

# مقالات آموزشی بنیاد سور

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

شبکه بلاکچین سور  
[www.surnet.org](http://www.surnet.org)



گردآورنده: بنیاد سور

نسخه: شماره ۳۴





## راهکارهای لایه دو، ابزاری برای مقیاس‌پذیری شبکه اتریوم

اتریوم به‌عنوان دومین رمزارز بزرگ جهان پس از بیت‌کوین، توانسته یک سیستم مالی غیرمتمرکز را بنا کند و بسیاری از نوآوری‌ها در فضای رمزارزی نیز حول این شبکه شکل گرفته است. متأسفانه، اتریوم قربانی موفقیت خود شده است. شبکه اصلی اتریوم که با عنوان لایه یک شناخته می‌شود، به صورت عادی، به خوبی توانایی پردازش یک میلیون تراکنش در روز را دارد؛ اما با توسعه کاربردهای مبتنی بر اتریوم، حجم تراکنش‌ها به شدت رو به رشد است. این امر باعث می‌شود شبکه با ازدحام روبرو شود و در نتیجه، کارمزد تراکنش و هزینه تمام شده برای پردازش تراکنش‌ها به شدت بالا می‌رود. هم‌زمان با رشد هزینه تراکنش‌ها در لایه یک، استفاده از کاربردهای مبتنی بر شبکه اتریوم همانند بازارهای NFT و صرافی‌های غیرمتمرکز جذابیت خود را برای عموم مردم از دست می‌دهد.

لایه دو، کلمه‌ای است که همانند چتری کلیه کاربردهای مبتنی بر لایه یک برای افزایش مقیاس‌پذیری شبکه اتریوم تحت پوشش خود قرار می‌دهد. به‌عبارتی‌دیگر، لایه دو تلاشی برای بدل کردن اتریوم به شبکه‌ای کاربردی‌تر برای تعداد بیشتری از کاربران است.

در شبکه اتریوم، تعداد راهکار لایه دو تاکنون پیشنهاد و طراحی شده است. در این مقاله، بنیاد سورنگاهی به این راهکارها و شیوه کار آن‌ها برای دستیابی به مقیاس‌پذیری در شبکه اتریوم داشته است.

### کانال‌ها

کانال‌ها در واقع چیزی شبیه شبکه لایت‌نینگ بیت‌کوین را در شبکه اتریوم پیاده‌سازی می‌کنند. کانال‌ها به افراد اجازه می‌دهد تعداد نامحدودی تراکنش را با افراد دیگر انجام دهند؛ اما تنها تراکنش اول و آخر آن‌ها بر بستر بلاکچین ثبت خواهد شد. بدین ترتیب، تمامی تراکنش‌ها به صورت خارج از شبکه مدیریت شده و در نتیجه، سرعت به شدت افزایش یافته و کارمزد کاهش چشم‌گیری می‌یابد.



در کنار مزایای کانال‌ها، ایراد اصلی کانال همان ایراداتی است که شبکه لایت‌نینگ نیز دارد. با بایستی با فردی می‌خواهید با وی تراکنش مالی داشته باشید، ارتباط مستقیم یا غیرمستقیم داشته باشید، سرمایه رمزآزاری بایستی به کانال اختصاص داده شود و در طول اعتبار کانال قابل برداشت نیست. همچنین آسیب‌پذیری‌های امنیتی بالقوه زیادی به کانال‌ها و راهکارهای خارج از شبکه یا off-chain وارد است.

فرض کنید شما مدیر عامل یک شرکت ساختمانی هستید و طبق نیازهای روزانه شرکت به سیمان برای ساخت ساختمان نیاز دارید. شما در اینجا به جای پرداخت روزانه بهای سیمان، یک صورت‌حسابی تهیه می‌کنید که تنها یک‌بار آن هم در اتمام کار خود، پول را پرداخت کنید. این کار را برای شما راحت می‌کند. علاوه بر آن در بلاکچین دیگر لازم نیست برای هر تراکنش کارمزد بدهید و فقط یک‌بار در انتها کارمزد آن را پرداخت می‌کنید. لازمی این کانال، اعتماد بین دو طرف است.

Raiden راهکاری است که از آن به‌عنوان لایت‌نینگ اتریوم یاد می‌شود.

### پلازما

نحوه شکل‌گیری پلازما مانند نمودار درختی است. در پلازما بلاکچین‌های اصلی برای مقیاس‌پذیری از بلاکچین‌های متعددی که نسخه کوچک‌تری از بلاکچین‌های اصلی هستند که اصطلاحاً به آن‌ها بلاکچین کودک گفته می‌شود، استفاده می‌کنند.

مزیت این روش این است که هرگاه مشکل مقیاس‌پذیری پیش بیاید به تعداد بلاکچین‌های کودک اضافه می‌شود، همچنین امنیت این بستر را خود اتریوم تأمین می‌کند.

از معایب این راه‌حل می‌توان به پراکندگی داده‌ها اشاره کرد. همچنین در صورت حمله به بلاکچین، همه داده‌ها در بلاکچین‌های کودک به سمت بلاکچین اصلی می‌روند و این باعث ایجاد هرج‌ومرج بزرگی در سیستم می‌شود.

در واقع پلازما چارچوبی است که برای ایجاد زنجیره‌های کوچک (Child Chain) مورد استفاده قرار می‌گیرد. زنجیره‌هایی که از زنجیره اصلی اتریوم به‌عنوان بستری



برای ایجاد اعتماد استفاده می‌کنند. زنجیره‌های کوچک امکان تراکنش‌هایی با سرعت بالا و کارمزد پایین را فراهم می‌آورد؛ اما تنها انواع مشخصی از تراکنش‌ها همانند انتقال و سوآپ را پشتیبانی می‌کنند و نمی‌توان بر روی زنجیره‌های کوچک، همه نوع قراردادهای هوشمند تعریف و اجرایی کرد. یکی دیگر از ایرادات راهکارهای پلاسما، زمان بر بودن ثبت انتقال از زنجیره کوچک به زنجیره اصلی شبکه اتریوم است.

OMG و MATIC از پروژه‌های موفق این راه‌حل هستند.

### زنجیره جانبی مستقل

با اینکه از یک دیدگاه، تمامی راهکارهای لایه دوم، به نوعی مبتنی بر زنجیره‌های جانبی هستند، اما به صورت خاص زمانی که صحبت از راهکارهای مبتنی بر زنجیره جانبی مستقل پیش می‌آید، منظور ارتباط دو بلاکچین کاملاً مستقل از یکدیگر است. این دو زنجیره از طریق یک بستر دوطرفه با یکدیگر در ارتباط‌اند و هر دو زنجیره با ماشین مجازی اتریوم سازگاری دارند.

Sidechain‌ها یا بلاکچین‌های جانبی، به مقیاس‌پذیری بلاکچین اصلی کمک می‌کند. در اینجا بلاکچین جایگزین می‌تواند از اجماع دیگری استفاده کند. همچنین امنیت شبکه را خودش تأمین می‌کند. تفاوت آن‌ها با کانال‌های پرداخت این است که کانال پرداخت نرم‌افزار است ولی بلاکچین‌های جانبی خود یک بلاکچین جدا هستند و نودهایی برای اجماع دارند و هدف آن‌ها صرفاً کمک به بلاکچین اصلی است.

فناوری بستر ساز زنجیره‌های جانبی مستقل، کاملاً مشخص و شناخته شده است. به همین سبب، پروژه‌های زیادی به دلیل سرعت بالا و کارمزد پایین تراکنش‌ها در زنجیره جانبی مستقل، به این بستر مهاجرت کرده‌اند. زنجیره‌های جانبی مستقل، خود مسئولیت تأمین امنیت شبکه خود را بر عهده‌دارند در نتیجه به دلیل آنکه این شبکه‌ها برای تأمین امنیت خود به شبکه اتریوم وابسته نیستند و شبکه‌های کوچک‌تر با تعداد ولیدیتور کمتر هستند، در نتیجه امنیت آن‌ها از شبکه اصلی اتریوم کمتر است.



xDAI یکی از مثال‌های زنجیره جانبی اتریوم است. همچنین، بازی معروف Axie Infinity یک مثال خوب از پروژه‌های لایه یک است که برای افزایش سرعت تراکنش‌های خود و کاهش کارمزد آن‌ها به زنجیره جانبی مستقل مهاجرت کرده است.

### رول آپ‌ها

رول آپ‌ها، تراکنش‌های بلاکچینی را جمع‌آوری می‌کنند و به عنوان یک تراکنش در شبکه اصلی ارسال می‌کنند که باعث خلوت شدن شبکه می‌شود. با رول آپ، کار ماینرها راحت‌تر می‌شود.

رول آپ‌ها دارای دو نوع optimistic roll up و zero knowledge roll up هستند. پشتیبانی از EVM و مهاجرت ساده‌تر پروژه‌های قرارداد هوشمند از لایه اول به لایه دوم مزیت optimistic است اما نسبت به رول آپ‌های zk از امنیت کمتری برخوردارند.

- **رول آپ خوش‌بینانه:** در رول آپ خوش‌بینانه، لایه فرض را بر آن می‌گذارد که تراکنش‌های موجود در لایه دو به صورت پیش‌فرض درست و مورد تأیید هستند مگر خلاف آن ثابت شود و صحت تراکنش‌ها در لایه یک صرفاً در صورت بروز چالش بررسی خواهد شد.
- **رول آپ آگاهی صفر:** اثبات صحت تراکنش‌ها در لایه دو بررسی و نهایی شده و تنها در لایه یک ثبت نهایی می‌شود.

در مقالات بعدی در مورد انواع راهکارهای لایه دوم صحبت خواهد شد.