مقیاس پذیری زنجیره بلوک برای پرداخت های خرد
Block Chain Scalability for Micro Payments

عماد ایرانی، معاونت فنی شرکت فناوران ایمن شبکه فاش، e.irani@faash.ir

{پرداخت های خرد، پرداخت هوشمند، زنجیره بلوک، توسعه پذیری، مقیاس پذیری، پرداخت هوشمند، پرداخت سریع، توزیع شدگی، فناوری مالی، فناوری پرداخت، پرداخت الکترونیک، بلاک چین}

چکیده

زنجیره بلوک و فناوری‌های مرتبط با آن در سالهای اخیر بسیار مورد توجه قرار گرفته اند. در بخشهای مالی و خدمات بانکی و پرداخت های الکترونیک، به دلیل نزدیکی بیشتر به این فناوری، توجه بیشتری به این حوزه جلب شده است. یکی از بخشهای مهم و تاثیرگزار در پرداخت‌های فرد به فرد در جوامع امروزی، پرداخت‌های خرد با رقم های کم و تعداد بسیار بالا می باشد. این تراکنشها معمولا به ازای دریافت خدمات روزمره یا خریدهای خرد انجام می شوند و معمولا بین افراد یا افراد و پذیرندگان اصناف شکل می‌گیرند.

استفاده از زنجیره بلوک برای مدیریت این قبیل تراکنشها سوالاتی را در ذهن ایجاد می‌نماید که در این مقاله سعی شده است به این سوالات پاسخ داده شود و راه‌کارهای مرتبط با این حوزه، مورد بررسی واقع گردند.

مقدمه

پرداخت‌های خرد روزانه حجم عمده‌ای از تراکنش‌های مالی را در سطح کشور به خود اختصاص می‌دهند. این تراکنش‌ها با وجود مبالغ بسیار کم، عمدتا جهت پرداخت‌های روزانه استفاده می شوند و از نظر تعدادی بسیار زیاد هستند. پیش بینی می-شود در طی یک روز در کشور بیش از ۲۰۰ میلیون تراکنش خرد در حال وقوع می باشد که بخشی از آن به صورت الکترونیکی صورت می پذیرد. این تراکنش‌ها عمدتا به دلیل عدم وجود نظام پرداخت خرد، بر روی شبکه شاپرک انجام می

شوند و به همین دلیل پرداخت کنندگان کارمزد از انجام این قبیل تراکنش‌ها رضایت ندارند.

باقی تراکنش‌های خرد از طریق شبکه های برونخط یا به صورت نقدی در بین افراد جامعه در حال انجام است که رقم قابل توجهی نیز به شمار می‌رود.

زنجیره بلوک به عنوان یک فناوری نوظهور راه‌کارهایی را در زمینه پرداخت‌های الکترونیک ایجاد نموده‌است که شامل پرداخت‌های بزرگ و متوسط می باشند. مهمترین اشکال وارده به شبکه‌های مبتنی بر زنجیره بلوک، عدم مقیاس پذیری آنها در حجم بالا و همچنین نیازمندی به منابع پردازشی بسیار انبوه است و این نکته باعث شده است تا استفاده از این فناوری در حوزه پرداخت‌های خرد جلوه ویژه ای به خود نگیرد.

در این مقاله سعی داریم با بررسی نظام پرداخت خرد و نیازمندی‌های آن، بررسی نماییم آیا زنجیره بلوک توانایی انطباق با این نیازمندی‌ها را دارد یا خیر و راه‌کار آن به چه شکل خواهد بود و در مقایسه با مدل‌های سنتی خدمت رسانی بر روی سرویس دهنده‌های مرکزی، نظام‌های منطبق بر زنجیره بلوک چه جایگاهی را دارا می‌باشند.

همچنین در این مقاله سعی شده است، حضور یا عدم حضور زنجیره بلوک به دلیل نیازمندی به حجم بالای منابع پردازشی و ذخیره‌سازی در نظام پرداخت خرد مورد بحث قرارگیرد و بر اساس نیازسنجی صورت گرفته تحلیل گردد که آیا پرداخت‌های خرد ارزش راه‌اندازی یک نظام مبتنی بر زنجیره بلوک را دارند یا خیر. در این حوزه با رویکرد تحلیلی به تراکنش‌های پرداخت خرد توجه ویژه‌ای صورت گرفته است و نیازمندی به زنجیره بلوک نه تنها صرفا به عنوان یک فناوری بلکه به عنوان یک راه‌کار برای ذخیره‌سازی تراکنش های خرد مورد واکاوی قرارداده شده است.

در انتها سعی شده است بر اساس نتایج کسب شده، و بررسی راه‌کارهای زنجیره بلوک برای شبکه‌هایی با تراکنش بالا، مقیاس پذیری و دردسترس بودن این فناوری مورد بحث واقع شود.

استفاده از فناوری‌های نوین در زمینه‌هایی که نیازمندی به آنها وجود دارد همواره راه‌کاری برای افزایش راندمان، کاهش خطا، افزایش دسترسی پذیری و استحکام سامانه‌های پرداخت الکترونیک بوده است. نگاه معکوس به این فرآیند یعنی تغییر در سامانه‌های پرداخت الکترونیک به منظور همخوانی با یک فناوری نوظهور گاها کل نظام پرداختی را با مشکلاتی روبرو کرده که در برخی از نمونه‌ها امکان بازگشت و بازسازی به صورت کامل از بین رفته است.

سامانه‌های نرم افزاری و سخت افزاری امروزه در زمینه پرداخت‌های الکترونیک با مقیاس بالا به توانمندی ویژه ای دست پیدا کرده‌اند. این توانمندی در زمینه‌های پایداری، مقیاس پذیری، اطمینان پذیری، امنیت، دسترسی پذیری و سایر حوزه‌ها تعریف شده‌است و تغییر آنها به مدلهای کاملا جدید و متفاوت بر اساس فناوریهای نوین، نیازمند تحلیل دقیق و پایه‌ای بر روی کلیه حوزه‌های ذکرشده می باشد.

ادبیات موضوع

اولین استفاده از زنجیره بلوک، در حوزه رمز ارزها[1] شکل گرفته است. این موضوع خود نمایان دو مطلب است که اولا این فناوری نگاه بسیار ویژه ای به بخش مالی داشته و دوم آنکه جذابیت ایجاد شده برای محققان و کارشناسان در سطح جهان بیشتر به دلیل منافع مالی حاصل شده از فعالیت در زمینه مالی بوده است. البته زنجیره بلوک به صورت خاص، ارتباطی با

[1] Crypto Currency

فناوری مالی ندارد می تواند در هرجایی که رشته‌ای از اطلاعات در زمان‌های مختلف تولید می‌گردند و نگهداری و استفاده از آنها بر منافع جمعی گروهی از افراد تاثیر گذار است، استفاده گردد.

در سالهای اولیه، تمرکز بیشتر بر روی پایداری، امنیت و توسعه پذیری زنجیره بلوک بوده است و دور از ذهن نیست که این تمرکز در ابتدای امر که توجهات بیشتر به پایداری این فناوری بوده، به درستی صورت گرفته است.

اما در ادامه، زمانی که تعداد زیادی از محققان جذب فناوری نوپای زنجیره بلوک شدند، و اعتماد ایشان به پایداری و امنیت این فناروی ایجاد گردید، بخش دوم رشد فناوری زنجیره بلوک شروع شد و آن چیزی نیست به جز استفاده پذیری.

در این زمان، بیشتر فعالیتها در حوزه تعریف سرویس های جدید بر روی داشته های قبلی معطوف گردید. البته گروهی نیز به صورت موازی در حال بررسی فرآیندهای جدید امنیتی، روشهای جلوگیری از تقلب و کاهش هزینه‌های اجرایی زنجیره بلوک، ایجاد الگوریتم‌های جدید اجماع[1] و سایر بخشهای مرتبط با این فناوری بوده‌اند.

برخلاف تصورات شکل گرفته در رابطه با زنجیره بلوک، استفاده از این فناوری نه تنها به کاهش هزینه کمک نخواهد نمود بلکه در اکثر حالات با افزایش هزینه منابع روبرو هستیم. دلیل این موضوع ماهیت توزیع شدگی و گستردگی شبکه‌های زنجیره بلوک می باشد که افراد می بایستی برای اتصال و استفاده از داده‌های زنجیره بلوک خاص، حتما دارای فضای کافی اطلاعات و منابع کامل پردازشی باشند. البته در شبکه های بزرگتر و جا افتاده، بسیاری از خدمات ذکر شده به صورت PaaS به مشتریان ارائه می گردد، اما مراکز ارائه دهنده همین خدمات با هزینه های بسیار زیادی به جهت حفظ سرویس و امنیت آن روبرو هستند.

بعد از گذشت سالهای اولیه از استفاده زنجیره بلوک در فناوریهای مالی، توجه بسیاری از کارشناسان به این حوزه جلب گردید که آیا امکان استفاده از زنجیره بلوک در پرداخت‌های خرد وجود دارد؟ پرداخت‌های خرد چندین مشخصه اصلی دارند:

- رقم بسیار کم نسبت به تراکنش های عادی بانکی
- کم ارزش از نظر منابع مالی (برای موسسات مالی و بانکها)
- تعداد بسیار زیاد در بازه زمانی کم
- نیازمندی به سرعت بالا جهت پردازش (به دلیل اینکه عموما به صورت C2C صورت می پذیرند)

در بخشهای بعدی سعی می کنیم، با بررسی و تحقیق در مورد مدلهای پیاده شده در بستر زنجیره بلوک آماده بودن آنها جهت استفاده در پرداخت های خرد را بسنجیم و برای مشخصه های معرفی شده در پرداخت‌های خرد پاسخ مناسبی را ارائه نماییم.

روش تحقیق

[1] Consensus

یکی از مزایای فناوری زنجیره بلوک، استانداردسازی اولیه به صورت De facto بوده است. تمام افرادی که در این حوزه فعالیت می کنند ناخواسته از قوانینی نانوشته تبعیت می‌کنند که دسترسی به اطلاعات مورد نیاز را به راحتی برای همه افراد ایجاد می نماید. برخی از این قوانین نانوشته که در زمینه این تحقیق بسیار موثر بوده اند عبارتند از:

- افرادی که بر اساس یک ایده اولیه اقدام به راه اندازی یک زنجیره بلوک جدید می‌نمایند، روش خود را در یک مستند White Paper به سایرین منتقل می کنند. البته زنجیره‌های بلوک خصوصی با الگوریتم‌های مخفی نیز وجود دارد که به طور حتم توسط جامعه آزاد پس زده می‌شوند و در نهایت تبدیل به یک نظام خصوصی متمرکز خواهند شد.
- سرویس دهنده‌های آنها به صورت بازمتن وجود دارد و کلیه کدهای منبع قابل دریافت و مشاهده هستند. دلیل این موضوع نیز مانند بخش اول، عدم اعتماد جامعه به سرویس دهنده هایی بدون وجود کد منبع می باشد. صرفا نمونه-هایی موفق می‌شوند که بتوانند امنیت کافی را به سایرین اثبات نمایند و این اثبات راهی جز در اختیار قراردادن کدهای منبع در محل‌های عمومی قابل دسترس نخواهد داشت.
- چه افراد حقیقی و چه افراد حقوقی که اقدام به تولید یک طرح جدید می نمایند در انجمن‌های اینترنتی و Mailing Listها پاسخگوی سوالات، ابهامات، ایرادات، انتقادات و پیشنهادات هستند و طرحهایی که توسط شرکتهای بسیار بزرگ بدون پاسخگویی به کارشناسان ایجاد گردند اتفاقا شانس بسیار کمتری در موفقیت دارند و طرحهایی که تا کنون موفق شده اند و توسط بیش از میلیون‌ها نفر مورد استفاده واقع شده اند، گاها توسط یک نفر با رعایت کلیه اصول ذکر شده در بالا، ایجاد شده اند.
- با توجه به تعدد سرویس‌های این حوزه، تولیدکنندگان و طراحان شبکه‌های مبتنی بر زنجیره بلوک، خود اقدام به معرفی، تفاوت سنجی و مقایسه طرح خود با سایر طرحهای مشابه می‌نمایند و بر خلاف محصولات تجاری که همواره با تبلیغات رنگین و توضیحات عامه پسند ارائه می گردند، طرحهای ارائه شده در این حوزه در صورتی که دارای برتری‌های علمی و ثابت شده نسبت به طرحهای مشابه نباشند حتما در زمان کوتاهی حذف خواهند شد و از بین خواهند رفت. برای همین موضوع توضیحات ارائه شده توسط طراحان همواره دارای کیفیت کافی برای پاسخگویی به سوالات هستند.

همانطور که دقت کردید هیچکدام از توضیحات بالا در هیچ قانونی مستند نشده است اما همانطور که عنوان شد این قوانین نانوشته در صورتی که رعایت نشوند باعث تخریب و از بین رفتن موضوع خواهند شد و به همین دلیل همواره توسط طراحان شبکه های مبتنی بر زنجیره بلوک رعایت می گردند.

در این مقاله سعی شده است، نمونه‌هایی از زنجیره بلوک مورد بررسی قرار گیرند که خود آنها در زمینه سرعت، امنیت، هزینه، دسترسی پذیری و مقیاس پذیری تفاوت‌هایی را برای خود قائل هستند و خود را آماده بهره برداری در این حوزه می‌دانند.

همچنین در این تحقیق سعی شده است، مسائل مرتبط با پرداخت های خرد در کشور ایران نیز در تصمیم گیری‌ها و نتیجه گیری‌ها تاثیرگذار باشند. این مسائل عبارتند از موضوعات فرهنگی، موضوعات فنی، موارد قانونی بانک مرکزی جمهوری اسلامی ایران، موضوعات اجتماعی مانند اعتماد پذیری، موضوعات تجاری و ...

بررسی پرداخت های خرد

قبل از بررسی سرویس دهنده های مبتنی بر زنجیره بلوک در زمینه پرداخت‌های خرد، در این بخش کلیات مورد نیاز در مورد این قبیل پرداخت‌ها مورد بررسی واقع شده است. در این قسمت سعی شده، تا با موشکافی دقیق صنعت پرداخت در کشور و به طور خاص پرداخت‌های خرد، مطالعه کنندگان با یک ادبیات یکسان در این زمینه به خواندن ادامه مقاله اهتمام ورزند.

در حال حاضر پرداخت های خرد به صورت نقدی یا الکترونیکی صورت می پذیرند. بخش نقدی پرداخت‌های خرد توسط سکه یا اسکناس انجام می‌شود. در سالهای اخیر به دلیل افزایش تورم و عدم در اختیار داشتن پول خرد مورد نیاز توسط افراد، حجم عمده‌ای از تراکنش های خرد به سمت شبکه شاپرک منتقل شده اند تا جایی که بیش از ۹۰٪ از تراکنش های این شبکه زیر ۲,۰۰۰,۰۰۰ ریال صورت می پذیرند[2].

در بخش الکترونیکی به جز شبکه شاپرک، سرویس دهنده‌های خصوصی نیز به صورت مسیر-بسته[1] فعالیت می کنند که حجم عمده‌ای از تراکنش ها را پوشش نمی‌دهند.

در حوزه‌های خدمات شهری و سرویس‌های مرتبط با حمل و نقل مسافر، به دلیل نیازمندی به زمان کوتاه تراکنش، اکثرا از روشهای پرداخت برون‌خط با کارتهای هوشمند یا کارت‌های بلیت استفاده صورت می پذیرد. دلیل استفاده از شبکه‌های برون خط در این سرویس ها عبارتند از:

- کاهش هزینه های اجرایی از جمله شبکه و هزینه های کارمزدی
- افزایش سرعت تراکنش در لحظه
- کاهش وابستگی به شبکه‌های ارتباطی به دلیل عدم پایداری آنها و سرویس دهی در تمامی حالات
- افزایش امنیت مشتریان و ایجاد قابلیت محافظت از منابع مالی ایشان

در تمامی روشهای پرداخت ذکر شده در بالا، شامل نقدی، شاپرکی، برخط خصوصی و برونخط یک هدف اصلی دنبال می‌گردد و آن انتقال هزینه یک خدمت از یک فرد به فردی دیگر است تا خدمت یا کالا بر اساس ارزش ارائه شده به نفر اول ارائه گردد. در این تعریف مهمترین بخش همان انتقال هزینه و ارزش از نفر اول به نفر دوم است به صورتی که نفر دوم که همان ارائه دهنده خدمت یا کالا است اطمینان حاصل کند که ارزش ریالی مورد انتظار توسط ایشان دریافت شده است و توسط فرد اول غیر قابل بازگشت خواهد بود و بر اساس توافق صورت گرفته اولیه به همان میزان ارزش یا متفاوت با میزان اولیه(مثلا بر اساس کسر کارمزد شبکه)، منابع مالی به حساب بانکی ایشان منتقل خواهد گردید.

ایجاد این اطمینان در افراد جامعه به راحتی صورت نمی پذیرد و مخصوصا در زمانهایی که سرویس‌دهنده‌های یک فناوری خاص به دلیل عدم پیاده سازی صحیح و یا مشکلات و خطاهای فردی به صورت عمد یا غیر عمد خسارتی را متوجه پذیرندگان یا طرف‌های دوم می نمایند، بازسازی اعتماد در بین آنها با سختی و زمان بسیار زیادی صورت می پذیرد.

در مورد استفاده از فناوری های مالی در کشور، مردم به دلیل وجود نام بانک مرکزی و یا بانکهای تجاری در کلیه عملیات،

[1] Closed Loop

کمی راحت تر به روش پرداخت اعتماد می نمایند اما در مورد سایر روشهای پرداخت که نام بانک یا شبکه مالی معتبر در آن دخیل نباشد کمی با تردید عمل می کنند. البته تجربه نشان داده است، این عدم اعتماد به راحتی با یک عامل سازنده از بین می رود و آن سوددهی یا منفعت پذیری عامل خاص است.

برای مثال گاها مشاهده شده است که افراد استقبال چندانی به یک فناوری جدید مالی (برای مثال بیت کوین بر روی زنجیر بلوک) نشان نمی دهند. اما زمانی که متوجه می شوند در نزدیکی آنها یک دوست، یکی از اقوام یا همکاران اقدام به فعالیت در آن سرویس نموده‌است و سود سرشاری را برای خود جذب کرده است، فارغ از موضوعات امنیتی و توجه به سرویس خاص اقدام به فعالیت در آن می‌نماید و در این زمان سوددهی یا همان منفعت پذیری بر سایر المان های جلوگیری کننده مانند عدم اعتماد پذیری، عدم تمایل مردم به فناوری‌های نوین مانند کارت یا تلفن همراه، عدم دسترسی به اینترنت و سایر مشکلات چیره خواهد شد. این موضوع، بر اساس یک تجربه اجتماعی با عنوان ترس از عقب ماندن[1] اتفاق می‌افتد و غیر قابل جلوگیری خواهد بود.

در پرداخت‌های خرد یک نکته بسیار اساسی دیگر وجود دارد و آن ارزش گذاری خدمات است. کلیه خدمات خرد در کشور ایران بر اساس ارزش ریال محاسبه می‌گردند. در شبکه‌های پرداخت خرد نیز، در صورت استفاده از هریک از روشهای پرداخت نقدی و الکترونیکی در نهایت ارزش ریالی می بایستی به طرف دوم منتقل گردد. در صورت استفاده از فناوری‌های مالی باید این نکته را مورد توجه قرار داد که سرویس‌دهنده مالی می‌بایستی بر روی بستر ریال فعالیت نماید و کلیه عملیات مالی در آن بر این بستر شکل گیرند.

نکته دیگر در مورد پرداخت‌های خرد، حفظ محرمانگی اطلاعات است. با وجود آنکه عنوان شد این قبیل پرداخت‌ها در شبکه بانکی کم ارزش هستند، اما برای مشتریان محرمانگی جزو اصول اولیه به حساب می آید. برای مثال هیچ‌کدام از مشتریان علاقه مند نیستند که مسیرهای حرکت ایشان در اتوبوس یا مترو برای همه شهروندان قابل مشاهده باشد. به طور حتم ایشان علاقمند نیستند که خریدهای خرد روزانه از سوپرمارکت ها و ... نیز در اختیار همه قرار گیرد. همچنین موضوعات تجاری نیز بر این حوزه حاکم هستند و داده های تولید شده توسط پرداخت های خرد توسط نهادهای مرتبط به شدت محافظت می-گردند و دسترسی به آنها می بایستی با شرایط خاص صورت پذیرد.

ارزهای مجازی مبتنی بر زنجیره بلوک

در این بخش، تعدادی از ارزهای مجازی معروف که در بستر زنجیره بلوک فعالیت می‌کنند به طور خاص در حوزه پرداخت‌های خرد بررسی شده اند:

- بیت کوین (BitCoin)
- لایت کوین (LiteCoin)
- اتریوم (Ethereum)

[1] FOMO – Fear of Missing Out

- استلار (Stellar)
- شبکه لایتنینگ+بیت کوین (Lightning Network + Bitcoin)

بیت کوین

شبکه بیت کوین قدیمی ترین بازیگر صنعت ارزهای مجازی منطبق بر زنجیره بلوک است که منطبق بر POW[1] می باشد. این ارز مجازی حجم زیادی از مشتریان را در بر دارد و اعتماد پذیری به آن بر اساس مدل ارائه شده بسیار بالاست. شبکه بیت کوین صرفا قادر است ۴ تا ۷ تراکنش در ثانیه را جابجا کند[1] که این مقدار برای شبکه‌های پرداخت خرد که حجم زیادی از تراکنش‌ها را در ثانیه جابجا می کند بسیار کم است. همچنین شبکه بیت کوین برای فعالیت نیاز به ارتباط برخط دارد.

لایت کوین

لایت کوین دقیقا به عنوان یک توزیع شده جدا از بیت کوین فعالیت خود را شروع نموده است و کلیه قوانین آن بر اساس بیت کوین تعریف شده. تنها تغییر ایجاد شده در لایت کوین افزایش طول بسته‌ها و کاهش فاصله زمانی بین بلاک‌ها می باشد که در بهترین حالت ۵۶ تراکنش در ثانیه جابجا خواهد شد[5]. با وجود تغییر بسیار زیاد ایجاد شده در این زمینه، بازهم تعداد فوق مناسب اجرای پرداخت‌های خرد نمی باشد.

اتریوم

بعد از بیت کوین، بیشترین توجهات به اتریوم است. اتریوم با ارائه یک مدل جدید از شبکه، با قابلیت تعریف قراردادهای هوشمند، فرآیندها و امکانات جدیدی را به ارزهای مجازی و برنامه‌های توزیع شده مبتنی بر زنجیره بلوک معرفی نمود، اما در رابطه با تعداد تراکنش‌های قابل انجام بر روی این شبکه نیز باید اعلام نمود که اتریوم تنها قادر است ۱۵تا ۲۵ تراکنش را در ثانیه جابجا نماید[3] که دقیقا مانند بیت کوین در رابطه با پرداخت‌های خرد این موضوع مسدود کننده خواهد بود.

استلار

در شبکه استلار، تغییرات عمده‌ای در زمینه تایید تراکنشها و تغییر از POW به مدلهای مبتنی اجماع صورت گرفته است. استلار در اصل یک نسخه تغییر یافته از شبکه ریپل است که در تبادلات بین بانکی در بین شبکه های مبتنی بر زنجیره بلوک نسبت به باقی پیشرو می باشد.

استلار قادر است بین ۲۰۰۰ تا ۴۰۰۰ تراکنش را در بهترین حالت جابجا نماید[4]، که از نظر حجم تراکنشی نسبت به مدل-های پیشین بسیار متفاوت است. استلار کمک میکند تا با تعریف هرگونه ارزش قابل سنجش به واحدهای قابل شمارش، نقل و انتقالات بین افراد صورت پذیرد و در ضمن حضور در این شبکه با توجه به بازمتن بودن آن (برخلاف ریپل) برای همگان انجام پذیر است.

شبکه لایتنینگ به همراه بیت کوین

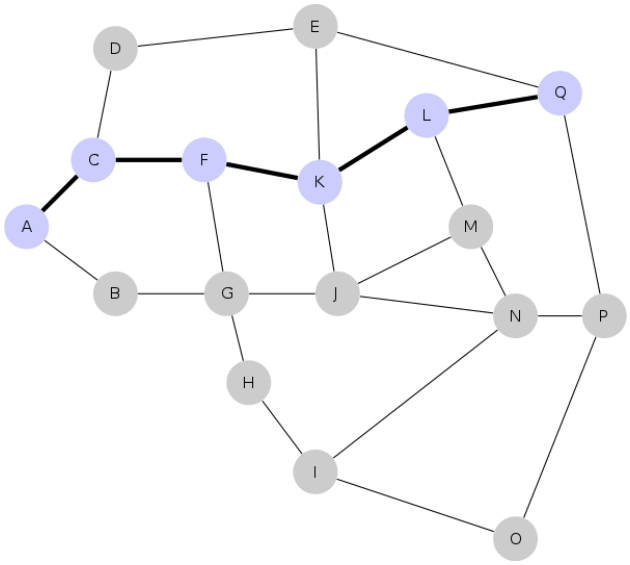
یک طرح بسیار عالی در زمینه تراکنشهای مبتنی بر زنجیره بلوک طی دو سال گذشته ارائه گردید که ترجمه کلمه به کلمه

[1] Proof of Work

آن شبکه رعدآسا است که نشان دهنده سرعت بالای این شبکه در مبادلات می‌باشد.

در شبکه رعدآسا یا همان لایتنینگ، از یک ایده جدید در زمینه افزایش سرعت تراکنشها و خارج کردن آنها از مسیراصلی یا First Layer صورت گرفته است. اصطلاحا تراکنش های لایتنینگ در لایه فرعی انجام می‌شوند و طرز کار آنها به صورت ساده به شکل زیر است[6]:

- یک تراکنش پایه در شبکه اصلی انجام می‌پذیرد. در این تراکنش طرفین یا یکی از آنها مبلغی(بر اساس ارز مجازی همان شبکه) را به عنوان پیش پرداخت در یک قرارداد هوشمند بلوکه می کنند. در این شرایط اصطلاحا یک کانال بین دو فرد شکل گرفته است. این مبلغ از طرفین کسر گردیده و به یک قرارداد هوشمند منتقل می‌گردد تا طرفین از وجود وجه کافی به ازای ارائه خدمات به طرف مقابل اطمینان حاصل نمایند.
- طرفین شروع به معامله با یکدیگر می‌نمایند. معاملات خرد صورت گرفته توسط هرکدام از طرفین، در شبکه اصلی ثبت نمی‌گردد و صرفا بر اساس اصول رمزنگاری و به طور خاص امضای دیجیتال طرفین تعهداتی به یکدیگر می-دهند که چه بخشی از مبلغ بلوکه شده به هرکدام از آنها تعلق دارد.
- این تراکنش‌ها به صورت دائم بین طرفین جابجا می‌شود و سطح نهایی آنها آنجاست که کل مبلغ بلوکه شده به یک نفر منتقل شود (برای مثال فردی که خدمتی را به طرف دیگر ارائه میکند و به ازای آن وجهی را دریافت می کند). در این زمان، امکان استفاده از کانال برای طرفین وجود ندارد، مخصوصا در شرایطی که خدمت دهنده تنها یکی از طرفین باشد (مانند خدمت پرداخت خرد اتوبوس و مترو، کافی شاپ، کتاب فروشی و ...). در این شرایط طرفین با رضایت طرف دیگر اقدام به بستن کانال با آخرین تراکنش‌های امضا شده از طرف دیگری می نمایند.
- بستن کانال منجر به انجام یک تراکنش مجدد بر روی لایه اصلی خواهد شد و منابع به نسبت مشخص به حساب اصلی طرفین در همان زنجیره بلوک منتقل می‌گردد.



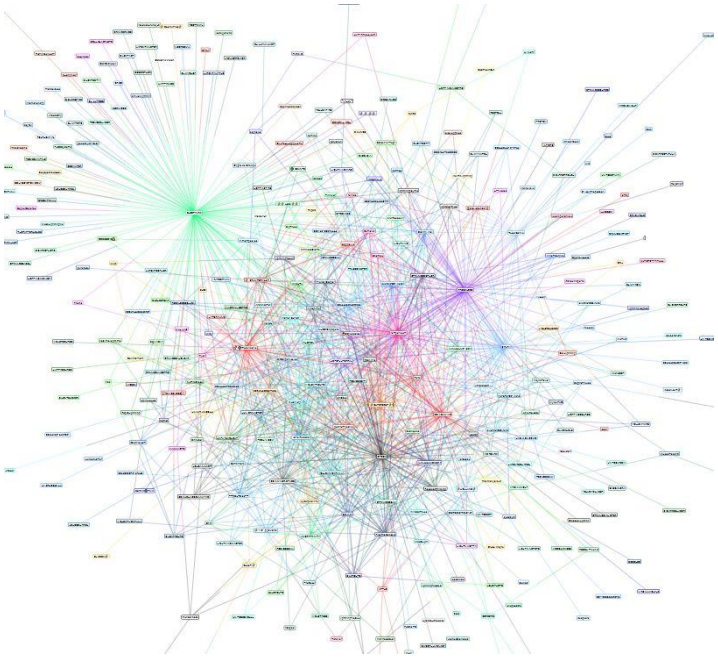
تصویر ۱ - ارتباطات در شبکه لایتنینگ

همانگونه که مشخص شد، در لایتنینگ امکان ایجاد کانال باز بین همه افراد وجود دارد و البته با شرایط ویژه‌ای که در قرارداد

هوشمند مشخص شده است، در صورتی که طرفی اقدام به تخلف نماید و تراکنشهای امضا شده قدیمی خود با طرف دوم را جهت دریافت کل مبلغ به شبکه ارسال نماید طرف دیگر می‌تواند با اثبات وجود تراکنشهای جدید تر جریمه ای معادل کل ارزش کانال به طرف دیگر تحمیل نماید. به همین منظور در زمان بستن کانال توسط یکی از طرفین یک مدت زمان کافی برای اعتراض طرف دیگر در نظر گرفته شده است و در صورتی که طرف دوم هم در همان لحظه اقدام به بستن کانال نماید و اعتراضی نداشته باشد، تراکنش سریعا به عنوان یک تراکنش جدید در زنجیره بلوک ثبت خواهد شد.

با توجه به ماهیت شبکه لایتنینگ و عدم توانایی افراد به پایش لحظه‌ای شبکه جهت جلوگیری از تخلف فرد دیگر، تعدادی پردازشگر به عنوان گره‌های لایتنینگ[1] این وظیفه را برعهده می گیرند و دائما در حال پایش شبکه جهت مدیریت تراکنش-های لایتنینگ هستند. در ضمن در این مدل پیش بینی شده است که افراد بتوانند با افراد ناشناسی که کانال مشترک ندارند، بر اساس کانال‌های میانی مانند (A->B و B->C پس A->C) فعالیت نمایند.

با توجه به تمهیدات چیده شده در شبکه لایتنینگ، می توان عنوان نمود که در این شبکه موضوعی به نام تراکنش در ثانیه یا همان TPS وجود ندارد و میلیون‌ها تراکنش در ثانیه میتواند بین افراد انجام شود که البته استفاده از گره‌های لایتنینگ این تعداد را بسیار کاهش خواهد داد. پس آیا می توان به لایتنینگ بر روی شبکه بیت کوین، به عنوان یک ابزار جهت انجام پرداخت‌های خرد اتکا نمود؟



تصویر ۲ - پردازشگران فعلی در شبکه لایتنینگ

در بخش بعد، شبکه های فعلی مالی بر بستر زنجیره بلوک از زاویه دیگری بررسی خواهند شد و تطبیق پذیری آنها جهت انجام پرداختهای خرد بررسی می گردد.

تطبیق پذیری با پرداخت های خرد

[1] Lightning Nodes

در بخش قبلی، تعدادی از پرطرفدار ترین شبکه های مالی مبتنی بر زنجیره بلوک بررسی شدند، حتی در انتهای بخش از لایتنینگ به عنوان یک جهش فوق‌العاده در زمینه تراکنش های مبتنی بر زنجیره بلوک، با حفظ امنیت و ناشناس بودن و همینطور عدم وابستگی به سرویس دهنده مرکزی صحبتی به میان آمد. اما آیا توان پذیرش تعداد بالای تراکنش تنها موضوع مهم در زمینه پرداخت‌های خرد به شمار می‌رود ؟ در این بخش از زوایای دیگری به موضوع پرداخته خواهد شد و پاسخی به این سوال خواهد بود.

برخط بودن شبکه‌های مبتنی بر زنجیره بلوک

شبکه‌های مبتنی بر زنجیره بلوک برخط هستند. در بسیاری از فرآیندهای پرداخت خرد مخصوصا در پرداخت‌های خرد شهری که سرعت عملیات بسیار مورد نظر است، انجام تراکنشها به صورت برخط نیازمند دراختیار داشتن تجهیزات کافی و دسترسی پذیری به شبکه می باشد که در صورت کندی شبکه یا قطع بودن از آن، خسارات اجتماعی و اعتراض کاربران را در پی خواهد داشت. طراحی و پیاده سازی یک شبکه برونخط مبتنی بر زنجیره بلوک نیز، با توجه به عدم توانایی در جلوگیری از تقلب در زمینه هزینه کرد دوباره[۱] یک مبلغ، بسیار آسیب رسان خواهد بود. البته می توان از زنجیره بلوک برونخط به همراه رسانه‌های هوشمند با قابلیت ذخیره‌سازی کلیدهای امنیتی بهره برد که این موضوع هزینه اجرایی طرح را بسیار افزایش خواهد داد.

سرعت تایید تراکنش

ایراد دیگر در زمینه استفاده از شبکه‌های مبتنی بر زنجیره بلوک، سرعت تایید تراکنش در آنهاست. این زمان بین سه ثانیه تا یک ساعت متغیر است که در بهترین حالت آن یعنی سه ثانیه، ایجاد نارضایتی در بین افراد ایجاد خواهد شد. دو راه کار برای این موضوع شاید پیشنهاد گردد. دریافت تراکنش، بررسی اولیه، تایید خدمت و سپس بررسی آن به صورت داخلی توسط سیستم و اعلام هشدار تراکنش‌های انجام نشده به خدمت دهنده.

در این مدل، فرض می‌کنیم محل خدمت یک اتوبوس با ۴۰ مسافر باشد. در صورتی که افراد تراکنش‌های خود را ثبت کنند و برای مثال ۱۰ ثانیه بعد چند تراکنش با موفقیت انجام نشوند (به دلایل مختلف)، امکان شناسایی افراد توسط راننده وجود نخواهد داشت، زیرا تراکنشها در همان زمان ابتدایی تایید شده اند و راننده اجازه ورود به مسافران داده است و راننده با مشکلات فراوانی روبرو خواهد شد.

روش دیگر به منظور کاهش این زمان، تولید یک شبکه مبتنی بر زنجیره بلوک به صورت خصوصی برای کشور ایران می‌باشد که برای مثال کمتر از یک ثانیه تراکنش‌ها تایید خواهند شد. فارغ از مشکلات اعلام شده در بخش قبلی در رابطه با ارتباطات شبکه‌ای، به علت خاص بودن و خصوصی بودن شبکه تولید شده جدید، عملا اتفاقی که خواهد افتاد تبدیل شبکه زنجیره بلوک به یک سرویس دهنده مرکزی[۲] خواهد بود که با اصول اساسی زنجیره‌بلوک باز، مغایر است.

از طرف دیگر شاید نهادها، شرکتها و افراد خصوصی علاقمند به ایجاد پردازشگر برای این شبکه خصوصی باشند که اشکال دیگری به عنوان کارمزد پردازش عملیات ایجاد خواهد نمود.

کارمزد شبکه های مبتنی بر زنجیره بلوک

[۱] Double Spending Issue

[۲] Centralized Service

شبکه‌های مبتنی بر زنجیره بلوک، فارغ از برخط بودن، زمان پردازش تراکنش، اطمینان پذیری و ... یک ایراد عمومی دیگر برای پرداخت کنندگان خرد ایجاد می‌نمایند و آن کارمزد شبکه است. بسیاری از ارزهای مجازی و شبکه‌های مبتنی بر زنجیره بلوک که به صورت عمومی در دنیا وجود دارند و مورد اطمینان و استقبال همه هستند، به ازای خدمات ارائه شده در شبکه که توسط Minerها یا پردازشگران تصمیم‌گیر در اجماع صورت می‌پذیرد، کارمزدی را دریافت می‌کنند. این کارمزد معمولا به صورت مستقیم به رقم تراکنش مرتبط نیست و با وجود تاثیرپذیری از آن بیشتر بر اساس میزان منابع پردازشی مصرف شده توسط پردازشگر مشخص می‌گردد. برای مثال در شبکه بیت کوین، حجم دیتای تراکنش مشخص کننده کارمزد عرف است و در شبکه اتریوم، میزان توان مورد نیاز برای پردازش قرارداد هوشمند به عنوان مبنای کارمزد در نظر گرفته می‌شود.

در این شرایط، پرداخت‌های خرد که معمولا دارای رقم بسیار کمی هستند، به طور خاص در حوزه حمل و نقل و خریدهای خرد روزانه افراد، در صورت ملزم شدن به پرداخت کارمزد که ممکن است از حجم مالی تراکنش نیز بیشتر باشد، به طور حتم با مشکل روبرو خواهند شد و مشتریان به صورت منطقی از انجام تراکنش با شیوه مربوطه سر باز خواهند زد.

در رابطه با شبکه‌هایی که اقدام به دریافت کارمزد ناچیز می‌کنند نیز، به دلیل عدم استقبال عمومی به پردازش در شبکه، همان اشکال تبدیل به سرویس دهنده مرکزی صورت خواهد پذیرفت که مطمئنا مورد استقبال واقع نخواهد شد.

عدم ثبات ارزشی در ارزهای مجازی

همانطور که عنوان شد، یک ترازو با دو کفه وجود دارد. استفاده از شبکه مبتنی بر زنجیره بلوک عمومی با استقبال و اطمینان بالا و در کفه دیگر، یک شبکه خصوصی با مشخصات و نیازهای پرداخت خرد در کشور و ریسک تبدیل به سرویس دهنده مرکزی.

در صورتی که از کفه اول ترازو استفاده نماییم با مشکلی روبرو خواهیم بود با عنوان ارزش گذاری خدمت. فرض کنید توافقی صورت پذیرد تا افراد با استفاده از شبکه لایتنینگ اقدام به پرداخت هزینه کرایه تاکسی نمایند. برای پذیرنده این تراکنش که همان راننده تاکسی می‌باشد، به طور حتم مهمترین موضوع تبدیل پذیری بیت کوین به ریال است. با فرض وجود تعداد زیادی صرافی در کشور و مجاز بودن این موضوع، در صورت کاهش ارزش بیت کوین طی یک روز، راننده تاکسی با خسارت مالی روبرو خواهد شد و به همین دلیل علاقمندی خود به دریافت کرایه از طریق این شبکه را از دست می‌دهد. با همین منطق در صورتی که مشتریان در طرف دیگر شاهد رشد ارزش بیت کوین باشند، رضایتی به پرداخت هزینه تاکسی با استفاده از یک دارایی با ارزش بالارونده نخواهند داشت.

کفه دوم ترازو، یا حتی استفاده از شبکه‌های کوچکتر خصوصی که اقدام به ایجاد یک سکه ثابت[1] ریالی نمایند، یا شبکه‌هایی مانند استلار با قابلیت تولید سکه برای هرچیزی، در بخشهای قبلی به دلیل سرعت، اطمینان پذیری، کارمزد و ... نقد شدند. در ضمن بانک مرکزی جمهوری اسلامی ایران، به عنوان یک نهاد ناظر و سیاست گذار در حوزه مالی، به طور حتم راضی به انجام تراکنشهای خرد که حجم زیادی از مبادلات را انجام میدهند، با ارزشی غیر از ریال رسمی کشور، نخواهد بود. انجام حجم زیادی از تراکنش‌ها بین افراد، از طریق شبکه‌های غیر قابل دسترسی در بانک مرکزی، امکان ایجاد پولشویی در حجم خرد و انجام اعمال خلافکارانه بین افراد را افزایش خواهد داد. از طرف دیگر ارزشمند شدن واحد مالی غیر ریالی در بین مردم، باعث افزایش استفاده و کاهش اتکا به ریال به دلیل سختی‌های مرتبط با آن (جذب، انتقال، دسترسی پذیری، نظارت بانکی و ...)

[1] Stable Coin

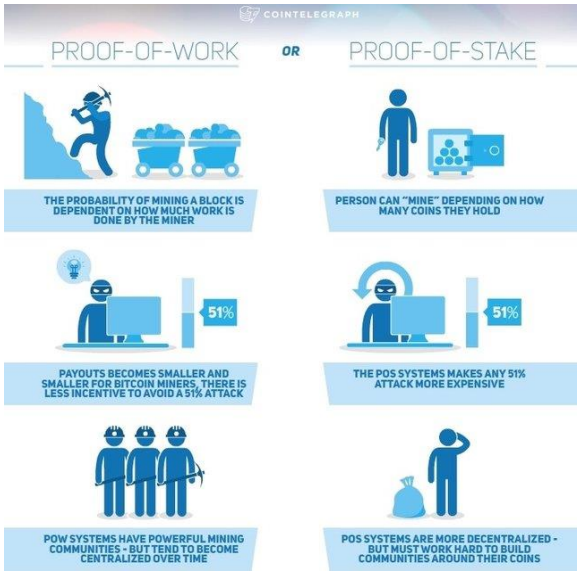
خواهد شد.

این ترازو، نیازمند بحث‌های جدی در حوزه‌های فنی، اجتماعی، پولی و بانکی، اقتصادی، فرهنگی و ... خواهد بود که از حوصله این مستند خارج است. اما به جای پرداختن به این موارد، ابتدا شاید بهتر باشد بررسی کافی در زمینه لزوم استفاده از زنجیره بلوک در پرداخت‌های خرد به جای سرویس دهنده‌های مرکزی بحث شود. در بخش بعد، این دو رقیب اصلی در زمینه پرداخت‌های خرد با هم مقایسه خواهند شد و مزایا و معایب هر کدام مطرح خواهد گردید.

اجماع در مقابل اثبات

در برخی از ارزهای مجازی مبتنی بر زنجیره بلوک، از روشهای اثبات سختی کار استفاده می‌شود و در برخی دیگر از مدلهای مبتنی بر اجماع پردازشگران.

در مدل اثبات سختی کار، هزینه، زمان و منابع بسیار زیادی به جهت جلوگیری از حمله به کل نظام زنجیره بلوک صورت می-پذیرد و در مقابل این فعالیت پر هزینه، کارمزد خوبی پرداخت می‌گردد. این مدل شاید برای تراکنش‌هایی با حجم بالا و با قابلیت منتظر ماندن جهت تایید، مناسب باشد اما در مورد تراکنش‌هایی که نیاز است با سرعت بالا در کسری از ثانیه انجام شوند و همچنین هزینه بالایی برای کارمزد آنها نمی‌توان در نظر گرفت مناسب نخواهد بود.



تصویر ۳ - اجماع در مقابل اثبات

در مقابل در روش‌های مبتنی بر اجماع با توجه به اینکه تایید تراکنش بین پردازشگران، به جهت حضور در یک بلاک و ثبت در دفتر کل به روش رای‌گیری با الگوریتم‌های متفاوت صورت می‌پذیرد، سرعت بالاتر و کاهش هزینه منابع مصرفی به دست خواهد آمد. هرچه روش اجماع پیچیده‌تر باشد، سرعت پردازش تراکنش کندتر و پایداری شبکه بالاتر خواهد رفت و در مقابل اگر از روش‌های پرریسک مبتنی بر اجماع استفاده گردد، سرعت انجام تراکنش افزایش خواهد یافت و اما امکان تقلب در شبکه و یا یتیم[۱] شدن تراکنشها و بلاکها بیشتر خواهد شد.

[۱] Orphan

مقایسه مدل توزیع شده مبتنی بر زنجیره بلوک با سرویس دهی مرکزی

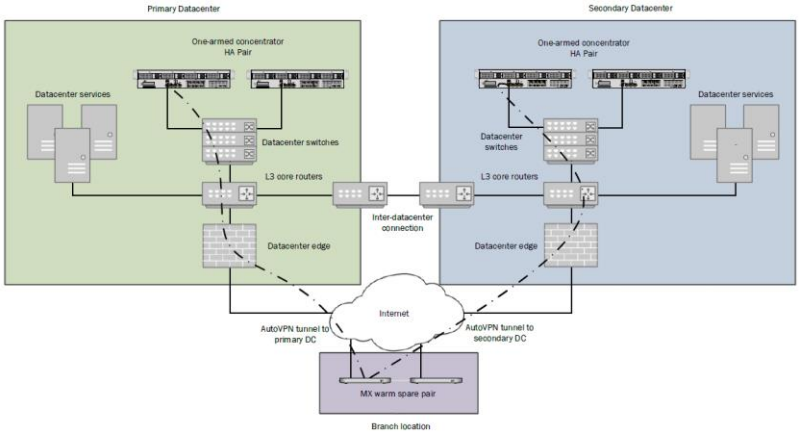
استفاده از فناوری‌های نوین در زمینه پیاده‌سازی سامانه‌های خدمت رسانی به مشتریان، همواره با نتایج مثبتی همراه نبوده است. گاها یک فرهنگ جامع در بین افراد و استفاده از فناوری‌های قدیمی تر، ثبات و پایداری بیشتری را به ارمغان آورده است. این بخش بین مدل سنتی سرویس دهی مرکزی و استفاده از شبکه‌های توزیع شده مبتنی بر زنجیره بلوک، مقایسه کاملی را انجام خواهد داد و به صورت خاص در مورد پرداخت‌های خرد، هر کدام را مورد نقد قرار می‌دهد.

سرویس دهنده مرکزی

سرویس‌دهنده های مرکزی، امروزه در تمامی جوامع و کشورها مشاهده می گردند. به طور خاص در صنعت بانکی و پرداخت می‌توان از شبکه‌های تبادل تراکنش مانند Visa، Master و شبکه شتاب نام برد. شبکه کارتی شاپرک، سرویس های Core Banking بانکها، پرتال‌های مشتریان، اینترنت بانک، سرویس دهنده های تلفن همراه و سرویس‌های Accounting، سرویس‌های ارزش افزوده و ... همگی با اتکا به سرویس‌دهنده مرکزی طراحی و پیاده سازی شده اند.

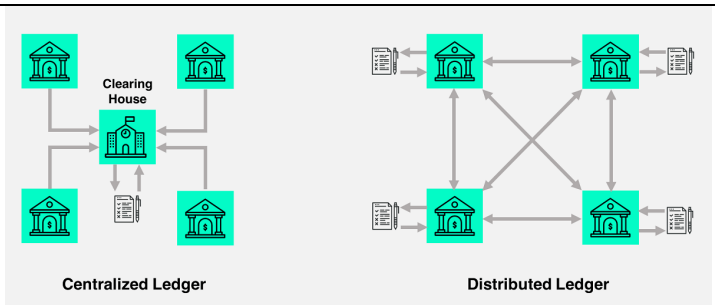
استفاده از سرویس‌دهنده مرکزی، مزایای بسیاری را نسبت به مدل توزیع خدمت به صورت محلی در اختیار سازمان‌ها قرار داده است. این معماری شاید بیش از ۲۰ سال قدمت داشته باشد و در طول زمان با افزایش تعداد مشتریان تغییرات عمده‌ای در آن صورت پذیرفته است. در این قسمت، سعی داریم یک مدل مبتنی بر سرویس دهنده مرکزی به منظور انجام تراکنش-های خرد را بررسی نماییم و مشکلات مرتبط با آن‌را نقد کنیم.

در گذشته سرویس‌دهنده‌های مرکزی بر اساس یک نرم افزار پیچیده و حجیم طراحی و پیاده سازی می‌گردیدند. این نرم-افزارها به منظور اجرا، نیازمند تجهیزات خاص سخت افزاری، معمولا با هزینه بالا بودند و توسعه پذیری آن معمولا به شکل افزایش منابع سخت افزاری صورت می‌گرفت.



تصویر ۴ - شماتیک ارتباطات به صورت سرویس دهنده مرکزی

در این مدل، از بین رفتن سخت افزار سرویس دهنده مرکزی، به دلیل مشکلات سخت افزاری یا جریان برق، امری غیر قابل انکار بود. به منظور جبران این موضوع، از روشهایی مانند تامین چندگانه سرویس دهنده بهره برداری می‌شد که هزینه‌های اجرایی چندین برابری به سازمان تحمیل می‌نمود و در صورت نیاز به افزایش توان اجرایی، تمامی نسخه‌های سخت افزاری موجود می بایستی به روز رسانی می‌گردیدند.



تصویر ۵ - تفاوت سرویس دهنده مرکزی و مدل توزیع شده مبتنی بر زنجیره بلوک

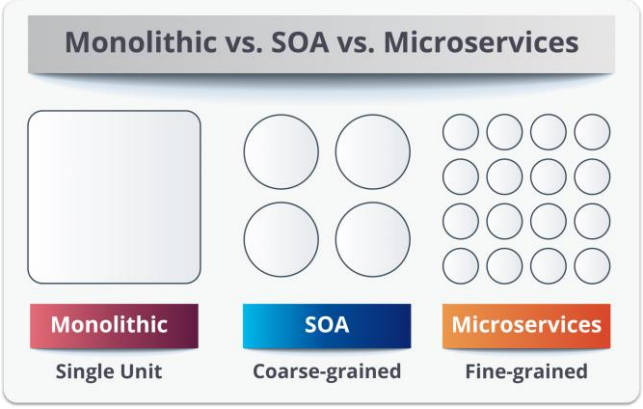
بعد از مشکلات ایجاد شده در مورد توسعه طولی سخت‌افزارها، معماری جدیدی با عنوان معماری مبتنی بر خدمت[۱] پا به عرصه ظهور نهاد که باعث افزایش توان خدمت رسانی و کاهش شدید وابستگی به سرویس‌دهنده سخت افزاری خاص گردید. در این معماری، به جای طراحی نقطه‌ای کلیه خدمات، هر خدمت به شکل یک Service در نقطه‌ای مشترک یا متفاوت با منابع سخت افزاری مرتبط با خود فعالیت می‌نماید و بر اساس مدل‌های تعریف شده در این معماری، این سرویس‌ها قادر به همکاری با یکدیگر به صورت پیام‌های ارسالی هستند. روش SOA همانند یک اداره عمل می‌نماید که یک پرونده جهت تکمیل شدن بین افراد خاصی جابجا می‌گردد و سپس پاسخ نهایی به مشتری تحویل می‌شود. در مورد یک مشتری خاص، ممکن است بخش اعتبارات اداره درگیر نشود و در مورد مشتری خاص دیگر به دلیل تسهیلات درخواستی بالاتر بخش اعتبارات نیز درگیر گردد. در این شرایط منابع تخصیص داده شده به بخش اعتبارات صرفا در مورد پرونده‌هایی استفاده می‌شود که نیازمند آن هستند و به همین دلیل سرعت خدمت رسانی به مشتریان در کنار کاهش هزینه‌ها و منابع مصرفی تجربه بهتری را ایجاد می کند.

در معماری SOA به دلیل جداسازی سرویس‌ها از یکدیگر، قابلیت طراحی و تولید آنها با زبان‌های مختلف برنامه‌نویسی و ابزار متفاوت وجود دارد و تنها وجه اشتراک بین آنها، گرامر پیام رسانی و قوانین معماری می‌باشد.

سرویس‌دهی به صورت SOA که از ماژول‌های بزرگ برای خدمت رسانی استفاده می‌نماید منجر به ایجاد معماری جدیدی گردید که طی دو سال اخیر از آن بهره برداری صورت گرفته است و با سرعت باور نکردنی به رشد خود ادامه می‌دهد. معماری جدید که از ماژول‌های به مراتب کوچکتر از SOA با وظیفه بسیار محدود و خاص استفاده می‌کند به معماری سرویس‌های جزئی[۲] معروف است.

[۱] Service Oriented Architecture

[۲] Micro Services



تصویر ۶ - تصویر شماتیک از مدل واحد، معماری SOA و معماری سرویس‌های جزئی

در این معماری، اجزای یک نرم افزار، به کوچکترین بخش‌های ممکن تقسیم بندی می‌شوند و توسط ابزارهای خاص توسعه پذیری مانند Docker و Kubernetes مدیریت می‌گردند. در این معماری امکان وجود چندین نسخه از یک سرویس جزئی وجود دارد و بسته به کارهای ارجاع شده به یک سرویس جزئی، اصطلاحا توسعه عرضی[۱] صورت می‌پذیرد. در این شرایط استفاده از تجهیزات سخت افزاری چندگانه، با محیط‌های جغرافیایی دور ازهم به منظور کنترل حوادث و مخاطرات از دید کاربران سامانه مرکزی به صورت کامل پوشیده خواهد بود و سرویس رسانی با استفاده از این معماری به مشتریان نهایی با کیفیت عالی و بدون قطعی در سرویس دهی به صورت ۷/۲۴ انجام خواهد پذیرفت و توسعه سامانه به منظور پاسخگویی به حجم بالاتری از مشتریان، در کسری از زمان بدون تغییر در معماری سرویس و یا قطع شدن حتی لحظه‌ای سرویس انجام می‌پذیرد.

با توجه به رشد فناوری در حوزه نرم‌افزار و به طور خاص پیشرفت‌های شکل گرفته در زمینه سرویس‌های جزئی، پیاده سازی یک معماری مرکزی با توزیع‌شدگی بالا پاسخگوی نیازهای پردازشی و تراکنش در هر حجمی خواهد بود و مدیریت یکپارچه، سیاست گذاری کلان و به روزرسانی دائمی از قابلیت‌های این مدل به شمار می‌رود.

مدل توزیع شده مبتنی بر زنجیره بلوک

رشد فناوری در حوزه نرم افزار، هیچگاه پاسخی را برای اعتماد پذیری، کاهش سیاست گذاری بدون اجماع، ریسک خرابی نرم-افزار به صورت عمدی یا اتفاقی، عدالت جمعی و ... نداشته است.

شبکه‌های مبتنی بر زنجیره بلوک، با وجود اشکالات ذکر شده در بخش قبلی، از یک ایدئولوژی اساسی پر توان بهره می‌برند که منجر به تولید قابلیت‌های متفاوتی در این شبکه‌ها گردیده است.

اعتماد پذیری به سامانه‌های مبتنی بر زنجیره بلوک، در مقابل در اختیار قراردادن کلیه داده‌های حیاتی به یک مجموعه مرکزی، یکی از این قابلیت‌ها به شمار می‌رود. در بخش قبلی در رابطه با مدل بسیار جذاب و کاربردی سرویس‌های جزئی صحبت به میان آمد. در این مدل با وجود توزیع شدگی فراوان سرویس دهنده‌ها از داده‌های مرکزی بهره برداری می کنیم. حتی با وجود نگاه داشت نسخه‌های پشتیبان فعال، با وجود مدل‌های Sharding یا توسعه خطی عرضی، بازهم اعتبار یک فرد به دلیل عدم ایجاد Inconsistency صرفا در یک نقطه نگاه داشته می‌شود و سایر نقطه‌های پشتیبان بر اساس تغییرات

[۱] Horizontal Scaling

نقطه اصلی صرفا تاثیر می‌یابند. تغییر در نقطه اصلی بدون اجازه مشتری، توسط سرویس دهنده مرکزی به آسانی انجام می-گیرد و کلیه نقاط پشتیبان نیز به دلیل همگام بودن با نقطه اصلی تغییر خواهند یافت. در این شرایط مالک اطلاعات هیچ راهی به جهت اثبات عدم صحیح بودن اطلاعات خود در سامانه مرکزی ندارد و صرفا می بایستی از تغییرات ایجاد شده تبعیت نماید.

در شبکه‌های مبتنی بر زنجیره بلوک، هر پردازشگر صرفا بر اساس تمهیدات چیده شده در ابتدای راه اندازی شبکه و بر اساس پروتکل ها و قوانین عمومی تعریف شده از قبل اجازه ورود اطلاعات و تغییرات جدید به خود را می‌دهد. حتی ایجاد یک ارتباط نا سالم بین تعدادی از پردازشگران به صورت یک تقلب دست جمعی، در کل شبکه تاثیری نخواهد داشت و صرفا منجر به حذف خود آن پردازشگران از تصمیمات بعدی خواهد گردید. البته در شبکه‌هایی مانند بیت کوین یک اتفاق نادر به نام توان ۵۱٪ میتواند این قوانین را نقض نماید که با توجه به رشد شبکه و تعداد بالای پردازشگران با نام و بی نام در این نظام، این اتفاق به صورت عملی هرگز رخ نخواهد داد.

موضوع بعدی ریسک خرابی نرم افزار می‌باشد. برای مثال در یک Core Banking طراحی شده بر اساس مدل سرویس دهی مرکزی و بر اساس معماری سرویس‌های جزئی در صورتی که سود حساب یک مشتری به اشتباه محاسبه گردد، کلیه اجزای شبکه شامل پردازشگران، سرویس‌دهنده‌ها و ... از اشتباه صورت گرفته استقبال می کنند زیرا در این شبکه‌ها کلیه عملیات از نظر بخشهای مختلف مورد تایید است و هیچ بخشی نظارتی بر بخش دیگر نخواهد داشت. صرفا ممکن است سازمان‌های مالی بعد از انجام اشتباه اقدام به بازرسی و مدیریت اطلاعات بر اساس نرم‌افزارهای جانبی طراحی شده توسط خود سازمان نمایند که بازهم ریسک وجود اشتباه مذکور در آن نرم افزارها هم محتمل خواهد بود.

در صورتی که در مدل‌های مبتنی بر زنجیره بلوک، افرادی از کشورهای مختلف، از سازمانهای مختلف، از شرکت‌های مختلف، با نگاه‌های نرم افزاری و مالی متفاوت در یک محیط یکپارچه مبتنی بر کدهای بازمتن، اقدام به نقد دائمی، رفع اشکالات یکدیگر و ارائه طرحهای اصلاحی و کلیدی می نمایند و به این شکل مشکلات موجود در نهان طراحی آنها به دلیل وجود نگاه-های بسیار زیاد با سرعت بالا و دقت بسیار بالا برطرف می گردد.

در شبکه های مبتنی بر زنجیره بلوک، هیچ کس به هیچ کس برتری و اهمیت ندارد و در صورتی که تراکنشی نسبت به تراکنش دیگر اهمیت یا اولویت داشته باشد، حتما این موضوع از روز اول در تعریف و طراحی شبکه گنجانده شده است و افراد با آگاهی به این موضوع اقدام به استفاده از شبکه نموده‌اند در حالی که در سرویس دهنده‌های مرکزی معمولا قوانین به صورت دوره‌ای و صرفا با نظر سرویس دهنده مرکزی به صورت چارچوب‌های عملیاتی و فنی به دیگران اعلام می‌گردد و همگان ملزم به اجرای قوانین فوق و یا خروج از شبکه هستند.

موضوعات مطرح شده در این بخش، شاید در نگاه افرادی مثبت و در نگاه افراد دیگری منفی به نظر آیند. شاید نقدی که به شبکه‌های مبتنی بر زنجیره بلوک باشد، آن است که هیچ نهاد مرکزی قابلیت اعمال سیاست‌های خود را نداشته باشد در حالی که ممکن است مستحق ترین فرد در این زمینه باشد. اما به دلیل آنکه تغییرات و به روزرسانی های شبکه می بایستی توسط تمامی پردازشگران یا حداقل حجم عمده‌ای از آنها انجام پذیرد، لذا تعریف یک خدمت جدید و به روز رسانی پردازشگران گاها با مقاومت و یا زمان بسیار طولانی روبرو خواهد شد که این موضوع برای ناظرین و مسئولین مرتبط با آن خدمت به طور قطع خوشایند نخواهد بود.

از طرف دیگر، عدم کنترل بر نظام مبتنی بر زنجیره بلوک توسط نهادهای نظارتی و عدم وجود شفافیت در بیشتر شبکه‌های

مطرح حوزه زنجیره بلوک، از دیگر نگرانی‌های مطرح شده در زمینه استفاده از این شبکه‌ها می‌باشد. موضوعات مطرح شده در رابطه با AML و KYC و موضوعات نظارتی مانند پیگیری تراکنش‌ها، اثبات مالکیت و ... در بسیاری از شبکه‌های مطرح وجود ندارد و این موضوع درمورد اخذ مجوز در زمینه پرداخت‌های خرد بر روی شبکه‌های مذکور حتما تاثیرگذار خواهد بود.

یافته‌ها و نتایج

به منظور ایجاد یک نگاه کلی در زمینه سرویس‌دهی به صورت مرکزی و یا توانمند بودن شبکه‌های مبتنی بر زنجیره بلوک در رابطه با پردازش تراکنش‌های خرد، در این بخش نگاهی جامع به مزایا و معایب هر کدام و مقایسه آن دو خواهیم داشت.

در هر عنوان یک سوال یا موضوع مطرح شده و در مقابل آن، پاسخ هر کدام از روشهای پردازش مرکزی و یا استفاده از زنجیره بلوک در پرداخت‌های خرد ثبت گردیده است:

موضوع	پردازش مرکزی	شبکه مبتنی بر زنجیره بلوک
پایداری کل سامانه	نیازمند راه اندازی تجهیزات مرکزی و تجهیزات موازی در محل‌های فیزیکی غیر یکسان می‌باشد. تخریب منطقی در اطلاعات سامانه، فارغ از تعدد پردازشگران و تعدد محل-های فیزیکی باعث از بین رفتن بخشی از اطلاعات و یا آسیب‌های دیگر خواهد شد.	می‌توان از ضعیفترین پردازشگران تا مراکز پیچیده پردازشی را در این زمینه درگیر نمود. در کل شبکه SPOF[1] وجود ندارد و شبکه در مقابل خرابی، از بین رفتن و یا خاموش شدن حجم بالایی از پردازشگران Fault Tolerant خواهد بود.
سرعت انجام تراکنش	بر اساس معماری انتخاب شده می‌توان بین ۳۰۰۰ تا بینهایت تراکنش درثانیه باشد. البته اشکالات پیاده سازی در معماری به طور چشمگیری بر روی این مقدار تاثیر گذار است.	بر اساس مدل‌های پیاده سازی شده فعلی بین ۳ تراکنش در ثانیه تا ۱۰۰،۰۰۰ در تراکنش در ثانیه. افزایش تعداد تراکنش در شبکه‌های مبتنی بر زنجیره بلوک منجر به مرکزی شدن شبکه خواهد شد.
امنیت	امنیت وابسته به تمهیدات دائمی تیم‌های امنیتی می‌باشد. در این مدل همواره باید آخرین به روزرسانی‌های امنیتی و مسائل امنیتی بررسی گردد و بر روی کل شبکه اعمال شود.	امنیت وابسته به طرح پیشنهادی و سپیدنامه[2] ارائه شده در ابتدای راه‌اندازی شبکه خواهد بود. در صورتی که اشکالی در ابتدای طراحی وجود داشته باشد، شبکه به صورت کامل از بین خواهد رفت زیرا به روز رسانی تمامی پردازشگران در یک شبکه مبتنی بر زنجیره بلوک امری بسیار مشکل خواهد بود. در نگاه کلی امنیت در این مدل به علت استفاده از مکانیزم‌های رمزنگاری پایه بالاتر از مدل پردازش مرکزی خواهد بود.
منابع پردازشی	منابع پردازشی بر اساس نیاز شبکه طراحی، نصب و راه اندازی می‌گردند. با توجه به اینکه	منابع پردازشی بسیار زیادی در این مدل درگیر خواهند شد، زیرا افراد مختلف در

[1] Single Point of Failure

[2] White Paper

	اعتماد در این نوع شبکه به سامانه مرکزی وجود دارد، لذا نیاز به راه‌اندازی مجدد منابع در محل‌های دیگر به علت جلوگیری از تقلب وجود ندارد.	فضاهای فیزیکی مختلف اقدام به راه‌اندازی یک پردازشگر با دانش کامل به شبکه می‌نمایند و به همین دلیل هزینه در این مدل بسیار بالاتر از مدل مرکزی خواهد بود. تنها تفاوت آن است که به علت تقسیم هزینه بین گروه‌های مختلف، فشار مالی به یک بخش وارد نمی-گردد.
کارمزد	می‌توان کارمزدی منطبق بر هزینه‌های اجرایی در نظر گرفت. این کارمزد به دلیل رشد فناوری و کاهش هزینه‌های ارتباطی کم خواهد بود. صرفا ممکن است به دلیل اضافه شدن خدمات جانبی مانند بیمه تراکنش، نظارت فیزیکی یا ... هزینه‌های بیشتری در تراکنش اعمال گردد.	کارمزد در این تراکنش‌ها زیاد است. دلیل این موضوع ایجاد انگیزه برای پردازشگران خصوصی به منظور راه اندازی یک پردازشگر است. همانطور که عنوان شد هزینه در این مدل بسیار بالاتر از مدل مرکزی خواهد بود و پردازشگران به منظور بازدریافت هزینه‌های خود می بایستی کارمزد تراکنش دریافت کنند.
نظارت	نظارت صرفا توسط نهاد مرکزی صورت می-پذیرد و درصورتی که بخشی از این نظارت توسط ایشان به بخش دیگری تفویض گردد، حتما با محدودیت‌های خاص می‌باشد و در ضمن در هر زمانی در آینده این تفویض قابل بازگشت خواهد بود.	نظارت در این شبکه به دلیل ماهیت بازمتن بودن آن و در دسترس بودن شبکه برای همگان قابل دسترسی است. البته در شبکه های مبتنی بر زنجیره بلوک خصوصی امکان دسترسی به دیتای شبکه وجود ندارد که البته هرچه به خصوصی بودن این بخش افزوده شود به مشکل مرکزی شدن آن کمک خواهد کرد.
رگولاتوری	تغییر در سیاست‌ها، فرآیندها، ساختارها و الگوریتم‌ها، فارغ از پایبند بودن نظام مرکزی به ایجاد یک محفل هم‌فکری، یا اطلاع رسانی قبلی به ذینفعان، کامل از طریق خود ایشان صورت می‌پذیرد و برای انجام این قبیل فرآیندها هیچگونه مجوزی یا محدودیتی وجود ندارد.	هرگونه تغییر در سیاست‌ها، فرآیندها و ... می بایستی با تایید همه یا حداقل بخش عمده‌ای از شبکه صورت پذیرد. این موضوع فارغ از پیچیدگی وجود نظرات مختلف در مورد هر زمینه‌ای، از نظر فنی و اجرایی بسیار پیچیده خواهد بود و هرچه تغییر بزرگتر باشد اختلالات شبکه بیشتر به چشم خواهد آمد.
شفافیت عملکرد شبکه برای نهادهای نظارتی	میتواند شفاف یا مخفی باشد	میتواند شفاف یا مخفی باشد
نیروی کار	نیروی کار متخصص جهت توسعه بخش‌های مختلف این نوع شبکه در زمان ویرایش این مقاله، در جغرافیای فیزیکی کشور جمهوری اسلامی ایران، بیشتر یافت می‌شود.	نیروی کار متخصص جهت توسعه بخش‌های مختلف این نوع شبکه در زمان ویرایش این مقاله، در جغرافیای فیزیکی کشور جمهوری اسلامی ایران، با محدودیت‌های فراوانی همراه است.
نقطه نظر تجاری و کسب و کار	پرداخت‌های خرد توسط نهادهای مختلفی مدیریت می‌گردد. داده های تولید شده توسط این شبکه، به صورت کامل در اختیار نهادهای	در صورت عمومی بودن شبکه، کلیه اطلاعات تراکنش‌های انجام شده توسط افراد، برای سایرین قابل مشاهده خواهد بود. حتی

	مربوطه خواهد بود. به صورت عمومی، اشتیاقی برای به اشتراک گذاشتن اطلاعات با دیگران در این نهادها وجود ندارد.	دسترسی به این اطلاعات غیرقابل کنترل خواهد شد و مضاف بر آن دسترسی قابل پیگیری نیز نخواهد بود.
توسعه پذیری[۱]	در صورت پیاده سازی صحیح معماری توزیع شده، با افزایش منابع، توسعه صورت خواهد پذیرفت. توسعه پذیری با سرعت و دقت بالا صورت می-پذیرد و از دید مشتریان و ذینفعان کاملا شفاف[۲] خواهد بود.	کاملا منطبق بر معماری پیاده سازی شده اولیه و طرح امنیتی مبتنی بر سختی کار یا اجماع است و اضافه شدن پردازشگران کمک شایانی به توسعه پذیری نخواهد نمود. نکته: ممکن است در یک شبکه مبتنی بر زنجیره بلوک، با الگوریتم خاص امنیتی، افزایش پردازشگران در سرعت پردازش تراکنش نقش داشته باشد.
استحکام[۳]	استحکام در این مدل تاثیر پذیرفته از استحکام سخت افزاری، استحکام امنیتی و استحکام نرم‌افزاری است. هرگونه اشکال در بخش سخت افزاری، یا ایرادات امنیتی که باعث حمله‌های موفق از بیرون شبکه یا داخل شبکه شوند و باگ‌های نرم افزاری دیده نشده در بخش‌های اجرایی کار، به شدت بر روی استحکام شبکه تاثیر می‌گذارند.	استحکام شبکه بر اساس دو فاکتور سپیدنامه اولیه و استقبال از حضور به عنوان پردازشگر تعیین میگردد. در صورتی که طرح اولیه از نظر معماری صحیح باشد، شبکه مستحکم خواهد بود. افزایش تعداد پردازشگران به افزایش استحکام شبکه کمک شایانی خواهد نمود.

جمع بندی

استفاده از زنجیره بلوک، با نگاه به طرح‌های پیاده سازی شده فعلی در دنیا، ایده‌ها و الگوریتم‌های مطرح شده توسط خبرگان و متخصصین این حوزه، در پرداخت‌های خرد مشتریان، جایگاه مناسبی را ندارند. در بخش‌های قبلی به تفصیل در این باره صحبت شد که مشخصات یک نظام مالی بر روی زنجیره بلوک، فارغ از امنیت مناسب آن، استحکام و توسعه پذیری، با مشخصات یک نظام پرداخت خرد سریع و چابک فاصله زیادی دارد.

در این باره سوالاتی در ذهن همه مطرح می‌شود:

- آیا در آینده مدل‌های جدید مبتنی بر زنجیره بلوک مانند Hash Graphها یا مدلهای مبتنی بر اجماع جزئی، قابلیت جایگزینی نظام‌های مرکزی را دارند یا خیر؟
- آیا استفاده از زنجیره بلوک با توجه به هزینه‌های بالای آن در رابطه با تراکنش‌های کم ارزش مالی امری به صرفه است یا خیر؟
- آیا پیشرفت فناوری و تجهیزات سخت افزاری همچنان نظام‌های مرکزی را در کل دنیا پایدار نگاه خواهند داشت یا با

[۱] Scalability
[۲] Transparent
[۳] Robustness

افزایش تعداد مشتریان و تراکنش‌ها به ناچار به سمت مدل‌های توزیع شده مستقل پیش خواهیم رفت ؟

- آیا نظام‌های قانونی و حقوقی در کشور سازگاری لازم با مدل‌های مبتنی بر زنجیره بلوک را دارند و در صورتی که هرگونه اشکالی برای هر کدام از ذینفعان پیش آمد، راهکاری برای پاسخگویی قضایی و حقوقی برای آن دیده شده است یا تا کنون بیشتر نگاه به مدل‌های فنی و امنیتی در زنجیره بلوک بوده است؟
- بازبودن فضای اطلاعاتی و در اختیار همه بودن اطلاعات مالی، آیا از نظر منطقی صحیح است ؟ نظر بانک مرکزی در این زمینه چه خواهد بود؟ نهادهای متولی پرداخت خرد چه برخوردی با باز بودن اطلاعات خواهند داشت؟ شفافیت کافی در زمینه این نوع پرداخت‌ها وجود دارد یا تبدیل به محلی برای پولشویی خواهد شد؟
- پرداخت‌های خرد نظام‌های ثابتی هستند که سالها مردم از نظر فرهنگی در آنها به پایداری رسیده‌اند. الکترونیکی کردن آنها برای ایشان، می بایستی با تمهیدات خاصی صورت پذیرد. استفاده از زنجیره بلوک با توجه به تجربیات سالهای اخیر که دائما شاهد Fork های متعدد بر روی آنها هستیم، آیا در شرایط فعلی پاسخگوی نیاز مطرح شده هستند؟

بسیاری سوالات دیگر در ذهن هر شخصی ایجاد خواهد شد. پاسخگویی به این سوالات نیازمند زمان بسیار زیاد تحلیل، و در برخی از موارد نیازمند گذشت زمان و پاسخگویی در آینده خواهد بود.

منابع

[1] B. Luxembourg, "Transaction Rate Chart," 2019. [Online]. Available: https://www.blockchain.com/en/charts/transactions-per-second.

[2] شاپرک, "گزارش اقتصادی شاپرک," ۲۰۱۹. [Online]. Available: https://shaparak.ir/content?id=754.

[3] CoinDesk, "How Will Ethereum Scale?," 2018. [Online]. Available: https://www.coindesk.com/information/will-ethereum-scale.

[4] Lumenauts, "How Many Transactions Per Second can Stellar Process," 2018. [Online]. Available: https://www.lumenauts.com/blog/how-many-transactions-per-second-can-stellar-process.

[5] Medium, "Understanding Cryptocurrency Transaction Speeds," 2018. [Online]. Available: https://medium.com/coinmonks/understanding-cryptocurrency-transaction-speeds-f9731fd93cb3.

[6] L. Network, "Lightning Network Documents," 2017. [Online]. Available: http://lightning.network/docs/.