کریپتوگرافی (Cryptography) چیست؟

انسان‌ها همواره به دنبال روشی هستند تا از حریم خصوصی خود محافظت نمایند. احتمالا در ایام کودکی شما هم با دوستان خود به دنبال اختراع یک زبان جدید رفته‌اید و از این طریق می‌خواستید دیگران متوجه صحبت‌های شما با همدیگر نشوند. دنیایی را تصور کنید که پیام‌های میان شما و دوستانتان پیش از این که به دستتان برسند توسط افراد دیگری خوانده شوند. چه احساسی به شما دست می‌دهد؟ کریپتوگرافی (Cryptography) و رمزنگاری همان دانشی است که به افراد کمک می‌کند اطلاعات و داده‌های خود را به صورت ایمن ذخیره و منتقل نمایند.

با گسترش استفاده از فناوری‌های رمزنگاری، ارزهای رمزپایه از دل این فناوری ظاهر شده و انقلابی بزرگ در حوزه امور مالی به پا کرده‌اند. حال ما در این مقاله از بلاگ کیف پول من قصد داریم به این سوال که کریپتوگرافی چیست و چه معنایی در دنیای رمزارزها دارد؟ پاسخ دهیم. اگر شما هم در این زمینه کنجکاو هستید و می‌خواهید اطلاعات جامع‌تری در ارتباط با امنیت رمزارزها پیدا کنید، تا انتهای این مطلب با ما همراه باشد.

نگاهی بر تاریخچه رمزنگاری (Cryptography)

رمزنگاری دانشی نیست که به تازگی اختراع شده باشد و هزاران سال در شکل و شیوه‌های مختلف در جوامع بشری مورد استفاده قرار می‌گرفته است. اولین نمونه ثبت شده از کریپتوگرافی در جهان به کتیبه حکاکی شده در زمان **خنوم هوتپ (Khnumhotep)** دوم مصر برمی‌گردد که 1900 سال پیش از میلاد مسیح حکومت می‌کرد؛ هرچند که در حکاکی این کتیبه از رمزنگاری به معنا و مفهوم امروزی استفاده نشده بود، ولی متن آن تغییراتی با زبان عامیانه مورد استفاده مردم آن زمان داشت. استفاده از دانش کریپتوگرافی در طول 1800 سال پس از نگارش این کتیبه تغییرات چشمگیری داشت؛ به طوری که ژولیوس سزار (Julius Caesar) حدودا 100 سال پیش از میلاد مسیح از نوعی شیوه رمزگذاری ویژه به منظور انتقال محرمانه پیام‌های خود بهره می‌برد و روش کار وی به این صورت بود که هر کاراکتر در متن پیام را 3 واحد از حروف الفبا جابه‌جا می‌کرد تا هر فردی قادر به فهم منظور واقعی سزار نباشد.
ریشه کلمه کریپتوگرافی نیز به زبان یونانی برمی‌گردد که از ترکیب دو لغت «kryptós» به معنای راز و امری که پنهان است و «graphein» به معنای نوشتن به دست آمده است. روند تاریخی کریپتوگرافی در سیر تحولاتی که داشت، در قرن شانزدهم میلادی به وسیله فردی به نام Battista Bellaso Giovan دستخوش تحولاتی شد. وی شیوه جدیدی را در حوزه کریپتوگرافی به نام ویژنر (Vigenere cipher) طراحی کرد که از آن تحت عنوان اولین شیوه کریپتوگرافی و رمزنگاری با کلید یاد می‌شود. در این نوع خاص از کریپتوگرافی، از کلیدی خاص برای رمزگشایی پیام‌ها و داده‌ها استفاده می‌شد. در این روش متن مورد نظر با استفاده از یک کلمه به عنوان کلید و یک جدول که دارای 26 ردیف حروف الفباست، نوشته و رمزنگاری شده و در نهایت به گیرنده تحویل داده می‌شود.
ادامه تحولات حوزه کریپتوگرافی به سه قرن بعدتر یعنی به قرن نوزدهم مربوط می‌شود که برق اختراع شده و هبرن (Hebern) با استفاده از یک ابزار به نام الکترومکانیکی نسبت به رمزگذاری پیام‌ها و داده‌ها اقدام می‌کرد. ماشین یاد شده از روتر به منظور مخفی نمودن پیام‌ها بهره می‌گرفت و با هر بار فشردن کلید، رمزگذاری جدیدی در آن خلق می‌شد. آلمانی‌ها در طول جنگ‌های جهانی اول و دوم، استفاده‌های بسیار زیادی از این ماشین کردند که در نهایت رمزهای تولید شده به وسیله این ماشین از سوی لهستانی‌ها شکسته شد؛ اما چنین مسئله‌ای روند حرکتی کریپتوگرافی را متوقف نکرده و با ورود کامپیوترها فرآیند رمزنگاری و الگوریتم‌های کریپتوگرافی پیچیده‌تر از گذشته شده‌اند.

مطلب پیشنهادی: بررسی الگوریتم رمزنگاری در دنیای کریپتو

منظور از کریپتوگرافی چیست؟

احتمالا با مطالعه تاریخچه شکل‌گیری و استفاده از کریپتوگرافی یک ذهنیت کلی نسبت به دانش رمزنگاری و کریپتوگرافی در ذهنتان شکل گرفته است؛ اما در یک تعریف ساده از کریپتوگرافی می‌توان چنین گفت که منظور از آن روشی است که در انتقال ایمن و مطمئن اطلاعات و پیام‌ها مورد استفاده قرار می‌گیرد و متن آن به گونه‌ای تغییر پیدا می‌کند که صرفا فرستنده و گیرنده آن قادرند اطلاعات موجود در پیام را مطالعه نمایند. در یک کلام منظور از کریپتوگرافی، علم پنهان کردن داده‌ها و اطلاعات بوده و بستر امن ساخته شده برای انتقال داده‌ها در کریپتوگرافی از 4 عنصر مهم تشکیل یافته‌اند که این عناصر به شرح زیر هستند:

- **احراز هویت (Authentication):** با توجه به اهمیت اصالت هویت فرستند و گیرنده در طول یک جریان رمزنگاری، لازم است احراز هویت به شکلی صحیح انجام گیرد.
- **یکپارچگی داده‌ها (Data Integrity):** عدم دستکاری و تحریف داده‌ها و اطلاعات در طول فرآیند ارسال و دریافت، یکپارچگی داده‌ها را می‌طلبد و این یکپارچگی است که ثابت می‌کند این پیام‌ها دستکاری نشده‌اند.
- **محرمانه بودن (Confidentiality):** بیایید مجددا نگاهی به اسم رمزنگاری داشته باشیم. چه زمانی از واژه «رمز» استفاده می‌کنید؟ طبیعتا هنگامی به سراغ کریپتوگرافی می‌رویم که تمایلی به این مسئله که پیام‌ها و اطلاعات ما به دست افراد غیرمجاز افتد، نداریم.

- **عدم انکار (Non Repudiation):** منظور از این عنصر این است که فرستنده پیام قادر نخواهد بود اطلاعات ارسال شده را انکار یا تکذیب نماید.

امروزه در علوم کامپیوتر، کریپتوگرافی از طریق الگوریتم‌هایی که با کمک ضوابط و قواعد فیزیک، ریاضی و مهندسی طراحی شده‌اند، صورت می‌گیرد؛ الگوریتم‌هایی که پیام‌های عادی را به گونه‌ای رمزنگاری می‌کنند تا امکان رمزگشایی آن‌ها به راحتی امکان‌پذیر نباشد.

مطلب پیشنهادی: بررسی الگوریتم کریپتونایت

الگوریتم های کریپتوگرافی

با نگاهی کلی به شیوه کریپتوگرافی از زمان اختراع آن تا به امروز، متوجه پیشرفته‌تر شدن نحوه تامین امنیت پیام‌ها و داده‌ها خواهیم شد که این محرمانگی اطلاعات بیش از هر چیزی به الگوریتم‌های کریپتوگرافی وابسته هستند. در واقع سیستم‌های رمزنگاری از سه الگوریتم رمزگذاری متقارن، نامتقارن و توابع هش به منظور رمزگذاری و رمزگشایی پیام‌ها در ارتباط میان سیستم‌ها، دستگاه‌ها و برنامه‌های رایانه‌ای کمک می‌گیرند که توضیح تفصیلی هر یک از این الگوریتم‌های کریپتوگرافی به شرح زیر است:

الگوریتم رمزگذاری متقارن (Symmetric)

در رمزنگاری متقارن کلیه تمرکزها بر روی یک کلید است و فرستنده پیام و گیرنده آن، یک کلید عمومی را با همدیگر به اشتراک می‌گذارند تا از این کلید هم برای رمزگذاری و هم رمزگشایی استفاده شود. از معروف‌ترین الگوریتم‌های رمزنگاری متقارن می‌توان به مواردی همچون DES، DES3 و AES اشاره کرد. حفظ امنیت این کلید عمومی بسیار مهم است و در صورتی که این کلید سهوا در دسترس شخص ثالثی قرار بگیرد، این فرد به راحتی قادر خواهد بود کلیه پیام‌های رد و بدل شده میان طرفین را رمزگشایی نماید.

الگوریتم رمزگذاری نامتقارن (Asymmetric)

رمزنگاری نامتقارن که برخی از صاحب‌نظران حوزه کریپتوگرافی از آن تحت عنوان رمزگذاری کلید عمومی نیز یاد می‌کنند، در اصل از دو کلید به نام‌های **کلید خصوصی (Private Key)** و **کلید عمومی (Public Key)** شکل گرفته و این دو کلید یاد شده کاملا به همدیگر متصل بوده و به صورت جفت در دسترس هستند. نحوه کار در رمزنگاری نامتقارن به این صورت است که داده‌ها در مبدا که برای ارسال آماده می‌شوند، با استفاده از کلید عمومی رمزگذاری شده و در مقصد با

استفاده از کلید خصوصی رمزگشایی می‌گردند. از این نوع خاص رمزنگاری نامتقارن در امضای الکترونیک، کیف پول‌های رمزارزی، کارت‌های هوشمند و مواردی از این دست استفاده می‌شود. به نظر می‌رسد در میان الگوریتم‌های موجود رمزنگاری، رمزگذاری نامتقارن امنیت چشمگیری را برای انتقال داده‌ها فراهم می‌نماید؛ چراکه در این شیوه خاص از کریپتوگرافی، کلیدها منطبق با توابع پیچیده ریاضی به هم متصل شده‌اند. در این شیوه، کلیه افرادی که کلید عمومی را در اختیار دارند، می‌توانند پیام‌های رمزگذاری شده ارسال نمایند؛ اما کلیه این پیام‌ها صرفا از سوی فردی رمزگشایی خواهد شد که دارای کلید خصوصی است. از مهم‌ترین الگوریتم‌های رمزنگاری نامتقارن می‌توان به مواردی همچون ELGamal، RSA، DSA، ECC و Diffie–Hellman اشاره کرد.

مطلب پیشنهادی: بررسی کلید خصوصی و عمومی

توابع هش (Hash)

در الگوریم کریپتوگرافی توابع هش، هیچ خبری از کلید وجود ندارد! بلکه متن ساده به یک رشته کاراکتر از حروف و عدد که دارای طول ثابتی است، تبدیل می‌گردد. عدم وجود کلید در این الگوریتم و شیوه کریپتوگرافی سبب شده تا در آن شاهد میزان امنیتی باشیم که کمتر در سایر الگوریتم‌های رمزنگاری دیده شده است؛ چراکه عملا امکان بازیابی و رمزگشایی آن نزدیک به صفر است! جالب است بدانید که این رشته کاراکتر از اعداد و حروف به صورت تصادفی انتخاب نشده و در تولید آن‌ها از روابط و مسائل ریاضی خاصی کمک گرفته می‌شود.
این سطح از امنیت سبب شده تا توابع هش، کاربرد فراوانی در شبکه‌های بلاک چین داشته باشند و همزمان با تولید هر بلاک جدید، اطلاعات مندرج در آن هش شده و به این ترتیب امکان دستکاری اطلاعات از کلیه کاربران سلب می‌گردد. از محبوب‌ترین توابع هش مورد استفاده در حوزه ارزهای رمزپایه می‌توان به مواردی همچون SHA–256، Argon2، SHA–512، SCRYPT و BCRYPT اشاره کرد.
به طور کلی توابع هش دارای ویژگی‌های زیر هستند:

- **تفکیک‌پذیری:** در توابع هش هر یک از خروجی‌ها متعلق به یک ورودی بوده و تحت هیچ شرایطی امکان ندارد که خروجی یکسانی برای دو ورودی متفاوت در نظر گرفته شود.
- **برگشت‌ناپذیری:** این موضوع که با دسترسی به هش خروجی امکان دسترسی به ورودی وجود خواهد داشت، امکان‌پذیر نبوده و به همین علت به توابع هش برگشت‌ناپذیر گفته می‌شود.
- **قطعیت:** خروجی برای یک ورودی همواره یکسان است و امکان ندارد که شما یک ورودی یکسان را در اختیار تابع هش قرار دهید و خروجی‌های متفاوتی از آن دریافت کنید.

ارتباط کریپتوگرافی با کریپتوکارنسی

هنگامی که صحبت از دارایی‌های دیجیتالی به میان می‌آید، اولین مسئله به امنیت آن مربوط می‌شود. ساتوشی ناکاموتو، خالق بیت کوین، هنگام طراحی شبکه بلاک چین بیت کوین کاملا بر این نکته اشراف داشته است. طبیعتا با توجه به این واقعیت که ارزهای دیجیتالی دارای ماهیت غیرمتمرکز هستند و هیچ نهاد مرکزی و متمرکزی بر آن‌ها نظارت ندارد، سبب شده این دارایی‌های دیجیتالی ارزشمند بیشتر در معرض خطرات حملات سایبری قرار بگیرند و این مسئله با استفاده از دانش کریپتوگرافی تا حد قابل قبولی برطرف شده و به همین علت اعتماد مردم نسبت به روند فعالیت و عملکرد شبکه‌های بلاک چینی بیش از پیش جلب شده است.

نحوه کار کریپتوگرافی در مارکت ارز دیجیتال

ارزهای رمزپایه برای تامین امنیت به سراغ استفاده از الگوریتم‌های رمزنگاری متقارن، نامتقارن، توابع هش و امضای دیجیتال رفته‌اند. پروتکل بیت کوین می‌تواند بهترین مثال برای این موضوع باشد که در آن شاهد استفاده از عناصر یاد شده در راستای اطمینان از اعتبار تراکنش‌ها و ایمن‌سازی شبکه هستیم. در واقع وجود امضای دیجیتال (Digital signature) در شبکه‌های بلاک چینی تضمین کننده این امر است که هر کاربر صرفا قادر است وجوه موجود در کیف پول خود را خرج نموده و امکان خرج کردن این دارایی‌ها بیش از یکبار را نخواهد داشت. به بیان ساده‌تر، مثلا فرض کنید که رضا 5 واحد بیت کوین را به سارا ارسال می‌کند و با انجام این تراکنش، رضا این 5 واحد بیت کوین را از دست داده و دیگر کنترلی بر روی آن‌ها نخواهد داشت؛ مگر آن که به حساب سارا دسترسی پیدا کرده و با امضای دیجیتال وی آن‌ها را به فرد دیگری انتقال دهد که چنین کاری بدون رضایت سارا و نداشتن کلید خصوصی کیف پول سارا امکان‌پذیر نیست.

از عناصر مهم دیگر پروتکل بیت کوین، تابع هش بوده و این تابع است که الگوریتم اجماع اثبات کار (PoW) و فرآیند استخراج را تعریف می‌کند. بیت کوین برای چنین منظوری از تابع رمزنگاری SHA-256 بهره می‌برد. با چنین توضیحاتی، روشن می‌گردد که کریپتوگرافی عضو حیاتی برای فناوری بلاک چین به شمار می‌رود و معماری این شبکه‌ها را به شکل خارق‌العاده‌ای تغییر داده است.

کریپتوگرافی؛ ضامن تامین امنیت داده‌ها و اطلاعات

همان طور که در مطالب فوق مشاهده کردید، منظور از کریپتوگرافی دانشی است که در آن پیام‌ها و اطلاعات با استفاده از الگوریتم‌هایی رمزگذاری شده و سپس به طریقی در دست فرستنده رمزگشایی می‌شوند و اشخاص ثالث که در این فرآیند نیستند، امکان کسب آگاهی از محتویات این پیام‌ها را نخواهند داشت. با رشد تکنولوژی و دیجیتالی شدن زندگی انسان‌ها دانش رمزنگاری و کریپتوگرافی نیز بیش از پیش اهمیت پیدا کرده؛ چراکه خطرات حملات سایبری همواره حریم خصوصی کاربران را تهدید می‌کند و این مسئله زمانی که با دارایی کاربران در ارتباط باشد بیش از پیش اهمیت پیدا می‌کند. به نظر شما کدام یک از الگوریتم‌های مورد استفاده در کریپتوگرافی قادر است امنیت خوبی را برای حریم خصوصی کاربران تامین نماید و دلیل شما برای انتخاب این الگوریتم در چیست؟