همه چیز درباره الگوریتم! Scrypt

اگر قصد فعالیت در حوزه کریپتوکارنسی را دارید، باید اطلاعات جامع و کاملی در ارتباط با نحوه عملکرد شبکه‌های بلاک‌چینی داشته باشید. یکی از موضوعات مهم موجود در آشنایی با شبکه‌های بلاکچینی به موضوع **الگوریتم‌های هشینگ** مربوط است. الگوریتم‌های هشینگ در بحث استخراج رمزارزها در شبکه‌های بلاکچینی که از الگوریتم اجماع اثبات کار (PoW) بهره می‌برند، بسیار حائز اهمیت هستند و هنگام خرید دستگاه‌های ماینری باید توجه ویژه‌ای نسبت به آن‌ها داشته باشید. الگوریتم Scrypt یکی از الگوریتم‌های رمزنگاری مهمی است که از آن به عنوان جایگزینی برای الگوریتم SHA-256 یاد می‌شود. با توجه به اهمیت آشنایی با این الگوریتم این مطلب از کیف پول من به معرفی جامع الگوریتم Scrypt و تجهیزات مورد نیاز برای استخراج رمزارزها توسط اسکریپت ماینینگ اختصاص پیدا کرده است. اگر شما هم در این زمینه سوالاتی دارید، مطالعه این مطلب از بلاگ کیف پول من را از دست ندهید.

الگوریتم اسکریپت (Scrypt) چیست؟

اسکریت (Scrypt) را می‌توان یکی از اولین الگوریتم‌های هشی به شمار آورد که در شبکه‌های بلاکچینی مورد توجه قرار گرفت. الگوریتم Scrypt در اصل با هدف بهبود الگوریتم هش قبلی یعنی الگوریتم SHA-256 که در بیت کوین مورد استفاده قرار می‌گرفت، معرفی گردید. این الگوریتم غالباً در شبکه‌های بلاک‌چینی کاربرد دارد که از الگوریتم اجماع PoW بهره می‌برند و اولین بار در سال 2011 همراه با راه‌اندازی Tenebrix (TBX) معرفی شد. از این سال تا به امروز الگوریتم Scrypt در بسیاری از پروژه‌های کریپتویی مورد توجه قرار گرفت و به لحاظ ارزش بازار، این الگوریتم در حال حاضر از سوی پروژه‌هایی مورد استفاده قرار گرفته که در مجموع بالغ بر 3 میلیارد دلار ارزش دارند.
اگر نگاهی به تاریخچه دنیای کریپتوکارنسی داشته باشید، متوجه خواهید شد که در آن روزهای ابتدایی، بسیاری از افراد چنین تصور می‌کردند که خرید ارز دیجیتال تنها راه ورود به این مارکت و کسب سود از آن است؛ اما با گذشت زمان و افزایش سطح آگاهی‌های عمومی، بسیاری از افراد به سراغ ماین و استخراج ارز دیجیتال آمده و راه امن‌تری را برای کسب درآمد از چنین دنیایی انتخاب کردند. البته این افراد به هنگام خرید دستگاه ماین و اسیک ماینر (Miner ASIC) به یک عامل کلیدی توجه داشتند و آن الگوریتم هشینگ شبکه بلاک‌چینی مورد نظر است. توجه داشته باشید که شبکه‌های بلاک‌چینی از الگوریتم‌های متنوعی استفاده می‌کنند، به عنوان مثال بیت کوین از SHA-256 و اتریوم پیش از مرج از الگوریتم هشینگ Ethash بهره می‌برد.
هنگامی که در ارتباط با تجهیزات مورد نیاز در ارتباط با استخراج رمزارزهایی که شبکه بلاک‌چینی آن‌ها از الگوریتم Scrypt پشتیبانی می‌کنند، سخنی به میان می‌آید، عموماً از اصطلاح «اسکریپت ماینینگ» استفاده می‌کنند و در اسکریپت ماینینگ برای استخراج رمزارزها همچون آنچه که در بلاکچین بیت کوین رایج است ماینر باید به حل مسائل پیچیده ریاضی بپردازد.

نگاهی به تاریخچه الگوریتم Scrypt

برای درک بهتر جایگاه الگوریتم اسکریپت لازم است نگاهی به تاریخچه و نحوه شکل‌گیری این الگوریتم هشینگ داشته باشیم. الگوریتم Scrypt در روزهای اول به عنوان یک الگوریتم Memory Hard به منظور بهبود امنیت شبکه در برابر حملاتی که از سخت‌افزارهای سفارشی برای رسیدن به اهداف خود بهره می‌برند، توسعه داده شد. منظور از الگوریتم Memory Hard نیز تابعی بوده که برای انجام محاسبات به مقدار حافظه بسیار بالایی نیاز دارد و غالباً برای مقاومت در برابر دستگاه‌های اسیک ماینر مورد استفاده قرار می‌گیرد.
با چنین توضیحی روشن می‌شود که الگوریتم Scrypt برخلاف سایر الگوریتم‌های هشینگ همچون CryptoNight و Equihash که صرفاً برای بلاک‌چین‌هایی زی‌کش و مونرو طراحی شده

بودند، با هدف دیگری توسعه پیدا کرد و سپس راه خود را به سمت شبکه‌های بلاکچینی هموار نمود. در واقع در می سال 2009 بود که کالین پرسیوال (Colin Percival) در مقاله‌ای تحت عنوان «Via Sequential Memory-Hard Functions Stronger Key Derivation» الگوریتم Scrypt را برای سرویس پشتیبانی آنلاین Tarsnap معرفی نمود. طبیعتاً در چنین تاریخی، بیت کوین در روزهای اولیه عمر خود به سر می‌برد و آشنایی کلی نسبت به آن وجود نداشت؛ همین موضوع سبب شد تا در این مقاله اشاره‌ای به کاربرد این الگوریتم در شبکه‌های بلاک‌چینی نشود.
این روند در سال 2011 و با معرفی ارز دیجیتال TBX تغییر پیدا کرد. در این سال، برنامه‌نویس ناشناسی با نام مستعار «Artfortz» برای اولین بار از الگوریتم Scrypt به عنوان الگوریتم هشینگ در شبکه بلاکچینی خود بهره برد. هرچند که این پروژه به موفقیت چندان زیادی دست پیدا نکرد؛ اما این عمل خالق تنبریکس راه و مسیر جدیدی را در مارکت ارز دیجیتال ایجاد کرد. راه تنبریکس از سوی فردی به نام چارلی لی (Charlie Lee) در پروژه فربریکس ادامه یافت. هرچند لی در مسیر خود با چالش‌هایی همچون حمله 51 درصدی مواجه بود؛ اما از ایده خود که ساخت یک شبکه بلاک‌چینی مبتنی بر Scrypt بود، دست نکشید. او با بررسی کلیه کارهای انجام شده برای فربریکس و همچنین کدهای بیت کوین، فورکی از این رمزارز به نام لایت کوین (LTC) را به بازار معرفی نمود که در حال حاضر یکی از مهم‌ترین رمزارزهای استفاده کننده از الگوریتم Scrypt به شمار می‌رود.

مقایسه الگوریتم اسکریپت و SHA-256

انتخاب الگوریتم Scrypt یا SHA-256 به عنوان سیستم پایه استخراج ارز دیجیتال به طور کلی به اهداف اعضای تیم توسعه‌دهنده شبکه بلاکچین مورد نظر بستگی دارد؛ اما مقایسه این دو الگوریتم می‌تواند دید خوبی را در اختیار ما قرار دهد. به طور کلی، ویژگی‌های این دو الگوریتم را می‌توان در جدول زیر خلاصه نمود:

الگوریتم هشینگ SHA-256

- نیازمند هش ریت TH/s یا بالاتر
- کاربرد در استخراج بیت کوین و تعداد قابل توجهی از رمزارزها
- استفاده از آن برای کلیه ماینرها ساده نیست.
- پیچیدگی بیشتری در مقایسه با الگوریتم Scrypt دارد.
- پردازش عاری از خطا و بهترین گزینه برای حفاظت از داده
- کند بودن زمان پردازش بلاک داده

الگوریتم هشینگ Scrypt

- عملکرد سریع در مقایسه با SHA-256
- امکان استفاده در CPUها و نیاز به انرژی کمتر

- بیشتر ارزهای دیجیتال جدید به سراغ این الگوریتم می‌روند.
- هش ریت پایین‌تر در مقایسه با SHA-256

امنیت الگوریتم Scrypt

به لحاظ تئوری و نظری، الگوی اسکریپت از امنیت بالاتری در هر واحد زمان محاسبه در مقایسه با الگوریتم‌های شناخته شده دیگر برخوردار است. به طور کلی با استفاده از الگوریتم اسکریپت می‌توان سرعت حافظه مورد نیاز برای محاسبه نتیجه را نیز مشخص نمود که چنین امری موجب افزایش هزینه مهاجمان بروت فورس (Brute-Force) به لحاظ GPU، پردازنده و منابع مموری می‌گردد.
به بیان بهتر، کارآمدی الگوریتم Scrypt در همین نکته خلاصه شده که قادر است حملات سخت‌افزاری شخصی‌سازی شده را به دلیل الگوریتم مموری هارد بسیار پرهزینه نماید. امنیت بالای الگوریتم Scrypt در دنیای کریپتوکارنسی سبب شده تا امروزه بسیاری از توسعه‌دهندگان از مزایای این الگو که عبارتند از سرعت 4 برابری و کارمزد حداقلی به راحتی بهره‌مند شوند.

کدام ارزهای دیجیتالی از الگوریتم Scrypt استفاده می‌کنند؟

در حال حاضر بسیاری از پروژه‌های رمزارزی به سراغ استفاده از الگوریتم Scrypt آمده‌اند که برخی از آن‌ها دارای مارکت کپ پایین و برخی دارای مارکت کپ بالا هستند؛ به عنوان مثال گرید کوین (GRC)، فلو (FLO)، امنی (OMNI)، لایتنینگ بیت کوین (LBTC)، گولدن (BLG) نمونه‌هایی از این ارزهای دیجیتالی به شمار می‌روند. مشهورترین ارزهای دیجیتال استفاده کننده از این الگو نیز به شرح زیر می‌باشند:

- **لایت کوین (LTC):** لایت کوین که در سال 2011 راه‌اندازی شد در گام اول خود را به عنوان یک شبکه مقاوم در برابر اسیک ماینرها معرفی نمود.
- **دوج کوین (DOGE):** دوج کوین در سال 2013 به عنوان فورکی از شبکه لایت کوین متولد شد و به تبعیت از آن از الگوریتم Scrypt بهره برد. هرچند که در آن روزهای اولیه عرضه چنین ارزی شوخی بیش نبود؛ اما با گذشت زمان و با حمایت‌های ایلان ماسک از آن، امروزه لقب پادشاه میم کوین‌ها را به خود اختصاص داده است.

ویژگی های اصلی الگوریتم Scrypt

الگوی اسکریپت دارای ویژگی‌های منحصربه‌فردی است که مهم‌ترین نمونه‌های آن را می‌توان در جدول زیر مشاهده نمود:

- **کارایی بالا:** تابع Scrypt در مقایسه با پیچیدگی مسئولیتی که برعهده گرفته است، بار کاری کمی دارد؛ درواقع استفاده از یک کلید و موازی‌سازی فرآیندها، تولید اعداد تصادفی و قابلیت تعدیل مقادیر تابع بدون به خطر افتادن امنیت، موجب افزایش سطح کارایی الگوریتم Scrypt شده است.
- **مقاومت در برابر اسیک و FPGA:** الگوی اسکریپت در روزهای ابتدائی کار خود مقاومت خوبی در برابر اسیک‌ها از خود نشان داد که چنین امری سبب می‌شد تا از آن به عنوان یک الگوریتم هشینگ کارآمد در حوزه تمرکززدایی یاد شود؛ البته از سال 2014 برخی اسیک‌های سازگار با این الگو به بازار عرضه شده و معادلات را برهم زدند.

الگوریتم Scrypt؛ الگویی مقاوم در برابر اسیک‌ها

امروزه دنیای کریپتو صرفاً به خرید بیت کوین و سرمایه‌گذاری بر روی ارزهای دیجیتال اختصاص پیدا نکرده است و در کنار آن شاهد کسب درآمد کاربران از روش‌های فرعی نظیر استیک رمزارزها و استخراج آن‌ها هستیم. به بیان بهتر، با افزایش آگاهی‌های جمعی نسبت به روش‌های کسب درآمد از چنین بستری، امروزه بیش از هر زمان دیگری لازم است که با نحوه عملکرد شبکه‌های بلاک‌چینی آشنا شویم. یکی از بخش‌های مهم چنین امری آشنایی با الگوریتم‌های هشینگ بوده که الگوی اسکریپت را می‌توان یکی از انواع مهم چنین الگویی به شمار آورد و به همین علت ما این مقاله از بلاگ کیف پول من را به معرفی جامع آن اختصاص دادیم.
همان طور که در مطالب فوق مشاهده کردید، الگوریتم Scrypt یک الگوی هشینگ در مکانیزم اجماع PoW بوده که با هدف غلبه بر دستگاه‌های اسیک در دنیای کریپتو مورد استفاده قرار گرفت. این الگوریتم در مقایسه با SHA-256 به حافظه ذخیره‌سازی بالایی نیاز دارد و به همین علت برخی متعقدند می‌توان آن را جایگزینی برای الگوی SHA-256 در نظر گرفت؛ نظر شما چیست؟ آیا این الگوریتم توان مقابله با الگوریتم SHA-256 را دارد؟ نظرات خود را برای ما بنویسید.