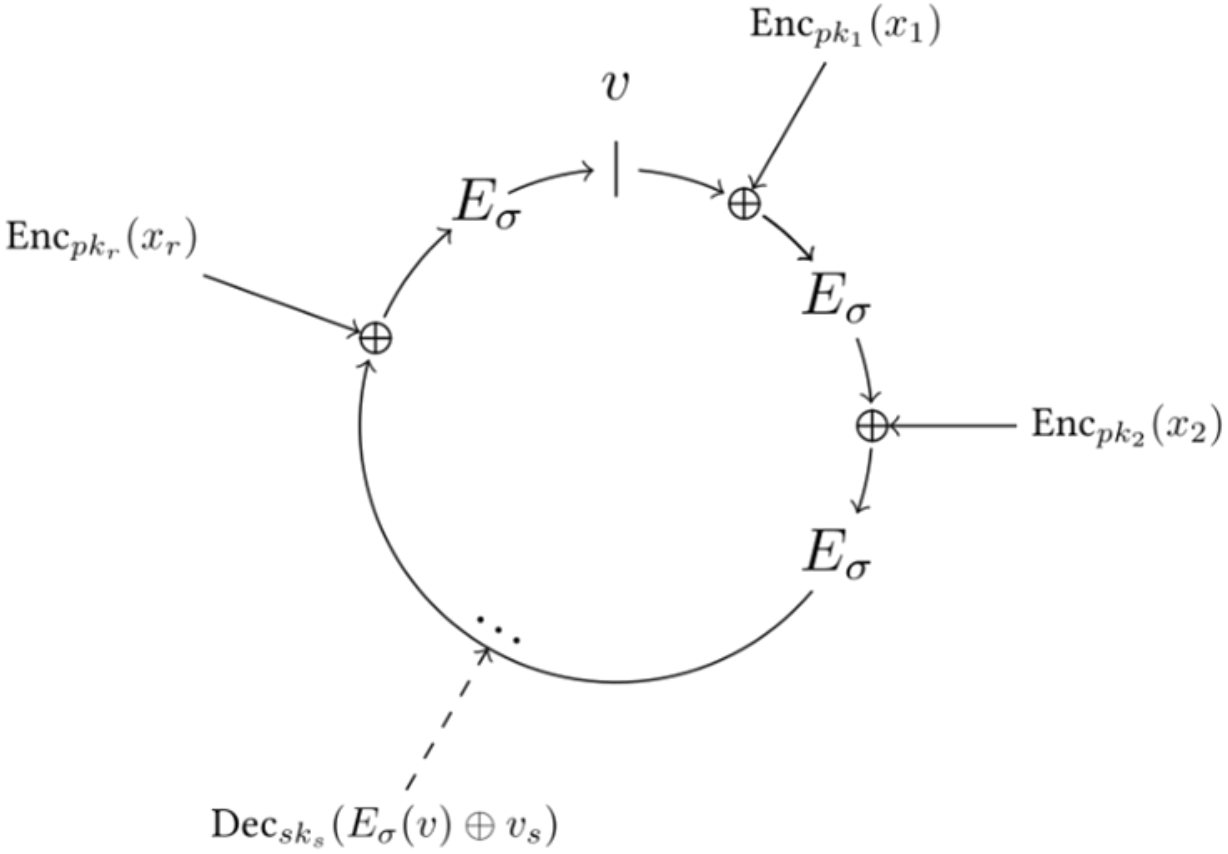
امضای حلقوی (Ring Signature) چیست؟

یکی از موضوعاتی که همواره ذهن کاربران را در استفاده از امکانات شبکه‌های بلاک‌چینی به خود مشغول می‌سازد، به موضوع اصالت و امنیت تراکنش‌های انجام یافته در شبکه مربوط است. با گذشت زمان و نیاز ویژه دنیای کریپتوکارنسی در **مسئله حفظ حریم خصوصی** کاربران سبب شده تا پیشرفت‌های قابل توجهی در حوزه ناشناس ماندن کاربران در چنین دنیایی رخ دهد. یکی از راه‌حل‌های مورد استفاده شبکه‌های بلاکچینی، امضای حلقوی (Ring Signature) نام دارد که در آن گروهی از شرکت‌کنندگان در شبکه بلاک‌چینی دور هم جمع شده و یک نفر از آن‌ها تراکنش انجام یافته را امضا می‌نماید. به بیان بهتر، در امضای حلقوی، اطلاعات تراکنش از سوی یک الگوریتم رمزنگاری به عنوان پیام اصلی محاسبه شده و سپس با کلید خصوصی حلقه‌ای امضا و تائید می‌گردد. احتمالا مطالعه چنین جملاتی کمی موجب سردرگمی شما در شناخت امضای حلقوی مورد استفاده در دنیای کریپتوکارنسی شده است؛ با ما تا انتهای این مطلب از بلاگ کیف پول من همراه باشید تا با این مفهوم به بیان کاملاً ساده و جامع آشنا شوید.

نگاهی به تاریخچه امضای حلقوی

پیش از ورود به بحث چیستی امضای حلقوی در دنیای کریپتوکارنسی لازم است کمی به عقب برگشته و مروری بر تاریخچه این تکنیک امنیتی داشته باشیم تا با دستیابی به یک دید روشن راحت‌تر بتوانید مطالب بعدی را مطالعه نمائید.
امضای حلقوی صرفاً به دنیای کریپتو اختصاص ندارد و یک امضای دیجیتالی است که اولین بار در سال 2001 و از سوی افرادی همچون آدی شامیر، یائل ومن و ران ریوست ابداع و سپس در Asiacrypt معرفی شد. همان طور که در بحث بررسی ماهیت امضای حلقوی روشن خواهد شد، این امضا بیش از هر چیزی به یک امضای گروهی شباهت دارد؛ امضایی که راهی برای شناسایی فرد امضا کننده در این گروه وجود ندارد!
به عنوان مثال تصور کنید از یک وزارتخانه اطلاعاتی محرمانه به بیرون درز کرده است و وزیر نیز با تیم امنیت تماسی داشته و می‌گوید مطمئن است که می‌داند یکی از کارکنان بخش نگهداری اسناد محرمانه این اطلاعات را فاش کرده، ولی دقیقاً نمی‌داند که کار کدام یک از آن‌هاست! این موضوع به نوعی در امضای حلقوی نیز وجود دارد و به همین علت گاهاً از

آن تحت عنوان امضای ناشناس یاد می‌شود؛ چراکه مشخص نمودن این که کدام یک از کلیدهای اعضای موجود در گروه برای تولید امضا استفاده شده است، امری غیرممکن است.
در روزهای اولیه ابداع امضای حلقوی، این تکنیک امنیتی غالباً به منظور جلوگیری از افشای اطلاعات محرمانه و عمدتاً از سوی مقامات بلندپایه دولتی مورد استفاده قرار می‌گرفت؛ اما با گذشت زمان و آگاهی عموم توسعه‌دهندگان از میزان کارایی فناوری امضای حلقوی، این امضا نخستین بار از سوی تیم توسعه دهنده بیت کوین کر (Bitcoin Core) و سپس از سوی آزمایشگاه تحقیقاتی مونرو استفاده و رسماً وارد دنیای کریپتوکارنسی گردید.



مفهوم امضای حلقوی به زبان ساده

در یک تعریف ساده از امضای حلقوی می‌توان آن را نوعی امضای دیجیتالی رمزنگاری شده معرفی کرد که از جهات مختلفی به امضای گروهی شباهت دارد؛ اما تفاوت‌های ظریف موجود در میان آن‌ها سبب شده تا به عنوان یک نوع مستقل مورد بحث و بررسی قرار بگیرد. توجه داشته باشید که در امضای حلقوی صرفاً از مفهوم امضای گروهی استفاده شده تا حریم خصوصی کاربران بهتر رعایت گردد و همان طور که قبلاً اشاره شد در عمل امکان شناسایی فرد امضا کننده وجود ندارد. به بیان بهتر، کاربرد امضای حلقوی به این صورت است که با پوشاندن سمت ورودی تراکنش از فرستنده محافظت کرده و به نحوی عمل می‌کند تا به لحاظ محاسباتی امکان تعیین دقیق فرد امضا کنند وجود نداشته باشد.
با چنین توضیحی روشن می‌شود که آنچه با آن در امضای حلقوی مواجه هستیم بسیار با آنچه که در سایر امضاهای دیجیتالی نظیر امضای اشنور (Schnorr Signature) وجود دارد، تفاوت داشته و بسیار پیچیده‌تر از آن‌هاست. ناگفته نماند که امضای حلقوی با استفاده از ترکیب کلیدهای حساب کاربری شخص فرستنده و کلید عمومی موجود در شبکه بلاکچین تولید می‌گردد و با توجه به این که در عمل امکان دسترسی به این که کدام یک از کلیدها در تولید امضای حلقوی به کار رفته وجود ندارد، هویت واقعی فرد فرستنده به خوبی مورد محافظت قرار گرفته و مخفی باقی می‌ماند.

بررسی مثال عملی استفاده از امضای حلقوی

برای درک بهتر مفهوم امضای حلقوی در ادامه به بررسی یک مثال عملی از فرآیند استفاده از امضای حلقوی در مونرو (Monero) می‌پردازیم:
فرض کنید بنابر یک توافقی که با دوست خود داشته‌اید قرار است که 15 مونرو به کیف پول وی واریز کنید. برای انجام این تراکنش باید به سراغ کیف پول مونرو خود رفته و تراکنش را با امضای دیجیتالی خود نهایی می‌کنید؛ حال در فرآیند امضای حلقوی، در کنار امضای اصلی چندین امضای خروجی تراکنش دیگر نیز که غالبا به گذشته مربوط می‌شوند به طور کاملاً تصادفی از شبکه بلاکچین انتخاب و مسئولیت عملیات پوششی فریب در تراکنش را برعهده می‌گیرند.
توجه داشته باشید که کلیه اعضای حلقه ایجاد شده را در اصل امضا کنندگانی شکل می‌دهند که از دید شبکه بلاکچینی قادر به انجام چنین معامله و تراکنشی هستند و دقیقاً به همین علت است که امکان تشخیص امضا کننده واقعی تراکنش از سوی شخص ثالث وجود ندارد.

انتقاد از امضای حلقوی و موضوع هزینه مضاعف!

مشکلی که ممکن است با داشتن تراکنش‌های ناشناس در در شبکه‌های ارز دیجیتال متمرکز بر حریم خصوصی همچون مونرو متوجه آن شوید به بحث دشوار بودن جلوگیری از هزینه‌های مضاعف مربوط می‌شود و در صورتی که برای جلوگیری از چنین مشکلی تضمینی وجود نداشته باشد، شبکه مورد نظر به یک شبکه بلاک‌چینی بلااستفاده بدل خواهد شد.
چنین موضوعی با استفاده از تصاویر کلیدی در ارتباط با طرح امضای حلقوی به طور هوشمندانه‌ای حل شده است.
منظور از کلید تصویری نوعی کلید رمزنگاری بوده که از خروجی خرج شده مشتق و بخشی از هر تراکنش امضای حلقوی را شکل می‌دهد. لازم به ذکر است که صرفا یک کلید تصویری منحصربه‌فرد برای هر خروجی در بلاکچین وجود دارد که لیستی از کلیه تصاویر کلیدی استفاده شده در بلاکچین در آن نگهداری می‌شود. هر امضای حلقوی از یک تصویر تکراری بهره می‌برد که چنین امری انتقاد موجود در زمینه هزینه کردن مضاعف را رد می‌نماید.

نحوه ایجاد امضای حلقوی در شبکه بلاکچین

برای ایجاد یک امضای حلقوی در شبکه بلاکچین با مراحل زیر مواجه خواهیم بود:

مرحله اول	انتخاب الگوریتم رمزنگاری	انتخاب الگوریتم قدرتمند برای ایجاد امضای حلقوی نظیر RSA یا ECC
مرحله دوم	تولید کلید	تولید یک جفت کلید عمومی (برای تایید امضا) و خصوصی (برای ایجاد امضا)
مرحله سوم	محاسبه امضا	محاسبه با استفاده از کلید خصوصی و اطلاعات تراکنش
مرحله چهارم	ممانعت از تقلب	ارسال اطلاعات تراکنش (همراه با امضا) به شبکه برای عبور از سیستم امنیتی
مرحله پنجم	تایید اصالت	استفاده از کلید عمومی برای تایید اصالت امضای حلقوی و صحت تراکنش

نقاط قوت و ضعف امضای حلقوی

برای شناخت بهتر کاربردهای امضای حلقوی باید به سراغ بررسی مزایا و معایب امضای حلقوی برویم که به شرح زیر هستند:

مزایای استفاده از امضای حلقوی

- **ارتقا اعتبار:** استفاده از امضای حلقوی در ارتقا میزان اعتبار اشخاص حقیقی و حقوقی نقش داشته و اطلاعات تراکنش همراه با چنین امضایی نشانه‌ای از اصالت و اعتبار است.
- **افزایش امنیت تراکنش‌ها:** امضای حلقوی مانع دستکاری و بروز تقلب در اطلاعات تراکنش‌ها می‌گردد و نشانگر این واقعیت است که تراکنش‌ها از سوی فردی مجاز انجام یافته است.
- **مقابله با حملات میان منبعی:** امضای حلقوی موجب می‌شود تا حملات میان منبعی (Man-in-the-Middle) که در آن یک عامل مخرب میان فرستنده و گیرنده قرار می‌گیرد، مشکل‌ساز نگردد و از ریشه این مشکل را برطرف می‌سازد.

معایب استفاده از امضای حلقوی

- **مقیاس‌پذیری:** با افزایش تعداد تراکنش‌ها و کاربران فعال در شبکه مسئله مقیاس‌پذیری در امضای حلقوی پیش می‌آید که بهبود وضعیت سیستم را به یک امر ضروری تبدیل می‌کند.
- **حملات امضای تکراری:** در حالتی که یک امضای حلقوی بازنشر گردد امکان ایجاد حملات امضای تکراری (Replay Attacks) امری محتمل بوده که امنیت تراکنش‌ها را تهدید می‌کند (البته چنین امری صرفا چالش است و از این نظر در میان معایب و نقاط ضعف امضای حلقوی جای گرفته است).

امضای حلقوی؛ تکنیکی امنیتی برای ارتقا حریم خصوصی در تراکنش‌ها

همان طور که در مطالب فوق مشاهده کردید با توجه به ضرورت آشنایی با تکنیک‌های امنیتی موجود در شبکه‌های بلاکچینی و تاثیر آن‌ها بر میزان خرید ارز دیجیتال، این مقاله از بلاگ کیف پول من به بررسی جامع مفهوم امضای حلقوی اختصاص پیدا کرده که در آن با گروهی از کلیدها مواجه هستیم که هر یک از آن‌ها به تنهایی واجد شرایط برای انجام تراکنش مورد نظر بوده و همین مسئله سبب می‌شود تا اشخاص ثالث امکان شناسایی امضا کننده حقیقی تراکنش را نداشته باشند که چنین امری موجب محافظت هرچه بهتر شبکه‌های بلاکچینی از حریم خصوصی کاربران می‌گردد. حال که با چیستی امضای حلقوی در دنیای کریپتوکارنسی بهتر آشنا شدید، نظر شما درباره آن چیست؟ نظرات خود را برای ما بنویسید.