

دانشگاه تهران
پردیس دانشکده‌های فنی
دانشکده‌ی مهندسی برق و
کامپیوتر



بررسی و بهبود عملکرد شبکه‌های پرداخت در زنجیره‌بلوکی

پایان‌نامه برای دریافت درجه کارشناسی ارشد
در رشته مهندسی برق، شبکه‌های مخابراتی

حمیدرضا کاشانی

استاد راهنما:

سید پویا شریعت‌پناهی

مرداد ماه ۱۴۰۳

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه تهران
پردیس دانشکده‌های فنی
دانشکده‌ی مهندسی برق و
کامپیوتر



بررسی و بهبود عملکرد شبکه‌های پرداخت در زنجیره‌بلوکی

پایان‌نامه برای دریافت درجه کارشناسی ارشد
در رشته مهندسی برق، شبکه‌های مخابراتی

حمیدرضا کاشانی

استاد راهنما:
سید پویا شریعت‌پناهی

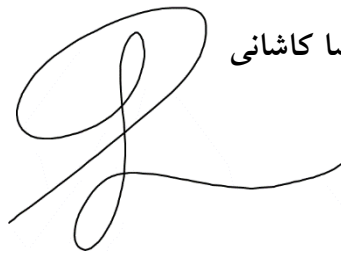
مرداد ماه ۱۴۰۳

تعهدنامه اصالت اثر

باسمه تعالی

اینجانب حمیدرضا کاشانی تأیید می‌کنم که مطالب مندرج در این پایان‌نامه حاصل کار پژوهشی اینجانب است و به دستاوردهای پژوهشی دیگران که در این نوشته از آنها استفاده شده است مطابق مقررات ارجاع گردیده است. این پایان‌نامه قبلاً برای احراز هیچ مدرک هم سطح یا بالاتر ارائه نشده است.

کلیه حقوق مادی و معنوی این اثر متعلق به دانشکده فنی دانشگاه تهران می‌باشد.



نام و نام خانوادگی دانشجو: حمیدرضا کاشانی

امضای دانشجو:

چکیده

در این پژوهش، ابتدا به معرفی مفاهیم پایه و ساختار شبکه‌های زنجیره‌بلوکی و پرداخت توجه شده است. سپس، مشکلات و چالش‌های موجود در شبکه‌های پرداخت، به‌ویژه شبکه لایت‌نینگ، تحلیل و شناسایی شده‌اند. پس از آن، برای بهبود کارایی و کاهش مشکل مرکزی شدن شبکه، با تغییر الگوریتم مسیریابی مرسوم یک الگوریتم مسیریابی اکتشافی جدید پیشنهاد شده است که باعث کاهش مرکزی شدن شبکه می‌شود. این تغییر به ما کمک می‌کند با اضافه کردن قیدی برای جلوگیری از مرکزیت شبکه، شبکه را در طول زمان از مرکزیت خارج کنیم.

به‌منظور ارزیابی عملکرد الگوریتم‌ها و بهینه‌سازی‌های پیشنهادی، شبیه‌سازی‌هایی انجام شده است. نتایج آن نشان می‌دهند که استفاده از الگوریتم‌های بهینه‌سازی پیشنهادی، منجر به کاهش هزینه‌های تراکنش، افزایش تعادل و کاهش نابرابری‌ها در شبکه شده است. به‌ویژه، با استفاده از قیدهای توزیع‌کننده، گره‌های مرکزی به سمت کاهش درجه و افزایش توزیع‌پذیری شبکه حرکت می‌کنند که این امر به کاهش تمرکزگرایی و بهبود کارایی کلی شبکه منجر می‌شود. این دستاوردها می‌توانند به توسعه و پذیرش بیشتر شبکه‌های پرداخت بلاک‌چینی کمک کنند و به نیازهای روزافزون کاربران پاسخ دهند.

واژگان کلیدی رمزارز، بیت‌کوین، زنجیره‌بلوکی، شبکه کانال پرداخت، کاهش مرکزیت، توزیع‌شدگی شبکه، شبکه لایت‌نینگ، مسیریابی، بهینه‌سازی چندپرداخته

فهرست مطالب

۱- فصل ۱: مقدمه و مفاهیم..... ۱

۱-۱- مقدمه..... ۱

۱-۲- مروری بر مفاهیم اولیه..... ۲

۱-۲-۱- بیت کوین..... ۲

۱-۲-۲- زنجیره بلوکی..... ۲

۱-۲-۳- تراکنش‌ها..... ۳

۱-۲-۴- مالکیت..... ۴

۱-۲-۵- استخراج..... ۵

۱-۲-۶- غیر متمرکز بودن..... ۶

۱-۳- مقدمه ای بر موضوع پایان نامه..... ۶

۱-۴- ساختار پایان نامه و نوآوری‌های صورت گرفته..... ۷

۲- فصل ۲: مرور ادبیات و ابزار حل مسئله..... ۹

۲-۱- مقدمه..... ۹

۲-۲- مفاهیم مورد نیاز برای ورود به موضوع، مشکلات و راه‌حل‌ها..... ۹

۲-۲-۱- مسئله سه‌گانه مقیاس‌پذیری در زنجیره‌های بلوکی..... ۱۰

۲-۲-۲- غیر متمرکز بودن..... ۱۰

۲-۲-۳- امنیت..... ۱۱

۲-۲-۴- مقیاس‌پذیری..... ۱۲

- ۲-۳- لایه‌بندی شبکه..... ۱۲
- ۲-۴- مشکل مقیاس‌پذیری مهم‌ترین رمزارزها و راه‌حل‌ها..... ۱۳
- ۲-۴-۱- روش‌های افزایش مقیاس‌پذیری در زنجیره‌بلوکی..... ۱۴
- ۲-۴-۲- راهکارهای لایه یک مقیاس‌پذیری در زنجیره‌بلوکی..... ۱۵
- ۲-۴-۳- راهکارهای لایه دو مقیاس‌پذیری در زنجیره‌بلوکی..... ۱۶
- ۲-۵- آشنایی با شبکه کانال پرداخت..... ۱۷
- ۲-۵-۱- کانال پرداخت..... ۱۷
- ۲-۵-۲- شبکه کانال پرداخت..... ۱۸
- ۲-۵-۳- قراردادهای قفل‌شده با چکیده و زمان..... ۱۹
- ۲-۵-۴- شبکه لایتینگ..... ۲۱
- ۲-۶- معرفی مسائل موجود در شبکه کانال پرداخت..... ۲۳
- ۲-۷- مرور ادبیات در حوزه مسیر‌یابی شبکه کانال پرداخت..... ۲۳
- ۲-۸- مرور ادبیات در حوزه تحلیل مرکزی شدن شبکه کانال پرداخت..... ۲۸
- ۲-۹- کاهش تمرکز شبکه‌های کانال پرداخت..... ۳۳
- ۲-۱۰- معرفی ابزار برای ورود به مسئله..... ۳۶
- ۳- فصل سوم: راه‌حل پیشنهادی..... ۳۹**
- ۳-۲- مدل مسئله..... ۳۹
- ۳-۳- تعریف مسئله اولیه و قیود آن..... ۴۱
- ۳-۴- تغییر در قید و روش بهینه‌سازی پیشنهادی..... ۴۲

۴۴ ۵-۳- مدل مسیریابی برای دو تراکنش همزمان

۴۶ ۶-۳- مدل مسیریابی برای چند تراکنش همزمان

۴۷ ۷-۳- بهینه‌سازی مسیریابی چندگانه با شرط کاهش مرکزیت

۴۹ ۸-۳- الگوریتم پیدا کردن کوتاه‌ترین مسیر

۵۱ ۹-۳- الگوریتم ابتکاری جهت کاهش گره‌های مرکزی

۵۵ ۴- فصل چهارم: ارزیابی و شبیه‌سازی‌ها

۵۶ ۲-۴- شبیه‌سازی مسئله

۵۷ ۳-۴- شبیه‌سازی پرداخت‌ها با الگوریتم اولیه

۵۹ ۴-۴- شبیه‌سازی پرداخت‌ها با الگوریتم مرکزی کننده شبکه

۶۱ ۵-۴- مقایسه شبیه‌سازی‌های انجام شده

۶۳ ۶-۴- حل عددی مسئله بهینه‌سازی

۶۴ ۷-۴- مقایسه عملکرد مسئله بهینه‌سازی با قید ساده شده

۶۵ ۸-۴- شبیه‌سازی مسیریابی با دو تراکنش همزمان

۶۶ ۹-۴- شبیه‌سازی مسیریابی با ده تراکنش همزمان

۶۸ ۱۰-۴- شبیه‌سازی پرداخت چندمسیره با قید مرکزی کننده

۷۱ ۵- نتیجه‌گیری

۷۱ ۲-۵- روند کلی پایان‌نامه

۷۲ ۳-۵- نتایج به دست آمده

منابع: ۷۴

فهرست اشکال

- شکل : ۱ سه ویژگی کلیدی بلاکچین ها ۱۰
- شکل : ۲ لایه بندی شبکه کانال پرداخت ، عکس از مقاله [52] ۱۳
- شکل : ۳ در اینجا یک کانال ایجاد شده که در آن ۵ تراکنش انجام شده و از آن فقط دو تراکنش در بلاکچین ثبت شده است [51] ۱۸
- شکل : ۴ مسیریابی پرداخت از عاطفه به حمیدرضا در شبکه کانال پرداخت ۱۹
- شکل : ۵ مشخصات و آمار کلی شبکه لایتینگ ۲۲
- شکل : ۶ نمای کلی از شبکه لایتینگ [53] ۳۳
- شکل : ۷ فلوچارت رسیدن به مسیر بهینه ۴۳
- شکل : ۸ نمودار توزیع گره ها بر اساس مقدار درجه است که نشان می دهند گره ها با هر درجه چقدر در آمد از این ۲۰۰۰۰۰ پرداخت در این الگوریتم داشته اند ۵۸
- شکل : ۹ نمودار مقدار کارمزد هر تراکنش براساس تعداد تراکنش ها ۵۸
- شکل : ۱۰ نمودار قیمت پرداخت ها بر حسب تعداد آنها است که رنگ قرمز پرداخت های با کارمزد ارزان تر از پرداخت در زنجیره است ، آبی کارمزد های گران تر را نشان می دهد و سبز نشان دهنده پرداخت هایی هستند که موفق به انتقال در شبکه نشدند. ۵۸
- شکل : ۱۱ نمودار طول مسیرهای پرداخت شده برحسب تعداد آنها که رنگ قرمز نشان دهنده مسیر هایی هستند که ارزان تر از پرداخت در زنجیره انجام شده اند و رنگ آبی نشان دهنده مسیر هایی هستند که گران تر از مقدار پرداخت در زنجیره کارمزد دارند. ۵۸
- شکل : ۱۲ نمودار دنباله پرداخت ها برحسب تعداد گره های یک طرفه شده که نشان دهنده نا متعادل شدن شبکه است برای الگوریتم اولیه ۵۹
- شکل : ۱۳ نمودار مقدار کارمزد هر تراکنش براساس تعداد تراکنش ها الگوریتم مرکزی کننده ۵۹
- شکل : ۱۴ نمودار توزیع گره ها بر اساس مقدار درجه است که نشان می دهند گره ها با هر درجه چقدر در آمد از این ۲۰۰۰۰۰ پرداخت در این الگوریتم مرکزی کننده داشته اند ۵۹
- شکل : ۱۵ نمودار طول مسیرهای پرداخت شده برحسب تعداد آنها که رنگ قرمز نشان دهنده مسیر هایی هستند که ارزان تر از پرداخت در زنجیره انجام شده اند و رنگ آبی نشان دهنده مسیر هایی هستند که گران تر از مقدار پرداخت در زنجیره کارمزد دارند. ۶۰

شکل : ۱۶ نمودر قیمت پرداخت ها بر حسب تعداد آنها است که رنگ قرمز پرداخت های با کارمزد ارزان تر از پرداخت در زنجیره است ، آبی کارمزد های گران تر را نشان می دهد و سبز نشان دهنده پرداخت هایی هستند که موفق به انتقال در شبکه نشدند. ۶۰

شکل : ۱۷ نمودار دنباله پرداخت ها بر حسب تعداد گره های یک طرفه شده که نشان دهنده نا متعادل شدن شبکه است برای الگوریتم مرکزی کننده ۶۰

شکل : ۱۸ نمودار توزیع موجودی گره ها در دو شبیه سازی در کنار هم نقاط و خطوط قرمز برای شبیه سازی الگوریتم اکتشافی و نقاط و خطوط آبی برای الگوریتم اولیه می باشد. ۶۱

شکل : ۱۹ اندازه و تعداد مسیر های پرداخت های موفق و گران ۶۷

شکل : ۲۰ تعداد و میزان پرداخت های موفق ، نا موفق و گران ۶۷

شکل : ۲۱ تغییرات تعادل شبکه بر حسب تعداد شبیه سازی ۶۷

شکل : ۲۲ در آمد گره بر حسب درجه،(هر نقطه یک گره است) ۶۷

شکل : ۲۳ اندازه و تعداد مسیر های پرداخت های موفق و گران برای شبیه سازی بهینه سازی ۲۰ پرداخته با قید توزیع شدگی ۶۸

شکل : ۲۴ تعداد و میزان پرداخت های موفق ، ناموفق و گران برای شبیه سازی بهینه سازی ۲۰ پرداخته با قید توزیع شدگی ۶۸

شکل : ۲۵ تغییرات تعادل شبکه بر حسب تعداد شبیه سازی گران برای شبیه سازی بهینه سازی ۲۰ پرداخته با قید توزیع شدگی ۶۸

شکل : ۲۶ در آمد گره بر حسب درجه،(هر نقطه یک گره است) گران برای شبیه سازی بهینه سازی ۲۰ پرداخته با قید توزیع شدگی ۶۸

شکل : ۲۷ نمودار درآمد گره ها در دو ارزیابی بهینه سازی در کنار هم که نقاط و خطوط نارنجی برای ارزیابی بهینه سازی با قید کاهش دهنده مرکزیت است و خطوط آبی برای ارزیابی بهینه سازی بدون این قید است. ۶۹

فهرست الگوریتم ها

- الگوریتم ۱ : الگوریتم دایجسترا تغییر یافته برای پیدا کردن کوتاه ترین مسیر از انتها به ابتدا در شبکه
با یال های معکوس شده [28] ۵۱
- الگوریتم ۲: ایجاد بودجه برای هر گره در شبکه مسیریابی ۵۲
- الگوریتم ۳: تابع حذف گره از الگوریتم در صورت صفر شدن بودجه ۵۲
- الگوریتم ۴: تابع کم کردن یک واحد از بودجه در صورت بودن در مسیریابی و فرستنده گیرنده نبودن
و اضافه کردن یک واحد در صورت نبودن در مسیریابی ۵۲

۱- فصل ۱: مقدمه و مفاهیم

۱-۱- مقدمه

در مقدمه حاضر، به بررسی مفاهیم اساسی زنجیره‌بلوکی و رمزارزها پرداخته می‌شود. مفاهیمی همچون زنجیره‌بلوکی، دفترچه کل، ایجاد حساب و رمزگذاری، ماینینگ و سیستم توزیع شده مورد بررسی قرار گرفته و روند انجام تراکنش‌ها نیز تشریح شده است.

قبل از ورود به جزئیات فنی، برخی اطلاعات مهم در مورد بیت‌کوین و وضعیت فعلی این رمزارز را بیان می‌کنیم. بیت‌کوین به‌عنوان یک وسیله‌ی پرداخت بین‌المللی، توانسته است توجه زیادی را به خود جلب کند. امروزه، تعداد زیادی از شرکت‌ها و بازارهای جدید از بیت‌کوین استفاده می‌کنند و این رمزارز در تراکنش‌های بسیاری به کار می‌رود. بیش از ۳ تا ۶ میلیارد دلار تراکنش در بیت‌کوین انجام می‌شود که معادل ۲۰۰ هزار تا ۳۵۰ هزار بیت‌کوین می‌شود و این نشان از رشد قابل‌توجه این بازار دارد. حدود ۳۲۰ میلیون مشترک فعال در سال ۲۰۲۲ در سراسر جهان برای بیت‌کوین وجود دارد که ۴۶ میلیون نفر از آنها آمریکایی هستند این عدد معادل ۲۲ درصد جمعیت آمریکا است و نشان از پذیرش گسترده‌ی این فناوری دارد. باتوجه‌به این تحلیل‌ها، اهمیت و ارزش رمزارزها به وضوح مشخص می‌شود که نشان‌دهنده‌ی ضرورت آشنایی دقیق‌تر با این فناوری‌هاست.

۱-۲-۱- مروری بر مفاهیم اولیه

در این قسمت مروری بر مفاهیم پایه و تعاریف مرتبط با این پروژه خواهیم داشت.

۱-۲-۱- بیت کوین

بیت کوین^۱ به عنوان یک ارز دیجیتال بی واسطه، بدون وابستگی به بانک مرکزی و با سیستم مدیریت متمرکز، امکان انتقال مقادیر ارزی را از طریق شبکه بیت کوین، به صورت مستقیم بین افراد، بدون نیاز به واسطه معتبر، فراهم می کند. تراکنش ها، با استفاده از رمزنگاری، در شبکه بیت کوین تأیید و در یک سیستم ثبت و نگهداری متمرکز و توزیع شده به نام زنجیره بلوکی، ثبت می شوند. این ارز دیجیتال، اختراعی از شخص یا گروهی به نام ساتوشی ناکاموتو، در سال ۲۰۰۸ میلادی بوده است. عمده استفاده از بیت کوین، پس از عرضه نرم افزار متن باز آن در سال ۲۰۰۹، آغاز شد [1].

در فرایند استخراج بیت کوین، ماینرها به عنوان افرادی که این عملیات را انجام می دهند، به ازای فعالیت خود پاداش مالی در قالب بیت کوین دریافت می کنند. این بیت کوین ها قابلیت استفاده برای خرید محصولات، خدمات یا حتی ارزهای دیگر را دارند. اما بیت کوین به دلیل مصرف بالای انرژی که منجر به افزایش ردپای کربنی می شود و نوسانات قیمت و همچنین مسائل امنیتی از جمله دزدی از مبادلات مورد انتقاد واقع شده است. در گذشته، برخی افراد و سرمایه گذاران بیت کوین را به عنوان یک حباب سرمایه گذاری معرفی کرده اند، در حالی که دیگران از آن به عنوان یک ابزار سرمایه گذاری استفاده کرده اند. بسیاری از نهادهای نظارتی همچنین، هشدارها و راهنمایی هایی را درباره بیت کوین برای سرمایه گذاران ارائه داده اند. در سپتامبر ۲۰۲۱، السالوادور به عنوان اولین کشوری که بیت کوین را به عنوان ارز قانونی تأیید کرد، معروف شد [2].

۱-۲-۲- زنجیره بلوکی

زنجیره بلوکی یک مجموعه متشکل از بلوک های متوالی است که هر کدام حاوی اطلاعاتی از تراکنش های بیت کوین و همچنین چکیده بلوک قبلی می باشد، این مجموعه همان دفترکل عمومی است. این دفترکل عمومی، تمامی

¹ Bitcoin

تراکنش‌های بیت‌کوین را به‌صورت دائمی و غیرقابل‌تغییر ثبت و نگهداری می‌کند. علاوه بر این، هر تراکنش باید توسط شبکه گره‌های بیت‌کوین تأیید شود تا به طور مستقل و امنیتی معتبر شمرده شود.

شبکه زنجیره‌بلوکی توسط یک مجموعه از گره‌های ارتباطی اداره می‌شود که هر یک از آن‌ها نرم‌افزار بیت‌کوین را اجرا می‌کنند. این گره‌ها مسئولیت نگهداری و تأیید تراکنش‌ها را بر عهده دارند. به‌عنوان نمونه، هرگاه فردی مثل فرد پرداخت‌کننده آلیس، از برنامه‌های نرم‌افزاری موجود استفاده کند تا بیت‌کوین‌ها را به گیرنده باب ارسال کند، تراکنش‌های مربوطه باید توسط این گره‌ها تأیید شوند و سپس به زنجیره‌بلوکی اضافه گردند.

گره‌های شبکه می‌توانند تراکنش‌ها را تأیید، آن‌ها را به دفتر خود اضافه و سپس برخی از تراکنش‌های اضافی را به سایر گره‌ها منتقل کنند. این فرایند ایجاد بلوک جدید بافاصله زمانی متوسط هر ۱۰ دقیقه، باعث می‌شود که زنجیره‌بلوکی به‌روز و تغییرات در تراکنش‌ها در کل شبکه منتشر شوند. از آنجاکه این فرایند بدون نیاز به نظارت مرکزی انجام می‌شود، اعتبار و امنیت زنجیره‌بلوکی حفظ می‌شود.

در نهایت، زنجیره‌بلوکی به نرم‌افزار بیت‌کوین اجازه می‌دهد تا تاریخچه تمامی بیت‌کوین‌های خرج شده را ثبت و رصد کند. این دفترکل موجودی‌ها را برای ثبت و انتقالات واقعی جایگزین نمی‌کند، بلکه فراتر از آن می‌رود و تمامی تراکنش‌های بیت‌کوین را با دقت و امنیت بالا ثبت می‌کند. همچنین، با استفاده از کاوشگر زنجیره‌بلوکی، می‌توان اطلاعات مربوط به بلوک‌های فردی، آدرس‌های عمومی و تراکنش‌های درون بلوک‌ها را بررسی و تجزیه و تحلیل کرد [3].

۳-۲-۱- تراکنش‌ها

در زنجیره‌های بلوکی، تراکنش‌ها با بهره‌گیری از یک زبان برنامه‌نویسی خاص انجام می‌شوند. این تراکنش‌ها شامل تعدادی مبدأ و مقصد هستند. وقتی کسی بیت‌کوین ارسال می‌کند، باید هر آدرس مقصد و مقدار بیت‌کوین ارسال شده را تعیین کند. برای اطمینان از صحت انتقال، هر مبدأ باید به مقصدی که قبلاً در زنجیره‌بلوکی ثبت شده، اشاره کند. با توجه به اینکه تراکنش‌ها می‌توانند چندین مقصد داشته باشند، امکان ارسال بیت‌کوین به چندین گیرنده در یک تراکنش وجود دارد. گاهی اوقات مقدار بیت‌کوین‌های استفاده شده برای پرداخت بیشتر از مقدار مورد نیاز است؛ در این مواقع، یک آدرس اضافی در تراکنش قرار می‌گیرد تا بیت‌کوین‌های اضافی به فرستنده

بازگردد. ساتوشی‌های باقی‌مانده که به هیچ مقصدی اختصاص نیافته‌اند، به‌عنوان هزینه تراکنش محاسبه می‌شوند. این فرآیند باعث می‌شود تا تراکنش‌ها به صورت دقیق و کارآمد انجام شوند [5] [4].

اگرچه هزینه معامله اختیاری است، استخراج‌کنندگان می‌توانند معاملاتی را که هزینه بیشتری پرداخت می‌کنند انتخاب و اولویت‌بندی کنند. ماینرها (اشخاص استخراج‌کننده) ممکن است معاملات را بر اساس هزینه پرداخت شده نسبت به فضای ذخیره‌سازی خود انتخاب کنند، نه بر اساس مقدار مطلق پولی که به‌عنوان هزینه پرداخت می‌شود. این هزینه‌ها معمولاً بر حسب ساتوشی در هر بایت اندازه‌گیری می‌شوند. اندازه معاملات به تعداد مبادلات استفاده شده برای ایجاد معامله و تعداد مقصدها بستگی دارد.

اندازه بلاک‌های موجود در زنجیره‌بلوکی ابتدا به ۳۲ مگابایت محدود بود. محدودیت اندازه بلاک یک مگابایت توسط ساتوشی ناکاموتو در سال ۲۰۱۰ معرفی شد. در نهایت، محدودیت اندازه بلاک یک مگابایت مشکلاتی را برای پردازش معاملات ایجاد کرد، از جمله افزایش هزینه‌های معامله و تأخیر در پردازش معاملات.

۴-۲-۱- مالکیت

بیت‌کوین‌ها در آدرس‌های بیت‌کوین ثبت می‌شوند. برای ساخت یک آدرس بیت‌کوین، نیاز به انتخاب یک کلید خصوصی معتبر داریم. این کلید خصوصی به‌صورت تصادفی انتخاب می‌شود و سپس با استفاده از الگوریتم‌های رمزنگاری مخصوص، آدرس بیت‌کوین مرتبط با آن محاسبه می‌شود. این فرایند به‌سرعت و بدون نیاز به زمان زیادی انجام می‌شود. اما محاسبه کلید خصوصی یک آدرس بیت‌کوین معین، بسیار دشوار و عملاً غیرممکن است. به‌عبارت دیگر، هیچ روش معمولی و کاربردی برای محاسبه کلید خصوصی از یک آدرس بیت‌کوین وجود ندارد. این ویژگی امنیتی بسیار مهمی است که از آن استفاده می‌شود تا اطمینان حاصل شود که فرایند تبادل بیت‌کوین‌ها امن و قابل‌اعتماد است. به همین دلیل است که کاربران می‌توانند به دیگران یک آدرس بیت‌کوین را بدون اینکه کلید خصوصی مرتبط با آن فاش شود، عمومی کنند. این به‌اصطلاح "آدرس عمومی" است که برای دریافت پرداخت‌ها و انجام تبادلات استفاده می‌شود.

با این وجود، اگر کلید خصوصی یک آدرس بیت‌کوین گم شود، این به معنای از دست دادن دسترسی به بیت‌کوین‌های موجود در آن آدرس است. بدون کلید خصوصی، امکان اثبات مالکیت و تصرف در این دارایی‌ها وجود ندارد که این موضوع می‌تواند منجر به اتلاف و گم‌شدن بیت‌کوین‌های قابل‌توجهی شود [6]. برای افزایش امنیت، حفظ کلید

خصوصی بسیار حیاتی است. هرگونه فاش شدن یا دسترسی شخص غیرمجاز به کلید خصوصی می تواند به سرقت بیت کوین ها منجر شود. این مسئله خصوصاً در زمینه امنیت اطلاعات بسیار حساس و حیاتی است و باید بادقت و توجه به امنیت انجام شود. در نتیجه، برای حفظ مالکیت و امنیت بیت کوین، اهمیت بسیاری به حفظ کلید خصوصی و کنترل دقیق بر آن اختصاص داده می شود.

۵-۲-۱- استخراج

استخراج یا ماینینگ بیت کوین یک فرایند اساسی در شبکه زنجیره بلوکی بیت کوین است که به وسیله قدرت پردازش کامپیوترها انجام می شود. در این فرایند، استخراج کنندگان به صورت مکرر تراکنش ها را در یک بلوک گروه بندی کرده و سپس این بلوک را به صورت ثابت، کامل و غیر قابل تغییر در شبکه زنجیره بلوکی نگه داری می کنند. این بلوک ها حاوی یک تابع چکیده رمزی است که از بلوک قبلی به عنوان ورودی استفاده می کند، بنابراین هر بلوک به بلوک قبلی پیوند دارد و در مجموعه این شبکه زنجیره بلوکی نامیده می شود. برای پذیرفته شدن توسط بقیه اعضای شبکه، یک بلوک جدید باید حاوی الگوریتم اثبات کار^۲ باشد. این الگوریتم ملزم می کند که استخراج کنندگان عددی به نام نانس^۳ را پیدا کنند، به گونه ای که هنگامی که محتوای بلوک همراه با نانس چکیده می شود، نتیجه از نظر عددی کوچک تر از هدف دشواری شبکه باشد. تأیید این اثبات برای هر گره در شبکه آسان است، اما تولید آن بسیار زمان بر است، زیرا استخراج کنندگان باید مقادیر غیر نانس مختلفی را امتحان کنند تا به نانس مناسب برای بلوک برسند [8] [7].

با تنظیم هدف دشواری، میزان کار مورد نیاز برای تولید یک بلوک قابل تغییر می شود. هر ۲۰۱۶ بلوک، گره ها باهدف حفظ میانگین زمان بین بلوک های جدید در ده دقیقه، هدف دشواری را بر اساس نرخ اخیر تولید بلوک تنظیم می کنند. این سیستم به طور خودکار با مقدار کل توان استخراج در شبکه سازگار می شود. محاسبات با این بزرگی بسیار گران هستند و از سخت افزارهای تخصصی استفاده می کنند. سیستم اثبات کار، تغییرات زنجیره بلوکی را بسیار سخت می کند؛ زیرا مهاجم باید تمام بلوک های بعدی را اصلاح کند تا تغییرات یک بلوک پذیرفته شود. همچنین، هر چه بیشتر زمان بگذرد، دشواری اصلاح یک بلوک افزایش می یابد و تعداد بلوک های بعدی نیز افزایش

^۲ Proof of work (PoW)

^۳ nonce

می‌یابد. این ویژگی باعث می‌شود که زنجیره‌بلوکی بیت‌کوین به مرور زمان با اطمینان بیشتری قابل‌اعتماد شود و از حملات مخرب محافظت شود [8].

۶-۲-۱- غیر متمرکز بودن

بیت‌کوین یک ارز غیرمتمرکز است که توسط یک شبکه همتا به همتا اداره می‌شود، بدون وجود سرور مرکزی یا نقطه کنترل مرکزی. در این شبکه، دفترکل بیت‌کوین (زنجیره‌بلوکی) به‌صورت توزیع شده در کامپیوترهای هر فرد ذخیره می‌شود و به‌عنوان یک دفترکل عمومی عمل می‌کند. هیچ مدیر مرکزی وجود ندارد و دفترکل توسط شبکه استخراج‌کنندگان که دارای امتیاز یکسان هستند نگهداری می‌شود. هر فرد می‌تواند به‌عنوان یک استخراج‌کننده به شبکه بپیوندد و تراکنش‌های اضافی توسط دفترکل حفظ می‌شود تا زمانی که یک بلوک جدید به دفترکل اضافه شود. انتشار بیت‌کوین نیز به‌صورت غیرمتمرکز است، به این معنا که هر فردی که بلوک جدیدی ایجاد کند، پاداش دریافت می‌کند و هیچ نیازی به تأیید ایجاد بلوک نیست.

استخراج‌کنندگان کوچک به گروه‌های استخراج‌کننده بزرگ‌تر می‌پیوندند تا تنوع درآمد خود را به حداقل برسانند و از تمرکز بیشتری در قدرت چکیده جلوگیری کنند. برای محافظت از شبکه، لازم است هیچ گروه یا استخراج‌کننده‌ای توانایی کنترل بیش از ۵۱ درصد از قدرت چکیده را نداشته باشد، زیرا این امر می‌تواند به آنها اجازه دهد سکه‌ها را دوباره خرج کنند و سایر تراکنش‌ها را رد کنند. تا سال ۲۰۱۳، شش گروه استخراج‌کننده ۷۵ درصد از کل قدرت چکیده بیت‌کوین را کنترل می‌کردند و در سال ۲۰۱۴، گروه استخراج‌کننده Ghash.io پنجاه و یک درصد قدرت چکیده را به دست آورد که برای امنیت شبکه خطرناک بود. این مسائل به‌وضوح نشان می‌دهند که حفظ غیرمتمرکز بودن بیت‌کوین به‌ویژه در مقابل تمامیت شبکه از اهمیت بالایی برخوردار است [9] [10].

۳-۱- مقدمه ای بر موضوع پایان نامه

ما در بخش "مفاهیم" پایان‌نامه به توضیح اساسی‌ترین مبانی و مفاهیمی خواهیم پرداخت که برای درک موضوع و حل مسئله تمرکز شبکه‌های بلاک‌چینی و بهینه‌سازی ساختار آنها ضروری است اما در اینجا با اشاره ای به آنها موضوع پایان نامه را مختصری باز میکنیم.

شبکه‌های بلاک‌چینی به عنوان سیستم‌های توزیع‌شده، امکان ثبت تراکنش‌ها و اطلاعات را بدون نیاز به یک مرجع مرکزی فراهم می‌کنند. یکی از ویژگی‌های کلیدی این شبکه‌ها، غیرمتمرکز بودن آنهاست که از طریق

الگوریتم‌های اجماع، امنیت و پایداری شبکه را تضمین می‌کنند. با این حال، با افزایش محبوبیت و استفاده از بلاک‌چین‌هایی نظیر بیت‌کوین، مشکلاتی مانند کاهش سرعت تراکنش‌ها و افزایش هزینه‌ها به وجود آمده است.

برای رفع این مشکلات، راه‌حلی به نام لایه‌های دوم معرفی شده‌اند که با کاهش بار تراکنش‌ها بر روی زنجیره اصلی، کارایی شبکه را بهبود می‌بخشند. شبکه‌های کانال پرداخت مانند شبکه لایت‌نینگ، از جمله این راه‌حل‌ها هستند. این شبکه‌ها به کاربران امکان می‌دهند بدون نیاز به تایید مستقیم توسط بلاک‌چین، تراکنش‌های سریع و ارزان‌تری انجام دهند. در شبکه‌های کانال پرداخت، کاربران با باز کردن کانال‌های دوطرفه می‌توانند چندین تراکنش را به صورت خارج از زنجیره ثبت و مدیریت کنند که نه تنها سرعت تراکنش‌ها را افزایش می‌دهد، بلکه هزینه‌ها را نیز به شکل قابل توجهی کاهش می‌دهد.

یکی از چالش‌های اساسی این شبکه‌ها، تمرکز است. گره‌های با ظرفیت بیشتر به تدریج بخش عمده‌ای از تراکنش‌ها را کنترل می‌کنند، که باعث تمرکز شبکه و تهدید اصول غیرمتمرکز بودن آن می‌شود. برای مقابله با این مشکل، روش‌هایی مانند ایجاد چرخه‌های سه‌گانه پیشنهاد شده‌اند که به تعادل بهتر تراکنش‌ها در شبکه و کاهش تمرکز کمک می‌کنند.

در این پایان‌نامه، قصد داریم روی بهبود کارایی شبکه و رفع مشکل مرکزیت آن از طریق تغییر مسئله بهینه‌سازی و اعمال قیدهای محدودکننده برای گره‌های مرکزی تمرکز کنیم. در بخش مفاهیم، به معرفی اصول کلی مرتبط با شبکه‌های کانال پرداخت در رمزارزها و مشکلات مقیاس‌پذیری زنجیره‌های بلوکی پرداخته می‌شود. مفاهیمی مانند غیرمتمرکز بودن، امنیت و مقیاس‌پذیری به تفصیل توضیح داده خواهند شد تا زمینه لازم برای درک عمیق‌تر موضوعات ارائه‌شده در مقالات علمی این حوزه فراهم گردد.

۴-۱- ساختار پایان‌نامه و نوآوری‌های صورت گرفته

در این بخش، قصد داریم ادامه‌ی راه پایان‌نامه را به خوانندگان معرفی کرده و نوآوری‌های صورت گرفته در این پایان‌نامه را به منظور فهم بیشتر، مورد تأکید قرار دهیم. هدف اصلی ما بررسی و بهبود روش‌های مسیریابی و تمرکززدایی در شبکه‌های کانال است.

در فصل دوم، ابتدا مفاهیم اساسی ورود به مسئله شرح داده می‌شود و سپس به بررسی مقالات مهم در حوزه‌ی مسیریابی بهینه و مشکلات مرکزی شدن شبکه‌های کانال می‌پردازیم. این مقالات بر مسائل بهینه‌سازی مسیرها و چالش‌های مرتبط با تمرکز شبکه‌ها توجه دارند.

در فصل سوم، یکی از مهم‌ترین مقالات به‌عنوان مبنای کار انتخاب می‌شود و با مدل بهینه‌سازی آن آغاز می‌کنیم. هدف ما تبدیل مدل مسیریابی تک‌پرداخته به چندپرداخته است و با اعمال محدودیت‌هایی بر روی گره‌ها، هزینه‌ی عبور از گره‌های مرکزی را افزایش داده تا شبکه به سمت توزیع‌شدگی حرکت کند. برای این کار، ابتدا یکی از قیود مسئله‌ی بهینه‌سازی در مدل اولیه را ساده‌سازی می‌کنیم تا ایجاد مسئله‌ی مسیریابی چندمسیره تسهیل شود. سپس، قید محدودکننده‌ی گره‌های مرکزی را اضافه می‌کنیم تا به هدف خود برسیم. همچنین، یک راه‌حل دیگر برای توزیع‌پذیر کردن شبکه در حالت تک‌مسیره را ارائه می‌دهیم که با استفاده از الگوریتم اکتشافی توسعه‌یافته از الگوریتم مسیریابی تک‌پرداخته‌ی مقاله‌ی پایه به‌دست آمده است.

در فصل چهارم هم با پیاده‌سازی شبیه‌سازی مسئله از ابتدا با استفاده از کتابخانه‌های پایتون، این دو راه‌حل را شبیه‌سازی و ارزیابی می‌کنیم و بهبودهای حاصل از آنها را نشان می‌دهیم.

فصل پنجم هم فصل نتیجه‌گیری است، نتایج کلی مقاله و کارهای آینده در این فصل مطرح می‌شود.

نواوری‌های صورت گرفته در این پایان‌نامه شامل:

- تغییر و ساده‌سازی قید مسیریابی مسئله در مقاله اصلی که باعث سرعت حل مسئله نیز می‌شود
- استفاده از تغییر ایجاد شده و ایجاد بهینه‌سازی مسیرهای دو تراکنش همزمان در شبکه
- تعمیم این بهینه‌سازی از دوپرداخته به k -پرداخته همزمان
- ایجاد قید محدودکننده نودهای مرکزی در بهینه‌سازی k -پرداخته
- ایجاد یک بودجه متناسب با درجه در الگوریتم مسیریابی
- تغییر الگوریتم مسیر یابی اولیه با بودجه ایجاد شده و محدود سازی گره مرکزی در الگوریتم اکتشافی تک پرداخته

۲- فصل ۲: مرور ادبیات و ابزار حل مسئله

۱-۲- مقدمه

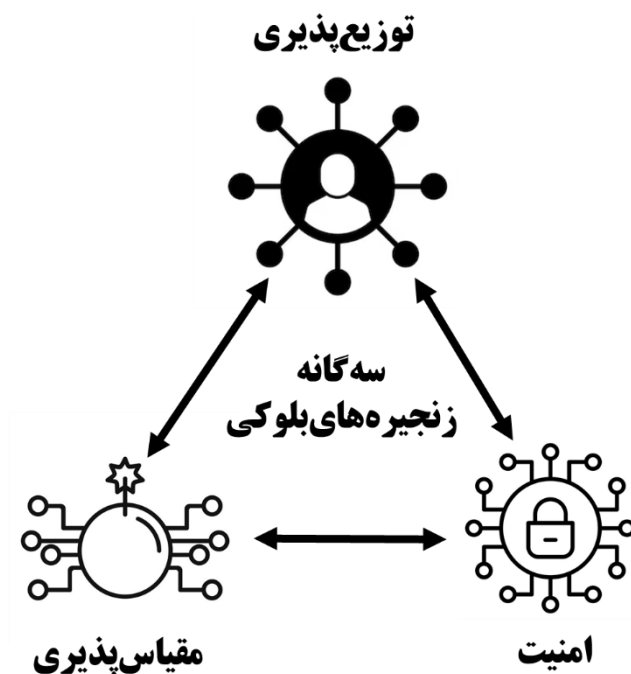
در فصل گذشته، به معرفی کلی زنجیره بلوکی پرداختیم و توضیح مختصری از تاریخچه و اصول اولیه آن ارائه دادیم. در این فصل، به بررسی مفاهیم مرتبط با شبکه‌های کانال پرداخت و مسائل مقیاس‌پذیری زنجیره‌های بلوکی می‌پردازیم. ابتدا محدودیت‌های سه‌گانه رمزارزها شامل غیرمتمرکز بودن، امنیت و مقیاس‌پذیری را شرح خواهیم داد. سپس مشکل اصلی بیت‌کوین که همان مسئله مقیاس‌پذیری است، به تفصیل بررسی می‌شود. در ادامه، راه‌حل‌های مختلف ارائه‌شده برای رفع این مشکل مرور شده و شبکه‌های کانال پرداخت به عنوان بهترین راه‌حل لایه دوم معرفی می‌شوند. به طور خاص، شبکه لایت‌نینگ به عنوان نمونه‌ای مهم از این شبکه‌ها بررسی خواهد شد. سپس، با تمرکز بر مسئله محوری پایان‌نامه، مروری جامع بر مشکلات موجود در شبکه‌های کانال پرداخت خواهیم داشت و در نهایت مقالات کلیدی این حوزه را مرور می‌کنیم تا ادبیات پژوهش را روشن سازیم. در پایان، ابزارهای حل مسئله مانند بهینه‌سازی محدب، نظریه گراف و الگوریتم‌های پیدا کردن کوتاه‌ترین مسیر معرفی می‌شوند تا در فصل بعد بتوانیم مدل‌سازی مسئله مورد نظر را انجام دهیم.

۲-۲- مفاهیم مورد نیاز برای ورود به موضوع، مشکلات و راه‌حل‌ها

در این بخش می‌خواهیم یک آشنایی نسبتاً کلی از شبکه‌های کانال پرداخت در رمزارزها پیدا کنیم. ابتدا مسئله سه‌گانه مقیاس‌پذیری در زنجیره‌های بلوکی را توضیح می‌دهیم و یکی از رایج‌ترین و اصلی‌ترین مشکلات رمزارزها را بیان می‌کنیم و شروع به بیان بهترین راه‌حل برای حل آن مشکل می‌کنیم از ایجاد کانال‌های پرداخت تا شبکه کانال‌های پرداخت و راه ایجاد امنیت آن و معرفی معروف‌ترین شبکه کانال پرداخت تا بتوانیم وارد فهمیدن مقالات مهم این حوزه شویم.

۱-۲-۲- مسئله سه گانه مقیاس پذیری در زنجیره های بلوکی

بنیان گذار شبکه اتریوم، ویتالیک بوتیرین^۴ برای اولین بار به مشکل همزمانی سه ویژگی کلیدی در زنجیره بلوکی اشاره کرد: غیرمتمرکز بودن، امنیت و مقیاس پذیری. وی به این نتیجه رسید که نمی توان همزمان تمام این ویژگی ها را به حداکثر رساند. در واقع، افزایش هر دو ویژگی باعث کاهش ویژگی دیگری می شود. البته این موضوع تاکنون به صورت تجربی مشاهده شده و اثبات ریاضی دقیقی وجود ندارد. اما ممکن است در آینده الگوریتم ها ارائه شود که این مشکل را حل کنند [11].



شکل: ۱ سه ویژگی کلیدی بلاکچین ها

که معمولاً یکی از آنها را نمی توان به همراه دو مورد دیگر در شبکه ایجاد کرد، امنیت، مقیاس پذیری و توزیع شدگی

۲-۲-۲- غیرمتمرکز بودن

در دنیای زنجیره بلوکی، شاهد توزیع اطلاعات و پردازش تراکنش ها در میان شبکه ای از گره ها (گره ها) هستیم. این امر در تضاد با سیستم های سنتی متمرکز است که در آنها یک نهاد مرکزی قدرت را در اختیار دارد. هرچه تعداد گره های فعال در شبکه بیشتر باشد، تمرکززدایی و پایداری آن نیز افزایش می یابد و شبکه زنجیره بلوکی

⁴ Vitalik Buterin

غیرمتمرکزتر خواهد شد. این ویژگی‌ها، امنیت، مقاومت در برابر سانسور و کارآمدی را به ارمغان می‌آورند. میزان تمرکززدایی در زنجیره‌های بلوکی می‌تواند متفاوت باشد. برخی از آنها مانند زنجیره‌های بلوکی خصوصی، برای مصارف خاص مانند زنجیره تأمین یا مدیریت هویت طراحی شده‌اند، درحالی‌که زنجیره‌های بلوکی عمومی مانند اتریوم یا بیت‌کوین برای کاربردهای عمومی‌تر مانند مبادلات مالی و ذخیره‌سازی داده‌ها مناسب هستند.

۳-۲-۲- امنیت

در دنیای زنجیره‌بلوکی، مقاومت در برابر حملات خارجی و دست‌کاری داخلی، نقشی اساسی در تعیین سطح امنیت این فناوری نوظهور ایفا می‌کند. دو چالش عمده در حوزه امنیت زنجیره‌بلوکی وجود دارد که راه‌حلهایی نیز برای آنها مطرح شده است.

چالش اول حمله ۵۱ درصدی است که زمانی رخ می‌دهد که گروهی از ماینرها با تسلط بر بیش از ۵۰ درصد قدرت پردازش شبکه، امکان کنترل و دست‌کاری در تراکنش‌ها و اطلاعات را به دست می‌آورند. این موضوع می‌تواند به فاجعه‌ای برای امنیت شبکه و اعتماد کاربران به آن منجر شود و تأثیرات آن از دست‌رفتن کنترل شبکه، امکان دست‌کاری تراکنش‌ها و اطلاعات، خدشه‌دار شدن اعتماد کاربران است و راه‌حل آن تمرکززدایی است که افزایش تعداد گره‌ها در شبکه، انجام این نوع حمله را به دلیل نیاز به منابع و قدرت پردازش بسیار بیشتر، دشوارتر می‌کند.

چالش دوم دو بار خرج کردن است که به وضعیتی اطلاق می‌شود که در آن یک کاربر با فریب‌دادن شبکه، امکان خرج کردن یک واحد پول دیجیتال را به طور غیرمجاز برای چندین بار به دست می‌آورد. این موضوع می‌تواند به کلاهبرداری و از بین رفتن اعتماد به ارزهای دیجیتال منجر شود تأثیرات آن کلاهبرداری، از بین رفتن اعتماد به ارزهای دیجیتال، خدشه‌دار شدن امنیت شبکه است و راه‌حل آن الگوریتم‌های اجماع است؛ مانند اثبات سهم^۵ (PoS) و اثبات کار (PoW) راه‌حلهایی هستند که برای جلوگیری از دو بار خرج کردن طراحی شده‌اند. این الگوریتم‌ها با ایجاد مکانیزم‌هایی برای تأیید تراکنش‌ها و شناسایی تراکنش‌های غیرمعتبر، امنیت شبکه را افزایش می‌دهند.

^۵ Proof-of-Stake (PoS)

۴-۲-۲- مقیاس پذیری

مقیاس پذیری در زنجیره بلوکی به توانایی و ظرفیت شبکه در مدیریت حجم تراکنش‌ها، تعداد گره‌ها و سرعت پردازش اطلاعات اشاره دارد. درحالی که زنجیره بلوکی پتانسیل‌های انقلابی زیادی را به ارمغان می‌آورد، مقیاس پذیری یکی از چالش‌های اساسی پیشروی این فناوری است.

مقیاس پذیری در زنجیره بلوکی شامل سه مؤلفه اصلی است؛ تراکنش در ثانیه: تعداد تراکنش‌هایی که شبکه می‌تواند در یک ثانیه پردازش و تأیید کند. تعداد گره‌ها: تعداد دستگاه‌هایی که در شبکه زنجیره بلوکی فعال هستند و از آن پشتیبانی می‌کنند. سرعت پردازش اطلاعات: سرعت انتقال و تأیید اطلاعات در شبکه.

برخی از زنجیره‌های بلوکی، مانند بیت کوین، با محدودیت‌های قابل توجهی در زمینه مقیاس پذیری مواجه هستند. برای مثال، شبکه بیت کوین در هر ثانیه تنها قادر به پردازش حدود ۷ تراکنش است، درحالی که شبکه‌های پرداختی سنتی مانند ویزا می‌توانند هزاران تراکنش را در یک ثانیه پذیرش و تأیید کنند.

دلایل اصلی این محدودیت‌ها شامل:

ذخیره سازی اطلاعات: رشد شبکه و افزایش تعداد تراکنش‌ها به معنای افزایش حجم اطلاعات برای ذخیره سازی است. این موضوع می‌تواند بار پردازشی شبکه را افزایش دهد و سرعت آن را کاهش دهد.

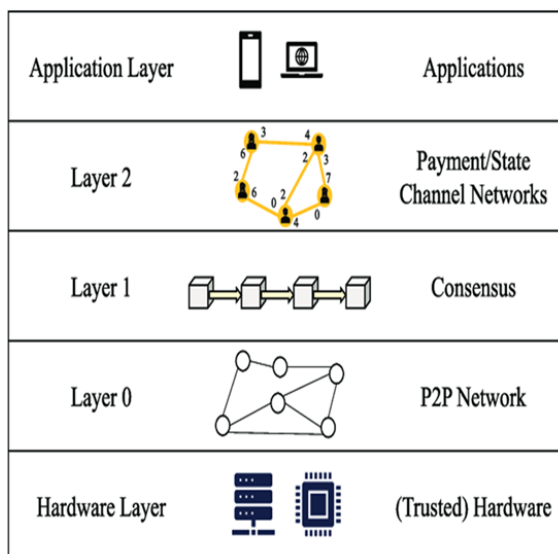
اجماع: در زنجیره‌های بلوکی مبتنی بر اثبات کار (PoW)، فرایند اجماع برای تأیید تراکنش‌ها می‌تواند بسیار زمان‌بر و پرمصرف باشد. این موضوع نیز بر مقیاس پذیری شبکه تأثیر منفی می‌گذارد.

مقیاس پذیری زنجیره بلوکی چالش پیچیده‌ای است که نیاز به توجه و تلاش مداوم دارد. با این حال، راه‌حل‌های مختلفی برای غلبه بر این محدودیت‌ها وجود دارد و تحقیقات و نوآوری در این زمینه به طور فعال در حال انجام است. با توسعه راه‌حل‌های مقیاس پذیر کارآمد، می‌توان انتظار داشت که زنجیره بلوکی نقشی اساسی در آینده امور مالی، زنجیره تأمین، مدیریت هویت و سایر زمینه‌ها ایفا کند.

۳-۲- لایه بندی شبکه

همانند شبکه‌های داده و مخابراتی رمزارزها را هم لایه بندی کرده‌اند تا بتوانند راحت تر توسعه یابند و هر کس روی قسمتی از این شبکه‌ها کار کند.

به این صورت است که لایه منفی یک یا سخت‌افزار را سخت‌افزار محاسبه کننده گذاشته‌اند که همان کامپیوترها است معمولاً و لایه صفر را شبکه p2p قرار می‌دهند که امکان ایجاد ارتباط مستقیم را هر کاربر با کاربر دیگر داشته باشد، لایه یک را شبکه زنجیره‌بلوکی قرار داده‌اند که پروتکل رمزارز موردنظر را روی هر کامپیوتر در هر بلاک انجام می‌دهند و لایه دوم را شبکه‌های کانال پرداختی قرار دادند که با کمک آن زنجیره‌بلوکی تراکنش‌ها را ایجاد می‌کنند و در لایه آخر هم لایه اپلیکیشن را قرار دادند که کاربر بدون نیاز به دانش خاصی با رابط کاربری خودش از تمامی این شبکه‌ها استفاده کند.



شکل ۲: لایه بندی شبکه کانال پرداخت، عکس از مقاله [52]

۴-۲- مشکل مقیاس‌پذیری مهم‌ترین رمزارزها و راه‌حل‌ها

با پیشروی بیت‌کوین به‌عنوان اولین رمزارزی که از فناوری زنجیره‌بلوکی بهره برد، ایده انتقال دارایی به‌صورت هم‌تا به هم‌تا و بدون واسطه مؤسسه‌ای معرفی شد. این ابزار، در میان کاربران جایگاهی خاص به دست آورد. فناوری زنجیره‌بلوکی قبل از ظهور بیت‌کوین نیز موجود بود، اما بیت‌کوین توانست آن را به‌صورت کاربردی برای عموم مردم به کار گیرد. با این حال، به‌عنوان اولین رمزارز که قابلیت پرداخت هم‌تا به هم‌تا را فراهم کرد، بیت‌کوین با مشکلاتی در مقیاس‌پذیری روبه‌رو است. مقایسه سرعت تراکنش‌ها در شبکه بیت‌کوین با سیستم‌های دیگر مانند شبکه پرداخت ویزا نشان می‌دهد که سرعت تراکنش‌ها در شبکه بیت‌کوین بسیار کمتر است. این مشکل باعث افزایش هزینه‌های پرداخت می‌شود، زیرا در صورت افزایش تقاضا برای انتقال وجه، ماینرها معمولاً دستمزد بیشتری برای ضمیمه کردن تراکنش‌ها به بلاک می‌گیرند؛ بنابراین، با افزایش تقاضا، کاربران مجبورند دستمزد پرداختی

خود را افزایش دهند و در نتیجه سرعت پرداخت کاهش می‌یابد، به‌ویژه زمانی که تعداد تراکنش‌ها بیشتر از ظرفیت شبکه باشد.

مشکل مقیاس‌پذیری در بیت‌کوین به‌گونه‌ای است که توانایی برون‌دهی^۶ شبکه بیت‌کوین تا حدود ۵ تراکنش در ثانیه محدود است و برای اطمینان از انجام یک تراکنش، باید حدود یک ساعت منتظر بمانید، همچنین کارمزد آن نیز از ۰.۱۵ تا ۳ دلار برای هر تراکنش در سال ۲۰۲۲ بوده است.

۱-۴-۲- روش‌های افزایش مقیاس‌پذیری در زنجیره‌بلوکی

همان‌طور که گفته شد در دنیای زنجیره‌بلوکی، همواره تناقضی بین سه اصل کلیدی وجود دارد: امنیت، تمرکززدایی و مقیاس‌پذیری. توسعه‌دهندگان اغلب با چالش فداکردن یکی از این عوامل برای ارتقای دو مورد دیگر مواجه هستند. با در نظر گرفتن این چالش، راه‌حل‌های مختلفی برای افزایش مقیاس‌پذیری زنجیره‌بلوکی ارائه شده است که می‌توان آن‌ها را به دودسته کلی تقسیم کرد:

۱. راهکارهای درون شبکه (لایه یک): این دسته از راه‌حل‌ها به دنبال ارتقای مقیاس‌پذیری با ایجاد تغییرات در ساختار و پروتکل‌های زنجیره‌بلوکی هستند. برخی از نمونه‌های این روش‌ها عبارت‌اند از افزایش اندازه بلاک، تغییر الگوریتم اجماع، بهینه‌سازی ساختار داده و

۲. راهکارهای خارج از شبکه (لایه دو): این دسته از راه‌حل‌ها به‌جای ایجاد تغییرات در لایه اصلی زنجیره‌بلوکی، بر روی سطوح جانبی یا لایه‌های دوم تمرکز دارند. هدف این راه‌حل‌ها، انتقال بخشی از بار پردازش تراکنش‌ها از زنجیره اصلی به این لایه‌های جانبی است. برخی از نمونه‌های راهکارهای لایه دو عبارت‌اند از: کانال‌های پرداخت، شبکه‌های جانبی، راه‌حل‌های جمع‌آوری تراکنش و

هیچ راه‌حل واحدی برای مشکل مقیاس‌پذیری زنجیره‌بلوکی وجود ندارد. انتخاب بهترین روش به نیازها و الزامات خاص هر زنجیره‌بلوکی بستگی دارد. تمرکز این پایان‌نامه روی راهکارهای خارج از شبکه یا لایه دو می‌باشد برای همین راهکارهای لایه دوم را شرح می‌دهیم.

^۶ throughput

۲-۴-۲- راهکارهای لایه یک مقیاس‌پذیری در زنجیره بلوکی

برای افزایش مقیاس‌پذیری بلاک‌چین، راه‌حل‌های لایه ۱ به طور مستقیم در پروتکل اصلی زنجیره بلوکی تغییراتی ایجاد می‌کنند تا عملکرد و کارایی شبکه را بهبود بخشند. این راه‌حل‌ها شامل دسته‌های مختلفی از جمله بلوک داده^۷، الگوریتم‌های اجماع جایگزین، شاردینگ^۸ و گراف جهت‌دار غیرمدور^۹ می‌باشند.

راه‌حل‌های دسته بلوک داده شامل تغییرات در ساختار و نحوه ذخیره‌سازی داده‌های بلاک است تا بتوان حجم بیشتری از داده‌ها را در یک بلاک جا داد. الگوریتم‌های اجماع جایگزین شامل الگوریتم‌های جدیدی برای رسیدن به توافق در شبکه هستند که از پروتکل‌های سنتی مانند اثبات کار و اثبات سهام فراتر می‌روند. شاردینگ به تقسیم کردن زنجیره بلوکی به بخش‌های کوچک‌تر می‌پردازد که هر یک از این شاردها قادر به پردازش تراکنش‌های خود به صورت مستقل هستند. در نهایت، گراف جهت‌دار غیرمدور ساختاری بدون حلقه برای ذخیره‌سازی تراکنش‌ها استفاده می‌کند که می‌تواند ترافیک تراکنش‌ها را بهبود بخشد. برای نمونه شاردینگ و دو پروتکل مهم گراف جهت‌دار غیرمدور که پروتکل سنگین‌ترین زیردرخت مشاهده شده حریص^{۱۰} (گوست) و پیشنهاد و رأی‌گیری در پروتکل‌های چندلایه خرد شده^{۱۱} (پریزم) را توضیح بیشتری می‌دهیم. دسته‌بندی گفته شده در این بخش مطابق دسته‌بندی [12] می‌باشد.

شاردینگ:

شاردینگ تکنیکی شناخته شده برای مقیاس‌پذیری پایگاه‌های داده است. ایده اصلی این است که دفترکل به چندین زیر-دفتر جدا تقسیم شود و ماینرها روی شاردهای مختلف کار کنند. چالش‌های اصلی شامل احتمال کنترل یک شارد توسط یک دشمن و ارتباطات بین شاردها است. برای مقابله با این چالش‌ها، تخصیص احتمالی و پویا بهترین گزینه به نظر می‌رسد [13].

سنگین‌ترین زیردرخت مشاهده شده حریص (گوست):

پروتکل گوست یک رویکرد نوآورانه برای بهبود مقیاس‌پذیری و امنیت بلاک‌چین است. به جای اینکه تنها به طولانی‌ترین زنجیره اعتماد کنیم، این پروتکل از یک ساختار درختی بهره می‌برد که در آن فورک‌ها (شاخه‌ها) نیز

⁷ Blockdata

⁸ Sharding

⁹ Directed Acyclic Graphs(DAG)

¹⁰ Greedy Heaviest Observed Subtree (GHOST)

¹¹ Proposing and Voting in Sharded Multilayer Protocols (PRISM)

مورد استفاده قرار می‌گیرند. در این پروتکل، گره‌های صادق به‌جای دنبال کردن طولانی‌ترین زنجیره، سنگین‌ترین زیرشاخه‌ها را دنبال می‌کنند، زیرا فورک‌ها دیگر به‌عنوان یک عمل مخرب در نظر گرفته نمی‌شوند. این تغییر رویکرد باعث می‌شود که بلوک‌های بیشتری مورد استفاده قرار گیرند و امنیت شبکه افزایش یابد. پروتکل گوست برای مقابله با حملات خصوصی با قدرت چکیده ۴۹٪ مقاوم است، زیرا دشمن نمی‌تواند به راحتی کنترل شبکه را به دست گیرد [14].

پیشنهاد و رأی‌گیری در پروتکل‌های چندلایه خرد شده (پریزم):

پروتکل پریزم یک روش جدید برای افزایش کارایی و مقیاس‌پذیری بلاک‌چین است. این پروتکل از دوزنجیره موازی استفاده می‌کند: زنجیره پیشنهاددهنده و زنجیره رأی‌دهنده. گره‌های کامل در هر دو زنجیره فعالیت می‌کنند. در زنجیره پیشنهاددهنده، بلوک‌ها پیشنهاد می‌شوند و در زنجیره رأی‌دهنده، بلوک‌ها رأی‌گیری می‌شوند. این ساختار باعث می‌شود که تأخیر کاهش یابد و نیاز به قانون تأیید ۶ بلوک حذف شود. پروتکل پریزم به دنبال بهره‌برداری بهینه از پهنای باند موجود در اینترنت و کاهش تأخیر ارتباطات بلاک‌چین است. با استفاده از این پروتکل، می‌توان به عملکرد بهتری در انتقال داده‌ها و تأیید تراکنش‌ها دست یافت [15].

۳-۴-۲- راهکارهای لایه دو مقیاس‌پذیری در زنجیره بلوکی

درست همان‌طور که در دنیای واقعی از بزرگراه‌ها برای حمل و نقل انبوه استفاده می‌شود، راه‌حل‌های لایه ۲ نیز در دنیای زنجیره بلوکی برای افزایش مقیاس‌پذیری و ارتقای کارایی شبکه به کار گرفته می‌شوند. این راه‌حل‌ها با انتقال بخشی از بار پردازش تراکنش‌ها از زنجیره اصلی زنجیره بلوکی به لایه‌ای جداگانه، به شبکه امکان می‌دهند تا تراکنش‌های بیشتری را در واحد زمان (معمولاً ثانیه) پردازش کند. برخلاف راه‌حل‌های لایه ۱ که مستلزم ایجاد تغییرات در پروتکل اصلی زنجیره بلوکی هستند، راه‌حل‌های لایه ۲ بر روی زیرساخت موجود زنجیره بلوکی بنا می‌شوند و مزایای متعددی از جمله سرعت بالا، کارمزد پایین و انعطاف‌پذیری را به ارمغان می‌آورند. راه‌حل‌های لایه دومی برای مقیاس‌پذیری بلاک‌چین که به‌منظور افزایش کارایی و کاهش مشکلات شبکه‌های بلاک‌چینی فعلی پیشنهاد شده‌اند شامل کانال‌ها، زنجیره‌های جانبی و کودک، زنجیره‌های متقابل و راه‌حل‌های ترکیبی است که از مهم‌ترین نمونه‌های آنها زنجیره‌های جانبی و شبکه لایتینگ (یک شبکه کانال پرداخت معروف) است که در زیر توضیح خواهیم داد [16].

زنجیره‌های جانبی:

زنجیره‌های جانبی بلاک‌چین‌های جداگانه‌ای هستند که به زنجیره اصلی متصل می‌شوند. این زنجیره‌ها می‌توانند تراکنش‌های کمتر مهم (مانند خرید یک فنجان قهوه) را پردازش کنند. چون امنیت کمتری نیاز دارند، سرعت بلوک می‌تواند افزایش یابد. زنجیره‌های جانبی از زنجیره اصلی به‌عنوان مرجع استفاده می‌کنند و انتقال سکه‌ها بین زنجیره‌ها امکان‌پذیر است (راه‌حل‌های فعلی عمدتاً بر صرافی‌های مرکزی تکیه دارند).

شبکه لایتنینگ^{۱۲}:

شبکه لایتنینگ راه‌حلی لایه ۲ برای بیت‌کوین است که به کاربران امکان می‌دهد تراکنش‌های خود را به‌صورت خارج از زنجیره اصلی و با سرعتی بسیار بالا و کارمزدی بسیار پایین انجام دهند. نحوه عملکرد شبکه لایتنینگ: کاربران دو کیف پول لایتنینگ را به یکدیگر متصل می‌کنند و یک کانال پرداختی بین خود ایجاد می‌کنند. بیت‌کوین‌ها در ابتدای کار به کانال واریز می‌شوند. تراکنش‌های بعدی بین کاربران در داخل کانال انجام می‌شوند و نیازی به ثبت هر تراکنش در زنجیره اصلی بیت‌کوین نیست. در نهایت، کاربران می‌توانند کانال را با تسویه حساب نهایی و بازگشت بیت‌کوین‌های باقی‌مانده به زنجیره اصلی، ببندند. مزایای شبکه لایتنینگ شامل سرعت تراکنش بالا: تراکنش‌ها در عرض چند میلی‌ثانیه انجام می‌شوند. کارمزد پایین: کارمزد تراکنش‌ها بسیار ناچیز است. قابلیت انعطاف‌پذیری: می‌توان از آن برای پرداخت‌های خرد و کلان استفاده کرد [17].

راه‌حل‌های لایه ۲ هنوز در مراحل اولیه توسعه خود هستند و چالش‌هایی مانند امنیت، حریم خصوصی و مقیاس‌پذیری در آن‌ها وجود دارد. بااین‌حال، این راه‌حل‌ها پتانسیل قابل توجهی برای ارتقای عملکرد بلاک‌چین‌ها و گسترش کاربردهای آن‌ها در دنیای واقعی دارند.

۵-۲- آشنایی با شبکه کانال پرداخت

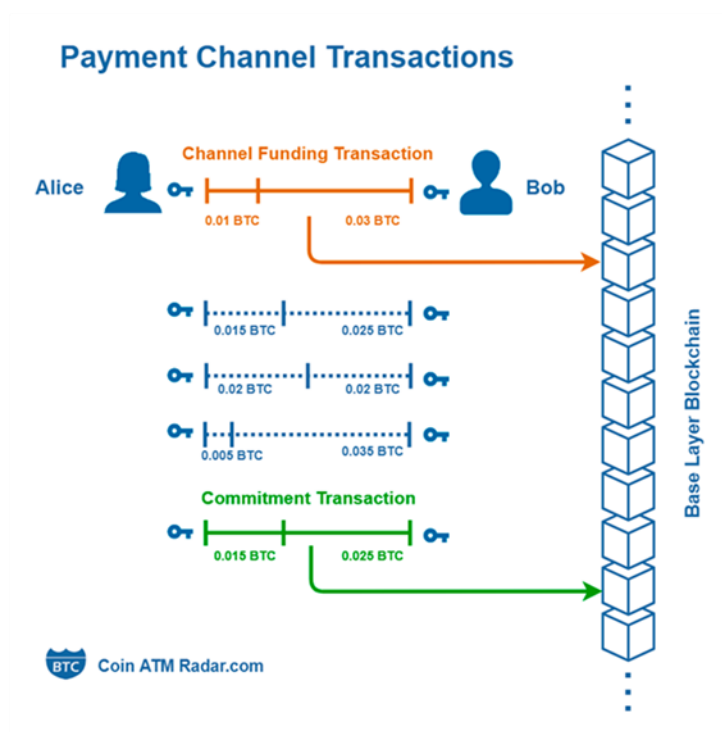
۱-۵-۲- کانال پرداخت

فرض کنید من و شما چندین بار تبادلاتی مالی بین خودمان داشته‌ایم. در این حالت، می‌توانیم از ثبت تبادلات بر روی زنجیره‌بلوکی صرف‌نظر کنیم و آن‌ها را خارج از زنجیره انجام دهیم. به زبان ساده، ما یک کانال پرداخت بین خودمان باز می‌کنیم و بازگشایی این کانال را در زنجیره‌بلوکی ثبت می‌کنیم. حال، ما هر زمان که خواستیم

¹² Lightning Network

می‌توانیم از این کانال پرداخت برای انجام تبادلات استفاده کنیم و این کانال می‌تواند برای مدت‌های طولانی باز بماند. تنها زمانی که دوباره نیاز به زنجیره‌بلوکی داریم، زمانی است که می‌خواهیم کانال را ببندیم. در ادامه، وضعیت نهایی تبادلاتی که از این کانال استفاده شده است را در زنجیره‌بلوکی ثبت می‌کنیم.

ایده این است که از زنجیره‌بلوکی به‌عنوان داور و اعتباردهنده تنها در صورت لزوم استفاده شود و بقیه تبادلات بین دو نفر از طریق رمزگذاری و با اعتماد انجام شود.

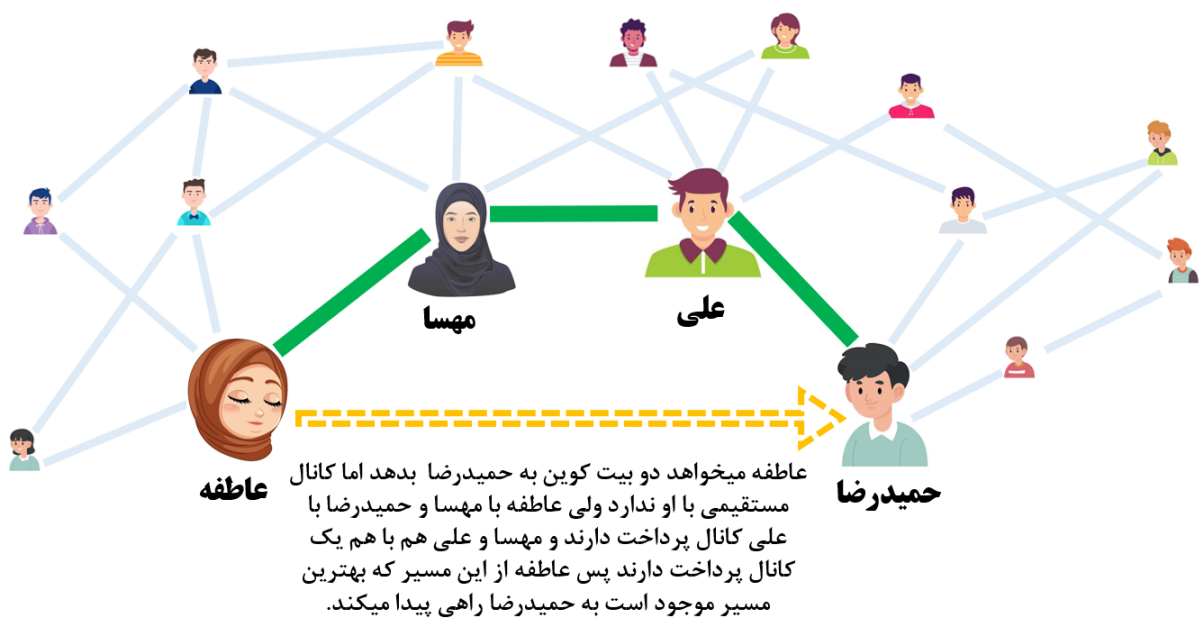


شکل ۳: در اینجا یک کانال ایجاد شده که در آن ۵ تراکنش انجام شده و از آن فقط دو تراکنش در بلاکچین ثبت شده است [51].

۲-۵-۲- شبکه کانال پرداخت

ایده کانال‌های پرداخت به‌گونه‌ای گسترش‌یافته است که به هر فردی که کانال پرداخت دارد، بدون لزوم وجود کانال مشترکی بین آنها، امکان پرداخت داده شود. این ایده با شبکه‌بندی تمامی گره‌ها و کانال‌های پرداختشان عملی شده است. در این روند، گره مبدأ با انتقال پول از خود به گره‌های میانی، پول را به کاربر مقصد می‌رساند و گره‌های میانی در مقابل این خدمت، کارمزدی از پرداخت‌کننده دریافت می‌کنند.

در این رویکرد، هر فردی که کانالی را ایجاد می‌کند، این اطلاعات را به صورت عمومی منتشر می‌کند و میزان ظرفیت کلی کانال را نیز اعلام می‌کند. این باعث می‌شود که تمامی کاربران یک توپولوژی از تعدادی گره و کانال داشته باشند که با یکدیگر وصل شده‌اند. به این ترتیب، هر کاربری اگر مسیری از خود به کاربر موردنظر در شبکه داشته باشد، می‌تواند پول را از طریق دست به دست کردن سکه‌ها در کانال‌های پرداخت جابه‌جا کند بدون نیاز به ایجاد کانال پرداخت جدید. برای تشویق گره‌ها به شرکت در این تراکنش‌ها، هر گره برای انتقال پول در مسیر مقداری کارمزد از پرداخت‌کننده دریافت می‌کند.



شکل ۴: مسیریابی پرداخت از عاطفه به حمیدرضا در شبکه کانال پرداخت

۳-۵-۲- قراردادهای قفل‌شده با چکیده و زمان

قراردادهای قفل‌شده با چکیده و زمان^{۱۳} از فناوری‌های کلیدی است که شبکه‌های کانال پرداخت را امکان‌پذیر می‌سازد. این قراردادها نوعی تراکنش بیت‌کوین است که از قابلیت‌های چند امضایی و قفل زمانی استفاده می‌کند. این ویژگی‌ها از قبل در پروتکل بیت‌کوین وجود داشته‌اند و با ترکیب آنها می‌توان این قراردادها را ایجاد کرد.

¹³ Hashed TimeLock Contract (HTLC)

چند امضایی^{۱۴}: این قابلیت به چند امضا برای خرج کردن بیت کوین ها نیاز دارد.

قفل زمانی^{۱۵}: این قابلیت اجازه می دهد تراکنش ها تا رسیدن به یک زمان مشخص یا شماره بلاک خاص خرج نشوند.

حال می خواهیم با توضیح مثالی کارکرد این قراردادهای قفل شده با چکیده و زمان را توضیح دهیم.

مثال: عبور تراکنش از مسیر عاطفه، مهسا، علی، و حمیدرضا بدون اعتماد به هم

فرض کنید عاطفه می خواهد یک کوین به حمیدرضا بفرستد. عاطفه و مهسا، مهسا و علی، و علی و حمیدرضا هر کدام کانال های پرداخت با یکدیگر دارند. مراحل قراردادهای قفل شده با چکیده و زمان به این شکل انجام می شود:

ایجاد مقدار تصادفی و چکیده^{۱۶}: حمیدرضا یک مقدار تصادفی مخفی (secret) ایجاد کرده و چکیده آن را محاسبه می کند ($hash = H(secret)$). حمیدرضا چکیده را به عاطفه می دهد.

شروع تراکنش توسط عاطفه:

عاطفه یک تراکنش دوامضایی با مهسا ایجاد می کند که شامل شرایط زیر است:

مهسا می تواند کوین را دریافت کند اگر مقدار مخفی را در زمان مشخصی ارائه دهد.

اگر مهسا نتواند مقدار مخفی را ارائه دهد، کوین به عاطفه بازگردانده می شود.

انتقال از مهسا به علی:

مهسا یک تراکنش دوامضایی با علی ایجاد می کند که شرایط مشابهی دارد:

علی می تواند کوین را دریافت کند اگر مقدار مخفی را در زمان مشخصی ارائه دهد.

اگر علی نتواند مقدار مخفی را ارائه دهد، کوین به مهسا بازگردانده می شود.

انتقال از علی به حمیدرضا:

¹⁴ Multi-Signature

¹⁵ Time Lock

¹⁶ hash

علی یک تراکنش دوامضایی با حمیدرضا ایجاد می‌کند:

حمیدرضا می‌تواند کوین را دریافت کند اگر مقدار مخفی را در زمان مشخصی ارائه دهد.

اگر حمیدرضا نتواند مقدار مخفی را ارائه دهد، کوین به علی بازگردانده می‌شود.

افشای مقدار مخفی:

حمیدرضا مقدار مخفی را با قرارداد قفل‌شده با چکیده و زمان به علی ارائه می‌دهد تا کوین را دریافت کند.

علی پس از دریافت مقدار مخفی، همان مقدار را با قرارداد قفل‌شده با چکیده و زمان به مهسا ارائه می‌دهد تا کوین را دریافت کند.

مهسا پس از دریافت مقدار مخفی، آن را با قرارداد قفل‌شده با چکیده و زمان به عاطفه ارائه می‌دهد تا کوین را دریافت کند.

تراکنش‌ها با استفاده از رمزنگاری و محدودیت‌های زمانی انجام می‌شوند، بنابراین نیازی به اعتماد به یکدیگر نیست. قرارداد قفل‌شده با چکیده و زمان می‌تواند در مبادلات بین زنجیره‌ای و شبکه‌های لایتینگ استفاده شود. با استفاده از قرارداد قفل‌شده با چکیده و زمان و شبکه لایتینگ، کاربران می‌توانند تراکنش‌های سریع، امن و بی‌نیاز به اعتماد انجام دهند. این فناوری یکی از مهم‌ترین اجزای بهبود مقیاس‌پذیری و کارایی شبکه‌های بلاک‌چینی مانند بیت‌کوین است.

۴-۵-۲- شبکه لایتینگ

شبکه لایتینگ که در سال ۲۰۱۷ معرفی شد، به‌عنوان اولین شبکه کانال پرداخت بیت‌کوین شناخته می‌شود. این شبکه باوجود نوپایی و چالش‌های پیشرو، مسیری روبه‌رشد را طی می‌کند و خدمات قابل‌توجهی به کاربران ارائه می‌دهد [17].

اگرچه شبکه لایتنینگ هنوز به جایگاه ایده‌آل توسعه‌دهندگان در زمینه پرداخت‌های روزمره نرسیده است، اما شاهد پیشرفت‌های چشمگیری در آن هستیم. طبق آمار سایت ml1 در مرداد ۱۴۰۳، این شبکه میزبان بیش از ۵۰۰۰ بیت‌کوین به ارزش تقریبی ۱۰۰ میلیون دلار است و ۱۳۳۷۲ گره فعال در آن مشغول به فعالیت هستند. تعداد کل کانال‌های مالی این شبکه در این تاریخ به بیش از ۵۰۰۰۰ کانال رسیده که این مقدار تغییرات زیادی داشته و متناسب با شرایط آن زمان بیشتر یا کمتر می‌شود.

Real-Time Lightning Network Statistics			
Number of Nodes	Number of Channels	Network Capacity	Node Countdown
13,372 ↓ -2.24%	50,061 ↓ -2.8%	5,225.27 BTC ↑ +2% \$349,890,241.08	986,631 1.3%
Nodes Observed	New Nodes (24h)	New Channels (24h)	Channel Countdown
52,661 ↑ +0.69%	12 ↑ +100.00%	218 ↑ +87.93%	949,939 5.0%
Nodes with Public IP	Updated Nodes (24h)	Updated Channels (24h)	Capacity Countdown
11,497	3,317	45,887	994,775 0.52%
Average Node Capacity	Average Channel Capacity	Layer 1 Capacity Ratio	
0.391 BTC \$26,166.02	0.104 BTC \$6,977.52	0.024882%	
Average Node Age	Average Channel Age	Average Channels per Node	
1,008.7 days 2 years	587.5 days a year	7.49	
IPv6 Nodes	Tor Onion Service Nodes	Median Base Fee	Median Fee Rate
210	9,504	0.998880 sat \$0.000668862	0.000077 sat/sat \$0.000000051651/sat

شکل ۵: مشخصات و آمار کلی شبکه لایتنینگ

باوجود این پیشرفت‌ها، شبکه لایتنینگ هنوز فاصله قابل‌توجهی با رقبای خود دارد. در زمان نگارش این متن ارزش دارایی‌های ذخیره‌شده در این شبکه ۳۵۰ میلیون دلار است، درحالی‌که این رقم در شبکه Flexa (یک بستر پرداخت مالی) به بیش از ۱.۲ میلیارد دلار می‌رسد.

۲-۶- معرفی مسائل موجود در شبکه کانال پرداخت

اکثر مقالات موجود در حوزه شبکه کانال پرداخت از نظر ما به چهار دسته کلی تقسیم می‌شوند:

دسته اول: مکانیزم‌های مسیریابی و بالانس ظرفیت‌ها

دسته دوم: استراتژی‌های پیوستن به شبکه یا تعیین کارمزد پس از پیوستن باهدف بهینه‌کردن تابع هدف خاصی

دسته سوم: تحلیل انواع شبکه‌های ایجاد شده با مکانیزم‌های متفاوت

دسته چهارم: امنیت و حملات قابل‌انجام به هر یک از این مکانیزم‌ها

و هدف هر چهار دسته معمولاً افزایش بهره‌وری، امنیت و حریم خصوصی شبکه‌های کانال پرداخت یا یک گره از این شبکه است که در هر کدام یک از این دسته‌ها مقالات بسیار زیادی نوشته شده‌اند. ما در این پایان‌نامه روی دسته اول تمرکز داریم یعنی پیشنهاد روش یا مکانیزمی در مسیریابی یا تغییر بالانس ظرفیت‌ها یا هر مکانیزمی در این شبکه تا بهره‌وری این شبکه را از حالت قبلی خود بهبود دهد.

به طور ویژه، تمرکز ما بر بهبود بهینه‌سازی مسیریابی در شبکه است تا تعداد بیشتری از پرداخت‌ها با کارمزد کمتر انجام شود. همچنین، تلاش داریم تا مشکل تمرکز شبکه را که در مقالات تحلیلی این حوزه به آن اشاره شده است، کاهش دهیم.

در این مرور ادبیات ابتدا مقالات مهم و مرتبط دسته اول با محوریت مسیریابی را شرح می‌دهیم، سپس به مقالاتی از دسته سوم اشاره می‌کنیم که مشکل مرکزیت شبکه‌های کانال پرداخت را تحلیل کرده‌اند و در آخر هم تعدادی از مقالات موجود که راه‌حلی برای مشکل مرکزیت شبکه ارائه داده‌اند را توضیح می‌دهیم.

مقالات دسته دوم و چهارم به علت ارتباط کم با موضوع و ابتکار صورت‌گرفته در مقاله شرح داده نمی‌شود.

۲-۷- مرور ادبیات در حوزه مسیریابی شبکه کانال پرداخت

ابتدا مروری بر مسیریابی‌های کارآمد پیشنهاد شده برای شبکه پرداخت و دسته‌بندی‌های شناخته شده در این مسیریابی‌ها خواهیم کرد که این دسته‌بندی بر اساس دسته‌بندی مقاله [18] بیان شده است تا با فضای ادبیات موضوع آشنا شویم و سپس بعضی مقالات مهم را به صورت مختصر توضیح خواهیم داد.

مسیریابی شبکه لایتینگ که امروزه در حال اجرا است به صورت مسیریابی پیازی [19] انجام می شود به این صورت که مبدأ و مقصد پرداخت ها توسط گره های میانی شناسایی نمی شود و هر گره باتوجه به شناختی که خود از شبکه دارد کوتاه ترین مسیر را از مقصد به مبدأ پیدا می کند.

اکثر مسیریابی های پیشنهادی کارآمد از الگوریتم های حداکثر جریان اصلاح شده استفاده می کنند که تقریباً به دودسته الگوریتم های لندمارک^{۱۷} و الگوریتم های تعبیه-پایه^{۱۸} یا فاصله-پایه^{۱۹} تقسیم می شوند. الگوریتم های لندمارک به این صورت هست که گره هایی به صورت روتر در شبکه قرار دارد که به آنها گره های لندمارک می گویند و همه گره های شبکه، پرداخت ها را به نزدیک ترین گره لندمارک انتقال می دهند و گره های لندمارک با توجه با جدول مسیریابی که دارند پرداخت ها را به گره لندمارک بعدی تا مقصد ارسال می کنند. مسیریابی های flare [20] و silent whispers [21] از جمله مسیریابی های لندمارک کارآمد هستند. اما الگوریتم های تعبیه پایه به این صورت است که هر گره یک بردار تعبیه دارد و در آن گره های با فاصله پرش شبکه^{۲۰} نزدیک خود را قرار می دهند و تراکنش ها به نزدیک ترین همسایه در فضای تعبیه خودانتقال داده می شود. مشکل اصلی این الگوریتم بروز نگه داشتن پویا این فضا در شبکه است. و مسیریابی های کارآمد موجود با این نوع الگوریتم شامل VOUTE [22] و SpeedyMurmurs [23] می شود.

ما مسیریابی ها را به دودسته کلی هم می توانیم تقسیم کنیم مسیریابی پویا و مسیریابی ایستا که مسیریابی پویا مسیر پرداخت در لحظه با کاوش در شبکه تغییر می کند و در آن مسئله هزینه فایده کاوش مسیر و بهینه سازی مسیر مورد توجه است و مهم ترین مسیریابی کارآمد این دسته spider [24] ، Flash [25] و CoinExpress [26] است. مسیریابی ایستا به این صورت است که به صورت دوره ای مسیری ثابت بین دو گره پیشنهاد می دهد مانند مسیریابی های SpeedyMurmurs [23] ، flare [20] و silent whispers [21].

گروه دیگری از ایده ها وجود دارد که علاوه بر بهبود مسیریابی، متعادل کردن مجدد کانال های پرداخت به صورت مؤثر را هدف خود قرار می دهند مانند مسیریابی REVIVE [27].

اگر بخواهیم توضیحی کوچک در مورد مسیریابی هایی که اسم آنها آورده شد داشته باشیم به صورت است که : flare [20] میزان زمان صرف شده برای یافتن مسیر پرداخت را به طور متوسط بهینه می کند، این مسیریابی

¹⁷ . landmark

¹⁸ . embedding-based

¹⁹ . distance-based

²⁰ . network hop distance

فاصله-پایه است به صورت محلی گره ها اطلاعات را بروز می کنند و مسیریابی را با استفاده از مشخص کردن کمترین فاصله پرش شبکه برای هر گره بهینه می کند، درواقع همسایگان را در یک فاصله پرش معین حفظ می کند که زمان پرداخت و وضعیت مسیریابی به حالت بهینه برسد. Flash [25] یک مسیریابی پویا است که بین پرداخت ها متناسب با اندازه ی تراکنش باتوجه به هزینه فایده بین بهینه سازی مسیر و هزینه کاوش، تعادل برقرار میکند. پرداخت های بزرگ و کوچک را از هم جدا می کند و با هر کدام به نحوی برخورد می کند به این صورت که الگوریتم حداکثر جریان اصلاح شده برای پرداخت های بزرگ استفاده می کند و به نحوی این پرداخت ها را انجام می دهد تا کارمزد تراکنش حداقل شود و پرداخت های کوچک مستقیماً با جستجو در جدول مسیریابی با چند مسیر از پیش محاسبه شده برای کاهش سربار کاوش استفاده می شود. CoinExpress [26] یک مسیریابی پویا مبتنی بر کاوش که بر اساس الگوریتم بیشترین جریان Ford-Fulkerson و Breadth-First-Search انجام می شود. فرستنده وضعیت کانال را با کاوشگرها بررسی می کند و موجودی ها را رزرو می کند و هر گره فقط اطلاعات محلی در مورد تمام اطلاعات ورودی و خروجی خود را دارد. REVIVE [27] یک مدل تعادل مجدد برای شبکه کانال پرداخت به صورت خارج از زنجیره است که به جای باز و بسته کردن کانال در زنجیره بلوکی، تخصیص مجدد وجوه بین کانال های پرداخت داخل شبکه صورت بگیرد. هر چه تعداد دورها در گراف شبکه بیشتر شود امکان ایجاد تعادل مجدد شبکه زیاد می شود.

حال به تشریح چند مقاله مهم در حوزه مسیریابی کانال های پرداخت می پردازیم:

مقاله [28] به بیان چالش های ابتدایی شبکه پرداخته و یک مدل اقتصادی از کانال های پرداخت ارائه می دهد و مسئله را به فرم یک مسئله بهینه سازی محدب می نویسد. نویسندگان مقاله با استفاده از الگوریتم مسیریابی دایجسترا راهکاری برای پیدا کردن کوتاه ترین مسیر را ارائه می دهد. در این کار تحقیقاتی، با معکوس کردن جهت گراف پرداخت مشکل عدم پیش بینی مقدار پرداخت دقیق یعنی میزان پرداخت و مجموع کارمزدهای مسیر را حل کرده اند و با این کار پرداخت ها را از آخر به ابتدا انجام می دهند. یعنی به جای کم کردن میزان کارمزد پرداخت در هر کانال مسیر، الگوریتم مقدار هر کارمزد را به میزان کل پرداخت اضافه می کنند و به سمت مبدا حرکت می کند زیرا مسیریابی از آخر انجام می شود و با رسیدن به مبدا مقدار دقیق کل پرداخت از آن مسیر محاسبه شده است با این کار دیگر با مسیری روبه رو نمی شوند که در ابتدا کانال های آن دارای ظرفیت بوده است ولی در طول مسیر با افزایش پرداخت توانایی عبور تراکنش را نداشته باشد. در آخر با شبیه سازی روش پیشنهادی خود به ارزیابی الگوریتم خود می پردازند و در انتها بیان می کنند که در بعضی از مواقع مانند زیاد بودن تعداد تعادل های مجدد شبکه در طول مسیر انجام تراکنش های روی زنجیره اصلی به صرفه تر هستند.

مقاله [24] و پایان نامه [29]، برای اولین بار پیشنهاد بسته‌سازی پرداخت‌ها و انتقال چند مسیر به کنترل نرخ ارسال هر مسیر را مطرح می‌کنند که از مقالات اصلی این حوزه به شمار می‌آیند. در این کار پژوهشی ابتدا چالش‌های رفع نشده، زمان و مسیر پرداخت تراکنش‌ها، مطرح شده و سپس به بیان چالش‌های جدید از جمله چالش بن‌بست پرداخت می‌شود. نویسندگان یک مدل سیال ارائه کرده و با قید تعادل کانال یک مسئله بهینه‌سازی محدب می‌نویسند. برای حل این مسئله بهینه‌سازی توزیع شده از الگوریتم اولیه-دوگان استفاده می‌کنند. بدین صورت که پرداخت‌ها را خرد کرده و از طریق گره‌های واسط که نقش مسیریاب را دارند و با پشتوانه انگیزه‌های مالی، بین گره‌هایی که کانال مستقیم ندارند ارتباط برقرار می‌کنند. گره‌های مسیریاب هر یک صفی با سائز مشخص دارند. انتقال بسته‌ها از مبدأ به مقصد از طریق چندین مسیر مجزا صورت می‌پذیرد. با تغییر اندازه پنجره ورودی مسیر و با استفاده از فیدبک گرفته‌شده از مسیر، نرخ پرداخت هر مسیر را کنترل می‌کنند. در این کار تحقیقاتی، گراف‌های پرداخت کل شبکه به دو گروه دایره ای و گراف جهت دار بدون دور تقسیم بندی شده و ثابت می‌کنند که در دسته اول بدون نیاز به انجام تراکنش در زنجیره اصلی و در دومی با نیاز به انجام تراکنش در زنجیره اصلی می‌توان کل پرداخت‌ها را انجام داد. در انتها با ارائه نتایج شبیه‌سازی برتری الگوریتم پیشنهادی خود را در مقایسه با الگوریتم‌های کارآمد پیشین نشان می‌دهند. به‌طور کلی راه‌حل ارائه شده در این مقاله تغییر مسیریابی اتمی که کوتاه‌ترین مسیر را به مقصد پیدا می‌کند (راه‌حل ذکر شده در مقاله قبلی) به مسیریابی است که پرداخت‌ها را به بسته‌های پرداختی کوچکی تقسیم کرده و چند مسیر غیر مشترک تا مقصد ایجاد و نرخ ارسال بسته‌ها را توسط فیدبکی که در هر مسیر گرفته کنترل می‌کند و گره‌های میانی مانند مسیریاب عمل می‌کنند و در هر طرف خود صف‌هایی دارند تا بسته‌ها را در صورت نداشتن ظرفیت نگهداری کنند. این الگوریتم با استنباط از حل مسئله بهینه‌سازی بیشینه کردن بهره‌وری شبکه با قید متعادل ماندن نرخ عبوری از هر کانال در مدل سیال به دست آمده است.

در مقاله [30] برای اولین بار یک مدل بسته از کانال‌های متقارن خارج از زنجیره ارائه شده است و الگوریتم کارآمدی را برای ساخت درخت پوشای حداقل هزینه، تحت این مدل ارائه می‌دهد و ثابت می‌کند که برای هر نیاز شبکه یک توپولوژی هاب ساده می‌توان ارائه کرد که یک تقریب دوتایی برای حداقل هزینه نگهداری است که نشان می‌دهد درخت پوشا به‌طور کلی کارآمد است. همچنین یک بازی حریصانه بین بازیگرها با قیمت نامحدود که هر بازیکن آرزو می‌کند که هزینه خودش را با تغییر ساختار شبکه کمینه کند ترتیب می‌دهد. در انتها نیز به مقایسه هزینه تراکنش با ساختار تقاضا بی‌مقیاس می‌پردازد.

در مقاله [31] به جای مدل سیال از مدل تصادفی استفاده می‌کند و هر لینک را یک صف دوطرفه در نظر می‌گیرد. بدین معنا که هر بار که یک بسته در دو طرف کانال قرار داشته باشد هر دو را عبور می‌دهد و در غیر این صورت بسته‌ها را نگه می‌دارد و ثابت می‌کند که این تغییر با وجود نبود کنترل‌کننده خارجی ناپایدار می‌ماند و پایداری را با انجام حداقل تراکنش روی زنجیره اصلی به دست می‌آورد و در صورت برقرار بودن قیود تعریف شده که تقریباً همان قیود مقاله [24] است پایداری را اثبات می‌کند.

در مقاله [32] با فداکردن توزیع‌پذیری، پرداخت سریع، امن و ناشناس را فراهم می‌کند. این مقاله بهبود دهنده راه حل قطب‌های کانال پرداخت²¹ است که در مقالات موجود است که در آن هر فرستنده و گیرنده به یک گره که قطب یا هاب کانال پرداخت نام دارد متصل می‌شود و آنها به صورت بهینه پرداخت‌ها را بین خود مسیریابی می‌کنند و کارمزدی از روی پرداخت‌ها کسر می‌کنند که سازوکار مسیریابی‌اش بسیار شبیه به مسیریابی در مقاله [24] است با این تفاوت که توزیع‌شدگی شبکه بسیار کم شده است و عملکردش تا دو برابر بهتر از راه‌حل‌های قبلی بوده و بدون بن‌بست است. در این مقاله علاوه بر مسیریابی، محل قرارگیری هاب‌ها نیز به صورت توزیع‌شده بهینه می‌گردد تا بار شبکه برای تمامی قطب‌های کانال پرداخت متعادل نگه داشته شود.

مقاله [33] مجموعه پرداخت‌ها را در نظر گرفته و تغییرات ظرفیت کانال‌ها برحسب ظرفیت گره‌ها را به نحوی در نظر می‌گیرد که تمامی تراکنش‌های ورودی با حداقل هزینه مسیریابی شوند و برای مسئله بهینه‌سازی دو نوع تابع کارایی در نظر می‌گیرد. تابع اول پله‌ای است که هر تغییر در تعادل کانال میزان ثابتی هزینه دارد و تابع دیگر خطی است که متناسب با تغییرات کانال، به صورت خطی هزینه ایجاد می‌شود. نتایج را برای سه حالت، تابع خطی و داده‌های انشعاب گرفته شده²² (با حل خطی در زمان چندجمله‌ای)، تابع پله‌ای با داده‌های انشعاب گرفته شده (که به np-complete بودن مسئله می‌انجامد) و تابع پله‌ای با داده‌های برخط (با الگوریتم‌های برخط و تجزیه و تحلیل رقابتی) به دست آورده و ثابت کرده‌است. همچنین چندین الگوریتم اکتشافی برای حالت آنلاین پیشنهاد داده‌است.

مقاله [34] مسئله هم‌پوشانی مسیر در شبکه‌های کانال پرداخت را بررسی کرده و یک مسیریابی با پرداخت غیرمتمرکز برای بهبود بهره‌وری و کاهش سربار ترافیک اضافی شبکه پیشنهاد می‌دهد. در این کار تحقیقاتی، نویسندگان از مسیریابی تطبیقی استفاده می‌کنند و در صورت موفق نبودن پرداخت در یک مسیر، کل مبادلات مربوط به پرداخت را در مسیر آزاد نمی‌کنند و وجوه را برای مسیر بعدی که هم‌پوشانی با این مسیر دارد نگه

²¹ payment channel hubs (pch)

²² branch

می‌دارد و آن مسیر را انتخاب می‌کند (این مسیریابی از مبدأ و به‌صورت پیازی و با سناریوهای از قبل تعیین شده انجام می‌شود). این مسیریابی از سایر مسیریابی‌های اتمی پیشنهاد داده شده، بهره‌وری بهتری داشته و زمان پرداخت کوتاه‌تری می‌دهد.

پایان‌نامه [35] شامل دو بخش است، در بخش اول یک سازوکار مسیریابی مبتنی بر یادگیری تعاملی، به اسم شبکه کانال پرداخت آگاه از اولویت، پیشنهاد می‌کند که در آن وضعیت را برابر مقدار کارمزد و وضعیت صف قرار داده، عمل را اولویت‌بندی در هر هاب و پاداش را متناسب با افزایش فاصله بین نرخ ارسالی و مقدار هزینه پرداختی تنظیم کرده است. در قسمت دوم به شرح مسئله مسیریابی تطبیقی مقاله [34] می‌پردازد که برای جلوگیری از قفل‌شدن‌های بی‌مورد پرداخت‌ها در کانال چندین مسیر جایگزین در کنار مسیر اصلی قرار می‌دهد که صورت از دست رفتن مسیر اصلی از این مسیرهای کمکی استفاده شود.

مقاله [36] مسیریابی توزیع شده و هم‌زمان چندین پرداخت را بدون نقض محدودیت‌های ظرفیت امکان‌پذیر می‌کند. از حل مسئله به‌صورت تک مسیری به چند مسیری روی آورده است و از مدل جریان شبکه استفاده کرده و از تجمیع مسیرهای موجود استفاده می‌کند تا حجم بیشتری تراکنش از شبکه عبور دهند، به طور کلی با گسترش الگوریتم push-relabel یک الگوریتم حداکثر جریان که جریان را بر اساس دانش محلی پیدا می‌کنند اما مشکل هم‌زمانی جریان پرداخت باعث دزدی جریان در فاز فشار جریان الگوریتم می‌شود که با تکنیک قفل کردن پرداخت این مشکل را رفع کردند.

۸-۲- مرور ادبیات در حوزه تحلیل مرکزی شدن شبکه کانال پرداخت

مرکزی شدن شبکه‌های کانال پرداخت با استراتژی موجود تقریباً مورد قبول تمامی متخصصین می‌باشد اما برای فهم دقیق جزئیات آن چندین مقاله مهم از دسته سوم که به تحلیل مرکزیت شبکه پرداخته‌اند را در زیر شرح می‌دهیم:

در مقاله [37] زابکا و همکارانش (۲۰۲۲) بر اساس تحلیل گسترده‌ای از داده‌ها، به بررسی میزان تمرکز در شبکه لایت‌نینگ پرداخته است. این تحلیل با استفاده از ابزار TimeMachine که به‌منظور مطالعه تکامل شبکه در طول زمان توسعه یافته، نشان می‌دهد که علی‌رغم ساختار نسبتاً غیرمتمرکز شبکه، تعداد کمی از گره‌ها توانسته‌اند بخش قابل توجهی از تراکنش‌ها را جذب کنند. این امر منجر به ایجاد تمرکز در شبکه شده است. در طول دو سال

۲۰۲۰ تا ۲۰۲۲، نتایج عددی حاکی از افزایش چشمگیر میزان تمرکز، با شاخص جینی بیش از ۱۰٪ افزایش یافته است. مقاله همچنین به بررسی نابرابری در شبکه لایتینینگ و تحلیل گره‌های برتر پرداخته است. این یافته‌ها نشان می‌دهند که توزیع تمرکز به‌مرورزمان به سمت تعدادی گره خاص متمایل شده و افزایش تمرکز در این گره‌ها مشاهده می‌شود. این موضوع می‌تواند خطراتی مانند تنگناهای نقدینگی^{۲۳} و حملات در-مسیر^{۲۴} را افزایش دهد که نشان می‌دهد حفظ درجه بالای غیرمتمرکز بودن در شبکه‌های کانال پرداخت امری ضروری است.

در مقاله [38] زابکا و همکارانش (۲۰۲۴) به تحلیل مرکزیت شبکه لایتینینگ پرداخته‌اند. آنها با استفاده از داده‌های گسترده از پروتکل Gossip و ابزار TimeMachine، دریافتند که شبکه لایتینینگ با وجود غیرمتمرکز بودن، عدم تعادل قابل توجهی دارد؛ به‌طوری‌که تعداد کمی از گره‌ها بخش عمده‌ای از تراکنش‌ها را کنترل می‌کنند. در دو سال ۲۰۲۲ تا ۲۰۲۴، مرکزیت شبکه افزایش یافته و شاخص جینی بیش از ۱۵ درصد افزایش یافته است. یافته‌ها نشان می‌دهند که تمرکز بیشتر شبکه می‌تواند به کاهش حریم خصوصی کاربران منجر شود. در یک مدل متمرکز، هاب‌ها می‌توانند پرداخت‌ها را شناسایی، پروفایل‌ها را ایجاد و پرداخت‌ها را سانسور کنند. این نگرانی‌های حریم خصوصی می‌تواند تأثیرات اقتصادی و اجتماعی منفی داشته باشد و به سیاست‌گذاران در شناسایی اثرات نامطلوب و نیاز به مقررات کمک کند.

مقاله [39] به بررسی روند متمرکز شدن شبکه لایتینینگ بیت‌کوین پرداخته و روشی برای سنجش میزان این تمرکز ارائه می‌دهد. این روش شامل جمع‌آوری و لینک‌دهی داده‌های مربوط به تراکنش‌ها از بلاک‌چین لایه ۱ (لایه اصلی بیت‌کوین) و لایه ۲ (شبکه لایتینینگ) است. به این ترتیب، اطلاعاتی مانند زمان انجام تراکنش، مقدار بیت‌کوین قفل‌شده، و وضعیت کانال‌ها (فعال یا غیرفعال بودن) از هر دوی لایه استخراج و در یک دیتابیس مشترک ذخیره می‌شود. سپس، با استفاده از این داده‌ها، محققان می‌توانند روند تغییرات شبکه را در بازه‌های زمانی مختلف بررسی کنند و میزان تمرکز را اندازه‌گیری کنند. در این مقاله، از ضریب جینی برای سنجش میزان تمرکز استفاده شده است. ضریب جینی یک معیار آماری است که نابرابری در توزیع منابع را اندازه‌گیری می‌کند. در شبکه لایتینینگ، ضریب جینی نشان می‌دهد که چه میزان از ظرفیت کانال‌ها به تعداد محدودی از گره‌ها تعلق دارد. اگر ضریب جینی نزدیک به ۰ باشد، نشان‌دهنده توزیع برابر ظرفیت بین گره‌ها است، و اگر نزدیک به ۱ باشد،

^{۲۳} تنگناهای نقدینگی به وضعیتی در شبکه‌های پرداخت مانند لایتینینگ اشاره دارد که در آن گره‌ها یا کانال‌های پرداخت به‌اندازه کافی موجودی (liquidity) برای انجام تراکنش‌ها ندارند. این موضوع می‌تواند مانع از تکمیل موفقیت‌آمیز تراکنش‌ها شود و کارایی شبکه را کاهش دهد.

^{۲۴} به حملاتی اشاره دارد که در آن مهاجمان با سوءاستفاده از تمرکز گره‌ها در شبکه، مسیر تراکنش‌ها را دست‌کاری یا مسدود می‌کنند تا تراکنش‌ها به‌درستی انجام نشوند یا به سمت مسیرهای پرهزینه هدایت شوند. این نوع حملات می‌تواند امنیت و کارایی شبکه را تهدید کند.

نشان‌دهنده تمرکز شدید و نابرابری زیاد است. یافته‌های این تحقیق نشان می‌دهد که ضریب جینی از ۰.۸۷ در سال ۲۰۱۸ به ۰.۹۵۵ در سال ۲۰۲۳ افزایش یافته است که نشان‌دهنده تمرکز بیشتر شبکه در طول زمان است.

مقاله [40] به بررسی ساختار توپولوژیکی شبکه لایت‌نینگ بیت‌کوین می‌پردازد و تمرکز اصلی آن بر تحلیل‌های مرکزیت و چرخش گره‌ها و کانال‌ها است. نویسندگان به شناسایی الگوی جدیدی به نام "دسته گل"^{۲۵} پرداخته‌اند که نشان می‌دهد در صورت حذف گره‌های خاص، بیش از ۴۰٪ از گره‌ها از بزرگ‌ترین مؤلفه شبکه جدا خواهند شد. این الگو به شناسایی نقاط ضعف احتمالی در پایداری شبکه کمک می‌کند و تأثیرات قابل‌توجهی در تحلیل شبکه‌های پرداخت دارد. نتایج این مطالعه نشان می‌دهد که شبکه لایت‌نینگ به‌طور کلی پایدار باقی می‌ماند، ولی در عین حال نوساناتی در تعداد کانال‌ها و گره‌ها وجود دارد که ممکن است بر عملکرد و ساختار شبکه تأثیر بگذارد و همچنین ظرفیت پایین اکثر کانال‌ها را مورد بررسی قرار می‌دهد. تحلیل‌های مرکزی نشان می‌دهد که گره‌های کمی نقش کلیدی در شبکه ایفا می‌کنند و گره‌های با مرکزیت بالا در تمام اندازه‌گیری‌های مرکزی قرار دارند. این مقاله به بهبود درک ما از ساختار و نقاط ضعف شبکه لایت‌نینگ و پیشنهاداتی برای بهبود طراحی و تحلیل‌های مربوط به آن می‌پردازد.

مقاله [41] روش‌های مختلفی را برای اندازه‌گیری مرکزیت در شبکه‌های کانال پرداخت، به‌ویژه شبکه لایت‌نینگ (LN) مورد بررسی قرار می‌دهد. با توجه به ویژگی‌های منحصر به فرد این شبکه‌ها مانند توازن کانال‌ها و هزینه‌های تراکنش، نویسندگان پیشنهاد می‌کنند که برای ارزیابی نقش و اهمیت هر گره، باید معیارهای مرکزیت جدیدی تعریف شود که این موارد را مدنظر قرار دهد. در بخش‌های مختلف مقاله، علاوه بر در نظر گرفتن پارامترهای سنتی مانند درجه گره و بینابینی، پارامترهای دیگری مانند محاسبه مرکزیت بر اساس مرکزیت مسیرها، بررسی تأثیر توازن کانال‌ها و هزینه‌های تراکنش مورد تحلیل قرار گرفته‌اند. نتایج تحقیق نشان می‌دهد که استفاده از معیارهای مرکزیت سفارشی که به ویژگی‌های خاص شبکه لایت‌نینگ توجه می‌کنند، دید بهتری از اهمیت گره‌ها و نقش آن‌ها در شبکه فراهم می‌کند. نویسندگان به این نتیجه می‌رسند که گره‌های مهم در شبکه لایت‌نینگ ممکن است در مقایسه با شبکه‌های سنتی متفاوت باشند، به‌ویژه وقتی که معیارهای جدیدی مانند مرکزیت بر اساس توازن کانال‌ها و هزینه‌ها در نظر گرفته شوند. همچنین، همبستگی بین معیارهای ساده‌تر و پیچیده‌تر مورد بررسی قرار گرفته و نشان داده شده است که معیارهای ساده نیز می‌توانند دیدی کلی از مرکزیت شبکه ارائه دهند.

²⁵ bouquet

مقاله [42] به بررسی ساختار و ویژگی‌های شبکه لایت‌نینگ بیت‌کوین در طول ۱۸ ماه، از ژانویه ۲۰۱۸ تا جولای ۲۰۱۹ می‌پردازد. نتایج این مطالعه نشان می‌دهند که حجم کل بیت‌کوین‌های منتقل‌شده تقریباً با مربع اندازه شبکه رشد می‌کند. با این حال، توزیع بیت‌کوین‌ها در شبکه بسیار نابرابر است و ضریب جینی به‌طور متوسط برابر با ۰.۸۸ است که نشان‌دهنده تمرکز بالای بیت‌کوین‌ها در میان درصد کمی از گره‌ها است. به‌طور خاص، ۱۰٪ از گره‌ها حدود ۸۰٪ و ۵۰٪ از گره‌ها تقریباً ۹۹٪ از بیت‌کوین‌ها را در اختیار دارند. مقاله همچنین به مدل‌های نظری برای توضیح ساختار توپولوژیکی شبکه می‌پردازد و به‌ویژه مدل پیکربندی باینری بدون جهت را بررسی می‌کند که توانایی بازسازی ویژگی‌های ساختاری شبکه لایت‌نینگ را دارد، اما نتایج نشان می‌دهند که شبکه لایت‌نینگ به‌طور فزاینده‌ای به سمت مرکزیت و ساختار هسته-پریفرال^{۲۶} پیش می‌رود. این امر به‌ویژه از طریق آسیب‌پذیری‌های احتمالی مانند حملات تقسیم^{۲۷} تأیید می‌شود که می‌تواند منجر به فروپاشی شبکه به اجزای متعدد شود.

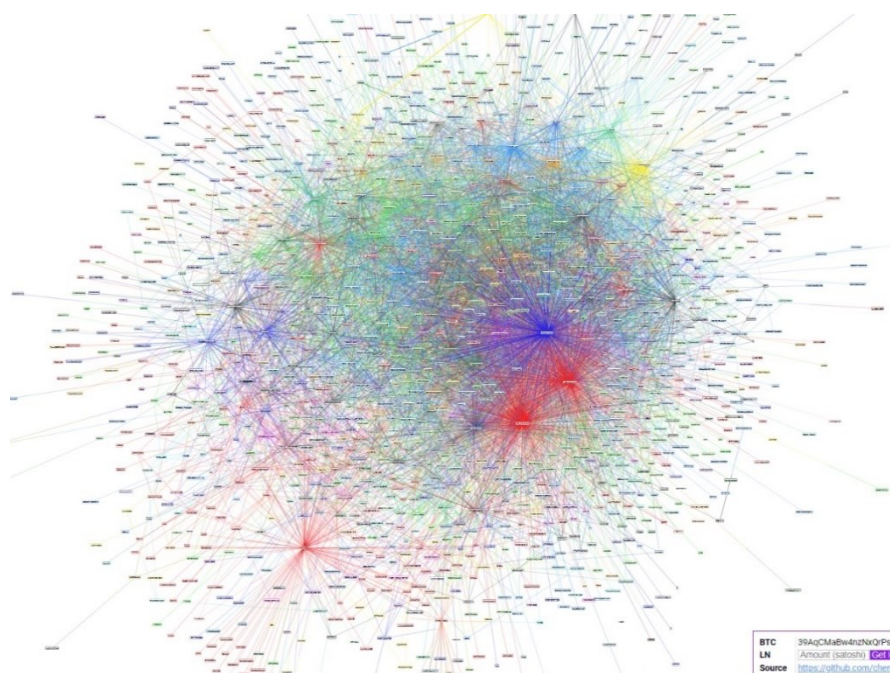
مقاله [43] به بررسی تغییرات توپولوژی شبکه لایت‌نینگ که یکی از پیشرفته‌ترین شبکه‌های کانال پرداخت است، می‌پردازد. نویسندگان با استفاده از داده‌های واقعی جمع‌آوری‌شده از پیام‌های اعلان کانال بین ژانویه ۲۰۲۰ تا اوت ۲۰۲۱، شبکه را بازسازی کرده و به تحلیل متریک‌های مختلف گرافی از جمله مرکزیت، توزیع ظرفیت و تمرکز منابع پرداخته‌اند. نتایج نشان‌دهنده تمرکز بالای منابع و اتصالات در تعداد کمی از گره‌هاست که آسیب‌پذیری شبکه را در برابر حملات هدفمند افزایش می‌دهد. همچنین، کاهش تعداد چرخه‌های سه‌گره‌ای و پایین‌بودن ترانزیویته شبکه^{۲۸} به محدودیت‌هایی در تکنیک‌های تعادل کانال‌ها اشاره دارد که می‌تواند بر ثبات شبکه تأثیر بگذارد. نتایج مقاله حاکی از تمرکز شدید منابع و اتصالات در گره‌های خاصی است که حدود ۳۸٪ از گره‌ها، ۵۰٪ از ظرفیت شبکه را در اختیار دارند. این تمرکز منابع موجب کاهش مقاومت شبکه در برابر حملات و افزایش هزینه‌های تراکنش برای کاربران می‌شود. همچنین، تحلیل تغییرات توپولوژیکی نشان می‌دهد که شبکه به سمت تمرکز بیشتر پیش می‌رود و تکنیک‌های فعلی تعادل کانال‌ها برای بسیاری از گره‌ها هزینه‌بر و غیرقابل اجرا هستند. مقاله تأکید می‌کند که نیاز به سیاست‌های جدیدی برای اتصال و توزیع بهتر منابع در شبکه برای افزایش تمرکززدایی و بهبود مقاومت شبکه وجود دارد.

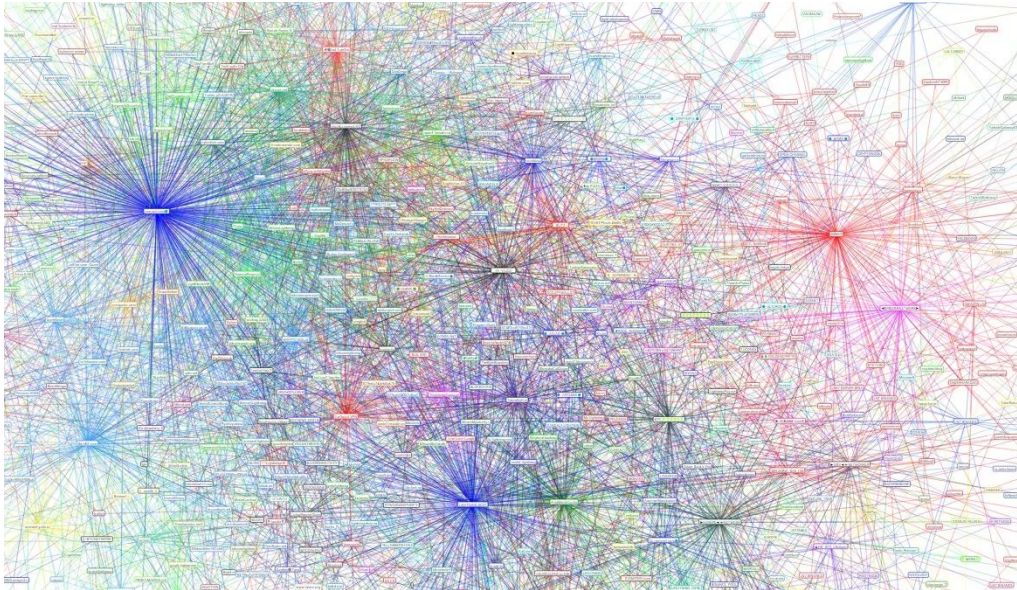
^{۲۶} ساختار هسته-پریفرال به تقسیم شبکه به دو بخش اصلی اشاره دارد: هسته که شامل گره‌های مرکزی با ارتباطات و منابع بیشتر است، و پریفرال که شامل گره‌های حاشیه‌ای با ارتباطات کمتر و تأثیر کمتری است. در این مدل، هسته نقش کلیدی در حفظ ارتباطات و عملکرد شبکه ایفا می‌کند.

^{۲۷} split attacks

^{۲۸} ترانزیویته شبکه (Network Transitivity) به میزان و احتمال وجود مثلث‌های کامل در گراف شبکه اشاره دارد، که نشان‌دهنده این است که گره‌ها به احتمال زیاد به یکدیگر متصلند. این معیار به تحلیل روابط و تعاملات درون شبکه کمک می‌کند و میزان انسجام و همکاری بین گره‌ها را نمایش می‌دهد.

مقاله [44] به تحلیل نظریه بازی‌ها در طراحی و بهینه‌سازی شبکه‌های پرداخت می‌پردازد، با تأکید ویژه بر کاربرد مفاهیم مرکزیت بینابینی و مرکزیت نزدیکی. مدل پیشنهادی با ترکیب این دو معیار، به شبیه‌سازی و ارزیابی ساختارهای مختلف شبکه پرداخته و نشان می‌دهد که چگونه این ساختارها می‌توانند از نظر کارایی و پایداری بهینه‌سازی شوند. یافته‌های تحقیق تأکید دارند که گراف ستاره‌ای در بسیاری از سناریوها به‌عنوان بهترین ساختار برای دستیابی به عملکرد مطلوب و ثبات شناخته می‌شود. دستاوردهای کلیدی مقاله شامل شناسایی ساختارهای شبکه‌ای بهینه، تحلیل تعادل نش و ارزیابی شاخص‌های عملکردی مانند قیمت ثابت (PoS) هستند. نتایج تحقیق نشان می‌دهند که ساختارهایی چون گراف ستاره‌ای (بیشتر مواقع) که نشان‌دهنده تمایل ذاتی شبکه به متمرکز شدن است و گراف کامل (به‌ندرت) که نشان‌دهنده امکان ایجاد توزیع‌شدگی کامل در این شبکه است می‌توانند به‌عنوان تعادل نش پایدار عمل کنند و شبکه‌های پرداخت می‌توانند به طور هم‌زمان هم پایدار و هم کارآمد باشند. این تحلیل‌ها به طراحان شبکه‌های پرداخت کمک می‌کنند تا ساختارهای بهینه‌ای را برای بهبود عملکرد و کاهش نواقص طراحی کنند.





شکل ۶: نمای کلی از شبکه لایتنینگ [53]

۹-۲- کاهش تمرکز شبکه‌های کانال پرداخت

به‌طور کلی روش‌های رایج برای کاهش مرکزیت شبکه شامل؛ ترغیب گره‌ها به استفاده از گره‌های کوچک در مسیریابی و پیوستن، بهبود الگوریتم‌های مسیریابی، افزایش تعداد کانال‌های بین گره‌ها، تقویت پروتکل‌های حفظ حریم خصوصی و بهبود الگوریتم‌های پیوستن به شبکه باهدف کاهش تمرکز می‌باشد.

در این بخش می‌خواهیم تعدادی از مقالات که برای رفع مشکل مرکزیت شبکه تلاشی انجام داده اند را شرح دهیم که بیشتر این مقالات از دسته دوم هستند، دسته دوم مقالات اکثراً به افزایش سود یا کاهش هزینه‌های یک گره با استفاده از تکنیک‌های بهینه‌سازی [45] یا یادگیری ماشین و یادگیری تقویتی [46] می‌پردازند اما در این مقالات با استفاده از نحوه پیوستن به شبکه سعی بر کاهش مرکزیت شبکه کرده‌اند. اما به غیر از راه‌حل‌های مقالات دسته دوم با استفاده از مسیریابی یعنی مقالات دسته اول نیز می‌توان به کاهش مرکزیت در شبکه کمک فروانی کرد که نمونه‌ای از آن در مقالات مرور شده اشاره می‌شود.

تحلیل نحوه پیوستن به شبکه و استراتژی‌های آن:

مقاله [47] تأثیر استراتژی‌های مختلف پیوستن به شبکه‌های کانال پرداخت را بررسی می‌کند. این تحقیق با استفاده از شبیه‌سازی‌های کامپیوتری، تأثیرات پنج استراتژی مختلف شامل بیشترین درجه، تصادفی، بینابینی،

k-مرکز^{۲۹}، و k-میان^{۳۰} را تحلیل کرده و به بررسی تأثیر آن‌ها بر روی ویژگی‌های توپولوژیکی و عملکرد شبکه پرداخته است.

برای کاهش تمرکز شبکه، مقاله پیشنهاد می‌کند از استراتژی‌های توزیع شده استفاده شود. به‌ویژه، استراتژی‌هایی مانند تصادفی و k-مرکز که به توزیع یکنواخت گره‌ها در سراسر شبکه کمک می‌کنند، به کاهش تمرکز و بهبود توزیع گره‌ها کمک می‌کنند. در مقابل، استراتژی‌های متمرکز مانند بیشترین درجه و بینابینی ممکن است منجر به تمرکز بالا و مشکلاتی در عملکرد شبکه شوند. استراتژی k-میان نیز به کاهش تمرکز کمک می‌کند، اما نتایج آن در مقایسه با دیگر استراتژی‌ها متفاوت است. این مقاله به اهمیت انتخاب استراتژی‌های مناسب برای بهبود عملکرد و کاهش مشکلات ناشی از تمرکز شبکه‌ها تأکید می‌کند.

بهبود مرکزیت شبکه با استفاده از پیشنهاد مناسب برای اتصال به گره جدید:

مقاله محمد صالح مهدی‌زاده و همکاران [48] به بررسی روش‌های موجود برای مقابله با تمرکزگرایی در شبکه لایت‌نینگ پرداخته و یک استراتژی جدید مبتنی بر امتیازدهی را برای بهبود سیستم اتوپایلووت معرفی می‌کند. اتوپایلووت به‌عنوان یک موتور توصیه‌گر برای اپراتورهای گره‌های شبکه لایت‌نینگ عمل می‌کند که به تجزیه و تحلیل گراف عمومی شبکه پرداخته و پیشنهاداتی برای باز کردن کانال‌ها و ظرفیت آن‌ها ارائه می‌دهد. این سیستم فعلاً از اطلاعات خصوصی مانند موفقیت‌ها و شکست‌های قبلی در مسیریابی استفاده نمی‌کند.

مدل پیشنهادی این مقاله به بررسی ویژگی‌های توپولوژیکی گره‌های شبکه و ایجاد امتیاز برای هر گره بر اساس این ویژگی‌ها می‌پردازد. امتیاز گره‌ها با استفاده از یک مدل رگرسیون لجستیک محاسبه می‌شود که معیارهایی نظیر درجه اتصال و موقعیت توپولوژیکی را در نظر می‌گیرد. نتایج نشان می‌دهد که با استفاده از این استراتژی، می‌توان تا ۱۷٪ کاهش در تمرکز منابع شبکه و تا ۲۷٪ کاهش در مالکیت کانال‌های در یک درصد هاب بزرگ شبکه نسبت به استراتژی‌های موجود در اتوپایلووت تجربه کرد. همچنین، این مدل باعث افزایش تاب‌آوری شبکه در برابر حملات هدفمند به هاب‌ها و کانال‌ها شده و می‌تواند به‌عنوان جایگزینی برای روش‌های فعلی توصیه در اتوپایلووت لایت‌نینگ پیاده‌سازی شود.

^{۲۹} پیوستن به k گره از شبکه که بیشترین فاصله از هر گره‌ای تا این گره‌ها کمینه باشد.

^{۳۰} پیوستن به k گره از شبکه که میانگین فاصله از هر گره‌ای تا این گره‌ها کمینه باشد.

پیوستن به کانال برای افزایش چرخه‌های کوتاه جهت متعادل‌سازی و تمرکززدایی شبکه:

مقاله [49] به معرفی یک الگوریتم جدید به نام ProfitPilot می‌پردازد که هدف آن بهبود ساختار و کارایی شبکه‌های کانال پرداخت است. این الگوریتم با تمرکز بر روی ایجاد و استفاده از حلقه‌های سه‌گره‌ای، سعی دارد که بهبودهایی در فرایند متعادل‌سازی اعتبار و کاهش تمرکز در شبکه‌های پرداخت ایجاد کند. ProfitPilot به طور خاص برای اتصال گره‌های جدید به شبکه طراحی شده است و تلاش می‌کند تا این اتصال به نحوی باشد که اعتبار در میان گره‌ها به طور متوازن توزیع شود و از ایجاد گلوگاه‌های احتمالی جلوگیری کند.

الگوریتم ProfitPilot به وسیله شناسایی گره‌های جدید و تحلیل اینکه آیا این گره‌ها می‌توانند به حلقه‌های سه‌گره‌ای موجود متصل شوند یا خیر، کار می‌کند. این روش به گره‌ها اجازه می‌دهد تا به صورت کارآمدتری به یکدیگر متصل شوند و از تبادل اعتبار درون شبکه بهره‌برداری بهتری داشته باشند. با استفاده از حلقه‌های جدید و بهبود مسیرهای انتقال اعتبار، ProfitPilot به متعادل‌سازی اعتبار و بهبود عملکرد کلی شبکه کمک می‌کند. یکی از ویژگی‌های کلیدی ProfitPilot، کاهش تمرکز در شبکه است. با ایجاد حلقه‌های جدید و بهبود توزیع اعتبار، این الگوریتم باعث می‌شود که بار و فشار شبکه به طور یکنواخت‌تری بین گره‌ها توزیع شود. این به معنی کاهش فشار بر روی گره‌های خاص و جلوگیری از ایجاد نواحی با بار زیاد است. به این ترتیب، شبکه از نظر کارایی و امنیت بهبود می‌یابد و کاربران تجربه بهتری از لحاظ عملکرد شبکه خواهند داشت.

مسیریابی مورچه‌ای و کاهش مرکزیت:

در مقاله [50] پروتکل مسیریابی مورچه‌ای³¹ با الهام از رفتار مورچه‌ها در طبیعت طراحی شده و هدف اصلی آن حل مشکلات مسیریابی در شبکه پرداخت لایت‌نینگ است. این پروتکل از طریق به‌روزرسانی مداوم اطلاعات محلی و تعامل با گره‌های همسایه، مسیرهای بهینه‌ای را از مبدأ به مقصد به صورت توزیع شده و با همکاری گره‌ها ایجاد می‌کند. گره‌ها در این پروتکل مشابه رفتار مورچه‌ها، اطلاعات مسیرها را ثبت کرده و بر اساس آن، بهترین مسیر برای تراکنش را پیشنهاد می‌دهند.

این پروتکل شامل چهار مرحله اصلی است: مرحله انتشار ماده شیمیایی (فرمون)، مرحله تطابق، مرحله تأیید، و مرحله بررسی شمارنده. در این مراحل، گره‌ها با استفاده از اطلاعات محلی و بر اساس تطابق یافتن فرمون ارسال شده از فرستنده و گیرنده در شبکه، مسیرهای بهینه را انتخاب می‌کنند. گره‌های فرستنده بر اساس معیار خود که می‌تواند تراکنش با کمترین هزینه یا تراکنش با حریم خصوصی بیشتر باشد از بین مسیرهای بهینه که به صورت

³¹ Ant Routing

توزیع شده توسط شبکه پیدا شده‌اند یکی را انتخاب کنند و این اختیار گره فرستنده در انتخاب مسیر امن‌تر و با حریم خصوصی بیشتر که معمولاً مسیرهای طولانی‌تر است باعث کاهش وابستگی به گره‌های بزرگ و متمرکز در شبکه می‌شود.

مزایای پروتکل مسیریابی مورچه‌ای شامل تمرکززدایی کامل، حفظ حریم خصوصی، و مقابله با گره‌های مخرب است. این ویژگی‌ها باعث می‌شوند که شبکه در برابر حملات و خرابی‌های ناگهانی مقاوم‌تر باشد و مقیاس‌پذیری و امنیت شبکه‌ی لایت‌نینگ را افزایش دهد. به‌طور کلی، پروتکل مسیریابی مورچه‌ای یک راه‌حل نوآورانه و مؤثر برای مسیریابی در شبکه‌های پرداخت است که با کاهش تمرکزگرایی و افزایش حریم خصوصی، عملکرد شبکه را بهبود بخشیده و آن را در برابر تهدیدات مختلف مقاوم‌تر می‌سازد.

مرتبط ترین مقاله به کار این پایان‌نامه مقاله [28] است که این پایان‌نامه از آن شروع می‌کند و سایر مقالات گفته شده در این مرور ادبی ارتباط مستقیمی با پایان‌نامه ندارند که بتوان در جدول مقایسه تمایز کار خود را با سایر مقالات مشخص کرده و مشخص کنیم چه خلاء‌هایی را که سایر مقالات ندیده‌اند پر کرده ایم.

۱۰-۲- معرفی ابزار برای ورود به مسئله

بهینه‌سازی محدب:

بهینه‌سازی محدب شاخه‌ای ضروری از بهینه‌سازی ریاضی است که با کمینه‌سازی توابع محدب سروکار دارد. بهینه‌سازی محدب یک حوزه حیاتی از تحقیقات است، زیرا بسیاری از مسائل بهینه‌سازی که در دنیای واقعی با آن مواجه می‌شوند را می‌توان به‌عنوان مسائل بهینه‌سازی محدب فرموله کرد. رایج‌ترین مسئله در بهینه‌سازی محدب، یافتن حداقل جهانی یک تابع محدب است. برای انجام این کار، چندین الگوریتم بهینه‌سازی، مانند نزول گرادیان، توسعه‌یافته است. با این حال، مهم است که توجه داشته باشید که این الگوریتم‌ها ممکن است بسته به حدس اولیه به راه‌حل‌های مختلفی همگرا شوند. به همین دلیل، لازم است از چندین حدس اولیه یا الگوریتم‌های متعدد برای یافتن حداقل جهانی یک تابع محدب استفاده شود.

مسائل بهینه‌سازی محدب را می‌توان به‌عنوان یک مسئله بهینه‌سازی مقید فرموله کرد که در آن تابع هدف باتوجه‌به مجموعه‌ای از قیدها به حداقل می‌رسد. یک مسئله بهینه‌سازی محدب با تابع هدف محدب و با قید تساوی خطی و نامساوی محدب، مسئله محدب نامیده می‌شود. رایج‌ترین شکل یک مسئله محدب یک مسئله بهینه‌سازی خطی است که یک مسئله بهینه‌سازی محدب است که در آن تابع هدف و محدودیت‌ها خطی

هستند. مسائل بهینه‌سازی محدب را به قالب زیر می‌نویسند که تابع f و توابع g بایستی محدب باشند و توابع h بایستی خطی باشد، m قید نامساوی و p قید تساوی داریم:

$$\begin{aligned} & \underset{x}{\text{Minimize}} && f(x) \\ & \text{subject to} && g_i(x) \leq 0 \quad i = 1, \dots, m \\ & && h_i(x) = 0 \quad i = 1, \dots, p \end{aligned}$$

بهینه‌سازی محدب طیف وسیعی از کاربردها در زمینه‌های مختلف مانند یادگیری ماشین، سیستم‌های کنترل، پردازش سیگنال، آمار و بسیاری موارد دیگر دارد. یکی از محبوب‌ترین کاربردها در آموزش مدل‌های یادگیری ماشینی است، زیرا بسیاری از مدل‌ها را می‌توان با استفاده از بهینه‌سازی محدب آموزش داد و فرایند بهینه‌سازی را سریع‌تر و پایدارتر می‌کند. بهینه‌سازی محدب همچنین نقش مهمی در پردازش تصویر و سیگنال ایفا می‌کند، زیرا می‌توان از آن برای بازسازی تصاویر از داده‌های ناقص، بهبود تصاویر و حذف نویز از سیگنال‌ها استفاده کرد. در سیستم‌های کنترلی، از بهینه‌سازی محدب برای طراحی کنترل‌کننده‌هایی استفاده می‌شود که عملکرد یک سیستم را تحت محدودیت‌ها بهینه می‌کند.

قابل ذکر است که کتابخانه‌های قدرتمندی برای حل این مسائل ساخته شده است که سریع‌ترین راه‌حل‌های عددی را برای مسئله بهینه‌سازی خود انتخاب کرده و حل می‌کنند کتابخانه‌ای مثل CVXPY برای پایتون و CVX برای متلب مثال‌هایی از این کتابخانه‌ها است.

نظریه گراف و پیدا کردن کوتاه‌ترین مسیر:

نظریه گراف شاخه‌ای از ریاضیات است که به مطالعه گراف‌ها می‌پردازد، گراف‌ها ساختارهای ریاضی هستند که برای مدل‌سازی روابط زوجی بین اشیاء استفاده می‌شوند. یکی از مهم‌ترین مسائل در نظریه گراف، مسئله کوتاه‌ترین مسیر است که شامل یافتن کوتاه‌ترین مسیر ممکن بین دو رأس در یک گراف است. این مشکل کاربردهای عملی متعددی دارد، مانند یافتن سریع‌ترین مسیر بین دو نقطه در نقشه راه. در این مورد، تقاطع‌ها به‌عنوان رئوس و بخش‌های جاده به‌عنوان لبه نشان داده می‌شوند که هر یال با طول بخش جاده مربوطه وزن می‌شود. با حل مسئله کوتاه‌ترین مسیر، می‌توانیم مسیری را پیدا کنیم که کمترین زمان را می‌گیرد. در تئوری گراف، مسئله کوتاه‌ترین مسیر، مسئله یافتن مسیری بین دو رأس (گره) در یک نمودار است، به‌طوری‌که مجموع وزن لبه‌های تشکیل‌دهنده آن به حداقل می‌رسد.

ما گرافی داریم جهت دار و وزن دار که هدف عبور از یال ها از یک گره خاص به یک گره خاص دیگر است به طوری که مجموع وزن های روی این یال های عبوری کمینه شود که آسان ترین راه حل آن با نوشتن مسئله بهینه سازی و اجرای الگوریتم های عددی حل آن به این مسیر خواهیم رسید. اما این راه حل بسیار زمان حل طولانی خواهد داشت. الگوریتم های مشخصی وجود دارد که تایم حل بسیار کمتری برای رسیدن به جواب را به ما می دهد. الگوریتم های Breadth-first search ، Dijkstra ، Bellman-Ford ، Floyd-Warshall و از جمله الگوریتم هایی هستند که این مسئله را با زمان های حل مختلف برای مسائل مختلف حل کرده اند.

۳- فصل سوم: راه حل پیشنهادی

در این فصل ابتدا علائم استفاده شده در مسئله و مدل اولیه بهینه‌سازی مسئله [28] را توضیح می‌دهیم. ما دو راه حل کلی ارائه می‌دهیم که اولی راه‌حلی جامع برای کاهش مرکزیت با استفاده از ارائه مسئله بهینه‌سازی جدید است و راه حل دوم یک راه‌حل اکتشافی ابتدایی برای کاهش مرکزیت شبکه با تغییر الگوریتم مسیریابی است.

در راه‌حل اول با استفاده از بهبودهایی که بر روی مدل می‌دهیم مسئله جدید تولید خواهیم کرد که می‌شود با ابزار توضیح داده شده آن را حل کرد. با تغییر مسئله، به مسئله جدید مسیریابی چندپرداخته می‌رسیم که هدف میانی برای ایجاد قید محدودکننده گره‌های مرکزی است و در آخر با اضافه کردن این قید به هدف خود خواهیم رسید. در راه‌حل دوم به تشریح الگوریتم پیدا کردن کوتاه‌ترین مسیر موجود در مسئله اولیه [28] پرداخته و بعد با تغییراتی در آن به الگوریتم اکتشافی دست پیدا می‌کنیم که مرکزی بودن گره‌ها را گران می‌کند. در این الگوریتم اکتشافی دیگر نیاز به انجام مسیریابی چندپرداخته به صورت هم‌زمان نیست و توزیع‌شدگی را با مسیریابی تک‌پرداخته و ذخیره تاریخچه محلی پرداخت‌ها در هر گره ایجاد می‌کند. و این نکته هم در نظر باشد که هر دو راه‌حل ارائه شده برای کاهش مرکزیت شبکه به صورت کاملاً متمرکز و توسط یک نهاد مرکزی اجرا می‌شوند، نه به صورت توزیع شده.

۳-۲- مدل مسئله

این فرمول‌بندی مشابه فرمول‌بندی مقاله پایه [28] پایان‌نامه است که در ادامه می‌خواهیم ابتکارات خود را در این مدل پیاده کنیم یک شبکه کانال پرداخت داریم با گره‌هایی به نمایندگی افراد شرکت‌کننده در شبکه کانال پرداخت که این گره‌ها را با علامت $v_i \in V$ که v_i نماینده گره‌ها و V مجموعه تمامی گره‌های موجود در شبکه هستند. این گره‌ها با استفاده از کانال‌های پرداخت دو طرفه به یکدیگر متصل شده است که این کانال‌ها

به عنوان یال های شبکه شناخته می شوند که یال بین دو گره v_i و گره v_j به صورت e_{ij} شناخته می شود و $e_{ij} \in E$ که E مجموعه تمام یال های موجود در گراف است و گراف را به صورت $G = (V, E)$ نشان می دهیم در آن G یک گراف دوجهته بین گره های V و یال های موجود در مجموعه E است. در این گراف، جهت ها با تغییر اندیس ها مشخص می شوند. به عنوان مثال، بین دو گره i و j جهت به صورت e_{ij} و e_{ji} تعریف می شود.

ظرفیت کانال ها در هر جهت متفاوت است پس ما ظرفیت کانال ها را با اندیس مشخص می کنیم و برای یال e_{ij} ظرفیت را به صورت w_{ij} تعریف می کنیم که ظرفیت عبور سکه از گره v_i به گره v_j است توجه داشته باشید که مقدار ظرفیت w_{ij} می تواند با ظرفیت w_{ji} متفاوت باشد که میزان توان کانال در عبور سکه از هر طرف گره به طرف دیگر را نشان می دهد اما همیشه مجموع این دو ظرفیت یک عدد ثابت است که به آن ظرفیت کلی کانال می گویند و با $W(i, j)$ نشان می دهند.

هر کانال برای عبور تراکنش tx از آن مقداری کارمزد دریافت می کند یعنی با عبور تراکنش tx از v_i به سمت گره v_j مقدار $\rho(e_{ij}, tx)$ کارمزد دریافت می شود که این مقدار به شرایط موجود در خود کانال e_{ij} و پرداخت tx بستگی خواهد داشت، که می تواند به مقدار بایت هر تراکنش، که به آن پهنای باند می گویند، یا مقدار پرداخت $\alpha(tx)$ و یا به میزان غیر متعادل بودن کانال و میزان تغییر تعادلی که عبور پرداخت از آن ایجاد می کند بستگی داشته باشد.

عبور تراکنش از هر یک از کانال ها مثل e_{ij} باعث کاهش ظرفیت آن w_{ij} به اندازه مقدار آن تراکنش $\alpha(tx)$ و افزایش ظرفیت کانال به همان اندازه در جهت مخالف عبور تراکنش w_{ji} در کانال می شود اما همواره مجموع ظرفیت دو طرف یکسان است یعنی $w_{ij} + w_{ji} = W(i, j)$ همیشه ثابت است.

هدف ما حداقل کردن میزان کارمزد در طول مسیر است؛ یعنی پیدا کردن مسیر با ارزان ترین حالت ممکن از فرستنده به گیرنده ما این مسیر را به صورت \mathcal{P} بیان می کنیم که مسیر پرداخت tx از فرستنده s به گیرنده r که شامل مجموعه یال های این مسیر است که سعی می کنیم تابع هدف $\sum_{e_{ij} \in \mathcal{P}, v_i \neq s} \rho(e_{ij}, tx)$ را کمینه کنیم و ما کارمزد یال فرستنده را کمینه نمی کنیم زیرا فرستنده برای پرداخت در کانال خود کارمزد نمی گیرد. و متغیرهای دیگری هم وجود دارد که در ادامه در حین توضیح مطالب اضافه شده تعریف خواهند شد.

۳-۳- تعریف مسئله اولیه و قيود آن

برای ایجاد فرمولاسیون مسئله، به یک ماتریس نیاز داریم که ابعاد آن مربوط به گره‌ها باشد و به صورت باینری تعریف گردد. در این ماتریس، مقدار یک برای هر گره به معنای عبور مسیر پرداخت از آن یال در نظر گرفته می‌شود. به همین منظور، متغیر x_{ij} معرفی می‌شود که نشان‌دهنده این است که آیا مسیر از یال e_{ij} عبور کرده است یا خیر. این متغیر به شکل زیر تعریف می‌شود:

$$x_{ij} := \begin{cases} 1 & \text{اگر مسیر پرداخت tx از یال } e_{ij} \text{ عبور کند} \\ 0 & \text{در غیر این صورت} \end{cases}$$

برای ایجاد قید مشخص‌کننده فرستنده و گیرنده در این مسئله، از متغیرهای تعریف‌شده استفاده می‌کنیم. برای هر مسیر، به جز فرستنده و گیرنده، هر گره دارای یک یال ورودی و یک یال خروجی است. در فرستنده تنها یال خروجی و در گیرنده تنها یال ورودی وجود دارد. بنابراین، اگر یال‌های مسیر را یک در نظر بگیریم و برای هر گره، تعداد یال‌های ورودی را منهای یال‌های خروجی کنیم، به جز در فرستنده و گیرنده، سایر نتایج برابر با صفر خواهند بود. در مورد گیرنده، نتیجه منفی یک و در مورد فرستنده، نتیجه یک خواهد شد. با استفاده از این تکنیک، می‌توانیم قید مشخص‌کننده فرستنده و گیرنده را تعریف کنیم. به این ترتیب، مقدار فرستنده برابر یک، گیرنده برابر منفی یک و باقی مقادیر برابر صفر قرار می‌گیرد و به عنوان یک قید به مسئله اضافه می‌شود:

$$\sum_j x_{ij} - \sum_j x_{ji} = \begin{cases} 1 & \text{اگر } v_i \text{ فرستنده s باشد} \\ -1 & \text{اگر } v_i \text{ گیرنده r باشد} \\ 0 & \text{در غیر این صورت} \end{cases}$$

قید بعدی که باید تعریف کنیم، مربوط به ظرفیت‌ها است. این قید باید به گونه‌ای باشد که در هر نقطه از مسیر پرداخت، یال مورد نظر باید به اندازه تراکنش و مجموع کارمزدهای یال‌های بعدی خود تا مقصد، ظرفیت کافی داشته باشد. بنابراین، برای هر زیرمجموعه‌ای از گره‌ها که فرستنده در آن قرار دارد و ما آن را S می‌نامیم، باید مجموع ظرفیت روی این برش‌های گره‌ای بیشتر از مقدار تراکنش و مجموع کارمزدهای یال‌های خارج از این مجموعه باشد. به عبارت دیگر، این نابرابری باید برای تمام این زیرمجموعه‌ها برقرار باشد تا شرط ظرفیت ما تأمین شود. برای توضیح بهتر این قید، به ازای هر برشی از گراف که شامل فرستنده است، مسیری که از فرستنده به گیرنده رسم می‌شود، این برش را قطع می‌کند. ظرفیت این برش‌های قطع‌شده باید برای تمام این برش‌ها از حاصل جمع مقدار تراکنش و همه کارمزدهای یال‌های خارج از برش بیشتر باشد تا قید ظرفیت به درستی اعمال گردد. عبارت ریاضی این قید به شکل زیر بیان می‌شود:

$$\sum_{i: v_i \in S} \sum_{j: v_j \notin S} \omega_{ij} x_{ij} \geq \alpha(tx) + \sum_{i: v_i \notin S} \sum_{j: v_j \in S} \rho(e_{ij}, tx) x_{ij}$$

و در آخر مسئله بهینه‌سازی محدب (خطی) برای پیدا کردن ارزان‌ترین مسیر به صورت زیر خواهد شد:

$$\min \sum_i \sum_j \rho(e_{ij}, tx) \cdot x_{ij}$$

با قید:

$$\sum_j x_{ij} - \sum_j x_{ji} = \begin{cases} 1 & \text{اگر } v_i \text{ فرستنده } s \text{ باشد} \\ -1 & \text{اگر } v_i \text{ گیرنده } r \text{ باشد} \\ 0 & \text{در غیر این صورت} \end{cases} \quad \text{برای تمامی گره های } i$$

$$\sum_{i: v_i \in S} \sum_{j: v_j \notin S} \omega_{ij} x_{ij} \geq \alpha(tx) + \sum_{i: v_i \notin S} \sum_{j: v_j \in S} \rho(e_{ij}, tx) x_{ij} \quad \text{برای تمامی } S \subset V \text{ که فرستنده عضو } S \text{ باشد}$$

حال با حل این مسئله بهینه‌سازی محدب و خطی با تعداد قید بسیار بالا می‌شود به ارزان‌ترین مسیر ممکن دست پیدا کرد اما مشکل اصلی این است که روش‌های عددی حل این مسئله اگر تعداد گره‌ها زیاد باشد بسیار طولانی خواهد شد.

۴-۳- تغییر در قید و روش بهینه‌سازی پیشنهادی

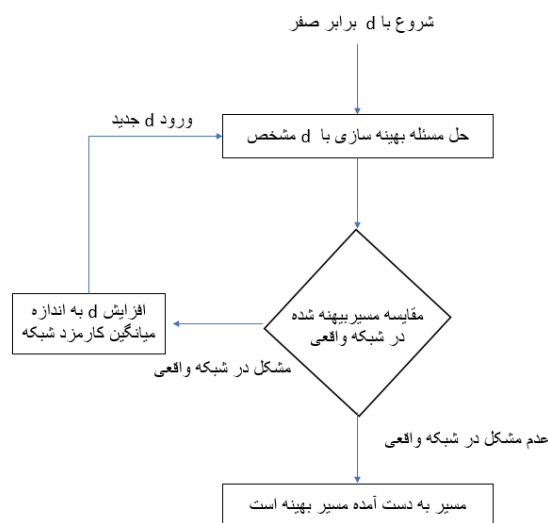
شروع نوآوری اصلی این پایان‌نامه از این بخش خواهد بود که می‌خواهیم مسئله بهینه‌سازی را از مدل تک پرداخته به چند پرداخته تغییر دهیم. برای رسیدن به مدل مسیریابی چند پرداخته توأم بایستی کمی در قیده‌های بهینه‌سازی تغییر ایجاد کنیم و رویکردی جدید برای ارضای آن قیدها ایجاد کنیم که شامل معرفی یک مقدار ثابت کوچک در هر پرداخت برای ارضای شرط است. این مقدار ثابت که همان کارمزد تراکنش را نمایندگی می‌کند که به دلیل کوچک بودن نسبت به مقدار تراکنش تأثیر قابل توجهی بر روی قیود و ظرفیت کانال‌ها نخواهد داشت. به این ترتیب، می‌توانیم فرایند حل مسئله را تسهیل کنیم.

ابتدا قید اولیه که نیازمند ارضای شرط پیچیده‌ای است، به صورت یک قید ساده‌تر و قابل پیاده‌سازی مجدد تعریف می‌شود. در این مرحله، مقدار ثابتی به نام d تعریف می‌کنیم که می‌تواند مقادیر مختلفی از جمله 0 ، $0.005 \cdot tx$ ، $0.01 \cdot tx$ ، $0.015 \cdot tx$ و... را بگیرد. این مقدار ثابت به ما امکان می‌دهد قید جدیدی را برای هر کانال تعریف کنیم که از مقدار پرداخت بیشتر یا مساوی باشد و همانند مقدار کارمزد عمل کند. قید جدید به شکل زیر خواهد بود:

$$\omega_{ij} - tx \cdot x_{ij} - d \cdot x_{ij} \geq 0 \quad \text{برای همه } i \text{ ها و } j \text{ ها}$$

این قید جدید تضمین می‌کند که وزن هر کانال از مقدار تراکنش به‌اضافه مقدار ثابت d ضربدر متغیر تصمیم بزرگ‌تر باشد.

پس از تبدیل قید اولیه به قید جدید، فرایند حل مسئله با جای‌گذاری این قید شروع می‌شود. مقدار d در ابتدا صفر در نظر گرفته می‌شود در صورت‌یافتن یک جواب معتبر که یعنی مسیر یافته شده در بهینه‌سازی در شبکه واقعی با محاسبه کارمزد بدون مشکل انجام شود، مسئله حل شده تلقی می‌شود زیرا بدون در نظر گرفتن این مقدار ناچیز کارمزد در مسئله تمام قیود ظرفیت در واقعیت برآورده شده‌است اما اگر در هنگام مسیریابی به مشکل برقرار نبودن قید ظرفیت در واقعیت شبکه برخورد، مقدار d را افزایش می‌دهیم یعنی $tx * 0.005$ و مجدداً مسئله را حل می‌کنیم که به این معنی است که به مقدار تراکنش به طور میانگین یک کارمزد کانال اضافه کردیم و باز در واقعیت جواب را چک می‌کنیم و اگر به مشکل برخوردیم باز مقدار d را افزایش می‌دهیم. این فرایند به‌صورت تکراری ادامه می‌یابد تا به یک جواب معتبر برسیم.



شکل ۷: فلوچارت رسیدن به مسیر بهینه

اگر به مشکلی برخوردیم چون تعداد میانگین مسیرها طبق شبیه‌سازی‌های صورت‌گرفته در بخش بعدی حدود ۴ است با ۳ بار افزایش d به جواب خواهیم رسید و در بدترین حالت، ممکن است نیاز باشد این فرایند را تا $n-2$ بار تکرار کنیم که n تعداد حداکثری گره‌ها است. با افزایش مقدار d ، ممکن است بهینه‌گی مسئله کاهش یابد، زیرا مقدار ثابت d ممکن است به‌تدریج تأثیر بیشتری بر روی قیود بگذارد و منجر به دور شدن از راه‌حل بهینه شود. اما شبیه‌سازی‌ها نشان داده‌اند که این روش معمولاً نتایج قابل‌قبولی تولید می‌کند و در ۹۹٪ مواقع تفاوت چندانی

با حالت اولیه قید ندارد. این روش پیشنهادی به ما این امکان را می‌دهد که مسئله پیچیده را با استفاده از یک قید ساده‌تر و قابل‌تنظیم حل کنیم. این باعث کاهش پیچیدگی محاسباتی و افزایش سرعت حل مسئله می‌شود و باتوجه به نتایج شبیه‌سازی‌ها، می‌توان گفت که تفاوت عملکرد این روش با حالت اولیه قید در اکثریت مواقع ناچیز است که این امر اعتبار و کاربردپذیری این روش را تقویت می‌کند.

۵-۳- مدل مسیریابی برای دو تراکنش هم‌زمان

ما برای ایجاد یک قید در مسئله بهینه‌سازی خود که بتواند مقدار تراکنش عبوری از هر گره شبکه را در طول زمان کنترل کند باهدف کنترل سود دریافتی هر گره بایستی ابتدا بتوانیم مسئله بهینه‌سازی چند پرداخته توأم را مدل‌سازی کنیم برای رسیدن به این هدف ابتدا می‌خواهیم مسئله انتقال دو پرداخت مستقل از فرستنده‌ها به گیرنده‌هایشان را مدل‌سازی بکنیم. برای مدیریت این مسئله، نیاز به اصلاح تابع هدف و همچنین قیود مربوط به فرستنده و گیرنده هر تراکنش داریم. در اینجا، به شرح تغییرات اعمال‌شده در مدل بهینه‌سازی و نحوه برخورد با قیود ظرفیت کانال‌ها می‌پردازیم.

تغییرات در تابع هدف به‌گونه‌ای تنظیم شده است که شامل هزینه‌های ایجاد شده در اثر عبور دو تراکنش از یک کانال، در صورت هم‌جهت یا خلاف جهت بودن آن‌ها، باشد. این تابع به‌صورت زیر تعریف می‌شود:

$$\min \sum_i \sum_{j < i} |tx^1 \cdot (\rho(e_{ij}, tx^1) \cdot x_{ij}^1 - \rho(e_{ji}, tx^1) \cdot x_{ji}^1) + tx^2 \cdot (\rho(e_{ij}, tx^2) \cdot x_{ij}^2 - \rho(e_{ji}, tx^2) \cdot x_{ji}^2)|$$

در این تابع هدف، tx^1 و tx^2 به ترتیب به تراکنش‌های اول و دوم اشاره دارند. $\rho(e_{ij}, tx^1)$ و $\rho(e_{ij}, tx^2)$ هزینه‌های مربوط به کانال e_{ij} برای هر تراکنش را نشان می‌دهند. این تابع به‌گونه‌ای طراحی شده است که اگر تراکنش‌ها در یک جهت باشند، هزینه‌ها را جمع کرده و اگر خلاف جهت باشند، از یکدیگر کم می‌کند. این رویکرد باعث می‌شود که تأثیرات هزینه‌ای در کانال به‌صورت دقیق‌تری مدل‌سازی شوند و به بهینه‌سازی بهتر مسئله کمک کند.

قیود جریان برای هر تراکنش به این صورت است که برای مدیریت جریان هر تراکنش، قیود جدیدی تعریف شده‌اند که به طور مستقل فرستنده و گیرنده هر تراکنش را مشخص می‌کنند. این قیود شامل قید جریان برای تراکنش اول:

$$\sum_j x_{ij}^1 - \sum_j x_{ji}^1 = \begin{cases} 1 & \text{اگر } v_i \text{ فرستنده } s \text{ باشد} \\ -1 & \text{اگر } v_i \text{ گیرنده } r \text{ باشد} \\ 0 & \text{در غیر این صورت} \end{cases}$$

این قید جریان را برای تراکنش اول مدل سازی می کند و اطمینان می دهد که جریان تراکنش اول از فرستنده به گیرنده به درستی هدایت شود.

قید جریان برای تراکنش دوم:

$$\sum_j x_{ij}^2 - \sum_j x_{ji}^2 = \begin{cases} 1 & \text{اگر } v_i \text{ فرستنده } s \text{ باشد} \\ -1 & \text{اگر } v_i \text{ گیرنده } r \text{ باشد} \\ 0 & \text{در غیر این صورت} \end{cases}$$

این قید نیز مشابه قید اول است، با این تفاوت که برای تراکنش دوم اعمال می شود. این قیود به تفکیک جریان هر تراکنش کمک می کنند و نقش حیاتی در بهینه سازی دارند.

قید ظرفیت کانال در این مدل به صورت تسهیل شده طراحی شده است تا تغییرات در جریان های هم جهت و خلاف جهت را به درستی مدیریت کند:

$$\omega_{ij} - (tx^1 + d^1) \cdot (x_{ij}^1 - x_{ji}^1) - (tx^2 + d^2) \cdot (x_{ij}^2 - x_{ji}^2) \geq 0 \quad \text{برای همه } i \text{ ها و } j \text{ ها}$$

این قید تضمین می کند که ظرفیت کانال ω_{ij} به اندازه جریان خالص از هر دو تراکنش در کانال کاهش می یابد. اگر جریان های تراکنش هم جهت باشند، ظرفیت به اندازه مجموع جریان ها کاهش یافته و اگر خلاف جهت باشند، ظرفیت کانال به اندازه تفاضل جریان ها کاهش می یابد و به صورت دینامیکی تنظیم می شود. ضرایب $d1$ و $d2$ نیز به عنوان مقادیر کوچک تنظیم کننده به مدل افزوده شده اند تا فرایند بهینه سازی تسهیل شود و از نقص های احتمالی جلوگیری کنند.

تغییرات اعمال شده در مدل مسیریابی، شامل اصلاح تابع هدف و قیود مربوطه، مسئله بهینه سازی را از یک مسئله خطی به یک مسئله بهینه سازی محدب تبدیل کرده اند. این اصلاحات به مدیریت دقیق تر جریان ها و هزینه های مرتبط کمک می کنند و اطمینان می دهند که کانال ها به درستی از لحاظ ظرفیت و جهت جریان ها تنظیم شده اند. با این روش بسیاری از مسیریابی هایی که به علت کمبود ظرفیت کانال قابل انجام نبودند با عبور هوشمندانه دو تراکنش در شبکه قابل انجام می شوند و در اکثر مواقع تراکنشی ارزان تر از مسیریابی غیر توأم خواهیم داشت و یا در بدترین حالت ممکن خود هزینه تراکنش برابر حالت غیر توأم می شود.

۶-۳- مدل مسیریابی برای چند تراکنش همزمان

حال این دو پرداخت را می‌خواهیم به چند پرداخت تبدیل کنیم، هدف انتقال بهینه چندین تراکنش (به طور همزمان) از فرستنده‌ها به گیرنده‌های مختلف است. این مدل با ریلکس کردن شرط ظرفیت و کم‌اثر دانستن مقدار کارمزدها (fee ها) به دلیل کم‌بودن مقدار کارمزد در مقایسه با خود تراکنش‌ها، طراحی شده است. این فرایند شامل بهینه‌سازی مسیرها برای چندین تراکنش مستقل به طور همزمان است. به‌طوری‌که تابع هدف جدید برای چند تراکنش به‌صورت زیر تعریف شده است ما k تراکنش همزمان را در نظر می‌گیریم:

$$\min \sum_i \sum_{j < i} \left| \sum_k tx^k \cdot (\rho(e_{ij}, tx^k) \cdot x_{ij}^k - \rho(e_{ji}, tx^k) \cdot x_{ji}^k) \right|$$

در این تابع هدف، tx^k به تراکنش k اشاره دارد $\rho(e_{ij}, tx^k)$ هزینه مربوط به کانال e_{ji} برای تراکنش k را نشان می‌دهد. این تابع هدف به‌گونه‌ای طراحی شده است که اگر تراکنش‌ها در یک جهت باشند، هزینه‌ها را جمع کرده و اگر خلاف جهت باشند، از یکدیگر کم می‌کند. این رویکرد باعث می‌شود که تأثیرات هزینه‌ای در کانال به‌صورت دقیق‌تری مدل‌سازی شوند و بهینه‌سازی بهتری در مسیریابی چندین تراکنش حاصل شود.

در این تابع ما کارمزد هرکانال را متناسب با مقدار تغییر تعادل آن کانال در نظر می‌گیریم نه مقدار تراکنش‌ها به صورت جداگانه، یعنی اگر چند تراکنش از یک کانال عبور کنند کارمزد کانال برابر جمع کارمزد عبور تک تراکنش‌ها نمی‌شود زیرا این تراکنش‌ها به طور همزمان انجام می‌شوند و کارمزد این کانال تنها متناسب به میزان تغییر تعادل کانال پرداخت می‌شود.

برای مدیریت جریان هر تراکنش، قیود جدیدی تعریف شده‌اند که به طور مستقل فرستنده و گیرنده هر تراکنش را مشخص می‌کنند:

$$\sum_j x_{ij}^k - \sum_j x_{ji}^k = \begin{cases} 1 & \text{اگر } v_i \text{ فرستنده } k \text{ ام باشد,} \\ -1 & \text{اگر } v_i \text{ گیرنده } k \text{ ام باشد,} \\ 0 & \text{در غیر این صورت,} \end{cases} \quad \text{برای همه } i, k$$

این قید جریان برای هر تراکنش به طور جداگانه اعمال می‌شود و به تفکیک جریان هر تراکنش کمک می‌کند که نقش حیاتی در بهینه‌سازی مسیرها دارد.

قید ظرفیت کانال به صورت تسهیل شده طراحی شده است تا تغییرات در جریان‌های هم‌جهت و خلاف جهت را به‌درستی مدیریت کند:

$$\omega_{ij} - \sum_k (tx^k + d^k) \cdot (x_{ij}^k - x_{ji}^k) \geq 0 \quad \text{برای همه } i \text{ ها و } j \text{ ها}$$

این قید تضمین می‌کند که ظرفیت کانال ω_{ij} به اندازه جریان خالص از تمام تراکنش‌ها در کانال کاهش می‌یابد. اگر جریان‌های تراکنش هم‌جهت باشند، ظرفیت به اندازه مجموع جریان‌ها کاهش یافته و اگر خلاف جهت باشند، ظرفیت کانال به صورت دینامیکی تنظیم می‌شود.

مدل مسیریابی چند تراکنشی قدرت زیادی در تنظیم مسیرها دارد، به طوری که با قراردادن جریان‌ها در خلاف جهت در کانال‌های مختلف، تعادل کانال‌ها تا حد ممکن کمتر به هم می‌خورد. این باعث می‌شود که هزینه‌های پرداخت‌ها به مراتب از مسیریابی مجزا ارزان‌تر باشد. این رویکرد به شبکه اجازه می‌دهد تا تراکنش‌هایی که ظرفیت آن‌ها از کانال بیشتر است را به راحتی مدیریت کرده و بهره‌وری شبکه را به طور قابل توجهی افزایش دهد.

این مدل باعث کاهش بار کانال‌ها شده و ظرفیت‌های اضافی را بهینه استفاده می‌کند. به دلیل بهینه‌سازی جریان‌ها و کاهش هزینه‌ها، شبیه‌سازی‌ها نشان داده‌اند که این رویکرد می‌تواند عملکرد شبکه را بهبود بخشد و زمان انجام تراکنش‌ها را کاهش دهد. با ترکیب تراکنش‌ها و استفاده از ظرفیت کانال‌ها به طور هم‌زمان، مدل جدید کارایی و انعطاف‌پذیری بالاتری در مدیریت چند تراکنش ارائه می‌دهد.

مدل مسیریابی برای چند تراکنش هم‌زمان، با استفاده از تغییرات در تابع هدف و قیود جریان، امکان بهینه‌سازی هم‌زمان چندین تراکنش را فراهم می‌کند. این مدل به شبکه اجازه می‌دهد تا با کاهش هزینه‌ها و افزایش بهره‌وری، تراکنش‌ها را به طور مؤثرتر و سریع‌تر مدیریت کند. با استفاده از این رویکرد، شبکه می‌تواند به تعادل بهتر در استفاده از ظرفیت کانال‌ها دست یابد و عملکرد کلی خود را بهبود بخشد.

۷-۳- بهینه‌سازی مسیریابی چندگانه با شرط کاهش مرکزیت

همان‌طور که در [38] و بسیاری از مقالات تحلیلی دیگر بیان شده است، شبکه‌های کانال پرداخت که از مسیریابی معمولی استفاده می‌کنند، مانند شبکه لایت‌نینگ، با مشکل تمرکزگرایی مواجه شده‌اند. به این معنا که چندین گره وجود دارند که کنترل تعداد زیادی از تراکنش‌ها را در دست دارند و اکثر پرداخت‌ها از یکی از این گره‌ها عبور می‌کنند. این امر با فلسفه وجودی رمزآرزی مانند بیت‌کوین که بر غیرمتمرکز بودن تأکید دارد، در تضاد است و

منجر به ایجاد مرکزیتی کنترل شده در شبکه می شود. این گره ها معمولاً در میانه شبکه قرار دارند و با تعداد زیادی از گره ها کانال ایجاد کرده اند، بنابراین جزو گره هایی با بیشترین درجه در شبکه پرداخت محسوب می شوند.

وجود این گره ها در شبکه باعث کاهش امنیت و حریم خصوصی گره ها شده و توزیع سود ناشی از پرداخت ها را نیز نامتعادل می کند، به طوری که برای تعداد زیادی از گره های شبکه، روتر بودن صرفه اقتصادی ندارد. تمرکزگرایی در شبکه می تواند خطرات امنیتی قابل توجهی ایجاد کند؛ زیرا هرگونه نقص یا حمله به این گره ها می تواند کل شبکه را تحت تأثیر قرار دهد. همچنین، تمرکز سود در دست چند گره، نابرابری اقتصادی را افزایش می دهد و انگیزه سایر گره ها برای مشارکت در شبکه را کاهش می دهد.

هدف ما در این بخش و در کل این پایان نامه ارائه راهکاری است که تمرکز را کاهش دهد و سود ناشی از کارمزدها در شبکه به صورت منصفانه تری بین گره های شبکه تقسیم شود. در این بخش قصد داریم با تغییر در الگوریتم اولیه مسیریابی شبکه، امکان مسیریابی متوالی تراکنش ها را برای گره های مرکزی نسبت به گره های غیرمرکزی کاهش دهیم. این کار می تواند سودآوری برای گره های غیرمرکزی را افزایش دهد و در نتیجه شبکه را به سمت توزیع شدگی بیشتر حرکت خواهد داد یعنی به مرور زمان گره های مرکزی متوجه می شوند که دیگر مرکز شبکه بودن برای آن سود کمتری خواهد داشت و خودشان شبکه را به سمت توزیع شدگی بیشتر سوق می دهند.

در این مدل بهینه سازی، هدف مدیریت و بهینه سازی مسیرهای چندین تراکنش به طور همزمان، با در نظر گرفتن درجه گره ها در شبکه است. به این ترتیب، تراکنش ها به گونه ای مسیریابی می شوند که تراکم تراکنش ها در گره های با درجه بالا کاهش یابد و بهینه سازی در توزیع تراکنش ها به گره های با درجه پایین تر صورت گیرد.

یک قید جدید به مسئله اضافه شده است که میزان تراکنش های عبوری از هر گره را با توجه به درجه آن گره تنظیم می کند:

$$\sum_k \sum_j x_{ij}^k \leq \left((M-1) \cdot \frac{\max\{\text{degree}\} - \text{degree}(v_i)}{\max\{\text{degree}\} - 1} \right) + 1 \quad \text{برای همه } i \text{ ها}$$

در اینجا، M مقدار حداکثر تراکنش های همزمان است که از گره های مختلف عبور می کند. این قید به گونه ای طراحی شده که گره هایی با درجه بالا، تراکنش های کمتری را همزمان پردازش کنند و تراکنش ها بیشتر از گره های با درجه کمتر عبور کنند.

قید جدید کاهش مرکزیت نقش حیاتی در توزیع تراکنش‌ها و جلوگیری از تراکم بیش از حد در گره‌های با درجه بالا ایفا می‌کند. با تنظیم این قید، می‌توان اطمینان حاصل کرد که جریان تراکنش‌ها به گره‌هایی با درجه کمتر هدایت می‌شود که باعث کاهش ترافیک و بهبود کارایی شبکه می‌شود. این قید از تمرکز تراکنش‌ها در یک گره خاص جلوگیری می‌کند و به توزیع یکنواخت تراکنش‌ها در کل شبکه کمک می‌کند.

مسئله کلی ما به شکل زیر خواهد شد:

$$\min \sum_i \sum_{j < i} \left| \sum_k tx^k \cdot (\rho(e_{ij}, tx^k) \cdot x_{ij}^k - \rho(e_{ji}, tx^k) \cdot x_{ji}^k) \right|$$

با قید :

$$\sum_j x_{ij}^k - \sum_j x_{ji}^k = \begin{cases} 1 & \text{اگر } v_i \text{ فرستنده } k \text{ ام باشد,} \\ -1 & \text{اگر } v_i \text{ گیرنده } k \text{ ام باشد,} \\ 0 & \text{در غیر این صورت,} \end{cases}$$

$$\omega_{ij} - \sum_k (tx^k + d^k) \cdot (x_{ij}^k - x_{ji}^k) \geq 0 \quad \text{برای همه } i \text{ و } j \text{ ها}$$

$$\sum_k \sum_j x_{ij}^k \leq \left((M-1) \cdot \frac{\max\{\text{degree}\} - \text{degree}(v_i)}{\max\{\text{degree}\} - 1} \right) + 1 \quad \text{برای همه } i \text{ ها}$$

۸-۳- الگوریتم پیدا کردن کوتاه‌ترین مسیر

همان‌طور که گفته شده پیدا کردن کوتاه‌ترین مسیر با استفاده از حل مسئله بهینه‌سازی به صورت عددی معقول نیست و در این قسمت الگوریتمی را معرفی می‌کنیم که این بهینه‌سازی را در زمان بسیار کمتری حل می‌کند. ما چندین فرض در این مسئله داریم به این صورت که ما توپولوژی کل شبکه و کانال‌های باز موجود در کل شبکه را می‌دانیم، ظرفیت کانال‌ها و تعادل ظرفیت بین طرفین را اطلاع داریم که این تعادل در شبکه لایتینگ پنهان است و فرض دیگر این است که پرداخت به صورت اتمی و بدون تقسیم‌شدن از یک مسیر انجام می‌شوند.

رایج‌ترین الگوریتم برای پیدا کردن کوتاه‌ترین مسیر الگوریتم دایجسترا^{۳۲} است اما این الگوریتم برای شبکه ما بدون هیچ تغییری کارا نیست زیرا اگر از فرستنده به گیرنده این الگوریتم را اجرا کنیم به علت وجود کارمزدها در مسیر و اضافه شدن مقدار کل پرداخت در طول مسیر ممکن است یال‌های ابتدایی گذشته از آنها در ابتدا ظرفیت داشته باشند ولی با افزایش طول مسیر و زیاد شدن مقدار تراکنش به علت اضافه شدن کارمزد کانال‌های میانی دیگر ظرفیت کافی را برای عبور کل تراکنش نداشته باشند.

برای رفع این مشکل جهت یال‌ها را برعکس می‌کنیم و مسیریابی را از مقصد به مبدأ انجام می‌دهیم و کارمزدهای هر کانال را به مقدار تراکنش اضافه می‌کنیم برای عبور از هر کانال و دیگر نگران افزایش مقدار اولیه تراکنش نیستیم زیرا تراکنش‌ها از ابتدا که حرکت می‌کردیم مقدارش زیاد می‌شود و کانال‌های ابتدایی بایستی ظرفیت بیشتری می‌داشتند ولی از انتها که حرکت کنیم هر کانال فقط باید به اندازه کارمزدهای کانال‌های جلوتر از خودش که قبلاً آنها را دیده‌ایم ظرفیت بیشتری داشته باشد، با این ابتکار مقدار کل مبلغی که به عنوان کارمزد باید پرداخت کنیم از ابتدا تراکنش معلوم می‌شود. الگوریتم دایجسترا تغییر یافته برای پیدا کردن کوتاه‌ترین مسیر از مقصد به مبدأ در الگوریتم ۱ آمده است که این الگوریتم با امتیازدهی به گره توجه به کارمزدی که در کانال خود می‌گیرند و با استفاده از شروط ظرفیت که با اگرهای موجود در الگوریتم ارضا می‌شود به ارزان‌ترین مسیر دست پیدا می‌کند.

الگوریتم ۱: الگوریتم ما برای یافتن ارزان‌ترین درخت پوشا از گیرنده

ورودی: گراف (V, E) ، گیرنده r ، تراکنش tx .
خروجی: یک درخت پوشای ارزان برای تراکنش‌ها به r .

$$1. \quad Q \leftarrow V$$

$$2. \quad T \leftarrow \emptyset$$

$$3. \quad \text{cost}(v) \leftarrow \infty, \text{cost}(r) \leftarrow 0 \text{ برای همه } v \neq r$$

$$4. \quad \text{تا زمانی که } Q \neq \emptyset \text{ انجام بده:}$$

$$5. \quad v_i \leftarrow \operatorname{argmin}\{\text{cost}(v), v \in Q\}$$

$$6. \quad Q \leftarrow Q \setminus \{v_i\}$$

$$7. \quad \text{برای همه } e_{ij} \in E \text{ انجام بده:}$$

$$8. \quad \text{اگر } \text{cost}(v_i) + \rho(e_{ji}, tx) + \alpha(tx) \leq \omega_{ji} \text{ باشد آنگاه:}$$

$$9. \quad \text{اگر } \text{cost}(v_i) + \rho(e_{ji}, tx) < \text{cost}(v_j) \text{ باشد آنگاه:}$$

$$10. \quad \text{cost}(v_j) \leftarrow \text{cost}(v_i) + \rho(e_{ji}, tx)$$

³² Dijkstra

۱۱. $\text{path}(vj) \leftarrow e_{ji}$
۱۲. پایان اگر
۱۳. پایان اگر
۱۴. پایان برای
۱۵. پایان تا زمانی که
۱۶. $\emptyset \leftarrow T$
۱۷. برای همه $v \in V$ انجام بده: $T \leftarrow T \cup \{\text{path}(v)\}$
۱۸. پایان برای
۱۹. T را بازگردان

الگوریتم ۱: الگوریتم دایجسترا تغییر یافته برای پیدا کردن کوتاه ترین مسیر از انتها به ابتدا در شبکه با یال های معکوس شده [28]

۹-۳- الگوریتم ابتکاری جهت کاهش گره های مرکزی

برای بهبود الگوریتم به منظور افزایش توزیع شدگی شبکه به الگوریتم ابتکاری زیر رسیده ایم:

الگوریتم از ابتدا به گونه ای فرض شده است که آن قدر سریع انجام شود که در هر بار اجرا تنها یک پرداخت در شبکه وجود داشته باشد و به صورت سری یکی پس از دیگری پرداخت ها انجام شود. ما برای هر گره یک بودجه قرار می دهیم که این بودجه متناسب با درجه یا مرکزی بودن هر گره است هر چه بودجه بیشتر باشد مرکزیت کمتر است و برعکس به طوری که گره با بیشترین درجه در شبکه داری بودجه یک است. (الگوریتم ۲)

با هر بار عبور تراکنش از گره ها از مقدار بودجه آن یک واحد کم می شود و در صورت عبور نکردن در هر نوبت از پرداخت به مقدار این بودجه یک واحد اضافه می شود تا به مقدار حداکثر موجود خود که متناسب با درجه آن گره مشخص شده است برسد. (الگوریتم ۳)

در صورتی مقدار بودجه هر گره صفر شود آن گره از شبکه برای مسیریابی حذف می شود تا دیگر نتواند از خود مسیری را عبور دهد و بعد از گذشت یک نوبت دوباره به مقدار بودجه آن یکی اضافه می شود و می تواند برای مسیریابی بعدی در شبکه باشد، یعنی در بدترین حالت یک پرداخت در میان به گره با بیشترین درجه اجازه مسیریابی داده می شود (البته این عدد می تواند جور دیگری باشد که برای رسیدن با آن با کمی تغییر الگوریتم می شود به آن رسید و تنظیم آن بده بستانی بین بهره وری و مرکزی شدن شبکه است). (الگوریتم ۴)

الگوریتم ۲: ایجاد بودجه برای هر گره

۱. برای هر گره در شبکه
۲. بودجه گره = $1 +$ درجه گره - بیشترین درجه گره در شبکه
۳. پایان برای

الگوریتم ۲: ایجاد بودجه برای هر گره در شبکه مسیریابی

الگوریتم ۳: تابع حذف گره از الگوریتم در صورت صفر شدن بودجه

- ورودی: گراف شبکه، فرستنده، گیرنده
خروجی: گراف شبکه با حذف گره‌های با بودجه صفر برای مسیریابی
۱. برای هر گره در شبکه
 ۲. اگر بودجه گره صفر نباشد و گره فرستنده یا گیرنده نباشد:
 ۳. گره را از شبکه مسیریابی حذف کن
 ۴. اضافه کردن
 ۵. پایان برای
 ۶. برگرداندن شبکه

الگوریتم ۳: تابع حذف گره از الگوریتم در صورت صفر شدن بودجه

الگوریتم ۴: تابع تغییر بودجه که در داخل حلقه پرداخت استفاده می‌شود

- ورودی: گراف شبکه، فرستنده، گیرنده، مسیر
خروجی: گراف شبکه با وجود تغییر در بودجه آن
۱. برای هر گره در شبکه
 ۲. اگر گره در مسیر باشد:
 ۳. از بودجه گره یکی حذف می‌کنیم
 ۴. در غیر این صورت اگر مقدار بودجه گره کمتر از $(1 + \text{درجه گره} - \text{بیشترین درجه گره در شبکه})$:
 ۵. یک واحد به بودجه گره اضافه می‌کنیم
 ۶. پایان اگر
 ۷. پایان برای
 ۶. برگرداندن شبکه

الگوریتم ۴: تابع کم کردن یک واحد از بودجه در صورت بودن در مسیریابی و فرستنده گیرنده نبودن و اضافه کردن یک واحد در صورت نبودن در مسیریابی

این الگوریتم ابتکاری یک عدالت نسبی بین گره‌ها ایجاد می‌کند تا گره‌های میانی و با درجه بالاتر، بیشترین پرداخت‌ها را از خود عبور ندهند، یعنی درآمد گره‌های غیرمرکزی‌تر را بیشتر کرده و درآمد گره‌های مرکزی‌تر را

کم می‌کند تا شبکه و گره‌های آن انگیزه‌ای برای افزایش درجه خود و مرکزی کردن خودشان نداشته باشند تا به‌مرور زمان شبکه از مرکزی شدن به سمت توزیع‌شدگی گره‌های آن حرکت کند تا تأثیر یک تک گره را در شبکه کمتر کند و یک گره نتواند قیمت تعداد زیادی از تراکنش‌ها را کنترل کند.

به‌طور کلی برای جمع‌بندی این فصل باید گفت، این پایان‌نامه دو راه‌حل کلی را برای کاهش مرکزیت شبکه پیشنهاد می‌دهد که هر دو از مسیریابی برای این کار استفاده می‌کنند. راه‌حل اول عمیق بوده می‌تواند دروازه‌ای باشد برای کارهای آینده و مسیریابی‌های که از این بهینه‌سازی استفاده کرده‌اند و بهبود قابل توجه‌ای در کارآمدی شبکه داده‌اند و راه‌حل دوم یک راه حل ساده اکتشافی است که به کمتر کردن مرکزیت شبکه کمک می‌کند.

در راه‌حل اول بهینه‌سازی مسیریابی چندگانه برای تراکنش‌ها در شبکه باتوجه به درجه گره‌ها و با استفاده از یک شرط کاهش مرکزیت بررسی شد. مدل جدید با تغییر تابع هدف و قیود مربوطه، به‌گونه‌ای طراحی شده است که توازن در توزیع تراکنش‌ها و کاهش ترافیک گره‌های با درجه بالا را تضمین می‌کند.

با ریلکس کردن قید ظرفیت و نادیده گرفتن مقادیر کوچک فی، مسئله بهینه‌سازی به صورتی ساده‌تر و کارآمدتر مطرح شده است. تغییر تابع هدف به‌گونه‌ای که هزینه‌ها باتوجه به جهت و مقدار جریان تراکنش‌ها در کانال‌ها بهینه‌سازی شوند، امکان استفاده بهینه از ظرفیت کانال‌ها را فراهم می‌آورد. این تغییرات باعث می‌شوند که جریان تراکنش‌ها در شبکه به طور هم‌زمان مدیریت شده و هزینه‌ها کاهش یابد.

اضافه کردن قید کاهش مرکزیت به مدل بهینه‌سازی، تضمین می‌کند که تراکنش‌ها به گره‌هایی با درجه کمتر هدایت شده و از تمرکز تراکنش‌ها در گره‌های با درجه بالا جلوگیری می‌شود. این امر باعث کاهش بار گره‌های با درجه بالا، بهبود کارایی شبکه، و جلوگیری از ایجاد گلوگاه‌های احتمالی می‌شود.

نتایج این بهینه‌سازی نشان می‌دهند که با کاهش ترافیک در گره‌های پرتراکم و بهینه‌سازی مسیرهای تراکنش، شبکه می‌تواند تراکنش‌ها را با بهره‌وری بالاتر و هزینه‌های کمتر مدیریت کند. این مدل بهینه‌سازی علاوه بر کاهش هزینه‌های تراکنش و بهبود بهره‌وری، منجر به تعادل بهتری در استفاده از منابع شبکه شده و عملکرد کلی سیستم را بهبود می‌بخشد. در این راه‌حل، تمامی تراکنش‌ها باید به‌صورت هم‌زمان و چندپرداخته انجام شوند تا مرکز شبکه تحت کنترل قرار گیرد.

در صورتی که بخواهیم از پرداخت چندمسیره استفاده نکنیم، ما در راه حل دوم خود یک الگوریتمی اکتشافی تک پرداخته ارائه کرده ایم که تا حدی می تواند مرکزیت شبکه را کنترل کند. ابتدا یک الگوریتم بهینه سازی برای یافتن کوتاه ترین مسیر در شبکه ها، به ویژه در شبکه لایتینگ، معرفی شد که این الگوریتم با معکوس کردن جهت یال ها و شروع مسیریابی از مقصد به مبدأ، مشکل افزایش کارمزدها و ظرفیت ناکافی کانال ها را حل می کند. با این تغییر، الگوریتم دایجسترا با تغییرات جدید، می تواند ارزان ترین مسیر را با توجه به کارمزدها و ظرفیت کانال ها پیدا کند.

سپس، یک الگوریتم ابتکاری برای کاهش تمرکز شبکه و افزایش توزیع شدگی گره ها ارائه شده است. در این روش، برای هر گره بودجه ای متناسب با درجه آن تعیین می شود و در صورت استفاده مکرر از گره های مرکزی، بودجه آنها کاهش می یابد، تا گره های مرکزی کمتر برای مسیریابی استفاده شوند. این الگوریتم به تدریج باعث کاهش تمرکز و بهبود توزیع شدگی تراکنش ها در شبکه با کاهش ارزش اقتصادی گره های مرکزی و افزایش ارزش اقتصادی گره های غیر مرکزی می شود.

در نهایت، لازم به یادآوری است که هر دو راه حل ارائه شده در این پایان نامه به صورت کاملاً مرکزی و با نظارت یک دالانای کل شبکه انجام می شوند و از مدل های توزیع شده بهره نمی گیرند. این بدان معناست که تصمیم گیری های مربوط به مسیریابی و بهینه سازی در هر دو راه حل، به طور متمرکز توسط یک نهاد مرکزی هدایت می شود و بر خلاف سیستم های توزیع شده، نیاز به اطلاعات کامل و دقیق از کل شبکه برای اجرای بهینه سازی ها وجود دارد.

۴- فصل چهارم: ارزیابی و شبیه‌سازی‌ها

در این فصل، به تفسیر جامعی از شبیه‌سازی و اجزای مختلف آن پرداخته خواهد شد. ابتدا، شبیه‌سازی انجام شده به طور مفصل شرح داده می‌شود. اجزای کلیدی شامل الگوریتم‌ها، مدل‌ها، و نحوه اجرای شبیه‌سازی با جزئیات مورد بررسی قرار می‌گیرند. سپس، نتایج به دست آمده از تغییر الگوریتم به منظور بهبود توزیع پذیری و نقش مرکزی شبیه‌سازی بررسی می‌شود. ما نشان می‌دهیم که تغییرات الگوریتم چگونه می‌تواند بهبودهای قابل توجهی در مرکزی شدن ایجاد کند و اثرات مختلف آن را مورد تجزیه و تحلیل قرار می‌دهیم. در ادامه، فرایند حل مسئله بهینه‌سازی به صورت عددی مورد بررسی قرار می‌گیرد. ما حل عددی مسئله را با الگوریتم مقایسه می‌کنیم تا درستی و کارایی آن را نشان دهیم و نتایج به دست آمده را به صورت گرافیکی و عددی ارائه می‌دهیم. سپس، ما مسئله بهینه‌سازی که قید آن ساده شده را با الگوریتم مسیریابی که جواب مسئله بهینه‌سازی کامل را نمایندگی می‌کند مقایسه می‌کنیم تا نشان دهیم که تأثیر ناچیزی از تغییر قید در نتایج وجود دارد و بهبودهای حاصله از این مقایسه را توضیح می‌دهیم. در ادامه، ما نتایج شبیه‌سازی برای حالت مسیریابی دو پرداخته را با حالت تک پرداخته بررسی می‌کنیم و بهبودهای حاصله را شرح می‌دهیم. همچنین، نتایج شبیه‌سازی برای حالت چند پرداخته را مورد بررسی قرار داده و بهبودهای حاصله را تشریح می‌کنیم و در پایان، ما نتایج حاصل از اضافه کردن قید توزیع پذیری را ارائه می‌دهیم و نحوه بهبود آن را نسبت به حالت نبود این قید توضیح می‌دهیم.

ما در این ارزیابی برخلاف فصل قبل ابتدا به ارزیابی راه حل دوم می‌پردازیم و سپس راه حل اول که راه حل اصلی پایان نامه است را بررسی می‌کنیم. علت این کار این است که ما برای نشان دادن صحت مسیریابی تغییر قید یافته با مسئله بهینه‌سازی اصلی بایستی آنها را در پرداخت‌های مشابه با یکدیگر مقایسه کنیم ولی به علت تعداد بسیار بالای قید در مسئله بهینه‌سازی ابتدایی این کار ممکن نبود. پس به جای اجرای این بهینه‌سازی از معادل الگوریتمی آن که در راه حل دوم توضیح داده‌ایم استفاده می‌کنیم تا نشان دهیم این تغییر قید در نتایج مسیریابی مشابه مسئله اولیه است که این بار با الگوریتم محاسبه شده است. پس ابتدا الگوریتم را پیاده‌سازی کرده و آن را با

الگوریتم ابتکاری مقایسه می‌کنیم سپس صحت مسئله بهینه‌سازی تغییر قید یافته را الگوریتم می‌سنجیم و در آخر هم بهبود شرایط مرکزی شبکه را با استفاده از بهینه‌سازی نشان می‌دهیم.

۴-۲- شبیه‌سازی مسئله

این شبکه را از ابتدا پیاده‌سازی شده است و از شبیه‌سازی‌های موجود استفاده نشده. برای این منظور، از زبان برنامه‌نویسی پایتون و به‌ویژه از کتابخانه NetworkX جهت ایجاد و تحلیل ساختار شبکه استفاده شده است. این کتابخانه برای ما امکان ساخت و ارزیابی شبکه‌های پیچیده را فراهم می‌کند.

شبکه‌ای که برای شبیه‌سازی ایجاد شده، شامل ۱۰۰۰ گره است و بر اساس مدل باراباشی - آلبرت (Barabási-Albert) با پارامتر ۲ طراحی شده است. این مدل که برای شبیه‌سازی شبکه‌هایی با توزیع توانی (Power Law) استفاده می‌شود، به ما این امکان را می‌دهد که شبکه‌ای با توزیع درجه نامتوازن بسازیم. در این ساختار، برخی گره‌ها نقش مهم‌تری در مسیریابی تراکنش‌ها ایفا می‌کنند، شبیه به شبکه‌های کانال پرداخت و سیستم‌های واقعی که در آن تعداد معدودی از گره‌ها (گره‌ها) نقش مرکزی دارند.

برای هر کانال بین گره‌ها، موجودی اولیه به مقدار ۱۰۰۰ واحد تنظیم شده است. این موجودی‌ها نمایانگر ظرفیت اولیه کانال‌ها برای پردازش تراکنش‌ها هستند. همچنین، برای تعیین حجم تراکنش‌ها، از یک توزیع لاگ - نرمال با میانگین ۲.۹۵ و انحراف معیار ۱.۲ استفاده شده است. این پارامترها بر اساس داده‌های واقعی تراکنش‌ها تنظیم شده و حجم پرداخت‌های معمول در شبکه را به طور واقع‌گرایانه شبیه‌سازی می‌کنند. فرستنده و گیرنده هر تراکنش به طور تصادفی از میان گره‌های شبکه انتخاب می‌شوند و مقدار پرداختی باتوجه‌به این توزیع به آن‌ها اختصاص می‌یابد.

هر تراکنش کارمزدی به میزان ۰.۵٪ از مبلغ پرداختی دارد که این کارمزد به‌صورت پویا باتوجه‌به ظرفیت و تعادل کانال‌ها تنظیم می‌شود. به این صورت که اگر ظرفیت یک کانال کاهش یابد، کارمزد عبور تراکنش از آن کانال که باعث کاهش بیشتر ظرفیت می‌شود، افزایش می‌یابد و برعکس، اگر تراکنش باعث افزایش ظرفیت کانال شود، کارمزد کاهش می‌یابد. این تنظیمات کمک می‌کند تا شبکه به‌صورت پویا تعادل خود را حفظ کرده و از ازدحام در برخی کانال‌ها جلوگیری شود.

این شبیه‌سازی به ما امکان می‌دهد تا رفتار شبکه و تأثیر تغییرات مختلف را بر روی عملکرد آن بدون درگیر کردن خود به مسائل حریم شخصی و تأخیر بین گره‌های شبکه و درواقع پیاده‌سازی یک شبکه آزمایشی واقعی به طور دقیق تحلیل کنیم و راهکارهایی برای بهینه‌سازی آن ارائه دهیم.

۳-۴- شبیه‌سازی پرداخت‌ها با الگوریتم اولیه

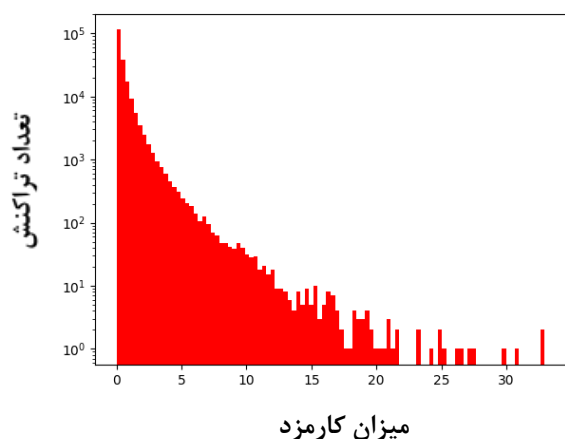
روند شبیه‌سازی الگوریتم اولیه (الگوریتم ۱) که مسیریابی بین دو گره فرستنده گیرنده بدون در نظر گرفتن کنترل مرکزی شدن شبکه است در این قسمت توضیح داده خواهد شد. این روند به این صورت است که در ابتدا یک گراف برای شبکه کانال پرداخت ایجاد می‌شود. این گراف بر اساس مدل باراباسی - آلبرت ساخته می‌شود که برخی گره‌ها تعداد بیشتری کانال دارند، به عبارتی دیگر، برخی گره‌ها بیشتر به عنوان هاب یا مرکز شبکه عمل می‌کنند. در این مرحله، گره‌ها و کانال‌ها با موجودی و ظرفیت‌های اولیه با مقدار ثابت گفته شده تنظیم می‌شوند که موجودی هر گره و ظرفیت هر کانال بر اساس عبور تراکنش از آنها تغییر می‌کند.

پس از ایجاد گراف، کارمزدهای مسیریابی برای تراکنش‌ها بر اساس ظرفیت کانال‌ها یا همان تعادلشان تنظیم می‌شود. این تنظیمات به گونه‌ای انجام می‌شود که تراکنش‌ها تمایل بیشتری به استفاده از کانال‌های با ظرفیت بالاتر داشته باشند. این روش باعث می‌شود که ظرفیت کانال‌ها به طور متعادل‌تری مورد استفاده قرار گیرند و از ایجاد تراکم در کانال‌ها جلوگیری شود.

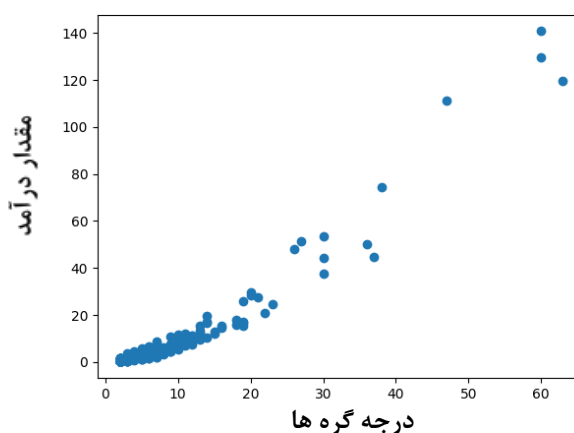
حال یک چرخه ۲۰۰۰۰۰ تایی برای هر پرداخت ایجاد می‌شود که در هر چرخه به صورت تصادفی یک فرستنده گیرنده در شبکه ایجاد می‌شود و با مقدار پرداخت گرفته شده از توزیع گفته شده. برای هر کدام از این پرداخت‌ها مسیرهای ارزان از طریق الگوریتم مسیریابی که بر اساس اصول اصلاح‌شده الگوریتم دایجسترا کار می‌کنند، تعیین می‌گردد که مطابق الگوریتم ۱ پیاده‌سازی شده است. این مسیریابی یک لیست از کانال‌های مسیر را برمی‌گرداند که برای هر کدام از این کانال‌ها مقدار ظرفیت و کارمزد آنها متناسب با پرداخت تغییر خواهد کرد و شبکه با توجه به پرداخت انجام شده در مسیر مشخص شده تغییر می‌کند و نتایج شامل مقدار کل پرداخت، هزینه تراکنش، مسیر استفاده‌شده، و تعداد کانال‌های طی شده ذخیره می‌گردد. در طول این چرخه اطلاعاتی مانند تراکنش‌های موفق، شکست‌ها، و مسیرهای پرهزینه‌تر (به معنی مسیرهایی که هزینه کارمزد آنها بیشتر از هزینه پرداخت بر روی زنجیره بلاک‌ها رمزارز باشد که در اینجا بیشتر از ۰.۴۱ واحد است مطابق مقاله [28]) جمع‌آوری می‌شود. نتایج این تراکنش‌ها شامل داده‌های مربوط به تعادل گره‌ها، تاریخچه پرداخت‌ها، اندازه مسیرها و هزینه‌ها است که در

نهایت برای تحلیل‌های بیشتر و ترسیم نمودارها ذخیره می‌شوند و در آخر نمودار توزیع موجودی گره‌ها، تاریخچه تراکنش‌ها و اندازه مسیرها، میزان کارمزدها و تعادل شبکه به‌عنوان خروجی داده می‌شود.

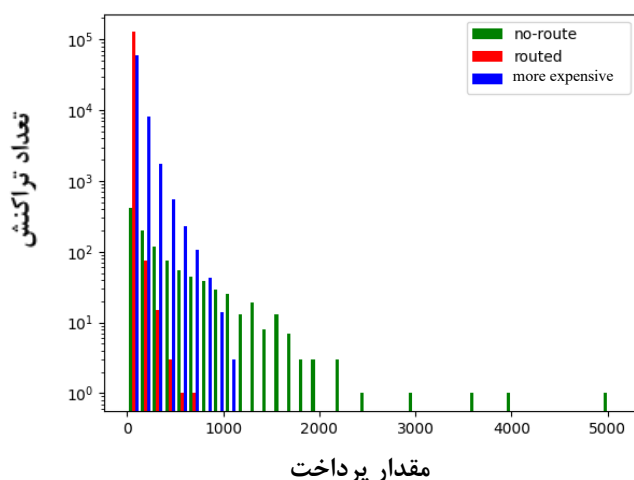
و حاصل شبیه‌سازی‌های ما به‌صورت زیر شده است:



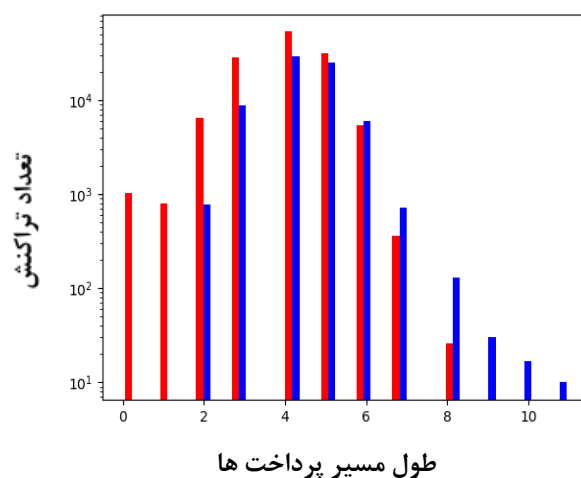
شکل: ۹ نمودار مقدار کارمزد هر تراکنش براساس تعداد تراکنش‌ها



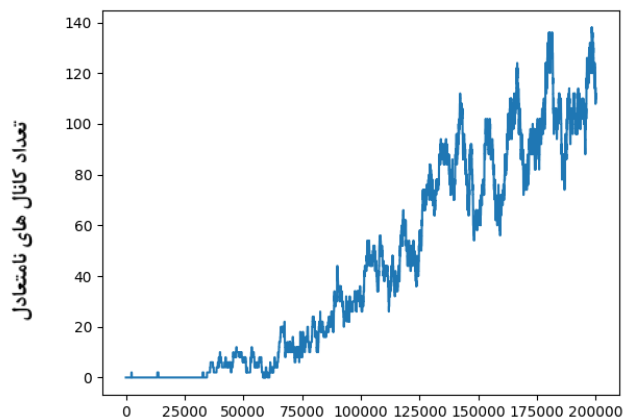
شکل: ۱۰ نمودار توزیع گره‌ها براساس مقدار درجه است که نشان می‌دهند گره‌ها با هر درجه چقدر در آمد از این ۲۰۰۰۰۰ پرداخت در این الگوریتم داشته اند



شکل: ۱۱ نمودار قیمت پرداخت‌ها برحسب تعداد آنها است که رنگ قرمز پرداخت‌های با کارمزد ارزان تر از پرداخت در زنجیره است، آبی کارمزد های گرانتر را نشان می‌دهد و سبز نشان دهنده پرداخت‌هایی هستند که موفق به انتقال در شبکه نشدند.



شکل: ۱۲ نمودار طول مسیرهای پرداخت شده برحسب تعداد آنها که رنگ قرمز نشان دهنده مسیرهایی هستند که ارزان تر از پرداخت در زنجیره انجام شده اند و رنگ آبی نشان دهنده مسیرهایی هستند که گران تر از مقدار پرداخت در زنجیره کارمزد دارند.

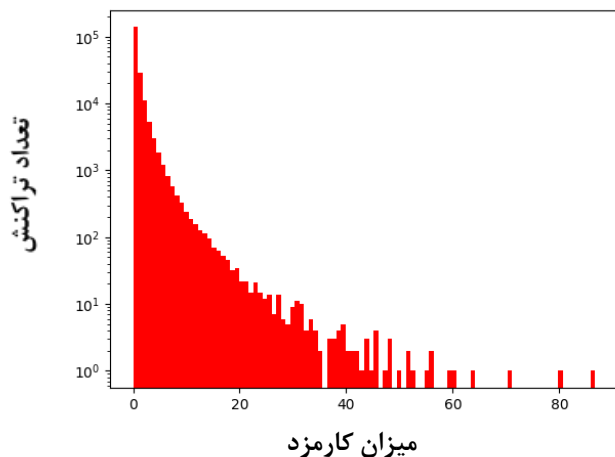


شماره پرداخت

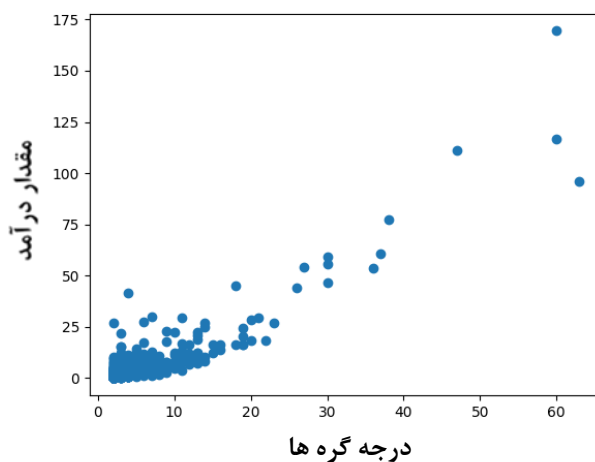
شکل ۱۳: نمودار دنباله پرداخت ها برحسب تعداد گره های یک طرفه شده که نشان دهنده نا متعادل شدن شبکه است برای الگوریتم اولیه

۴-۴- شبیه سازی پرداخت ها با الگوریتم مرکزی کننده شبکه

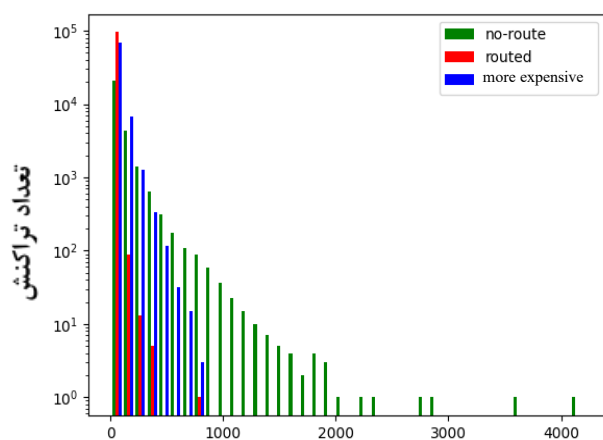
در حالت مسیریابی مرکزی، قبل از شروع تراکنش ها، شبکه به صورت خاصی متعادل سازی می شود تا عملکرد مسیریابی به سمت هزینه زا کردن گره های با درجه بالا حرکت کند. این متعادل سازی شامل حذف موقت گره هایی با بودجه ی کم درگراف مسیریابی است پس برای ایجاد آنها ما در ابتدا برای هر گره یک بودجه متناسب با درجه آنها با تناسب عکس میزان درجه آنها در نظر میگیریم و در هر تغییر شبکه بعد از مسیریابی اگر مسیر از آنها رد شده باشد یکی از این بودجه کم میکنیم و اگر نشده باشد تا رسیدن به مقدار حداکثرشان یکی اضافه میکنیم. قبل از شروع مسیریابی اگر گرهی بودجه صفر داشته باشد از گرافای که مسیریابی روی آن انجام می شود حذف می شود. این تغییرات که همان اعمال الگوریتم ۲، الگوریتم ۳ و الگوریتم ۴ است بر روی ۲۰۰۰۰۰ تراکنش با همان مقدار دهی گفته شده پیاده سازی شده است و نتایج زیر را ایجاد کرده است که شامل نمودار های توزیع موجودی گره ها، تاریخچه تراکنش ها و اندازه مسیر ها و میزان کارمزد ها می شود:



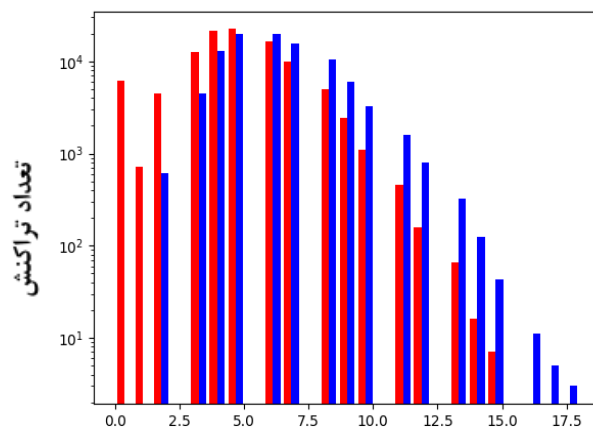
شکل ۱۳: نمودار مقدار کارمزد هر تراکنش براساس تعداد تراکنش ها الگوریتم مرکزی کننده



شکل ۱۴: نمودار توزیع گره ها بر اساس مقدار درجه است که نشان می دهند گره ها با هر درجه چقدر در آمد از این ۲۰۰۰۰۰ پرداخت در این الگوریتم مرکزی کننده داشته اند



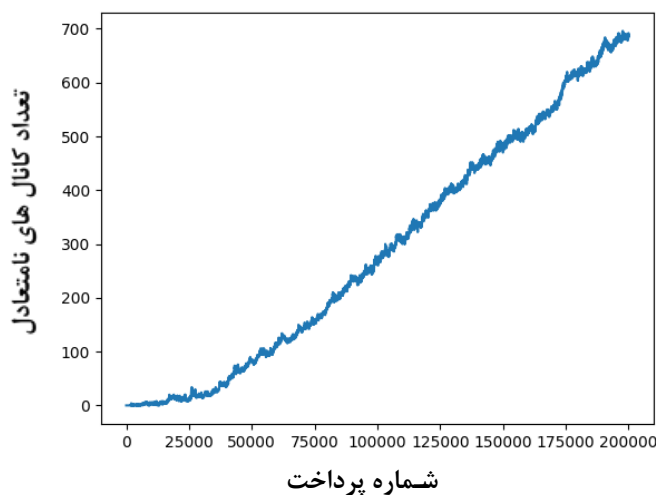
مقدار پرداخت



طول مسیر پرداخت ها

شکل ۱۶: نمودار قیمت پرداخت ها بر حسب تعداد آنها است که رنگ قرمز پرداخت های با کارمزد ارزان تر از پرداخت در زنجیره است، آبی کارمزد های گرانتر را نشان می دهد و سبز نشان دهنده پرداخت هایی هستند که موفق به انتقال در شبکه نشدند.

شکل ۱۵: نمودار طول مسیرهای پرداخت شده بر حسب تعداد آنها که رنگ قرمز نشان دهنده مسیر هایی هستند که ارزان تر از پرداخت در زنجیره انجام شده اند و رنگ آبی نشان دهنده مسیر هایی هستند که گران تر از مقدار پرداخت در زنجیره کارمزد دارند.

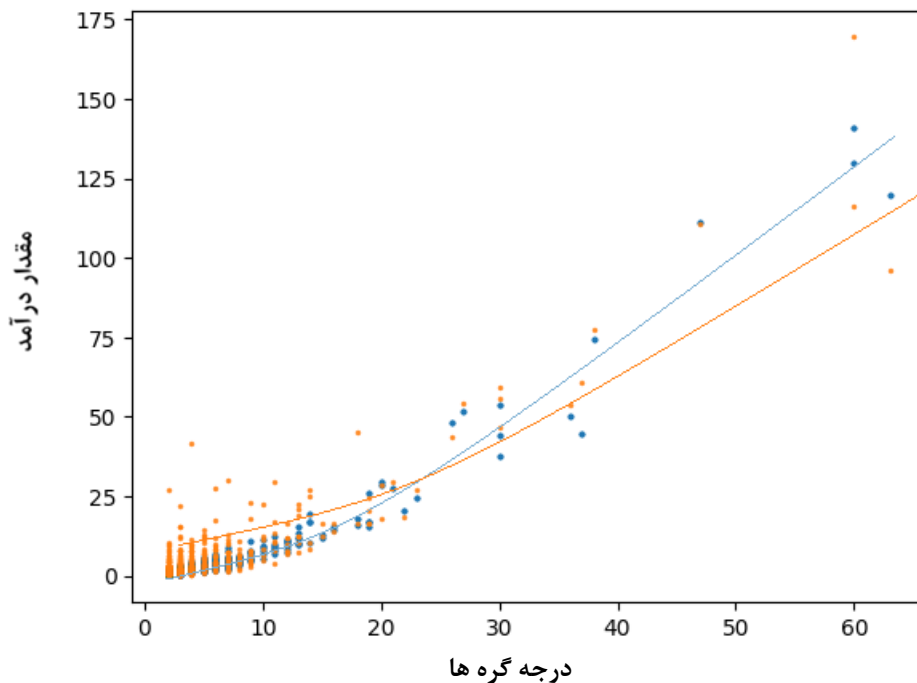


شکل ۱۷: نمودار دنباله پرداخت ها بر حسب تعداد گره های یک طرفه شده که نشان دهنده نامتعادل شدن شبکه است برای الگوریتم مرکزی کننده

در این روش، ابتدا شبکه تعدیل می شود تا تعادل در ظرفیت کانال ها ایجاد شود و سپس پرداخت ها بر اساس مسیرهای جدید و بهینه شده مسیریابی می شوند. مانند حالت غیرمتمرکز، هزینه ها بر اساس ظرفیت کانال ها و مسیرهای جدید تنظیم می شوند و سپس تراکنش ها از طریق مسیرهای ارزان ترین انجام می گیرد. برای این حالت نیز، ۲۰۰,۰۰۰ تراکنش انجام شد و نتایج ثبت و تجزیه و تحلیل گردید.

۵-۲- مقایسه شبیه‌سازی‌های انجام شده

در این دو شبیه‌سازی، ما پنج نمودار مختلف داریم که شامل: توزیع موجودی گره‌ها، کارمزد تراکنش‌ها، تاریخچه تراکنش‌ها، اندازه مسیرها، و نمودار تعادل شبکه است. این نمودارها تفاوت‌های کلیدی بین دو الگوریتم مورد بررسی را به خوبی نشان می‌دهند.



شکل ۱۸: نمودار توزیع موجودی گره‌ها در دو شبیه‌سازی در کنار هم نقاط و خطوط قرمز برای شبیه‌سازی الگوریتم اکتشافی و نقاط و خطوط آبی برای الگوریتم اولیه می باشد.

نمودار توزیع موجودی گره‌ها پس از انجام تراکنش‌ها و جمع درآمد هر گره در هر دو حالت ترسیم شده است. (شکل ۱۸) این نمودارها نشان می‌دهند که در حالت استفاده از الگوریتم مرکزی کننده، موجودی گره‌ها به تعادل نزدیک‌تری می‌رسد و تعداد بیشتری از گره‌ها دارای موجودی نسبتاً متعادل هستند. این بدان معناست که در الگوریتم مرکزی کننده، درآمدهای گره‌های مرکزی کاهش یافته و به گره‌های غیرمرکزی افزوده شده است. در مقابل، در حالت الگوریتم اولیه، برخی گره‌ها دارای موجودی‌های بسیار بالا یا پایین هستند که این نشان‌دهنده عدم تعادل در شبکه است. این وضعیت به وضوح نمایانگر اختلاف قابل توجه بین الگوریتم‌های مورد استفاده است.

تحلیل کارمزد تراکنش‌ها نیز انجام شد که نمودار کارمزد تراکنش‌ها نشان می‌دهد که در حالت الگوریتم مرکزی کننده، هزینه‌ها به طور میانگین کمی بیشتر است. این امر به دلیل حذف برخی گره‌های مرکزی در برخی پرداخت‌ها برای تعادل‌سازی است. در حالت غیرمتمرکز، به دلیل عدم تعادل شبکه و وجود مسیرهای کوتاه از

طریق گره‌های مرکزی، هزینه‌ها پایین‌تر است. البته این افزایش هزینه دائمی نیست و فقط تا زمانی ادامه دارد که شبکه دارای گره‌های مرکزی قدرتمند است. با اجرای الگوریتم مرکزی به‌مرورزمان، نقش این گره‌ها کاهش یافته و هزینه تراکنش‌ها نیز کمتر می‌شود. علاوه بر این، توزیع قیمت کارمزدها در الگوریتم اولیه بسیار نامتقارن‌تر است، به‌طوری‌که برخی پرداخت‌ها بسیار کم‌هزینه و برخی بسیار پرهزینه هستند. اما پس از تعادل حاصل‌شده با الگوریتم دوم، پرداخت‌ها به‌صورت یکنواخت‌تری صورت می‌گیرند.

در نمودار تاریخچه تراکنش‌ها، اطلاعات مربوط به تراکنش‌های موفق و ناموفق و تراکنش‌های پرهزینه است. تحلیل این تاریخچه نشان می‌دهد که در حالت الگوریتم اولیه، تعداد بیشتری از تراکنش‌ها با موفقیت انجام می‌شوند و هزینه‌ها به‌طور میانگین کمتر است. در مقابل، در حالت الگوریتم مرکزی کننده به دلیل عدم تعادل در ظرفیت کانال‌ها، تعداد تراکنش‌های ناموفق بیشتر و هزینه‌ها بالاتر است. با این حال، این مشکل نیز مانند کارمزدها، پس از اجرای الگوریتم غیرمرکزی به‌تدریج کاهش یافته و پرداخت‌ها موفق‌تر از حالت اولیه می‌شود.

همچنین، اندازه مسیرهای طی‌شدن برای تراکنش‌ها در طول شبیه‌سازی اندازه‌گیری و تجسم شده است. نمودار اندازه مسیرها نشان می‌دهد که در حالت الگوریتم اولیه، مسیرهای انتخاب‌شده کوتاه‌تر و کارآمدتر هستند، درحالی‌که در حالت متمرکزکننده، مسیرهای انتخاب‌شده طولانی‌تر بوده و در برخی موارد مسیرهای غیربهبوده برای تراکنش‌ها انتخاب شده‌اند. با این حال، با متعادل شدن شبکه، شرایط بهبود یافته و از حالت اولیه بهتر خواهد شد.

نمودار تعادل شبکه نشان می‌دهد که در طول ۲۰۰,۰۰۰ تراکنش، تعدادی از کانال‌های موجود به‌طور کامل ناپایدار می‌شوند و روند این ناپایداری را مشخص می‌کند. در حالت الگوریتم اولیه، تعادل کانال‌ها پایدارتر است، اما الگوریتم مرکزی کننده به دلیل تنش‌هایی که به شبکه وارد می‌کند، باعث ناپایداری برخی کانال‌ها شده و این ناپایداری به افزایش هزینه تراکنش‌ها منجر می‌شود.

به‌طور کلی، نتایج شبیه‌سازی نشان می‌دهد که استفاده از یک رویکرد مرکزی برای تعادل بخشی شبکه قبل با استفاده مسیریابی تراکنش‌ها می‌تواند به‌طور قابل‌توجهی کارایی و تعادل شبکه کانال پرداخت را افزایش دهد. این روش در ابتدا منجر به افزایش هزینه تراکنش‌ها، کاهش موفقیت تراکنش‌ها و طولانی‌شدن مسیر پرداخت‌ها می‌شود، اما به‌مرورزمان، درآمد گره‌ها را متعادل می‌کند. همچنین، تمامی نکات منفی این الگوریتم توزیع‌کننده با متعادل شدن شبکه به‌تدریج از بین رفته و بهبود می‌یابد و به توزیع یکنواخت‌تری منجر خواهد شد. به عبارت دیگر،

بهای متعادل سازی شبکه در شرایط مرکزی، ایجاد نابهینگی کنترل شده در تراکنش ها است تا به عنوان نیروی محرکه ای برای گره ها عمل کرده و آن ها را به سمت تعادل شبکه سوق دهد.

در نتیجه، باگذشت زمان، این رویکرد منجر به بهبود عملکرد کلی شبکه و کاهش هزینه های تراکنش ها خواهد شد، اگرچه در آغاز ممکن است شبکه با چالش هایی مواجه شود. در نهایت، این شبیه سازی نشان می دهد که گرچه پیاده سازی اولیه این الگوریتم با مشکلاتی همراه است، ولی نتایج بلندمدت آن بهبودهای قابل توجهی را در ساختار و کارایی شبکه به همراه دارد.

۴-۶- حل عددی مسئله بهینه سازی

حل عددی مسائل بهینه سازی از جمله موضوعات حیاتی در علم بهینه سازی است که برای پیدا کردن بهینه ترین مقدار یک تابع هدف در مقابل یک مجموعه از قیدها به کار می رود. بهینه سازی محدب یکی از انواع مسائل بهینه سازی است که در آن تابع هدف و تمامی محدودیت ها به صورت محدب تعریف می شوند. برای حل مسائل بهینه سازی، از روش های تحلیلی و عددی استفاده می شود. روش های تحلیلی مانند روش لاگرانژ و روش های تکراری بر اساس تئوری های ریاضی و فیزیکی عمل می کنند و برای مسائل خاصی می توانند بهینه باشند. اما در مسائل پیچیده تر، معمولاً از روش های عددی استفاده می شود که شامل الگوریتم هایی مانند الگوریتم های گرادیان، الگوریتم های شبیه سازی و الگوریتم های بهینه سازی محدب می باشد.

یکی از ابزارهای محبوب برای حل بهینه سازی محدب، کتابخانه cvxpy در زبان برنامه نویسی پایتون است. cvxpy به کاربر امکان می دهد تا به سادگی مسائل خود را با استفاده از سینتکس ساده ای تعریف کرده و با استفاده از الگوریتم های مناسب، مسائل خود را حل کند. این کتابخانه دارای ابزارهای پیشرفته ای برای تجزیه و تحلیل نتایج و بهبود کارایی بهینه سازی است. زمان حل مسائل بهینه سازی می تواند بسته به پیچیدگی مسئله، تعداد متغیرها و محدودیت ها، و الگوریتم استفاده شده، متفاوت باشد. مسائل ساده تر ممکن است در زمان کمتری حل شوند، در حالی که مسائل پیچیده تر نیاز به زمان بیشتری دارند تا به یک حل بهینه برسند.

در این مطالعه، یک شبکه با ۱۴ گره و ظرفیت ۱۰۰۰، به منظور بررسی عملکرد الگوریتم های حل عددی بهینه سازی محدب مسئله است و مقایسه جواب واقعی حل مسئله با جواب الگوریتم اولیه ارائه شده و اصلاح شده. به دلیل پیچیدگی بالای مسئله و افزایش نمایی زمان حل با افزودن گره های بیشتر، تعداد گره ها به طور محدود در نظر

گرفته شده است. این الگوریتم بیش از 2^n قید دارد که برای n بزرگتر از ۱۵، حل مسئله برای ما با دشواری مواجه می‌شود.

برای این شبیه‌سازی، یک تراکنش به مبلغ ۲۰۰ واحد از گره ۵ به گره ۲ صورت می‌گیرد. هدف از بهینه‌سازی، یافتن ماتریس باینری X است که نشان می‌دهد کدام مسیر برای تراکنش‌ها انتخاب شده‌اند و چگونه جریان‌ها در شبکه توزیع می‌شوند. هدف آن مینیمم‌سازی مجموع مطلق ارزش‌های ماتریس باینری X است که مسیر تراکنش‌ها را از گره مبدأ به گره مقصد مشخص می‌کند. قیود در نظر گرفته شده تضمین می‌کنند که جریان تراکنش در شبکه به درستی توزیع شده و تعادل ظرفیت‌ها رعایت می‌شود. خروجی بهینه‌سازی به صورت یک ماتریس باینری است که نشان می‌دهد کدام مسیرها در شبکه برای انجام تراکنش انتخاب شده‌اند.

حال برای مقایسه حل مسئله بهینه‌سازی شبکه با جواب الگوریتم مسیریابی گفته شده، یک شبکه با ۱۰ گره و ۸۰۰ پرداخت را در نظر می‌گیریم که مقادیر و فرستنده گیرنده‌های آنها به صورت تصادفی انتخاب می‌شوند، مشابه به شبیه‌سازی‌های قبلی. نتایج نشان می‌دهد که هر ۸۰۰ پرداخت، جواب حاصل از الگوریتم مسیریابی اولیه با جواب به دست آمده از الگوریتم حل عددی بهینه‌سازی مسئله، هم‌خوانی دارد.

این تطابق نشان می‌دهد که عملکرد مسئله بهینه‌سازی گفته شده و الگوریتم مسیریابی یکی است و هر دو قادر به پیدا کردن بهینه‌ترین مسیر برای انتقال پرداخت‌ها در شبکه هستند.

۷-۴- مقایسه عملکرد مسئله بهینه‌سازی با قید ساده شده

باتوجه به اینکه مشاهده کردیم جواب مسئله اصلی با جواب الگوریتم مسیریابی هم‌خوانی دارد، قصد داریم الگوریتم مسیریابی را با جواب حل عددی مسئله بهینه‌سازی با قیده‌های ساده‌تر مقایسه کنیم. این تصمیم به جای مقایسه با حل عددی مسئله اصلی گرفته شد، زیرا حل عددی مسئله اصلی به دلیل دشواری محاسبات چالش‌برانگیز است. هدف از این مقایسه، بررسی تأثیر ساده‌سازی قیدها بر روی جواب کلی مسئله است. با ساده‌سازی قیدها، تعداد قیدها از دو به توان n به مرتبه n کاهش می‌یابد که این کار باعث می‌شود محاسبات بسیار سریع‌تر انجام شود. سپس خروجی این مقایسه را برای شبکه‌ای با ۲۰ گره و ۸۰۰ پرداخت که فرستنده و مقادیر پرداخت‌ها به صورت تصادفی انتخاب شده‌اند، ارائه می‌دهیم.

این تحلیل نشان می‌دهد که ساده‌سازی قیدها تأثیر چندانی بر روی جواب کلی مسئله ندارد، درحالی‌که محاسبات را به شکل قابل‌توجهی سریع‌تر می‌کند. بدین ترتیب، روش ساده‌سازی قیدها می‌تواند به‌عنوان یک راهکار کارآمد برای حل مسائل بهینه‌سازی پیچیده در شبکه‌ها مورد استفاده قرار گیرد.

۴-۸- شبیه‌سازی مسیریابی با دو تراکنش هم‌زمان

حال می‌رویم سراغ بهینه‌سازی دو تراکنش هم‌زمان تا تفاوت آن را با پرداخت تک‌تراکنش متوجه شویم. در این آزمایش، شبکه‌ای شامل ۲۰ گره مورد بررسی و شبیه‌سازی قرار گرفت. هدف این مطالعه ارزیابی تأثیر الگوریتم بهینه‌سازی دو تراکنش بر کاهش هزینه تراکنش‌ها و بهبود کارایی شبکه است. در این شبیه‌سازی، شبکه با ۲۰ گره به‌گونه‌ای مدل‌سازی شد که ۲۰ بار عملیات بهینه‌سازی با ورودی‌های مختلف اجرا شود. به این ترتیب، در هر شبیه‌سازی دو بار الگوریتم تک‌مسیره برای دو تراکنش انتخاب شده به‌صورت تصادفی اجرا می‌شود و یک‌بار مسیریابی دو تراکنش با همان پرداخت‌ها و سپس مقدار کارمزد این دو مسیر با یکدیگر مقایسه خواهد شد یعنی در مجموع ۴۰ پرداخت برای هر دو بهینه‌سازی بیان شده اجرا و مقایسه می‌شود.

از نتایج به‌دست‌آمده، مشخص شد که در ۱۵ مسیریابی از ۲۰ مسیریابی انجام شده، هزینه تراکنش مشابه باحالتی بود که تنها یک پرداخت صورت می‌گرفت. اما در ۵ مورد، مسیریابی دو پرداخت به‌صورت هم‌زمان به کاهش هزینه تراکنش‌ها منجر شد که نشان‌دهنده موفقیت این روش در برخی از سناریوها است. به‌عنوان مثال، دو پرداخت با مقادیر مشخص به‌صورت زیر انجام شد: پرداخت اول از گره ۴ به گره ۱۸ با مبلغ ۵۴.۲۰ و پرداخت دوم از گره ۳ به گره ۶ با مبلغ ۱۲۸.۹۵ صورت گرفت. نتایج نشان داد که بهینه‌سازی با انتقال پرداخت از یال [۳، ۴] [منجر به کاهش ۰.۱۵۵ از میزان هزینه پرداختی شد. در شبیه‌سازی، مسیرهای انتخاب شده برای پرداخت‌ها به‌صورت زیر بودند: مسیر الگوریتم تک‌تراکنش برای پرداخت از گره ۴ به گره ۱۸ شامل مسیر [۴، ۷]، [۷، ۱۶]، [۱۶، ۱۸] بود، درحالی‌که مسیر بهینه‌سازی دو تراکنش برای این پرداخت به‌صورت [۳، ۴]، [۴، ۳]، [۳، ۲]، [۲، ۱۰]، [۱۰، ۱۸] تعیین شد. مسیر تراکنش دوم هم برای هر دو مسیریاب‌ها برای پرداخت از گره ۳ به گره ۶ به شکل [۳، ۴]، [۴، ۶] به دست آمد که این نمونه خود نشان‌دهنده کارایی مسیریابی هم‌زمان دو تراکنش گفته شده است.

این نتایج نشان‌دهنده‌ی قابلیت‌های بهینه‌سازی دو تراکنش هم‌زمان در کاهش هزینه‌ها و بهبود کارایی شبکه است، هرچند که در تمام سناریوها موفقیت‌آمیز نبوده است اما پیشرفت قابل‌قبولی برای بهبود کارایی شبکه به حساب می‌آید.

۹-۴- شبیه‌سازی مسیریابی با ده تراکنش هم‌زمان

حال از الگوریتم پرداخت چندتراکنش استفاده می‌کنیم و ده تراکنش هم‌زمان را امتحان می‌کنیم تا ببینیم کارایی پرداخت چگونه است. برای بررسی این موضوع، شبیه‌سازی شبکه‌ای با ۲۰ گره انجام شد که در آن ۱۰ بار بهینه‌سازی با ورودی‌های مختلف انجام گرفت. هر شبیه‌سازی شامل ۱۰ پرداخت مختلف بود که به طور هم‌زمان مسیریابی شدند. نتایج نشان داد که در تمام ۱۰ مسیریابی، تفاوت هزینه‌ای در مقایسه با حالت تک‌تراکنش وجود داشت و این مسیریابی باعث شد مقدار کارمزد پرداختی کاهش یابد. همچنین، مسیرهایی که در حالت تک‌تراکنش به راحتی پرداخت نمی‌شدند، در حالت چندتراکنش با احتمال بیشتری انجام شدند.

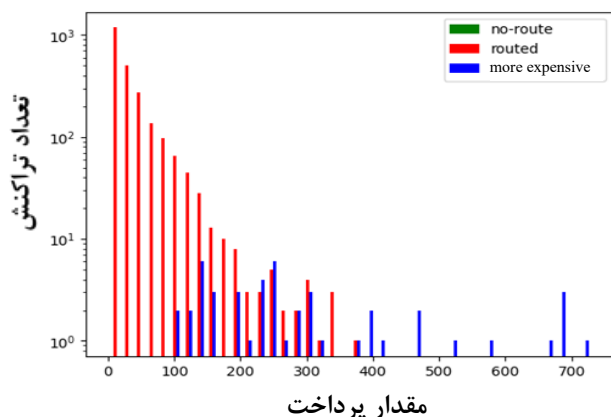
به عنوان نمونه، در یک شبیه‌سازی خاص، الگوریتم پرداخت چندتراکنش توانست با مسیریابی هم‌زمان ده تراکنش، پرداخت‌ها را با هزینه کمتری به سرانجام برساند. این بهینه‌سازی نه تنها باعث کاهش هزینه کل پرداخت‌ها شد بلکه امکان انجام تراکنش‌هایی را فراهم کرد که در حالت تک‌تراکنش قابل پرداخت نبودند. به ویژه، در یکی از موارد، پرداختی با مبلغ بالا که به صورت تکی انجام نمی‌شد، در حالت چندتراکنش با موفقیت انجام شد و هزینه کل پرداخت‌ها نیز کمتر از حالت تکی شد.

از این ده شبیه‌سازی به طور مثال در یکی از شبیه‌سازی‌های انجام شده پرداخت یکی مانده به آخر به دلیل مبلغ بالای ۷۷۸ به صورت تکی انجام نشده بود، اما با مسیریابی ده تایی به کمک هم انجام شد. حتی با اینکه حاصل کل هزینه‌های پرداختی باز هم کمتر از حالت تک‌تراکنش بود، این الگوریتم به بهبود کارایی شبکه و کاهش هزینه‌ها کمک کرد.

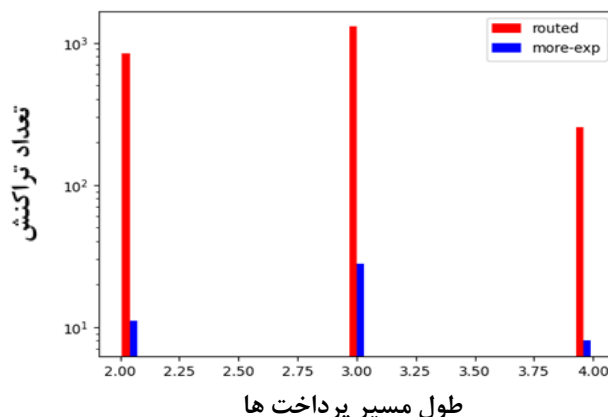
این نتایج نشان می‌دهند که استفاده از الگوریتم پرداخت چندتراکنش، بهبود قابل توجهی در مدیریت پرداخت‌ها و کاهش هزینه‌های فی پرداختی ایجاد می‌کند. الگوریتم چندتراکنش نه تنها باعث افزایش کارایی شبکه می‌شود بلکه پرداخت تراکنش‌های پیچیده‌تر را نیز با موفقیت بیشتری انجام می‌دهد. بنابراین استفاده از این روش در

مواردی که پرداخت‌های سنگین و پیچیده نیاز به مدیریت بهینه‌تری دارند، می‌تواند بسیار مفید باشد و هرچه تعداد این تراکنش‌های هم‌زمان بیشتر شود کارایی این مسیریابی هم‌زمان بیشتر خواهد شد.

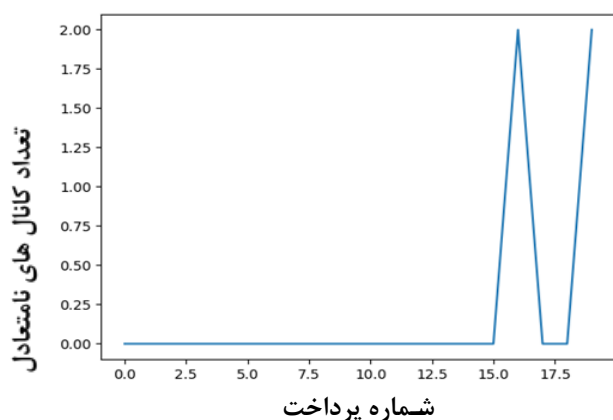
برای ارزیابی کارایی مسیریابی چندتراکنش، ۱۰۰ شبیه‌سازی با ۲۰ گره انجام شد. هر شبیه‌سازی شامل ۲۰ پرداخت هم‌زمان بود، و در مجموع ۲۰۰۰ پرداخت با مقادیر و فرستندگان و گیرندگان مختلف انجام شد. برای درک بهتر تأثیر این روش بر شبکه، چهار نمودار مختلف به‌عنوان خروجی ارائه شدند که هر یک جنبه‌ای از عملکرد شبکه را به تصویر می‌کشند.



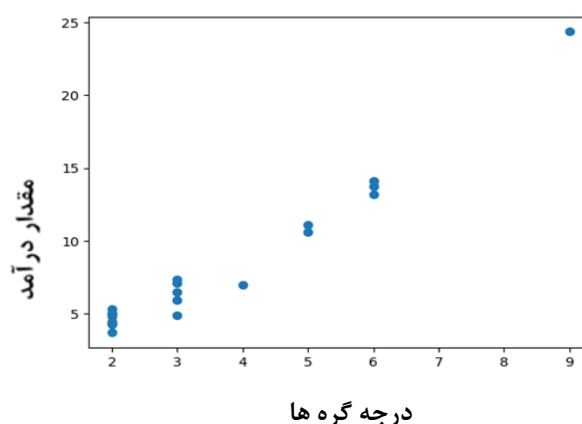
شکل ۲۰: تعداد و میزان پرداخت‌های موفق، نا موفق و گران



شکل ۱۹: اندازه و تعداد مسیرهای پرداخت‌های موفق و گران



شکل ۲۱: تغییرات تعادل شبکه برحسب تعداد شبیه‌سازی



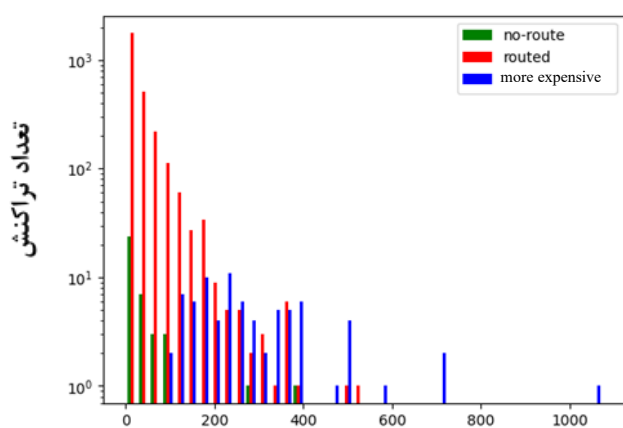
شکل ۲۲: درآمد گره بر حسب درجه، (هر نقطه یک گره است)

این تحلیل جامع از طریق بررسی نمودارهای توزیع موجودی گره‌ها، تاریخچه تراکنش‌ها و اندازه مسیرها و تعادل شبکه، به ما بینش عمیقی درباره عملکرد و کارایی روش مسیریابی چندتراکنش را ارائه می‌دهد. نتایج این بررسی‌ها

نشان می‌دهد که این روش نه تنها به بهبود توزیع منابع و کاهش کارمزدها کمک می‌کند، بلکه تعادل کلی شبکه را نیز بهبود می‌بخشد و بهره‌وری را در مدیریت پرداخت‌های پیچیده افزایش می‌دهد.

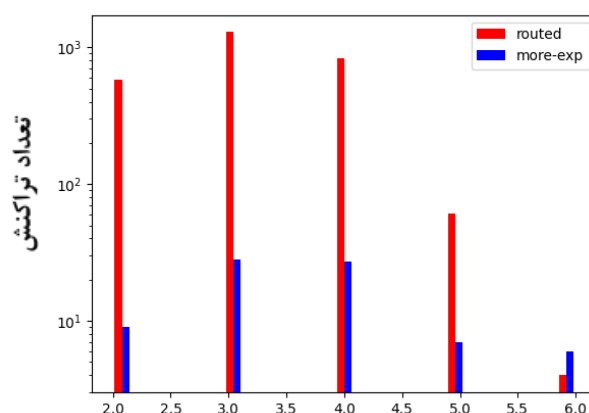
۱۰-۴- شبیه‌سازی پرداخت چندمسیره با قید مرکزی کننده

برای ارزیابی عملکرد بهینه‌سازی چندمسیره با قید توزیع‌کننده، ۱۰۰ شبیه‌سازی با ۲۰ گره انجام شد. هر شبیه‌سازی شامل ۲۰ پرداخت هم‌زمان بود و در مجموع ۲۰۰۰ پرداخت با مقادیر و فرستندگان و گیرندگان مختلف به اجرا درآمد. نمودارهای حاصل از این شبیه‌سازی‌ها تغییرات مهمی را در درآمد گره‌ها و عملکرد شبکه نشان می‌دهند.



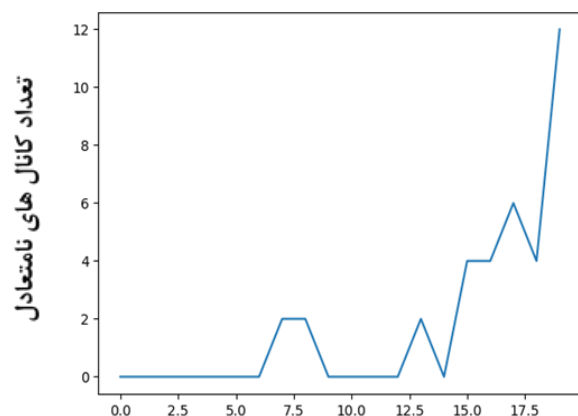
مقدار پرداخت

شکل ۲۴: تعداد و میزان پرداخت‌های موفق، ناموفق و گران برای شبیه‌سازی بهینه سازی ۲۰ پرداخته با قید توزیع شدگی



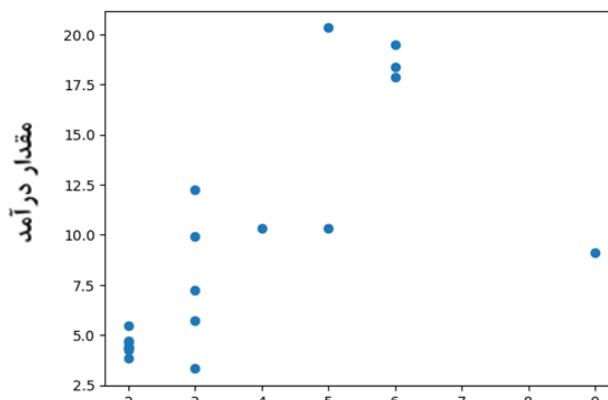
طول مسیر پرداخت‌ها

شکل ۲۳: اندازه و تعداد مسیرهای پرداخت‌های موفق و گران برای شبیه‌سازی بهینه سازی ۲۰ پرداخته با قید توزیع شدگی



شماره پرداخت

شکل ۲۵: تغییرات تعادل شبکه برحسب تعداد شبیه‌سازی گران برای شبیه‌سازی بهینه سازی ۲۰ پرداخته با قید توزیع شدگی

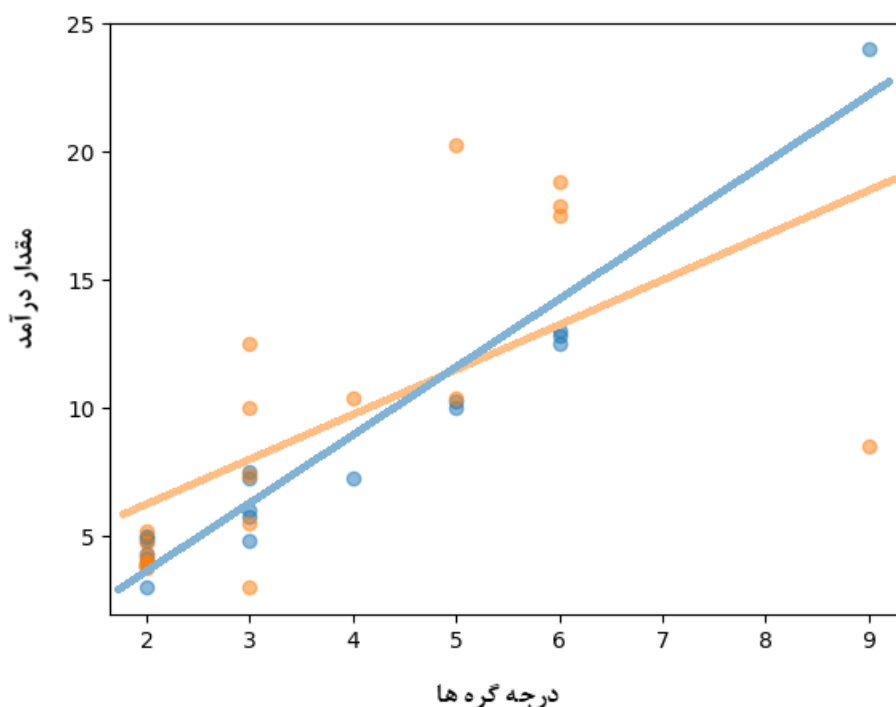


درجه گره‌ها

شکل ۲۶: درآمد گره بر حسب درجه (هر نقطه یک گره است) گران برای شبیه‌سازی بهینه سازی ۲۰ پرداخته با قید توزیع شدگی

با تحلیل نمودارها، مشاهده شد که در حالت استفاده از قید توزیع کننده، درآمد گره‌ها نسبت به حالت بدون قید بسیار یکنواخت‌تر و متعادل‌تر است. به این معنا که گره‌های با درجه بالا و پایین تقریباً درآمدهای مشابهی دارند. این در حالی است که در حالت بدون قید، گره‌های با درجه بالا درآمدهای بسیار بیشتری نسبت به گره‌های با درجه پایین دارند. این تفاوت‌ها نشان می‌دهد که استفاده از قید توزیع کننده منجر به تعادل بیشتر درآمدها و کاهش نابرابری‌ها در شبکه می‌شود، به طوری که پایداری شبکه به طور قابل توجهی افزایش می‌یابد.

همچنین، در نمودار تعداد پرداخت‌ها نیز بهبود قابل توجهی در حالت چندپرداخته مشاهده شد. در حالت بدون قید توزیع شده، هیچ پرداختی انجام نشده باقی نمی‌ماند و همه پرداخت‌ها به طور موفقیت‌آمیزی انجام می‌شوند. در حالت دارای قید توزیع شده نیز عملکرد بهتری نسبت به حالت الگوریتم‌های قبلی مشاهده شد. این بهبودها نشان می‌دهد که استفاده از روش چندپرداخته، به‌ویژه با اعمال قید توزیع کننده، نه تنها به توزیع یکنواخت‌تر منابع مالی کمک می‌کند بلکه تعداد بیشتری از پرداخت‌ها نیز به طور موفقیت‌آمیز انجام می‌شوند.



شکل ۲۷: نمودار درآمد گره‌ها در دو ارزیابی بهینه‌سازی در کنار هم که نقاط و خطوط نارنجی برای ارزیابی بهینه‌سازی با قید کاهش دهنده مرکزیت است و خطوط و نقاط آبی برای ارزیابی بهینه‌سازی بدون این قید است.

بر اساس نتایج این شبیه‌سازی‌ها، می‌توان نتیجه‌گیری کرد که روش بهینه‌سازی چندمسیره با قید توزیع کننده بهبودهای چشمگیری در توزیع درآمد گره‌ها و عملکرد کلی شبکه به همراه دارد. این روش می‌تواند به عنوان یک راه‌حل مؤثر برای مدیریت پرداخت‌های پیچیده و حفظ تعادل در شبکه‌های مالی به کار گرفته شود.

در پایان، ضریب جینی میانگین‌های درآمد هر درجه محاسبه و مقایسه می‌شود تا مشخص شود که توزیع ثروت در بین طبقات مختلف شبکه چقدر از حالت کاملاً عادلانه فاصله دارد. اگر این ضریب برابر با صفر باشد، به این معنی است که ثروت به طور کاملاً عادلانه بین درجات مختلف توزیع شده است؛ و اگر ضریب به یک نزدیک شود، نشان‌دهنده حداکثر نابرابری بین درجات است.

ابتدا میانگین درآمد هر درجه در شبکه محاسبه می‌شود و سپس ضریب جینی برای این میانگین‌ها به دست می‌آید. این ضریب جینی میانگین درآمد درجات در دو حالت، یکی با و دیگری بدون وجود توزیع‌کننده، و همچنین در الگوریتم اصلی با حضور توزیع‌کننده مقایسه می‌شود.

برای راه‌حل الگوریتم اصلی، ضریب جینی میانگین درآمد درجات برابر با ۰.۵۶۲ است، در حالی که در الگوریتم اکتشافی توزیع‌کننده این مقدار به ۰.۵۳۰ کاهش یافته است، که کاهش ۶ درصدی ضریب جینی و بهبود در توزیع ثروت را نشان می‌دهد.

در مورد راه‌حل بهینه‌سازی، ضریب جینی میانگین درآمدها برای بهینه‌سازی چندپرداخته بدون قید توزیع‌کننده برابر با ۰.۳۱۹ و در حالت با قید توزیع‌کننده برابر با ۰.۲۵۷ است که بیانگر بهبود ۲۰ درصدی ضریب جینی و کاهش نابرابری درآمدی میان درجات مختلف در شبکه است.

۵- نتیجه‌گیری

در این پایان‌نامه، ما به بررسی بهینه‌سازی مسیریابی در شبکه‌های کانال پرداخت با تأکید بر کاهش مرکزی‌سازی و افزایش بهره‌وری پرداختیم. ابتدا، مبانی نظری و ادبیات موجود در زمینه شبکه‌های کانال پرداخت را مرور کردیم. سپس به معرفی مدل‌های مختلف مسیریابی و بهینه‌سازی پرداختیم و در نهایت شبیه‌سازی‌هایی برای ارزیابی عملکرد مدل‌های پیشنهادی انجام دادیم.

۵-۲- روند کلی پایان‌نامه

مرور ادبیات: ابتدا مفاهیم پایه‌ای شبکه‌های کانال پرداخت و چالش‌های مرتبط با آن‌ها را بررسی کردیم. به‌ویژه تمرکز بر روی مشکلات مسیریابی و کاهش هزینه‌های تراکنش بود. همچنین مدل‌های موجود در ادبیات را معرفی کرده مقالات حوزه را به چهار دسته اصلی تقسیم کردیم، مقالات حوزه مسیریابی را مفصل بررسی کرده دسته‌بندی‌های مختلفی از آنها ارائه داده و نقاط قوت و ضعف آن‌ها را مورد بحث قرار دادیم. سپس مقالات تحلیلی حوزه را که به مشکل مرکزیت شبکه‌های کانال پرداخت توجه کرده بودند را به‌صورت مفصلی معرفی کردیم و در آخر هم تعدادی از مقالات که سعی بر حل مشکل مرکزی شدن شبکه را داشتند را شرح دادیم.

مدل‌سازی مسئله: مدل مسیریابی کوتاه‌ترین مسیر را از فرستنده به گیرنده ارائه دادیم. با تغییر بهینه‌سازی مدل ابتدا به مدل ساده‌ای رسیده از آن به مدل مسیریابی دوپرداخته رسیدیم و با استفاده از این مسیریابی، مسیریابی چندپرداخته خود را معرفی کردیم و سپس با اضافه کردن قیدی خاص به مدل مسیریابی کاهش‌دهنده مرکزیت شبکه دست پیدا کردیم. در این مدل‌ها، هدف اصلی کاهش هزینه‌های تراکنش و بهبود بهره‌وری شبکه بود. همچنین الگوریتم‌هایی برای پیدا کردن کوتاه‌ترین مسیر و کاهش مرکزی‌سازی شبکه پیشنهاد دادیم.

شبیه‌سازی و ارزیابی: شبیه‌سازی‌های متعددی برای ارزیابی عملکرد مدل‌های پیشنهادی انجام دادیم. این شبیه‌سازی‌ها شامل بررسی عملکرد مدل‌های مختلف در شرایط مختلف شبکه بود. از زبان برنامه‌نویسی پایتون و کتابخانه NetworkX برای پیاده‌سازی شبیه‌سازی‌ها استفاده کردیم. نتایج نشان داد که مدل‌های پیشنهادی توانسته‌اند بهبود قابل توجهی در کاهش هزینه‌های تراکنش و بهره‌وری شبکه ایجاد کنند.

۳-۵- نتایج به دست آمده

تغییرات اساسی در الگوریتم و مسئله بهینه‌سازی مسیریابی، به نتایج قابل توجهی در بهبود عملکرد، تعادل و کارایی شبکه‌های پرداخت منجر شده است. با معرفی بهینه‌سازی چندین تراکنش در یک مرحله، ما توانستیم به طور مؤثری از ویژگی‌های منحصربه‌فرد شبکه‌های کانال پرداخت استفاده کنیم. در این شبکه‌ها، عبور تراکنش‌ها از هر سمت، باعث افزایش ظرفیت طرف مقابل می‌شود، و این خاصیت می‌تواند در بهینه‌سازی مسیریابی نقش کلیدی ایفا کند.

بهینه‌سازی چندین تراکنش به صورت هم‌زمان: در مدل بهینه‌سازی جدید، چندین پرداخت به صورت هم‌زمان مسیریابی شدند. بهینه‌سازی این پرداخت‌ها به نحوی انجام گرفت که تراکنش‌ها با جهت‌های مختلف از یال‌های مشترک عبور کنند. این رویکرد، به سه مزیت عمده منجر شد ۱. **کاهش هزینه‌های پرداخت:** تراکنش‌ها به صورت بهینه و با هزینه‌های کمتری انجام شدند. این امر نه تنها کارایی اقتصادی شبکه را افزایش داد، بلکه از نظر عملیاتی نیز پرداخت‌ها با سرعت و دقت بیشتری پردازش شدند. ۲. **حفظ تعادل شبکه:** با عبور تراکنش‌ها از مسیرهای مختلف و استفاده بهینه از ظرفیت‌های موجود، تغییرات در تعادل شبکه به حداقل رسید. این به معنای پایداری بیشتر و کاهش نوسانات ظرفیت در نقاط مختلف شبکه است. ۳. **پرداخت تراکنش‌های بزرگ:** تراکنش‌های بزرگ که به ظرفیت‌های بیشتری نیاز دارند، با استفاده از بهینه‌سازی چندمسیره قابل پرداخت شدند. بدون این رویکرد، انجام این تراکنش‌ها با محدودیت‌های جدی مواجه بود و اغلب امکان پذیر نبود.

اضافه کردن قید توزیع‌کننده به شبکه: اضافه کردن قید توزیع‌کننده به شبکه، گامی در جهت بهبود توزیع‌شدگی شبکه بود. این قید، گره‌ها را وادار به تغییر رویه و حرکت به سوی توزیع‌پذیری بیشتر در جهت منافع خود کرد. به طور خاص، گره‌هایی که در شبکه درجه کمتری داشتند، توانستند سوددهی بیشتری کسب کنند. این امر، گره‌ها را تشویق کرد تا با کاهش درجه خود، به توزیع‌پذیری بهتر شبکه کمک کنند.

باوجود بهبود کارایی و توزیع پذیری شبکه، اعمال قید توزیع کننده، به طور موقت باعث تشدید مشکلاتی در ساختار شبکه شد. اما این وضعیت، یک هزینه قابل قبول برای غیرمرکزی کردن شبکه محسوب می شود و همین طور به نظر می رسد که این مشکلات، به مرور زمان و با تغییر تدریجی توپولوژی شبکه بهبود پیدا خواهند کرد. به عبارت دیگر، شبکه در طولانی مدت به سمت یک ساختار بهینه تر و متعادل تر حرکت خواهد کرد.

در نهایت، بهینه سازی چندین تراکنش هم زمان و اعمال قید توزیع کننده، دو استراتژی کلیدی بودند که به بهبود چشمگیر کارایی، تعادل و پایداری شبکه منجر شدند. این تغییرات، نه تنها پرداخت ها را اقتصادی تر کردند، بلکه شرایط را برای انجام تراکنش های بزرگ تر و پیچیده تر نیز فراهم آوردند. با توجه به نتایج مثبت به دست آمده، می توان پیش بینی کرد که استفاده از این روش ها در آینده می تواند به تحولاتی گسترده در نحوه مدیریت و بهره برداری از شبکه های پرداخت منجر شود.

رویکرد جدید ما در بهینه سازی چندمسیره و استفاده از قید توزیع کننده، کارایی شبکه های پرداخت را به طور قابل توجهی افزایش داده است. این روش ها نشان دادند که با استفاده هوشمندانه از ظرفیت ها و تغییر توپولوژی شبکه، می توان به بهبودهای قابل توجهی در عملکرد و تعادل شبکه دست یافت. با توجه به نتایج حاصل شده، می توان نتیجه گرفت که مدل های بهینه سازی پیشنهادی می توانند به عنوان یک راه حل مؤثر برای بهبود عملکرد شبکه های کانال پرداخت در دنیای واقعی مورد استفاده قرار گیرند. همچنین این مدل ها می توانند به عنوان پایه ای برای تحقیقات آینده در زمینه بهینه سازی شبکه های کانال پرداخت و کاهش هزینه های تراکنش مورد استفاده قرار گیرند.

در آخر هم فهرستی از کار هایی که در آینده بایستی انجام شود که نتایج این کار به ثمر بنشیند به این شرح است:

- تغییر مسیریابی مرکزی به مسیریابی توزیع شده با مکانیزم اجماع
 - استفاده از شبکه های واقعی لایتینگ در شبیه سازی به جای تولید شبکه
 - ارزیابی نظریه بازی برای بررسی نحوه پیوستن به شبکه با وجود قید مرکزیت
 - مقایسه تحلیلی نحوه پیوستن شبکه با راه حل ارائه شده در مقابل راه حل های قبلی گفته شده
 - پیدا کردن بهترین قید مرکزی سازی در دو راه حل گفته شده و استفاده از یادگیری تقویتی
- برای بهبود لحظه ای این قید

- [١] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, “Bitcoin and cryptocurrency technologies”, Princeton University Press, 2016 .
- [٢] O. Lopez و E. Livni, “In Global First, El Salvador Adopts Bitcoin as Currency ”,*The New York Times* ,p. Retrieved 30 September , 2021 .
- [٣] M. E. Peck, “Blockchains: How they work and why they'll change the world ”,*IEEE spectrum*., 26--35, 2017 .
- [٤] J. A. Kroll, I. C. Davey و E. W. Felten, “The economics of Bitcoin mining, or Bitcoin in the presence of adversaries ”,*Proceedings of WEIS* ,2013.
- [٥] S. Nakamoto و A. Bitcoin, “A peer-to-peer electronic cash system ”,*Bitcoin*--URL: <https://bitcoin.org/bitcoin.pdf> ,p. 15, 2008 .
- [٦] R. Bohme, N. Christin, B. Edelman و T. Moore, “Bitcoin: Economics, technology, and governance ”,*Journal of economic Perspectives* ,pp. 213--238, 2015 .
- [٧] E. J. Hartelius, ““The great chain of being sure about things”: blockchain, truth, and a trustless network ”,*Review of Communication* ,pp. 21--37, 2023 .

- [٨] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*, O'Reilly Media, Inc., 2014 .
- [٩] A. Gervais, G. O. Karame, V. Capkun و S. Capkun, "Is bitcoin a decentralized currency ", *IEEE security & privacy* ,pp. 54--60, 2014 .
- [١٠] A. Wilhelm, "Popular Bitcoin Mining Pool Promises To Restrict Its Compute Power To Prevent Feared 51 Fiasco ",*TechCrunch.(July 16 2014).[online]* ,p. ., 2014 .
- [١١] F. Mogavero, I. Visconti, A. Vitaletti و M. Zecchini, "The blockchain quadrilemma: When also computational effectiveness matters ",*IEEE Symposium on Computers and Communications (ISCC)* ,pp. 1--6, 2021 .
- [١٢] Q. Zhou, H. Huang, Z. Zheng و J. Bian, "Solutions to scalability of blockchain: A survey ", *Ieee Access* ,pp. 16440--16455, 2020 .
- [١٣] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin و B. C. Ooi, "Towards scaling blockchain systems via sharding ",*Proceedings of the 2019 international conference on management of data* ,pp. 123--140, 2019 .
- [١٤] Y. Sompolinsky و A. Zohar, "Secure high-rate transaction processing in bitcoin د ", *Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers 19* ,2015 ,pp. 507--527.
- [١٥] V. Bagaria, S. Kannan, D. Tse, G. Fanti و P. Viswanath, "Prism: Deconstructing the blockchain to approach physical limits ",*Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* ,2019 ,pp. 585--602.
- [١٦] A. Gangwal, H. R. Gangavalli و A. Thirupathi, "A survey of Layer-two blockchain protocols ",*Journal of Network and Computer Applications* ,p. 103539, 2023 .

- [١٧] J. Poon و T. Dryja, “The bitcoin lightning network: Scalable off-chain instant payments– ”, p. ., 2016 .
- [١٨] H. Khojasteh و H. Tabatabaei, “A survey and taxonomy of blockchain-based payment channel networks ”,*IEEE High Performance Extreme Computing Conference (HPEC)* ,pp. -, 2021 .
- [١٩] D. Goldschlag, M. Reed و P. Syverson, “Onion routing ”,*Communications of the ACM* 42.2 , pp. 39-41, 1999 .
- [٢٠] P. Prihodko, S. Zhigulin, M. Sahno, A. Ostrovskiy و O. Osuntokun, “Flare: An approach to routing in lightning network ”,*White Paper*, 2016 .
- [٢١] G. Malavolta, M. S. Pedro, A. Kate و M. Maffei, “Silentwhispers: Enforcing security and privacy in decentralized credit networks ”,*Cryptology ePrint Archive* , 2016 .
- [٢٢] S. Roos, M. Beck و T. Strufe, “Voute-virtual overlays using tree embeddings ”,*arXiv preprint arXiv:1601.06119*, 2016 .
- [٢٣] S. Roos, P. Moreno Sanchez, A. Kate و I. Goldberg, “Settling payments fast and private: Efficient decentralized routing for path-based transactions ”,*arXiv preprint arXiv:1709.05748* , 2017 .
- [٢٤] V. Sivaraman, S. Bojja Venkatakrishnan, M. Alizadeh, G. Fanti و P. Viswanath, “Routing cryptocurrency with the spider network ”,*In Proceedings of the 17th ACM Workshop on Hot Topics in Networks* ,pp. 29-35, 2018 .
- [٢٥] P. Wang, H. Xu, X. Jin و T. Wang, “Flash: efficient dynamic routing for offchain networks ”, *In Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies* ,pp. 370-381, 2019 .

- [٢٤] R. Yu, G. Xue, V. T. Kilar, D. Yang و J. Tang, “CoinExpress: A fast payment routing mechanism in blockchain-based payment channel networks ”,*In 2018 27th international conference on computer communication and networks (ICCCN)* ,pp. 1-9, 2018 .
- [٢٥] R. Khalil و A. Gervais, “Revive: Rebalancing off-blockchain payment networks ”,*In Proceedings of the 2017 acm sigsac conference on computer and communications security* , pp. 439-453, 2017 .
- [٢٦] F. Engelmann, H. Kopp, F. Kargl, F. Glaser و C. Weinhardt, “Towards an economic analysis of routing in payment channel networks ”,*Proceedings of the 1st workshop on scalable and resilient infrastructures for distributed ledgers*, 2017 .
- [٢٧] V. Sivaraman, “High-efficiency cryptocurrency routing in payment channel networks ”,*PhD diss., Massachusetts Institute of Technology*, 2019 .
- [٢٨] Y. Sali و A. Zohar, “Optimizing off-chain payment networks in cryptocurrencies ”,*arXiv preprint arXiv:2007.09410*, 2020 .
- [٢٩] S. M. Varma و S. Theja Maguluri, “Throughput optimal routing in blockchain-based payment systems ”,*IEEE Transactions on Control of Network Systems* 8.4 ,pp. 1859-1868, 2021 .
- [٣٠] L. Yang, X. Dong, S. Gao, Q. Qu, X. Zhang, W. Tian و Y. Shen, “Optimal Hub Placement and Deadlock-Free Routing for Payment Channel Network Scalability ”,*arXiv preprint arXiv:2305.19182*, 2023 .
- [٣١] M. A. Fazli, S. M. Nehzat و M. A. Salarkia, “Building Stable Off-chain Payment Networks ”,*arXiv preprint arXiv:2107.03367*, 2021 .

- [٣٤] X. Luo و P. Li, “LEAF: Let’s Efficiently Make Adaptive Forwarding in Payment Channel Networks ”,*IEEE Access 11* ,pp. 4194-4206, 2023 .
- [٣٥] X. Luo, “Intelligent Scheduling for Off-Chain Transactions in Payment Channel Networks ”, *PhD diss., The University of Aizu*, 2022 .
- [٣٦] E. Rohrer, J. F. Laß و F. Tschorsch, “Towards a concurrent and distributed route selection for payment channel networks ”,*In Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops* ,pp. 411-419, 2017 .
- [٣٧] P. Zabka, K.-T. Foerster, C. Decker و S. Schmid, “Short paper: A centrality analysis of the lightning network ”,*arXiv preprint arXiv:2201.07746* , 2022 .
- [٣٨] P. Zabka, K. T. Förster, C. Decker و S. Schmid, “A centrality analysis of the Lightning Network ”,*Telecommunications Policy 48.2* ,p. 102696, 2024 .
- [٣٩] L. Atmanavicius, T. Vanagas و S. Masteika, “Method for Determining the Level of Centralization in BTC Lightning Nodes: A Centrality Analysis of the Lightning Network ”, *Vilnius University Open Series* ,pp. 6--14, 2024 .
- [٤٠] A. Lisi, D. D. F. Maesa, P. Mori و L. Ricci, “Lightnings over rose bouquets: An analysis of the topology of the Bitcoin Lightning Network ”,*2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)* ,2021 ,pp. 324--331.
- [٤١] L. E. Oleas-Chavez, C. erez-Sola و J. Herrera-Joancomarti, “Apples and Oranges: On How to Measure Node Centrality in Payment Channel Networks ”,*IEEE Access* ,pp. 55469--55487, 2022 .

- [٤٢] J.-H. Lin, K. Primicerio, T. Squartini, C. Decker و C. J. Tessone, “Lightning network: a second path towards centralisation of the bitcoin economy ”,*New Journal of Physics*,p. 083022, 2020 .
- [٤٣] G. F. Camilo, G. A. F. Rebello, L. A. C. de Souza, M. Potop-Butucaru, M. D. Amorim, M. E. M. Campista و L. H. M. Costa, “Topological evolution analysis of payment channels in the lightning network ”,*2022 IEEE Latin-American Conference on Communications (LATINCOM)* ,2022 ,pp. 1--6.
- [٤٤] Z. Avarikioti, L. Heimbach, Y. Wang و R. Wattenhofer, “Ride the lightning: The game theory of payment channels و ”,*Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10--14, 2020 Revised Selected Papers 24* ,2020 ,pp. 264--283.
- [٤٥] O. Ersoy, S. Roos و Z. Erkin, “How to profit from payments channels ”,*International Conference on Financial Cryptography and Data Security* ,pp. 284--303, 2020 .
- [٤٦] V. Davis و B. Harrison, “Learning a scalable algorithm for improving betweenness in the lightning network ”,*2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)* ,2022.
- [٤٧] K. Lange, E. Rohrer و F. Tschorsch, “On the impact of attachment strategies for payment channel networks ”,*2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* ,2021 ,pp. 1--9.
- [٤٨] M. S. Mahdizadeh, B. Bahrak و M. Sayad Haghighi, “Decentralizing the lightning network: a score-based recommendation strategy for the autopilot system ”,*Applied Network Science* , p. 73, 2023 .

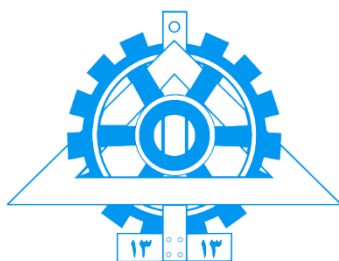
- [٤٩] G. F. Camilo, G. A. F. Rebello, L. A. C. de Souza, M. E. M. Campista و L. H. M. Costa, "ProfitPilot: Enabling Rebalancing in Payment Channel Networks Through Profitable Cycle Creation ",*IEEE Transactions on Network and Service Management*, 2024 .
- [٥٠] C. Grunspan, G. Lehericy و R. Perez-Marco, "Ant routing scalability for the lightning network ",*arXiv preprint arXiv:2002.01374*, 2020 .
- [٥١] T. Nikolov, "coinatmradar.com," 4 December 2019 ..Available: <https://coinatmradar.com/blog/the-promise-of-lightning-network-atms/>
- [٥٢] N. Papadis و L. Tassiulas, "Blockchain-based payment channel networks: Challenges and recent advances ",*IEEE Access* ,pp. 227596--227609, 2020 .
- [٥٣] N. Bhatia, "The Time Value of Bitcoin and LNRR," ., 18 Apr 2019 ..Available: <https://timevalueofbtc.medium.com/the-time-value-of-bitcoin-and-lnrr-e0c435931bd8>.

Abstract

This research begins by introducing the fundamental concepts and structure of blockchain networks and payment systems, with a focus on the Lightning Network. It then identifies and analyzes the existing problems and challenges within payment networks, particularly those related to centralization in the Lightning Network. To address these issues, a new exploratory routing algorithm is proposed, aimed at improving efficiency and reducing network centralization by altering the traditional routing algorithm. Further, by simplifying and modifying the structure of the conventional optimization problem, a new payment route optimization problem is formulated for multiple transactions with different sender-receiver pairs occurring simultaneously. The impact of this simultaneous multi-transaction routing approach is examined, demonstrating that it enhances the network's overall performance across various areas. This modification helps in gradually decentralizing the network over time by introducing constraints that prevent centralization.

Simulations were conducted to evaluate the performance of the proposed algorithms and optimizations. The results indicate that the implementation of these proposed optimization algorithms leads to reduced transaction costs, increased balance, and decreased inequalities within the network. Particularly, the use of distribution constraints drives central nodes towards a reduced degree and increased network decentralization, ultimately reducing centralization and improving the network's overall efficiency. These advancements can contribute to the further development and adoption of blockchain payment networks, addressing the growing needs of users.

Keywords: cryptocurrency, Bitcoin, blockchain, PCN (Payment Channel Network), network decentralization, LN (Lightning Network), routing, multi-payment optimization



University of Tehran
College of Engineering
School of Electrical and
Computer Engineering



Investigating and improving the performance of payment channel networks in the blockchain

A thesis submitted to the Graduate Studies Office

In partial fulfillment of the requirements for

The degree of Master in

Network communication

By:

Hamid reza Kashani

Supervisor:

Dr. Pooya Shariatpanahi