بررسی الگوریتم کریپتونایت

همواره بحث از امنیت ارزهای دیجیتالی مورد توجه کاربران دنیای کریپتوکارنسی بوده است و خوشبختانه این دنیای نوظهور با کمک گرفتن از فناوری‌های به‌روز رمزنگاری توانسته است به این نیاز کاربران به طور شایسته پاسخ دهد. در حال حاضر در دنیای کریپتوکارنسی از الگوریتم‌های رمزنگاری مختلفی همچون الگوریتم کریپتونایت (Cryptonight)، الگوریتم اسکریپت (Scrypt) و غیره کمک گرفته می‌شود. ناگفته نماند که الگوریتم کریپتونایت در واقع یک الگوریتم ماینینگ محسوب می‌شود و به عنوان CPU کارآمد و همچنین مقاوم در برابر ASICها ظاهر شده است. در سال‌های اخیر الگوریتم کریپتونایت به دلیل فراهم کردن شرایط تمرکززدایی بیشتر در استخراج ارزهای دیجیتالی به شدت مورد توجه ماینرها قرار گرفته است. جالب است بدانید که هدف از ایجاد الگوریتم کریپتونایت، پر کردن شکاف موجود میان ماینرهایی بوده است که منحصرا به پردازنده CPU دسترسی دارند و امکان تهیه سخت‌افزارهایی نظیر کارت‌های گرافیک و ASICها برای آن‌ها وجود ندارد و به همین علت است که گفته می‌شود وجود چنین الگوریتمی سبب ایجاد شرایط عادلانه‌تر در ماینینگ و استخراج ارزهای دیجیتالی شده است. با توجه به چنین محبوبیتی معرفی و بررسی الگوریتم کریپتونایت اجتناب ناپذیر می‌شود و به همین علت ما این مقاله از بلاگ کیف پول من را به بررسی این الگوریتم ماینینگ محبوب اختصاص داده‌ایم؛ بنابراین، اگر شما هم در این زمینه کنجکاو هستید تا انتهای این مقاله با ما همراه باشید.

آشنایی با الگوریتم کریپتونایت

احتمالا با شنیدن الگوریتم کریپتونایت به یاد مونرو (Monero) خواهید افتاد، در واقع استفاده از الگوریتم کریپتونایت را می‌توان به عنوان یکی از برجسته‌ترین وجوه تمایز مونرو با بیت کوین به شمار آورد و درواقع مونرو با کمک گرفتن از سیستم کریپتو نوت، به طور کلی خود را از جرگه رمزارزهای مشابه بیت کوین جدا ساخته است. الگوریتم هشینگ (یا همان درهم‌سازی) موجود در کریپتو نوت، «کریپتونایت» نامیده می‌شود. جالب است بدانید که الگوریتم کریپتونایت با هدف ایجاد سیستم منصفانه‌تر و همچنین غیرمتمرکزتر پا به عرصه ماینینگ و استخراج رمزارزها نهاده است و ارزهای رمزپایه ترکیب شده با الگوریتم کریپتونایت، قابلیت استخراج سازمانی نخواهند داشت که امید است با وجود چنین ویژگی بتوان از ایجاد استخرهای ماینینگ جلوگیری به عمل آورد و به حفظ ثبات و همچنان غیرمتمرکز باقی ماندن ارزهای دیجیتالی کمک کرد.

به طور کلی چند ویژگی منحصربه‌فرد سبب شده تا الگوریتم کریپتونایت مقاومت بسیار خوبی را از خود در برابر ASICها نشان دهد. این ویژگی‌های مهم به شرح زیر هستند:

1. الگوریتم کریپتونایت در واقع به یک حافظه سریع 2 مگابایتی به منظور اتمام فرآیند عملکردی خویش نیاز دارد. این نکته به این معنی است که هش‌های موازی شده به میزانی که امکان قرار دادن حافظه در تراشه وجود دارد محدود شده است و یک حافظه دو مگابایتی در مقایسه با مدار SHA256، به میزان سیلیکون بیشتری نیاز دارد.

2. طراحی الگوریتم کریپتونایت به شکلی بوده که با CPU و همچنین GPU سازگار باشد و علت این امر را می‌توان در این نکته جستجو کرد که این الگوریتم قصد دارد از دستورالعمل تنظیم شده AES-Ni نیز بهره ببرد.

مقایسه الگوریتم کریپتونایت با الگوریتم HashCash-SHA256

برای درک بهتر نحوه عملکرد الگوریتم کریپتونایت، مقایسه مونرو (که از الگوریتم کریپتونایت کمک گرفته) و بیت کوین (که از الگوریتم HashCash-SHA256 استفاده می‌کند) می‌تواند دید روشنی را در برابر شما قرار دهد. وجه اشتراک این دو پلتفرم‌ها در این نقطه خلاصه شده است که هر دوی آن‌ها از فناوری اثبات کار به منظور تائید بلاک‌ها کمک می‌گیرند؛ اما الگوریتم بیت کوین در هر 10 دقیقه توان تولید یک بلاک با محدودیت حافظه 2 مگابایتی را دارد و همین مسئله موجب پر شدن سریع بلاک تولیدی و همچنین افزایش هزینه کارمزد آن می‌گردد و این در حالی است که مونرو در همان قدم‌های نخستین خویش تلاش نموده تا این مورد را تغییر دهد و به همین منظور از الگوریتم کریپتونایت (CryptoNight) به منظور تائید بلاک‌های خود کمک گرفته است (البته هرچند که در حال حاضر این الگوریتم جای خود را به RandomX داده است ولی همچنان می‌توان ردپاهایی از الگوریتم کریپتونایت را در بخش‌های مختلف شبکه مونرو مشاهده کرد).

مطلب پیشنهادی : هش ریت چیست؟

جالب است بدانید که الگوریتم کریپتونایت برخلاف بسیاری از الگوریتم‌های رایج و متداول دیگر، به حافظه رم وابسته است و در این الگوریتم باید به میانگین اندازه صد بلاک قبلی توجه شود و دقیقا همین مسئله است که سبب شده تا فرآیند ماینینگ و استخراج در الگوریتم کریپتونایت، به حافظه رم وابسته باشد. براساس ادعای کارشناسان خبره فعال در حوزه استخراج ارزهای دیجیتالی وجود چنین وابستگی به حافظه رم در الگوریتم کریپتونایت به دلیل توجه حداکثری این الگوریتم به مسئله جلوگیری از تقلب بوده است. با کمک این الگوریتم شبکه مونرو با محدودیت حافظه مواجه نشده و از طرف دیگر نیز هر بلاک در عرض مدت زمان کوتاهی (در حد 2 دقیقه) تولید می‌شود. طبیعتا وابستگی به چنین حجمی می‌تواند خطرات پر شدن بلاک‌ها به وسیله اسپمرها را افزایش دهد و به همین علت میانگین 100 بلاک قبلی مورد توجه قرار می‌گیرد تا اگر چنانچه بلاک جدید تولیدی از این میانگین بیشتر باشد، کارمزد آن کاهش پیدا کند.

بررسی تاریخچه و هدف الگوریتم کریپتونایت

الگوریتم کریپتونایت حدودا در سال 2013 به عنوان بخشی از مجموعه کریپتونوت (CryptoNote) طراحی شد. به طور کلی یکی از اهداف اصلی از طراحی چنین الگوریتمی این بود که استخراج برای آن دسته از ماینرهایی که CPU برای فرآیند ماینینگ کمک می‌گیرند با استفاده از رمزگذاری بومی AES و ضرب کننده‌های سریع 64 بیتی راحت‌تر شود. هدف بلند پروازانه‌تر این طراحی این بود که قصد داشت آن را در مقابل ASICها به طور کارآمد محاسبه‌پذیرتر نماید، البته این هدف از همان زمان نیز محکوم به شکست بود؛ چراکه این امر با الگوریتم‌های «ASIC hard» اتفاق می‌افتد.

ناگفته نماند الگوریتم کارآمد CryptoNight ASIC در سال 2017 به وسیله Bitmain توسعه یافت. شبکه مونرو نیز در سال 2014 الگوریتم کریپتونایت را به عنوان الگوریتم اثبات کار خویش مورد استفاده قرار داد و از این سال شبکه مونرو در حد توان این الگوریتم کریپتونایت را توسعه و تکامل بخشید تا عمدا سازگاری آن با ASICها از بین برود و از آن زمان ما با سه ورژن از این الگوریتم به نام‌ها CryptoNightv1، CryptoNightv2 و CryptoNight-R مواجه هستیم. البته ناگفته نماند که مونرو در سال 2019 الگوریتم استخراج خویش را از کریپتونایت به RandomX تغییر داد. به طور کلی الگوریتم کریپتونایت از زمان راه‌اندازی تاکنون به وسیله بسیاری از پروژه‌های بلاک چینی مورد پذیرش قرار گرفته است.

نحوه عملکرد الگوریتم کریپتونایت

نکته مهمی که در نحوه عملکرد الگوریتم کریپتونایت وجود دارد، حساسیت بیش از حد این الگوریتم به تاخیر حافظه (Memory latency) است؛ چراکه این الگوریتم شامل یک حلقه است که در آن عملیات نوشتن حافظه و همچنین عملیات خواندن بعدی به صورت مداوم و مکرر انجام می‌شود و نتیجه این کار فشرده بر روی حافظه است که تعیین می‌نماید در مرحله بعدی باید از کدام تابع هش برای تولید خروجی راه‌حل بلوک استفاده شود. در طراحی این الگوریتم به این نکته که داده‌های کاری بایستی به اندازه حافظه پنهان مشترک در هر هسته یک CPU مدرن باشد توجه کافی شده است و چنین حافظه‌ای مسلما در مقایسه با DRAM معمولی سیستم یا VRAM یک GPU دارای میزان تاخیر بسیار کمتری است؛ در نتیجه می‌توان کارایی بیشتری را در اجرای الگوریتم کریپتونایت در مقایسه با GPU مشاهده کرد و دقیقا به همین علت بود که توسعه‌دهندگان پروژه مونرو متعهد شدند تا این الگوریتم را توسعه داده و نسخه‌های جدید آن را بر روی بلاک چین پیاده‌سازی نمایند و به این ترتیب تلاش طراحان ASICها را از بین ببرند؛ چراکه ASICها پس از تولید قابل برنامه‌ریزی مجدد نیستند.

الگوریتم کریپتونایت؛ ضامن حفظ ثبات و غیرمتمرکزی ارزهای دیجیتالی

همان طور که در مطالب فوق مشاهده کردید، الگوریتم کریپتونایت (**CryptoNight**) در واقع یک الگوریتم اثبات کار (proof-of-work) تلقی می‌شود و به گونه‌ای طراحی شده است تا برای CPUهای معمولی رایانه‌های شخصی مناسب باشد. الگوریتم کریپتونایت در ابتدای کار خویش در پایگاه کد کریپتونوت (CryptoNote) پیاده‌سازی شد. جالب است بدانید که الگوریتم کریپتونایت به دسترسی تصادفی به حافظه آهسته متکی بوده و همچنین بر وابستگی تاخیر (Latency dependence) تاکید دارد و به همین علت برخلاف الگوریتم Scrypt به کلیه بلوک‌های قبلی گره خورده است. در این الگوریتم در هر بلوک به 2 مگابایت فضا نیاز داریم که در حافظه نهان L3 (در هر هسته) پردازنده‌های مدرن قرار گرفته است. یک مگابایت حافظه داخلی تقریبا برای کلیه ASICهای مدرن غیرقابل پذیرش است! و به همین علت این الگوریتم مقاومت خوبی را از خود در برابر ASICها نشان داده است. ناگفته نماند که اگر در ارتباط با الگوریتم کریپتونایت سوالی دارید که در این مقاله از بلاگ کیف پول من، به آن اشاره نشده است، می‌توانید سوال خود را در بخش نظرات مطرح کنید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.

منابع لاتین:

1. https://academy.bit2me.com

2. https://cudominer.com

3. https://komodoplatform.com

4. https://monerodocs.org

5. https://phemex.com

6. https://en.bitcoin.it

7. https://coinguides.org