بررسی مفهوم رمزگذاری هش شده

آشنایی با تابع هش

در فرایند هشینگ با استفاده از یک فرمول تعدادی از ورودی‌ها با مقادیر مختلف تبدیل به یک خروجی یا به عبارتی رشته منحصر به فرد با مقدار ثابت می‌شوند. بنابراین آن چه که وارد فرمول هشینگ می‌شود، می‌تواند **حروف، اعداد و حتی تصاویر**باشد که طول نامعلوم دارند، اما در نهایت به یک خروجی با طول مشخص و معین تبدیل می‌شوند.

کاربرد هش در دنیای تکنولوژی

از هش برای ایجاد امنیت تکنولوژی در ارسال اطلاعات استفاده می‌شود؛ چرا که در هنگام ارسال اطلاعات باید رمز گذاری داده‌های کاربران صورت گیرد و فقط فرستنده و گیرنده اطلاعات توانایی خواندن آن‌ها را داشته باشند. لذا فرایند هشینگ در مبانی امنیت اینترنت و وب 3 بسیار کاربردی است و اهمیت آن در ذخیره مقادیر مختلف در دیتابیس آن نیز مشخص می‌شود.

برای این که با مفهوم هش بهتر آشنا شوید، برای شما مثالی می‌زنیم: در سایت‌ها رمز عبور شما به صورت هش شده ذخیره و نگهداری می‌شود؛ هر زمان که شما وارد وب سایت مربوطه شوید و رمز عبور مدنظر خود را وارد سایت کنید، هش این رمز عبور با مقدار هش ذخیره شده در دیتابیس سایت مقایسه می‌شود.

همچنین در یک مثال دیگر زمانی که یک آدرس ایمیل و رمز عبور برای خود در سایتی ایجاد می‌کنید، ارائه دهنده ایمیل شما به احتمال زیاد رمزعبورتان را ذخیره نمی‌کند، اما در عوض رمز عبور شما را از طریق الگوریتم و هش اجرا کرده و به این صورت رمز عبور شما را ذخیره می‌کند.

بنابراین هر بار که سعی کنید وارد ایمیل خود شوید ارائه دهنده ایمیل رمز عبور وارد شده شما را با فرایند هش وارد شده و ذخیره شده در خود مقایسه می‌کند و اگر هر دو هش مطابقت داشته باشد دسترسی شما به ایمیل مجاز می شود.

ویژگی‌های رمزنگاری انواع هش

هش‌ها یک سری ویژگی‌ها و مشخصات دارند که در تمامی انواع هش‌ها این ویژگی‌ها یکسان هستند که در ذیل به آن‌ها می‌پردازیم:

قطعی و ثابت

یعنی هر بار که یک مقدار ورودی خاص را به توابع هش بدهید تنها یک رشته یا خروجی منحصر به فرد را به شما می‌دهد.

محاسبات سریع

فرایند هش باید با سرعت زیادی انجام گیرد و نباید پردازش آن زمان بر باشد.

غیر قابل بازگشت

به این معنی که با داشتن خروجی نمی‌توان ورودی را محاسبه کرد.

تغییر کوچک تغییر بزرگ

منظور از این ویژگی به این نکته برمی‌گردد که اگر یک تغییر بسیار کوچکی در ورودی انجام دهید، تغییرات آن در مقدار هش خروجی بسیار زیاد خواهد بود.

هش کردن در ارزهای دیجیتال

هش در حفظ یکپارچگی و **امنیت رمز گذاری بلاک چین** بسیار اهمیت دارد. ستون یک ارز رمز نگاری شده شبکه بلاکچین یک دفتر کل جهانی محسوب می‌شود که با پیوند دادن بلوک‌های جداگانه داده‌های معاملات را تشکیل می‌دهد.

در این شبکه تنها معاملات معتبر نهایی می‌شوند و با استفاده از فرایند هش از معاملات جعلی و دو برابر شدن ارز جلوگیری می‌شود. به عبارتی دیگر فرایند هشینگ برای پردازش داده‌ها در دنیای ارزها و در بلوک‌های آن با استفاده از توابع ریاضی انجام می‌گیرد تا خروجی با طول ثابت ایجاد شود. به این ترتیب به دلیل نیاز به قدرت محاسباتی بسیار بالا و طول زیاد خروجی، تقریبا معکوس کردن یک تراکنش و رسیدن به ورودی آن غیر ممکن می‌شود.

بنابراین حتی اگر کسی بخواهد داده‌ای را در بلاک چین دستکاری کند، به ماهیت یک طرفه هش کردن نیاز خواهد داشت که در عمل غیرممکن است و همین امر امنیت شبکه بلاکچین را تضمین می‌کند.

در فرایند استخراج نیز یک ماینر برای ایجاد هش بلوکی که در حال ماین کردن آن است، ابتدا باید ورودی‌های متعددی را بررسی کند. در این شرایط ماینرها فقط موقعی می‌توانند اعتبار سنجی بلوک جدید را نهایی کنند که مقدار هش تطبیق داده شده با تعداد صفرهای اولیه را پیدا کنند. مقادیر این صفرها تعیین کننده میزان سختی فرایند استخراج هستند و تعداد آن به مقدار هشی بستگی دارد که با شبکه‌های بلاکچین تعیین می‌شود.

هش ریت

اگر در رابطه با استخراج ارزهای دیجیتال و کاربرد توابع هش در ارزهای دیجیتال مطالعه کرده باشید، به احتمال زیاد با عبارت هش ریت یا نرخ هش آشنایی دارید. هش ریت نشان دهنده قدرت پردازش شبکه در استخراج ارزهای دیجیتال است و برای تعیین و سنجش عملکرد یک دستگاه ماینر تعریف می‌شود.

یعنی هش ریت تعداد عملیات فرایند هش در بستر استخراج بیت کوین و ارزهای دیجیتال در حال اجرا را نشان می‌دهد و اگر میزان نرخ هش شبکه بلاک چین به دلیل افزایش عملیات ماینینگ رمز ارزها بالا برود، سیستم به صورت خودکار استخراج رمز ارز را طوری تنظیم می‌کند که میانگین زمان لازم جهت استخراج هر بلوک شبکه همان ده دقیقه باقی بماند.

به عبارت دیگر حتی اگر چندین ماینینگ در فرایند استخراج متوقف شوند، بازار شبکه بلاک چین سختی استخراج را طوری تنظیم می‌کند که میانگین زمان ماین کردن تغییر نکند.

تابع هش؛ عضو مهم جهان داده و رمزگذاری

توابع هش در در جستجو پایگاه‌های داده، تجزیه و تحلیل داده‌های سنگین، پرونده‌ها، مدیریت داده‌ها و زمینه‌های دیگر کاربرد زیادی دارد. این توابع رمزگذاری شده به صورت گسترده در زمینه امنیت اطلاعات مانند تایید اعتبار پیام، تایید پرداخت، اثر انگشت‌های دیجیتالی و سایر موارد امنیتی به کار گرفته می‌شود.

در فرایند استخراج بیت کوین توابع هش رمزگذاری شده نیز در حل کردن بلوک و حفظ امنیت شبکه نقش ویژه‌ای دارد. علاوه بر این‌ها، توابع هش زمانی که با حجم بسیار زیادی از اطلاعات روبرو هستیم، می‌تواند کمک حال ما باشد. در این شرایط اگر یک فایل بزرگ با داده‌های زیاد را به عنوان ورودی هشینگ وارد کنیم، خروجی با حجم بسیار کمتر را برای استفاده ارائه می‌دهد.

بنابراین در حالت کلی می‌توان توابع را عامل مهمی در امنیت اینترنت و دنیای وب و ارزهای دیجیتال نامید؛ آرامش خاطری که در زمان استفاده از اینترنت و دنیای ارزهای دیجیتال نصیب ما می‌شود به خاطر همین توابع حیاتی و پر اهمیت هستند که امنیت پیام‌ها، داده‌ها و اطلاعات را در پلتفرم‌ها و شبکه بلاک چین حفظ می‌کنند.