الگوریتمProof of Spacetime

اگر به دنیای کریپتوکارنسی علاقه‌مند باشید و زمانی از روز خود را به مطالعه در ارتباط با پروژه‌های موجود در این حوزه و اصطلاحات آن اختصاص دهید، احتمالاً به هنگام مطالعه ویژگی‌های شبکه فایل کوین با اصطلاح الگوریتم Proof of Spacetime که اختصاراً از آن تحت عنوان الگوریتم PoST نیز یاد می‌شود، مواجه شده‌اید. الگوریتم Proof of Spacetime در اصل نوعی الگوریتم اجماع بوده که در زیرمجموعه الگوریتم‌های اجماع اثبات وزن (Proof of Weight) جای گرفته و نسبتاً دارای پیچیدگی قابل توجهی است!

نودها در چنین الگوریتم اجماعی باید به طور مداوم و پیوسته اثبات نمایند که داده‌هایی که قبلاً دریافت کرده‌اند و همچنین در حال دریافت آن هستند را در اختیار دارند. متاسفانه هرچند که رفته رفته پروژه‌های رمزارزی بسیار زیادی بر روی شبکه فایل کوین اجرا می‌شود و میزان استفاده از الگوریتم Proof of Spacetime در دنیای کریپتوکارنسی روند افزایشی به خود گرفته است؛ اما هیچ یک از منابع فارسی فعال در حوزه کریپتوکارنسی توجهی به ماهیت و چیستی این الگوریتم نداشته‌اند و به همین علت ما این مقاله را به معرفی جامع الگوریتم PoST اختصاص داده‌ایم.

اگر شما هم سوالاتی در ارتباط با این الگوریتم نوظهور دنیای کریپتو دارید، مطالعه این مقاله را از دست ندهید.

الگوریتم اجماع PoST چیست؟

اثبات فضا و زمان (PoST) در اصل نوعی الگوریتم اجماع بوده که از آن در فناوری دفتر کل توزیع شده (DLT) براساس مفهوم مهر زمانی بلاک‌های داده مورد استفاده قرار می‌گیرد. مفهوم PoSt این است که بلاک‌های جدید داده صرفاً در صورتی مورد پذیرش قرار خواهند گرفت که با زمان فعلی مهر زمانی بلاک تطابق داشته باشند. در یک سیستم مبتنی بر بلاک‌چین این امر غالباً از طریق یک سیستم اثبات کار رمزنگاری حاصل می‌گردد. روند کار در الگوریتم اثبات کار به این صورت است که ماینرها بایستی یک معمای رمزنگاری را به منظور تولید یک بلاک جدید حل نمایند که در چنین فرآیندی به منظور اطمینان از پذیرش بلاک جدید از سوی شبکه، از مفهوم مهر زمانی (Timestamp) بهره گرفته می‌شود.
در نقطه مقابل، الگوریتم Spacetime Proof of که غالباً در بحث شبکه فایل کوین مورد استفاده قرار می‌گیرد، ثابت کننده این امر است که تامین کننده فضای ذخیره سازی یا همان Miner Storage، همچنان به ذخیره یک داده منحصربه‌فرد در شبکه ادامه می‌دهد؛ همین امر سبب شده تا در برخی منابع لاتین از این الگوریتم تحت عناوینی همچون اثبات فضا (Proof of Space) یا اثبات ذخیره‌سازی (Proof of Storage) نیز یاد شود. براساس نظر برخی تحلیل‌گران ارتباط نزدیکی میان الگوریتم Spacetime Proof of و اثبات ظرفیت (Proof of Capacity) وجود دارد.
در یک تعریف کلی و ساده از الگوریتم Proof of Spacetime، می‌توان آن را یک مکانیسم توافقی به شمار آورد که از یک تامین کننده فضای حافظه می‌خواهد تا ثابت نماید که یک فضای ذخیره‌سازی را به منظور نگهداری یک کپی از اطلاعات خاص یک فایل در یک بازه زمانی معین اختصاص داده است.

مقایسه الگوریتم PoSt با الگوریتم PoC

الگوریتم اثبات ظرفیت یک پروتکل اجماع بوده که در آن از درایوهای خالی استخراج‌کنندگان به منظور تائید تراکنش استفاده می‌شود. این الگوریتم اجماع بسیاری از چالش‌ها و معضل‌های موجود در الگوریتم‌های اثبات کار و اثبات سهام را برطرف می‌نماید؛ به طور که همچون PoW به انرژی زیادی نیاز نداشته و سازگاری خوبی با محیط زیست دارد و همچنین مثل الگوریتم PoS به مقدار زیادی توکن برای استیک نیاز ندارد. در یک کلام از الگوریتم اثبات ظرفیت (PoC) می‌توان به عنوان یک الگوریتم بهینه یاد کرد. احتمالا با مطالعه این جملات متوجه شباهت بسیار زیاد الگوریتم PoST به الگوریتم PoC شده‌اید.

اما با این وجود باید توجه داشت که الگوریتم اجماع Spacetime Proof of و الگوریتم Proof of Capacity مفهوم یکسانی ندارند؛ چراکه الگوریتم PoSt به اختصاص‌دهندگان فضای موجود در شبکه اجازه می‌دهند تا ثابت نمایند که یک منبع «Spacetime» را صرف نموده‌اند یا به بیان بهتر، بخشی از ظرفیت ذخیره‌سازی خویش را در یک دوره زمانی به شبکه اختصاص داده‌اند. Tal Moran و Ilan Orlov که خالقان الگوریتم PoSt به شمار می‌روند، رویکرد اتخاذ شده در این الگوریتم را یک رویکرد کاملاً منطقی نامیده‌اند؛ چراکه در آن هزینه واقعی ذخیره‌سازی متناسب با فایل مورد نظر، ظرفیت ذخیره‌سازی و در نهایت زمان آن برآورد می‌گردد.
به عنوان مثال، سرویس ذخیره‌سازی ابری Dropbox، قیمت اشتراک ماهانه را متناسب با میزان فضای ذخیره‌سازی استفاده شده از سوی کاربران در طول دوره زمانی تعیین شده، مشخص می‌کند؛ به طوری که استفاده از 3 ترابایت فضای ذخیره‌سازی به مدت 1 ماه، 10 دلار و استفاده از 3 ترابایت در بازه زمانی دو ماهه هزینه 20 دلاری برای کاربر در پی خواهد داشت. به طور کلی نقطه اشتراک الگوریتم PoSt با PoC در این است که هر دوی آن‌ها تلاش می‌کنند تا با ایجاد انگیزه‌های مالی ماینرها را تشویق نمایند که فعالیت صادقانه‌ای در شبکه در پیش گرفته و فعالیت مخربی در آن نداشته باشند.
با این وجود تفاوت میان الگوریتم PoSt و PoC نیز در این نکته است که در الگوریتم Proof of Spacetime شرکت‌کنندگان در شبکه را مجبور می‌سازد تا نشان دهند که داده‌ها را به صورت فیزیکی در یک دوره زمانی معین ذخیره کرده و همچنان از آن نگهداری می‌کنند. این اثبات در الگوریتم PoSt به گونه‌ای طراحی شده که ماینرها را به طور تصادفی انتخاب می‌کند و به منظور تائید چنین امری داده‌های آن‌ها خوانده می‌شود.

نحوه تائید ذخیره‌سازی داده‌ها در طول زمان از طریق الگوریتم PoSt

در پروتکل Proof of Spacetime، دو معمای هش رمزنگاری معروف به WinningPoSt و WindowPoSt به منظور آزمودن هر تامین کننده فضای ذخیره‌سازی درگیر در شبکه طرح می‌شود و این دو معما به گونه‌ای طراحی شده‌اند که یک ماینر صرفاً زمانی بتواند به درستی به آن پاسخ دهد که همچنان یک داده معین را ذخیره داشته باشد! معمای WinningPoSt همواره استخراج‌کننده‌ای را انتخاب می‌کند که انتظار می‌رود بلاک بعدی را به طور تصادفی استخراج نماید. این معما از چنین اشخاصی در ارتباط با یک کپی از داده‌های بلاکچین سوالی می‌پرسد و انتظار دارد که پاسخ مورد نظر را در یک بازه زمانی کوتاه دریافت کند. بازه زمانی کوتاه برای ارائه پاسخ، تضمین کننده این واقعیت است که ماینر مورد نظر یک کپی از داده‌ها را ذخیره کرده است.

در طرف دیگر نیز معما و چالش WindowpoSt با درخواست مکرر داده‌ها در بازه‌های زمانی معین، تضمین می‌کند که ماینر مورد نظر به طور پیوسته داده‌ها در فضای حافظه خویش ذخیره نگه داشته است. به بیان خلاصه، چالش‌های WinnigPoSt و WindowPoSt دو بازوی اصلی الگوریتم Proof of Spacetime به شمار می‌روند که اولی مسئولیت تائید وجود یک کپی از داده‌ها نزد استخراج‌کننده بلاک بعدی و دومی مسئولیت تائید نگهداری مداوم داده در نظر ماینر پس از ذخیره‌سازی اولیه را برعهده گرفته است.

مقایسه الگوریتم PoSt و PoS

دو الگوریتم اثبات سهام و PoSt هر دو پروتکل‌های اجماعی هستند که در شبکه‌های بلاک‌چینی کاربرد دارند و به گونه‌ای طراحی شده‌اند که راهی امن و غیرمتمرکز برای ذخیره‌سازی تراکنش‌های انجام یافته در شبکه باشند. الگوریتم اثبات سهام که احتمالا نام آن را به هنگام خرید اتریوم و آموزش راه‌های کسب درآمد از شبکه بلاکچینی اتریوم مشاهده کردید، الگوریتمی بوده که در ازای اعتبارسنجی تراکنش‌ها در شبکه به ولیدیتورها پاداش می‌دهد. در چنین الگوریتمی هرچه تعداد ارزهای استیک شده بیشتر باشد، به همان میزان شبکه به درستکاری نود مورد نظر بیشتر اعتماد کرده و فرد نفوذ بیشتری در شبکه خواهد داشت. این درحالیست که الگوریتم Proof of Spacetime به مدت زمان ذخیره‌سازی داده‌ها توجه داشته و متناسب با آن پاداشی را در اختیار آن‌ها قرار می‌دهد. به طور کلی هرچند که هر دو الگوریتم PoSt و PoC پروتکل‌های ایمن و مطمئنی هستند؛ اما الگوریتم Proof of Spacetime به لحاظ هزینه مقرون به صرفه‌تر است.

الگوریتم PoSt؛ پروتکل اجماعی ایمن برای ذخیره‌سازی غیرمتمرکز داده‌ها

امروزه دنیای کریپتو صرفاً به خرید ارز دیجیتال و سرمایه‌گذاری بر روی برنامه‌های دیفای منحصر نشده و وجود پروژه‌هایی همچون فایل کوین نشانگر این واقعیت است که فناوری بلاک‌چین در بسیاری از حوزه‌های دیگر نیز نفوذ پیدا کرده است و همین مسئله آشنایی کامل با اصطلاحات و الگوریتم‌های موجود در چنین شبکه‌هایی را می‌طلبد؛ به همین علت ما این مقاله از بلاگ کیف پول من را به معرفی جامع الگوریتم Proof of Spacetime اختصاص دادیم. همان طور که در مطالب فوق مشاهده کردید، منظور از الگوریتم PoSt، پروتکل اجماعی بوده که در آن تامین کنندگان فضای ذخیره‌سازی در ازای تخصیص فضای ذخیره‌سازی خویش برای مدت زمان معین از شبکه پاداش دریافت می‌کنند. حال که با چیستی الگوریتم Proof of Spacetime بهتر آشنا شدید، آیا به نظر شما چنین الگوریتمی تاب رقابت با الگوریتم‌هایی همچون اثبات کار و سهام را خواهد داشت؟ نظرات خود را برای ما بنویسید.