



کوین ایران 

آلتکوین‌هایی با قابلیت پشتیبانی از شبکه‌های

لایه دوم مانند لایت‌نینگ (Lightning)

فهرست مطالب

آلتکوین‌هایی با قابلیت پشتیبانی از شبکه‌های لایه دوم مانند لایتنینگ (Lightning).....	۱
لایتنینگ به عنوان راه‌حلی برای مشکل مقیاس‌پذیری.....	۱
بیت‌کوین و شبکه لایتنینگ.....	۲
لایت‌کوین و شبکه لایتنینگ.....	۳
اتریوم و شبکه Raiden.....	۳
ZCash و شبکه BOLT.....	۴
ریپل و شبکه لایتنینگ.....	۵
مونرو و شبکه لایتنینگ.....	۶
نئو و شبکه Trinity.....	۷
استلار و شبکه لایتنینگ.....	۷
منابع.....	۸

آلتکوین‌هایی با قابلیت پشتیبانی از شبکه‌های لایه دوم مانند

لایت‌نینگ (Lightning)

بیت‌کوین همواره ارزشمندترین و مهم‌ترین رمز ارز جهان بوده است و انتظار می‌رود برای مدت زمان زیادی جایگاه خود را حفظ نماید. با این وجود، بسیاری از مردم بر این باورند که بیت‌کوین با روند رو به رشد پذیرش آن به زودی با بحران‌هایی مواجه خواهد شد. اخیراً شکایت‌های فراوانی به دلیل زمان بالای انتظار تأیید تراکنش‌های بیت‌کوین و پرداخت هزینه‌های گزاف برای پردازش آن مطرح شده است. محدودیت بلاک‌چین بیت‌کوین به پردازش ۷ تراکنش در هر ثانیه اصلی‌ترین مشکل این شبکه است که افزایش زمان انتظار و هزینه‌های بالای تراکنش را در پی داشته است. شایان ذکر است که ۷ تراکنش در ثانیه حالت ایده‌آل این شبکه می‌باشد و در عمل بین ۲ تا ۳ تراکنش را در هر ثانیه پردازش می‌نماید. اگر بیت‌کوین به دنبال قرارگیری در جایگاه سیستم پرداختی است که به صورت گسترده مورد استفاده عموم قرار گیرد باید راه‌حل مناسبی برای این چالش پیدا کند. مشکل مقیاس‌پذیری پیش روی بسیاری از رمز ارزهای استفاده‌کننده از فناوری بلاک‌چین قرار دارد. تعداد قابل توجهی از رمز ارزها به استفاده از راه‌حل‌های لایه دوم مانند لایت‌نینگ روی آورده‌اند.

لایت‌نینگ به عنوان راه‌حلی برای مشکل مقیاس‌پذیری

راه‌حل‌های بالقوه متعددی برای حل مشکل مقیاس‌پذیری وجود دارد ولی شاید شبکه لایت‌نینگ^۱ مستعدترین آن‌ها باشد. در اصل، شبکه لایت‌نینگ یک لایه اضافه‌تر در بالای شبکه بیت‌کوین ایجاد می‌کند که با مدیریت الزام مربوط به همه‌پختی آنی تراکنش‌های بیت‌کوین در کل شبکه، امکان انجام تراکنش‌های سریع و ارزان آن را فراهم می‌نماید. این لایه اضافه‌تر از کانال‌های دو طرفه‌ای ایجاد شده توسط کاربران تشکیل شده است. این کانال‌ها به کاربران اجازه می‌دهند تا در هر زمان دلخواه و با حداقل هزینه برای یکدیگر پول ارسال کنند. شبکه لایت‌نینگ در اصل برای حل مشکلات بیت‌کوین طراحی شده است ولی آلتکوین‌های متعددی به سمت استفاده از آن گرایش پیدا کرده‌اند. برخی از آلتکوین‌ها در تلاشند تا یک نمونه از شبکه لایت‌نینگ بیت‌کوین را برای خود پیاده‌سازی نمایند در حالی که برخی دیگر به دنبال پیاده‌سازی راه‌حل‌های مشابه هستند. شاید فناوری‌هایی مانند شبکه لایت‌نینگ، گام منطقی بعدی در توسعه رمز ارزها باشند. در ادامه به بررسی رمز ارزهایی پرداخته می‌شود که به سمت استفاده از این راه‌حل حرکت کرده‌اند [۱].

^۱ Lightning Network

بیت کوین و شبکه لایتنینگ

شبکه لایتنینگ همچنان در ابتدای راه قرار دارد و به طور کامل عملیاتی نشده است. با این وجود، شبکه تست آن از دسامبر سال ۲۰۱۷ در دسترس عموم قرار دارد. نسخه بتای این شبکه در ۱۵ ماه مارس بر روی شبکه اصلی بیت کوین راه اندازی شد. این نسخه Lightning Daemon (Ind) نام دارد و توسط Lightning Labs توسعه داده شده است. Lightning Labs تنها استارت‌آپی نیست که بر روی شبکه لایتنینگ کار می‌کند. شرکت‌هایی مانند Blockstream و ACINQ نیز بر روی نسخه‌های دیگری از این شبکه کار می‌کنند. بنابراین، با وجود اینکه هر سه پیاده‌سازی انجام شده می‌توانند برای ارسال و دریافت بیت کوین مورد استفاده قرار گیرند ولی نسخه کاملاً روان و کاربرپسند شبکه لایتنینگ بیت کوین هنوز منتشر نشده است.

جزئیات مربوط به شبکه لایتنینگ به طور کامل منتشر شده است که به توسعه‌دهندگان اجازه می‌دهد تا کار بر روی کاربردها و دیگر پیاده‌سازی‌های این شبکه را ادامه دهند. مهم‌تر اینکه، کیف پول نسخه‌های بتای پیاده‌سازی شده در دسترس عموم قرار دارد و توسط جامعه بیت کوین مورد استفاده قرار می‌گیرد. Zap, Lightning-app, HTLC و Zap و Eclair از جمله مهم‌ترین کیف‌های پول شبکه لایتنینگ بیت کوین می‌باشند که امکان انجام تراکنش از طریق این شبکه را در اختیار علاقه‌مندان قرار می‌دهند.



لایت کوین و شبکه لایتینینگ

مقیاس پذیری یکی از رایج ترین چالش های پیش روی اکثر رمز ارزهاست و لایت کوین^۱ نیز از این موضوع مستثنی نیست. لایت کوین همواره یکی از رقبای مستقیم بیت کوین بوده است که هزینه تراکنش ۰,۴ دلاری آن از جمله نقاط قوت این رمز ارز به شمار می رود. با این وجود، این مزیت لایت کوین با راه اندازی شبکه لایتینینگ بیت کوین از یک مزیت به یک نقطه ضعف بزرگ تبدیل خواهد شد. بنابراین فعالیت آلت کوین ها در زمینه شبکه لایتینینگ یا دیگر شبکه های نظیر آن تعجب برانگیز نیست و لایت کوین از فعال ترین پروژه ها در این زمینه به شمار می رود. در واقع، نسخه ای از شبکه لایتینینگ که توسط Lightning Labs پیاده سازی شده بود، هم بر روی بلاک چین بیت کوین و هم بر روی بلاک چین لایت کوین راه اندازی شده است.

علاوه بر این، Lightning Labs در نوامبر سال ۲۰۱۷ اعلام کرد که تست های اولیه در مورد مبادله تجزیه ناپذیر^۲ توکن ها در بین چندین شبکه بلاک چین موفقیت آمیز بوده است. مبادله تجزیه ناپذیر روشی برای تبادل فوری توکن در بین شبکه های بلاک چین منتخب است. انتظار می رود راه اندازی شبکه لایتینینگ لایت کوین نقش ویژه ای در پذیرش هر چه بیشتر این رمز ارز داشته باشد.

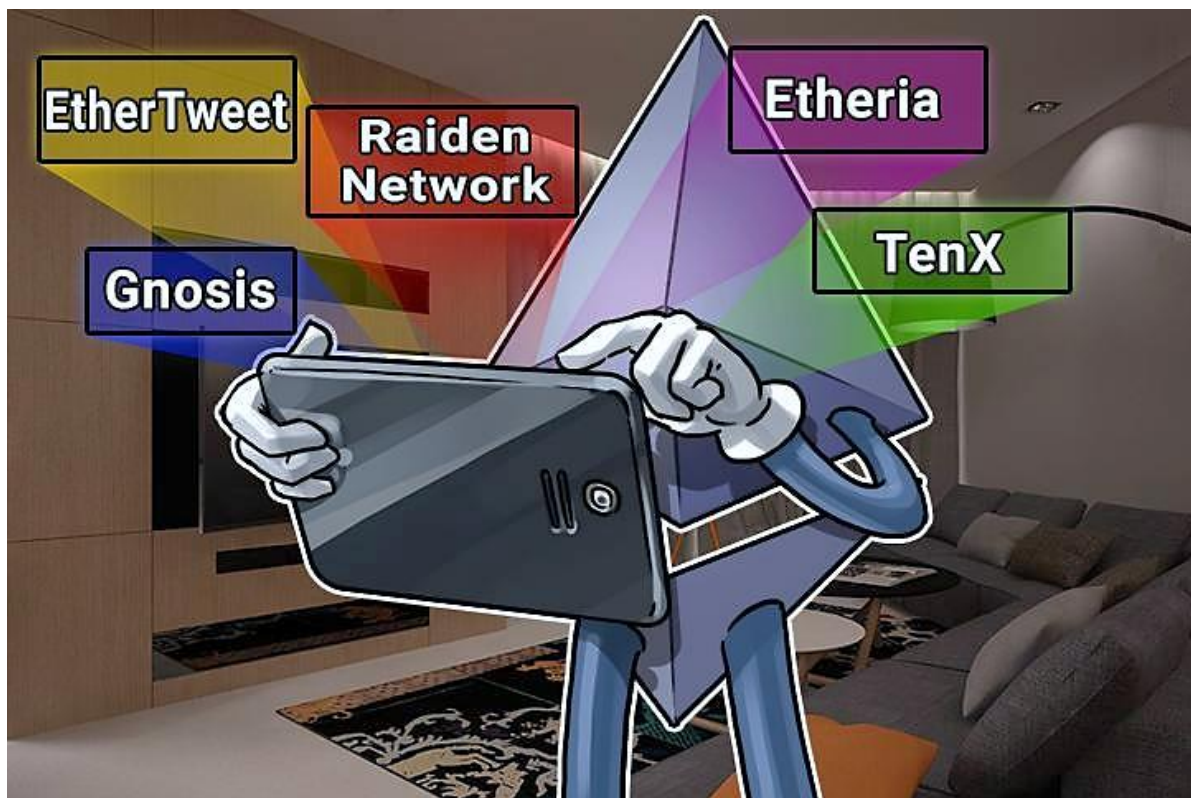
اتریوم و شبکه Raiden

شبکه اتریوم از نظر پردازش تعداد تراکنش در ثانیه وضعیت بهتری نسبت به بیت کوین دارد. این شبکه می تواند تا ۲۰ تراکنش را در هر ثانیه پردازش نماید که تقریباً سه برابر شبکه بیت کوین است. با این وجود، تعداد تراکنش های شبکه اتریوم با توجه به کاربردهای متعدد آن مانند برنامه های کاربردی توزیع شده و امکان ارائه عرضه اولیه سکه^۳ (ICO) بسیار بیشتر از شبکه بیت کوین است. اکثریت ICO های دنیای رمز ارزها بر روی شبکه اتریوم راه اندازی می شوند که با حجم عظیمی از تراکنش های مربوط به فروش توکن، کندی کل شبکه را در پی خواهند داشت. بنابراین حرکت شبکه اتریوم به سمت یک راه حل مقیاس پذیر اجتناب ناپذیر است. جامعه اتریوم چندین راه حل برای این مشکل ارائه کرده است که Raiden از قابل توجه ترین آن ها می باشد.

^۱ Litecoin

^۲ Atomic Swap

^۳ Initial Coin Offerings (ICOs)



مفهوم Raiden شباهت بسیار زیادی به لایتنینگ دارد. Raiden نیز یک لایه خارج از بلاکچین اصلی ایجاد می‌کند. کاربران در لایه جدید می‌توانند کانال‌های دوطرفه برای انجام تراکنش‌های فوری، تقریباً رایگان و ایمن ایجاد کنند. سازگاری با ERC20 یکی از مهم‌ترین مزیت‌های Raiden است چراکه امکان استفاده از تمامی توکن‌های صادرشده بر بستر اتریوم را فراهم می‌نماید.

Raiden از سپتامبر سال ۲۰۱۷ در شبکه تست اتریوم راه‌اندازی شده است. نسخه سبکی از این پروتکل با عنوان μ Raiden در ماه دسامبر همان سال بر روی شبکه اصلی اتریوم پیاده‌سازی شد. μ Raiden نیز امکان انجام تراکنش‌های سریع، بدون نیاز به اعتماد و رایگان را فراهم می‌نماید. با این وجود، پروتکل اصلی Raiden برای مدیریت شبکه‌ای از کانال‌های دوطرفه طراحی شده است درحالی‌که μ Raiden تنها امکان ایجاد کانال‌های پرداخت توسط کاربران و انتقال مستقیم توکن در یکی از آن‌ها را فراهم می‌کند [۱].

BOLT و شبکه ZCash

شبکه لایتنینگ تراکنش‌های تمامی بلاکچین‌های شفاف مانند بیت‌کوین را کمی محرمانه‌تر و خصوصی‌تر خواهد کرد چراکه اطلاعات تراکنش‌های مربوط به پرداخت‌های خرد انجام‌شده در کانال‌های دوطرفه در تمامی شبکه پخش نخواهد شد. با این وجود، باز و بسته شدن کانال باعث می‌شود تا سوابق مربوط به طرفین شرکت‌کننده و همچنین مقادیر اولیه و نهایی منابع مالی ثبت شود. ZCash شبکه رمز ارزی است که با هدف فراهم آوردن حریم خصوصی و

ناشناسی به مشتریان خود ارائه شده است؛ بنابراین این شبکه برای بهبود مقیاس پذیری بلاک چین خود مجبور بود تا راه حل خود را توسعه دهد. لایه اضافه تر پیشنهاد شده توسط این رمز ارز BOLT نام دارد و به طور کامل از شبکه لایتنینگ الهام گرفته است.



غیرقابل پیوند^۱ بودن تراکنش های انجام شده مهم ترین تفاوت BOLT با شبکه لایتنینگ است. BOLT این کار را با بهره گیری از دو تکنیک کلاسیک رمزنگاری با نام Commitment و امضاء انجام داده است. Commitment برای پنهان کردن مقادیر پرداخت شده و امضاء برای امضای تراکنش ها بدون نیاز به افشای ماهیت اصلی آن ها مورد استفاده قرار می گیرد.

توسعه دهندگان BIOT مدعی شده اند که این شبکه به شرط تأمین الزامات رمزنگاری مورد استفاده می تواند برای هر رمز ارزی استفاده شود. با این وجود، ماینرها معتقدند که این شبکه از کارایی بیشتری برای رمز ارزهای ناشناس مانند ZCash برخوردار است [۲، ۳].

ریپل و شبکه لایتنینگ

ریپل با توجه به طراحی آن برای داشتن قدرت بالای پردازش تراکنش نیازی به لایه اضافه تر ندارد. این شبکه با تکیه به توانایی بالقوه برای پردازش ۱۵۰۰ تراکنش در هر ثانیه حتی مدعی است که می تواند با پلتفرم های پذیرفته شده ای مانند ویزا نیز رقابت کند. با این وجود، ریپل در ماه آگوست ۲۰۱۷ با همکاری Bitfury کدی را منتشر کرد که شبکه لایتنینگ را با Interledger یکپارچه می نمود. Interledger پروتکلی است که توسط ریپل برای ایجاد امکان انجام تراکنش در بین بلاک چین های مختلف توسعه داده شده است. از قرار معلوم، ریپل به شبکه لایتنینگ به

^۱ Unlikable

عنوان راهی برای گسترش ظرفیت شبکه نگاه نمی‌کند بلکه در تلاش است تا از خاصیت مبادله تجزیه‌ناپذیر آن استفاده نماید و گامی دیگر به سمت سازگاری رمز ارزهای مختلف بردارد [۱].



این یک تحول بسیار مهیج است چراکه Interledger پیش از این نه تنها قادر به انجام تراکنش‌های شگفت‌انگیز بین بلاک‌چین‌های عمومی بود بلکه شبکه‌های خصوصی و مهم‌تر از همه، سیستم‌های پرداخت سنتی مانند PayPal را نیز پوشش می‌داد. ریپل در تلاش است با ترکیب این دو فناوری امکان دادوستد بدون مشکل مابین رمز ارزهای مختلف و ارسال منابع مالی به هر بلاک‌چین دلخواه از سیستم‌هایی مانند PayPal، Alipay، حساب‌های بانکی و بالعکس را فراهم نماید.

مونرو و شبکه لایتنینگ

مونرو یکی دیگر از رمز ارزهای با محوریت حریم خصوصی است بنابراین پیاده‌سازی کامل شبکه لایتنینگ کارایی چندانی برای آن نخواهد داشت. با این وجود، تیم توسعه‌دهنده مونرو به دنبال اضافه کردن لایه دوم به شبکه این رمز ارز است و لایتنینگ یکی از بهترین گزینه‌های در دسترس است. زیرساخت‌های مورد نیاز برای عملیات شبکه لایتنینگ مانند چند امضایی در بلاک‌چین مونرو وجود دارد. با این حال، تیم توسعه‌دهنده باید تغییراتی در پروتکل شبکه لایتنینگ ایجاد کند تا الزامات حریم خصوصی مونرو را برآورده سازد.

مونرو به جای بهبود مقیاس‌پذیری بیشتر تمرکز خود را بر روی ویژگی مبادله تجزیه‌ناپذیر شبکه لایتنینگ گذاشته است. مونرو در حال حرکت به سمت اندازه بلوک پویا است و این ویژگی می‌تواند مقیاس‌پذیری مد نظر جامعه آن را تأمین نماید [۱].

نئو و شبکه Trinity

نئو از نظر ارائه پلتفرم بلاک چین به عنوان سرویس شباهت بسیار زیادی به اتریوم دارد. کاربران با استفاده از این پلتفرم‌ها می‌توانند برنامه‌های کاربردی توزیع شده و قراردادهای هوشمند را اجرا کرده و ICO راه‌اندازی نمایند. بنابراین نئو نیز مانند اتریوم به پلتفرمی برای راه‌حل‌های اختصاصی خارج از زنجیره^۱ نیاز دارد که آنرا Trinity نامیده است. کار بر روی Trinity همچنان ادامه دارد و در اصل با توجه به توانایی پردازش ۱۰۰۰ تراکنش در هر ثانیه توسط بلاک چین نئو در آینده‌ی نزدیک به آن نیازی وجود نخواهد داشت.

Trinity، Raiden و شبکه لایتنینگ به یکدیگر شباهت بسیار بالایی دارند. تمامی این پروتکل‌های لایه دوم تلاش می‌کنند تا پرداخت‌ها را از بلاک چین اصلی به کانال‌های ایجاد شده توسط کاربر منتقل کنند. این کانال‌ها در پروتکل Trinity با عنوان State Channels شناخته می‌شوند. تنها تفاوت عمده این سه پروتکل در فناوری پایه‌ای مورد استفاده در آن‌ها است چراکه باید به بلاک چین‌هایی که دارای تفاوت‌های چشم‌گیر در طراحی هستند اعمال شوند [۴].

استلار و شبکه لایتنینگ

استلار از شبکه‌هایی است که می‌تواند تا ۱۰۰۰ تراکنش را در هر ثانیه پردازش نماید و مقیاس‌پذیری خود را به راحتی گسترش دهد. با این وجود استلار در تلاش است تا از اولین رمز ارزهایی باشد که با شبکه لایتنینگ یکپارچه می‌شود. علی‌رغم عدم نیاز استلار به گسترش قابلیت‌های خود، یکپارچه‌سازی آن با شبکه لایتنینگ می‌تواند بهبود مقیاس‌پذیری، حریم خصوصی و همکاری متقابل آن با دیگر رمز ارزها را به همراه داشته باشد. کانال‌های ایجاد شده توسط کاربر در این شبکه با عنوان State Channels شناخته می‌شوند [۵، ۶].

^۱ Off-chain

- [۱] CoinTelegraph, “Altcoins With Lightning Network Support,” CoinTelegraph, 2019 . . Available: <https://cointelegraph.com/lightning-network-101/altcoins-with-lightning-network-support#stellar-and-lightning-network>.۲۰۱۹ .
- [۲] I. Miers, “BOLT: Private Payment Channels,” Electric Coin Co, 2016 . .Available: <https://electriccoin.co/blog/bolt-private-payment-channels>.۲۰۱۹ ./
- [۳] J. Fargharson, “Lightning Network For Zcash? BOLT Labs To Create Private Scaling Solution,” CryptoBriefing, 2019 . .Available: <https://cryptobriefing.com/lightning-network-for-zcash-bolt-labs-to-create-private-scaling-solution>.۲۰۱۹ ./
- [۴] pandorasbox, “⚡ Trinity: Lightning network for the NEO blockchain!! ⚡,” steemit, 2017 . .Available: <https://steemit.com/cryptocurrency/@pandorasbox/trinity-lightning-network-for-the-neo-blockchain>.۲۰۱۹ .
- [۵] Stellar Development Foundation, “Lightning on Stellar: Technical Spec and Roadmap,” Stellar, 2018 . .Available: <https://www.stellar.org/developers/blog/lightning-on-stellar-roadmap>.۲۰۱۹ ./
- [۶] ProofofResearch (Editor), “Why is Stellar Implementing the Lightning Network?,” ZeroNoncense, 2018 . .Available: <https://blog.zerononcense.com/2018/10/30/why-is-stellar-implementing-the-lightning-network>.۲۰۱۹ ./

کوین ایران اولین و بزرگ‌ترین پایگاه خبری فارسی زبان در حوزه فناوری بلاک‌چین، رمز ارزها و پلتفرم‌های مرتبط با بلاک‌چین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیلود و آرش محبوب، با هدف اطلاع‌رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه‌مند به رمز ارزها راه‌اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید. هدف کوین ایران از معرفی این فناوری، ایجاد محیط پویای پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به ایرانیان است.

<https://coiniran.com>

نویسنده: تورج اکبری

آدرس ایمیل: turaj.akbati68@yahoo.com

