

مقالات آموزشی بنیاد سور

راهکارهای لایه دو، ابزاری برای
مقیاس‌پذیری شبکه اتریوم (بخش دوم)

شبکه بلاکچین سور
www.surnet.org



گردآورنده: بنیاد سور

نسخه: شماره ۳۵





راهکارهای لایه دو، ابزاری برای مقیاس‌پذیری شبکه اتریوم – بخش دوم

در مقاله قبلی، در مورد نیاز به راهکارهای لایه دو اتریوم برای افزایش مقیاس‌پذیری اتریوم صحبت شد. در این مقاله، در ادامه بررسی راهکارهای لایه دو، برخی دیگر از این موارد و راهکارها بررسی خواهند شد.

رول‌آپ خوش‌بینانه

رول‌آپ‌های خوش‌بینانه روی شبکه اصلی اتریوم اجرا می‌شوند و در نتیجه امکان اجرای قراردادهای هوشمند و انواع مختلفی از تراکنش‌ها بر روی آن‌ها میسر است. این رول‌آپ‌ها دقیقاً از همان سطوح امنیتی برخوردارند که شبکه اصلی اتریوم داراست. از سویی دیگر، رول‌آپ خوش‌بینانه، برای دستیابی به افزایش سرعت، ریشه‌های مرکب را محاسبه می‌کند. توان محاسباتی مورد استفاده در این روش در مقایسه پلاسما و رول‌آپ آگاهی صفر کمتر است. بزرگ‌ترین تفاوت بین رول‌آپ خوش‌بینانه و دانش صفر در آن است که رول‌آپ خوش‌بینانه از فناوری رمزنگاری استاندارد استفاده می‌کند. رول‌آپ خوش‌بینانه با EVM سازگار است و در نتیجه هر آنچه بر روی شبکه اتریوم قابل پیاده‌سازی باشد، در رول‌آپ خوش‌بینانه نیز اجرا شدنی است. بزرگ‌ترین ضعف رول‌آپ خوش‌بینانه آن است که انتقال دارایی از لایه یک به دو بسیار زمان‌بر است (هفت روز یا بیشتر). پروژه پالیگان در حال حاضر از رول‌آپ خوش‌بینانه استفاده می‌کند.

رول‌آپ آگاهی صفر

رول‌آپ‌های آگاهی صفر، از فناوری رمزنگاری جدیدی استفاده می‌کند. بر اساس بررسی‌های صورت گرفته تا فصل سوم سال ۲۰۲۱، هیچ راهکار عملیاتی در زمینه پیاده‌سازی رول‌آپ آگاهی صفر صورت نگرفته است. از سویی دیگر، قدرت محاسباتی مورد نیاز برای اثبات آگاهی صفر، بسیار زیاد است؛ اما با رشد فناوری‌های محاسباتی این مشکل در حال کم‌رنگ شدن است. در نهایت باید به این نکته توجه کرد که برخی از پیاده‌سازی‌های رول‌آپ آگاهی صفر، با ماشین مجازی اتریوم سازگاری



ندارند و رول‌آپ آگاهی صفر تمام مزایای رول‌آپ خوش‌بینانه را داراست با این مزیت که انتقال دارایی از لایه ۲ به یک، بر خلاف روش خوش‌بینانه، زمان زیادی نیاز ندارد.

رول‌آپ‌های آگاهی صفر، تراکنش‌های برون‌شبکه (off-chain) را دسته‌بندی کرده و یک گواهی رمزنگاری شده به نام اسنارک (SNARK) برای آن ایجاد می‌کند. در واقع درست برخلاف رول‌آپ‌های خوش‌بینانه که هیچ‌گونه محاسباتی برای امنیت تراکنش انجام نمی‌دهد، رول‌آپ‌های آگاهی صفر محاسبات برون زنجیره‌ای مخصوص به خود را داشته و گواه اعتبار حاصل‌شده از این محاسبات را به زنجیره لایه یک ارسال می‌کند. از طرفی دیگر در رول‌آپ‌های آگاهی صفر، وضعیت حساب‌ها و موجودی‌ها توسط ۲ درخت مرکب که حاصل هش موجودی و وضعیت حساب‌ها هستند، این اطمینان را می‌دهد که هیچ فردی نمی‌تواند اطلاعات را جعل کند.

راهکارهای ترکیبی

Hybrid solutions ترکیبی از دیگر راهکارهای لایه دو است. معروف‌ترین پروژه‌ای که این راه را در پیش گرفته سلر (Celer) است. سلر رویکردی کاملاً متفاوتی نسبت به دیگر پروژه‌ها دارد. این پروژه یک معماری ترکیبی را ارائه می‌دهد که امنیت زنجیره جانبی را از طریق اجماع اثبات سهام برای dApp‌های عمومی و امنیت زنجیره اصلی را از طریق optimistic rollup ها برای کاربردهای خاص مانند انتقال توکن، فراهم می‌کند. از دیگر پروژه‌هایی که به ارائه راه‌حل‌های ترکیبی می‌پردازد می‌توان به Arbitrum اشاره کرد.

راهکارهای آربیتروم

آربیتروم نیز یک راهکار لایه دو است که در راستای افزایش سرعت و مقیاس‌پذیری قراردادهای هوشمند طراحی شده است. همچنین این راه‌حل، ویژگی‌های جدیدی را نیز در راستای ارتقای سطح حریم خصوصی کاربران این شبکه ارائه می‌دهد. در واقع پلتفرم‌های لایه دو به توسعه‌دهندگان این امکان را می‌دهد تا بدون در خطر قراردادن امنیت لایه ۱، تراکنش‌های اصلاح‌نشده EVM را روی لایه ۲، اجرا کنند. علاوه بر این،



آر بی تروم خود را یک راهکار مقیاس پذیر ایدئال برای اپلیکیشن های غیرمتمرکز معرفی کرده است.

ولیدیوم

ولیدیوم یک راه حل لایه ۲ است که در آن اعتبار تمام معاملات با استفاده از zero-knowledge proofs بررسی می شود، در حالی که داده ها در خارج از زنجیره نگه داری می شوند. این موضوع مانع از سرقت سرمایه های موجود می شود زیرا مجوز هر تراکنش از یک حساب کاربری خاص باید توسط همان کاربر داده شود.

سازوکار Validium شباهت زیادی به zkRollup دارد، تنها تفاوت در این است که در دسترس بودن داده ها در zkRollup روی زنجیره است، در حالی که Validium آن را خارج از زنجیره نگه می دارد. این به Validium اجازه می دهد تا توان عملیاتی خود را به میزان قابل توجهی افزایش دهد اما این کار می تواند یک نقطه ضعف بزرگ باشد زیرا در این صورت اپراتورهای پروژه های اجرا شده با ولیدیوم می توانند سرمایه کاربران را مسدود کنند.

سخن پایانی

تمامی راهکارهای بیان شده، هر یک مزایا و معایب خود را دارد و هیچ یک راهکاری عمومی و فراگیر نیستند. بسته به هر محصول، اپلیکیشن و نیاز، می توان از یکی از این روش ها استفاده کرد. همان طور که بیان شد، شبکه پالیگان از دو راهکار پلاسما و رول آپ خوش بینانه استفاده می کند.

راهکارهای لایه دو تنها راه برای افزایش مقیاس پذیری اتریوم نیست. در کنار این روش ها، اتریوم ۲ و شاردینگ نیز وجود دارند که در صورت پیاده سازی موفق می توانند به شدت بر روی هزینه و سرعت تراکنش تأثیر مثبت داشته باشد.

به نظر می رسد پروژه های در جنگ راهکارهای لایه ۲ برنده است که بتواند مشکلاتی را که هم اکنون در لایه ۱ وجود دارد برطرف کند و اثر مثبتی بر dapp ها و کاربران شبکه



داشته باشد. هنگامی که کاربران به راهکارهای لایه دوم و پروژههای آن فکر می‌کنند سؤالاتی که از خود می‌پرسند این است:

آیا استفاده از این راهکار ارزان است؟ آیا من می‌توانم به راحتی و سریع از این راهکار استفاده کنم و هر موقع لازم شد از آن خارج شوم؟ آیا دپ های مورد علاقه من آنجا هستند؟ آیا نقدینگی کافی وجود دارد؟

پروژه‌های متعددی که در حال کار روی هرکدام از این راهکارها هستند نقاط قوت و ضعف خود را دارند بنابراین احتمال کمی دارد که یکی از این راه‌حل‌ها دیگران را شکست دهد، زیرا تعداد بسیار زیادی کاربر و دارایی برای پیوستن به این اکوسیستم وجود دارد و هرکدام از این پروژه‌ها نیز جذابیت خود را دارند. در واقع فناوری‌های مختلف لایه ۲ مشکلات مختلفی را حل می‌کنند و هیچ راه‌حل جامعی برای همه مشکلات وجود ندارد. در حال حاضر راه‌های زیادی مانده تا اتریوم ۲ در دسترس کاربران قرار بگیرد، تا آن زمان، برندگان بلامنازع، راهکارهای لایه ۲ هستند، هرچند نمی‌توان با قطعیت گفت با آمدن اتریوم ۲ نیز بهار راهکارهای لایه ۲ تمام می‌شود.