

کاهش هزینه و افزایش سرعت در بازی‌های زنجیره بلوکی: ارائه یک رویکرد مبتنی بر کانال پرداخت

امیرعلی احمد دوست

دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران
ahmaddoust.amirali@gmail.com

مهرداد آشتیانی*

دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران
m_ashtiani@iust.ac.ir

چکیده

می‌دهد. این دستاوردها اثربخشی کانال‌های پرداخت را به‌عنوان راهکاری عملی برای بهبود عملکرد و کاهش هزینه‌ها در بازی‌های زنجیره بلوکی تأیید می‌کند. **کلید واژه‌ها:** کانال‌های پرداخت، زنجیره بلوکی، کاهش هزینه تراکنش، بهینه‌سازی سرعت، بازی‌های زنجیره بلوکی.

۱- مقدمه

فناوری زنجیره بلوکی با ارائه مفاهیمی نوین مانند مالکیت واقعی دارایی‌های دیجیتال و اقتصاد غیرمتمرکز، صنعت بازی‌های رایانه‌ای را متحول کرده است [۱]. بازی‌های مبتنی بر این فناوری، به سرعت در حال جلب توجه کاربران و توسعه‌دهندگان هستند. با این حال، این رشد با یک چالش اساسی همراه است: محدودیت‌های مقیاس‌پذیری. ثبت هر تراکنش درون بازی بر روی زنجیره اصلی، منجر به افزایش هزینه‌های کارمزد (گس)^۱ و

رشد روزافزون بازی‌های مبتنی بر زنجیره بلوکی با چالش‌های مقیاس‌پذیری نظیر هزینه بالای کارمزد (گس) و سرعت پایین پردازش تراکنش‌ها مواجه است. این عوامل تجربه کاربری را مختل کرده و پذیرش گسترده این بازی‌ها را محدود می‌سازند. این پژوهش، یک مدل بهینه مبتنی بر کانال‌های پرداخت به‌عنوان یک راهکار لایه دوم برای مدیریت تراکنش‌ها در بازی‌های دیجیتال ارائه می‌دهد. در این مدل، تراکنش‌ها بین بازیکن و سرویس‌دهنده به‌صورت خارج از زنجیره انجام شده و تنها وضعیت نهایی بر روی زنجیره اصلی ثبت می‌گردد. معماری سامانه پیشنهادی شامل سرویس‌های مدیریت کانال، حل خودکار اختلافات و مدیریت وثیقه برای تضمین امنیت و کارایی است. نتایج حاصل از شبیه‌سازی در شبکه‌های اتریوم و پالیگان نشان می‌دهد که این مدل، زمان تراکنش را به طور میانگین به ۱/۲ ثانیه و هزینه کارمزد گس را بیش از ۵۰ درصد کاهش

1-Gas Fee

* نویسنده مسئول

بخش ۳ معرفی شده و ارزیابی عملکرد آن در بخش ۴ انجام می‌شود. در نهایت، بخش ۵ به نتیجه‌گیری و پیشنهاد کارهای آتی اختصاص دارد.

۲- مفاهیم پایه

به منظور درک جامع از مفاهیم کلیدی، در این بخش فناوری زنجیره بلوکی و کانال‌های پرداخت معرفی می‌شوند.

۲-۱- فناوری زنجیره بلوکی

زنجیره بلوکی یک فناوری دفتر کل توزیع شده است که امکان ثبت تراکنش‌ها را به صورت امن، شفاف و تغییرناپذیر فراهم می‌کند [۴]. این فناوری همان‌طور که در شکل ۱ آورده شده است، از زنجیره‌ای از بلوک‌ها تشکیل شده است که هر بلوک با استفاده از سازوکارهای رمزنگاری به بلوک قبلی خود متصل می‌شود. این ساختار، امنیت و یکپارچگی داده‌ها را تضمین می‌کند. با این وجود، شبکه‌های عمومی زنجیره بلوکی مانند اتریوم، به دلیل محدودیت در ظرفیت پردازش بلوک‌ها، با چالش جدی مقیاس‌پذیری مواجه هستند. این محدودیت باعث می‌شود توان پردازشی شبکه به چند تراکنش در ثانیه محدود شود که برای کاربردهای با حجم تراکنش بالا مانند بازی‌های دیجیتال، ناکافی است و به افزایش هزینه و تأخیر منجر می‌شود [۲].

۲-۲- کانال‌های پرداخت

برای غلبه بر مشکل مقیاس‌پذیری، راهکارهای لایه دوم طراحی شده‌اند که پردازش تراکنش‌ها را به خارج از زنجیره اصلی منتقل می‌کنند. کانال‌های پرداخت یکی از مؤثرترین این راهکارها هستند. یک کانال پرداخت، یک قرارداد هوشمند دوطرفه بین دو کاربر است که با قفل کردن مقداری سرمایه اولیه ایجاد می‌شود. پس از ایجاد کانال، طرفین می‌توانند تعداد نامحدودی تراکنش را

تأخیرهای طولانی در پردازش می‌شود. این موانع، تجربه کاربری را خدشه‌دار کرده و مانعی جدی برای پذیرش گسترده این نسل از بازی‌ها به‌شمار می‌روند [۲]. انگیزه اصلی این پژوهش، ناشی از ضعف ذاتی معماری سنتی زنجیره بلوکی در مدیریت حجم بالای تراکنش‌های خرد و مکرر است که مشخصه اصلی بازی‌های دیجیتال محسوب می‌شود. راهکارهای متداول که بر ثبت مستقیم تمام عملیات بر روی زنجیره تکیه دارند، فاقد چابکی و کارایی لازم برای یک محیط پویا و تعاملی هستند. این ناکارآمدی نه تنها هزینه‌های عملیاتی را برای بازیکنان افزایش می‌دهد، بلکه با کاهش سرعت پاسخ‌دهی، کیفیت سرویس و جذابیت بازی را نیز به شدت تحت تأثیر قرار می‌دهد.

برای غلبه بر این چالش‌ها، پژوهش حاضر یک مدل بهینه مبتنی بر کانال‌های پرداخت را به عنوان یک راهکار لایه دوم معرفی می‌کند. این رویکرد، بُن‌انگاره^۲ پردازش تراکنش‌ها را از حالت درون زنجیره‌ای^۳ به خارج از زنجیره^۴ منتقل می‌کند. در این مدل، بازیکنان و سرویس‌دهنده یک کانال امن و خصوصی ایجاد کرده و تعداد نامحدودی تراکنش را به صورت آنی و با هزینه نزدیک به صفر انجام می‌دهند. تنها وضعیت نهایی و تجمیع‌شده تراکنش‌ها بر روی زنجیره اصلی ثبت می‌شود که این امر به کاهش چشمگیر بار شبکه و هزینه‌ها می‌انجامد [۳]. نوآوری این مقاله در طراحی یک معماری جامع و سرویس‌گرا است که فراتر از پیاده‌سازی یک کانال پرداخت ساده عمل می‌کند. سامانه پیشنهادی با ترکیب سازوکارهایی مانند حل خودکار اختلافات و مدیریت هوشمند وثیقه، امنیت و اعتماد را در محیط خارج از زنجیره تضمین می‌کند. هدف اصلی، ارائه یک چارچوب عملی است که نه تنها سرعت و هزینه را بهینه کند، بلکه زیرساختی قابل اعتماد برای نسل بعدی بازی‌های زنجیره بلوکی فراهم می‌آورد. ساختار ادامه مقاله به این شرح است: در بخش ۲، کارهای مرتبط پیشین مورد بررسی قرار می‌گیرد. رویکرد پیشنهادی در

2-Paradigm

3-On-chain

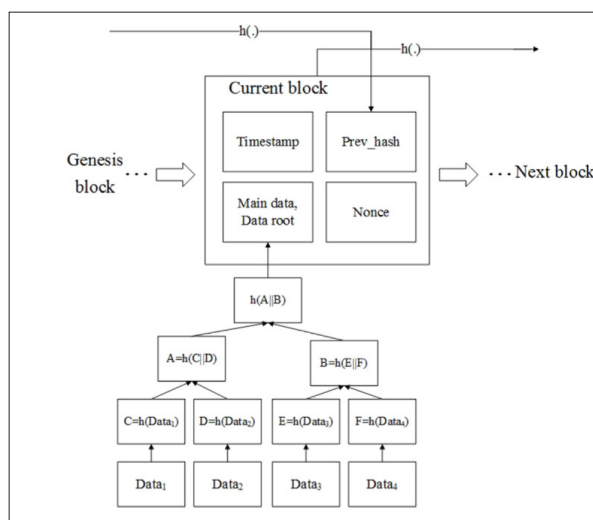
4-Off-chain

سهام^۸، به دنبال کاهش زمان تولید بلوک و افزایش سرعت تراکنش‌ها بوده‌اند [۶]. رویکرد دیگر، استفاده از شار دینگ^۹ است که در آن شبکه به بخش‌های کوچک‌تر (شارد) تقسیم می‌شود تا تراکنش‌ها به صورت موازی پردازش شوند [۷]. اگرچه این روش‌ها سرعت را تا حدی بهبود می‌بخشند، اما اغلب با افزایش پیچیدگی شبکه همراه هستند و همچنان برای مدیریت حجم بسیار بالای تراکنش‌های خرد در بازی‌های دیجیتال، محدودیت دارند.

۳-۲- بهینه‌سازی در شبکه‌های کانال پرداخت

راهکارهای لایه دوم، با انتقال بار پردازشی به خارج از زنجیره، راه حلی مؤثرتر برای مقیاس‌پذیری ارائه می‌دهند. پژوهش‌های اخیر در این حوزه بر جنبه‌های مختلفی تمرکز کرده‌اند. برخی از آنها به بهینه‌سازی شبکه‌های کانال پرداخت پرداخته‌اند. برای مثال، [۲] به مدل‌سازی نظریه بازی‌ها برای یافتن راهبرد بهینه جهت اتصال کاربران جدید به یک شبکه پرداخت موجود می‌پردازد و [۸] الگوریتم‌های مسیریابی آگاه از تراز مالی کانال‌ها را برای افزایش نرخ موفقیت تراکنش‌ها در شبکه‌های پیچیده پیشنهاد می‌دهد. گروه دیگری از پژوهش‌ها، ابزارهایی برای کاهش هزینه‌ها در لایه دوم ارائه داده‌اند؛ به عنوان نمونه، [۹] با استفاده از یادگیری ماشین، یک مدل برای پیش‌بینی قیمت گس ارائه می‌دهد تا کاربران بتوانند تراکنش‌های خود را در زمان‌های کم‌هزینه‌تر انجام دهند. با وجود پیشرفت‌های صورت گرفته، اکثر این پژوهش‌ها بر روی شبکه‌های پرداخت عمومی و چند-گره‌ای (مانند شبکه لایتینگ) متمرکز هستند. در مقابل، معماری رایج در بازی‌های برخط، یک ساختار ستاره‌ای است که در آن تمام بازیکنان به صورت مستقیم با یک سرویس‌دهنده مرکزی در ارتباط هستند. شکاف تحقیقاتی موجود، کمبود یک مدل جامع و بهینه برای این معماری خاص است که علاوه بر سرعت و هزینه، مکانیزم‌های کاربردی مانند حل اختلاف و

به صورت آنی و مستقیم با یکدیگر انجام دهند، بدون آن که نیازی به ثبت هر تراکنش بر روی زنجیره اصلی باشد. در نهایت، با بستن کانال، تنها وضعیت نهایی تراز مالی طرفین به عنوان یک تراکنش واحد بر روی زنجیره ثبت می‌شود. این سازوکار به طور چشمگیری تعداد تراکنش‌های روی زنجیره را کاهش داده و باعث بهبود سرعت و کاهش هزینه‌ها می‌شود [۳].



شکل ۱: ساختار زنجیره بلوکی [۵].

۳- پژوهش‌های مرتبط

در این بخش، مطالعات مرتبط با بهبود عملکرد شبکه‌های زنجیره بلوکی بررسی می‌شود. ابتدا راهکارهای لایه اول که بر بهینه‌سازی خود زنجیره تمرکز دارند معرفی شده و سپس، پژوهش‌های مرتبط با راهکارهای لایه دوم، به ویژه کانال‌های پرداخت، مورد تحلیل قرار می‌گیرند.

۳-۱- راهکارهای لایه اول برای بهبود مقیاس‌پذیری

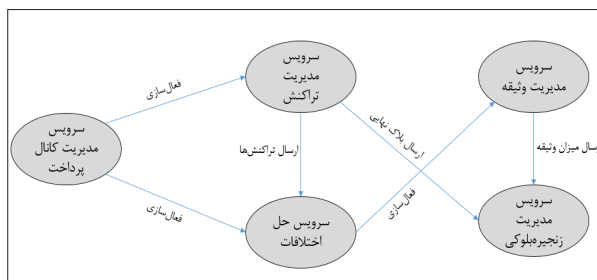
راهکارهای لایه اول^۶ تلاش می‌کنند تا با تغییر در ساختار اصلی زنجیره بلوکی، توان پردازشی آن را افزایش دهند. پژوهش‌های متعددی در این زمینه انجام شده است. برای مثال، برخی با تغییر الگوریتم اجماع از اثبات کار^۷ به اثبات

8-Proof- of- Stake (PoS)
9-Sharding

6- Layer-1
7- Proof- of- Work (PoW)

۴-۱- معماری سامانه و طراحی

سیستم پیشنهادی بر پایه یک معماری سرویس‌گرا طراحی شده است که انعطاف‌پذیری و مقیاس‌پذیری بالایی را فراهم می‌کند. این معماری از پنج مؤلفه اصلی و مستقل تشکیل شده است که وظایف مشخصی را بر عهده دارند و از طریق واسط‌های برنامه‌نویسی با یکدیگر در ارتباط هستند. همان‌گونه که در شکل ۱ آورده شده است، این سرویس‌ها عبارتند از: مدیریت کانال، مدیریت تراکنش، مدیریت وثیقه، حل اختلافات و مدیریت زنجیره بلوکی.



شکل ۱: ارتباطات بین سرویس‌ها در معماری سرویس‌گرا

پایاده‌سازی این معماری در سناریوی بازی، که در آن هر بازیکن به‌صورت مستقیم با سرویس‌دهنده در تعامل است، منجر به شکل‌گیری یک همبندی ستاره‌ای می‌شود. در این همبندی، سرویس‌دهنده (که میزبان این پنج سرویس است) به‌عنوان گره مرکزی و بازیکنان به‌عنوان گره‌های پیرامونی عمل می‌کنند.

۴-۱-۱- تعادل بین تمرکز و عدم تمرکز

ممکن است این پرسش مطرح شود که آیا معماری ستاره‌ای با یک سرویس‌دهنده مرکزی، اصل عدم تمرکز زنجیره بلوکی را نقض نمی‌کند؟ پاسخ به این پرسش در تفکیک لایه‌های عملیاتی و تسویه نهفته است. در مدل ما، لایه عملیاتی (خارج از زنجیره) برای دستیابی به حداکثر سرعت و کارایی، این لایه به‌صورت متمرکز توسط سرویس‌دهنده بازی مدیریت می‌شود. این امر برای پردازش آنی هزاران تراکنش در ثانیه که در محیط بازی ضروری است، یک انتخاب مهندسی بهینه محسوب می‌شود.

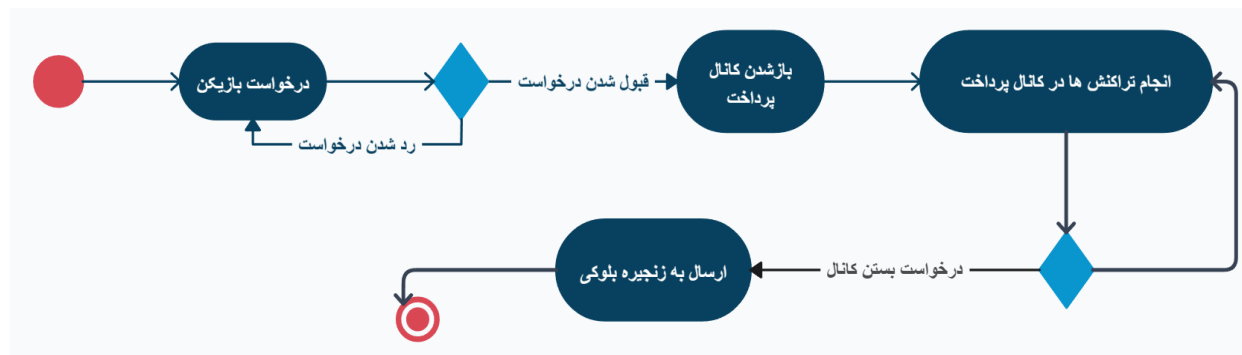
مدیریت وثیقه را نیز برای افزایش اعتماد و امنیت در نظر بگیرد. پژوهش حاضر با هدف پر کردن این شکاف ارائه شده است و مقایسه انواع رویکردها را می‌توان در جدول ۱ مشاهده کرد.

جدول ۱: مقایسه رویکردهای موجود در کانال‌های پرداخت

رویکرد	نوع راهکار	کاهش هزینه گس	افزایش سرعت
شاردینگ [۷]	لایه اول	محدود	متوسط (۱/۷ ثانیه)
اثبات سهام [۶]	لایه اول	محدود	بالا (۰/۲۵ ثانیه)
پیش‌بینی قیمت گس [۹]	لایه دوم (ابزار)	بالا (۶۴/۳ درصد)	نامشخص
مسیریابی بهینه [۸]	لایه دوم	متوسط	بالا
روش پیشنهادی	لایه دوم	بالا (بیش از ۵۰ درصد)	بالا (۱/۲ ثانیه)

۴-۲- روش پیشنهادی

در این بخش، مدل پیشنهادی برای بهینه‌سازی تراکنش‌ها در بازی‌های زنجیره بلوکی معرفی می‌شود. هدف اصلی این مدل، ایجاد یک زیرساخت کارآمد با استفاده از کانال‌های پرداخت است که سرعت را افزایش داده، هزینه‌ها را کاهش دهد و امنیت را از طریق سازوکارهای داخلی تضمین کند. چالش‌های عملیاتی مانند مدیریت هم‌زمان هزاران کانال یا تأخیر در پردازش، از طریق طراحی یک معماری سرویس‌گرا مدیریت شده‌اند. مدل پیشنهادی به پنج سرویس مستقل تفکیک شده است: مدیریت کانال، مدیریت تراکنش، مدیریت وثیقه، حل اختلافات و مدیریت زنجیره بلوکی. این استقلال سرویس‌ها به ما اجازه می‌دهد تا بار کاری را توزیع کنیم. به‌عنوان مثال، سرویس مدیریت تراکنش مسئولیت پردازش پرسرعت و پرتکرار تراکنش‌های بیرون زنجیره را بر عهده دارد، در حالی که سرویس حل اختلافات تنها در صورت بروز اختلاف فعال می‌شود و از ایجاد گلوگاه در خط اصلی پردازش جلوگیری می‌کند. این طراحی ماژولار، امکان مقیاس‌پذیری افقی را فراهم می‌آورد.



شکل ۲: نمودار فعالیت انجام تراکنش‌ها از طریق کانال پرداخت بازی‌های زنجیره بلوکی

بستن کانال را ارسال کنند. با این درخواست، آخرین وضعیت معتبر و امضاشده تراز مالی، به عنوان یک تراکنش نهایی بر روی زنجیره اصلی ثبت شده و وثیه‌ها آزاد می‌شوند.

۳-۴- الگوریتم ساخت کانال‌های پرداخت برای بازی‌های زنجیره بلوکی

الگوریتم ساخت کانال‌های پرداخت برای بازی‌های زنجیره بلوکی که در شکل ۳ نمایش داده شده است، با هدف ایجاد یک ساختار گرافی برای تحلیل و مدیریت کانال‌های پرداخت طراحی شده است. این الگوریتم بازیکنان و سرویس‌دهنده بازی را به صورت گره‌هایی در گراف نمایش می‌دهد و کانال‌های پرداخت میان آنها را به عنوان یال‌هایی تعریف می‌کند که اطلاعات و ویژگی‌های مربوط به تراکنش‌ها را ذخیره می‌کنند. در ابتدا، الگوریتم یک مجموعه خالی برای ذخیره‌سازی داده‌های گراف ایجاد می‌کند. یک گره مرکزی برای سرویس‌دهنده مشترک تعریف می‌شود و برای هر بازیکن، یک گره متناظر در گراف ثبت می‌شود. سپس، اگر یک کانال پرداخت بین بازیکن و سرویس‌دهنده ایجاد شود، یک یال بین گره بازیکن و سرویس‌دهنده برقرار می‌شود. ویژگی‌های مربوط به بازیکن، مانند موجودی و تعداد تراکنش‌ها، به صورت بردارهای ویژگی رمزگذاری شده و به ماتریس ویژگی‌های گره‌ها اضافه می‌شود. علاوه بر این، اطلاعات تراکنش‌ها به صورت موقت در کانال پرداخت ذخیره می‌شوند. مهمترین نکته این

و همچنین لایه تسویه و اعتماد (درون زنجیره) در مدل ما، لایه زیرین همچنان زنجیره بلوکی است. تمام عملیات افتتاح و اختتام کانال و مهمتر از آن، فرآیند حل اختلافات، توسط قراردادهای هوشمند بر روی زنجیره اصلی اجرا و تضمین می‌شود. این بدان معناست که سرویس‌دهنده نمی‌تواند به صورت یک طرفه دارایی کاربران را تصاحب کند یا از تعهدات خود سر باز زند. در واقع، زنجیره بلوکی به عنوان یک داور نهایی و غیرمتمرکز عمل می‌کند. این مدل ترکیبی، بهترین ویژگی‌های هر دو جهان را به ارمغان می‌آورد: سرعت و کارایی یک سیستم متمرکز در کنار امنیت و اعتماد یک سیستم غیرمتمرکز.

۲-۴- فرآیند عملکرد کانال پرداخت

چرخه حیات یک تراکنش در سامانه پیشنهادی شامل سه مرحله اصلی است که شکل ۲ نمایش داده شده است.

۱. ایجاد کانال: بازیکن درخواستی برای ایجاد کانال به سرویس‌دهنده ارسال می‌کند. پس از توافق، یک تراکنش اولیه برای باز کردن کانال و قفل کردن وثیقه اولیه بر روی زنجیره اصلی ثبت می‌شود.

۲. انجام تراکنش‌های خارج از زنجیره: پس از فعال‌سازی کانال، بازیکن و سرویس‌دهنده می‌توانند تعداد نامحدودی تراکنش را به صورت آنی و با هزینه نزدیک به صفر انجام دهند. هر تراکنش شامل به روزرسانی تراز مالی کانال است که به امضای دیجیتال هر دو طرف می‌رسد.

۳. بستن کانال: هر یک از طرفین می‌توانند درخواست

را به سرویس‌دهنده ارسال می‌کند و سرویس‌دهنده شرایط لازم از جمله کارمزدهای اولیه را بررسی می‌کند.

۲. ایجاد کانال در صورت رعایت شرایط: در صورتی که شرایط (مانند هزینه‌ها) مطلوب باشد، یک کانال پرداخت بین بازیکن و سرویس‌دهنده ایجاد می‌شود.

۳. بهینه‌سازی هزینه‌ها: هزینه‌های تراکنش درون کانال بهینه‌سازی می‌شوند تا مجموع هزینه‌ها کمتر از تراکنش‌های مستقیم روی زنجیره بلوکی باشد.

۴. ارسال تراکنش‌ها در کانال: پس از ایجاد کانال، بازیکن می‌تواند تراکنش‌های خود را با هزینه‌های بهینه شده از طریق این کانال انجام دهد.

در ادامه بخش ۲ که حل اختلافات به‌صورت خودکار است را مورد بررسی قرار می‌دهیم. یکی از ویژگی‌های نوآورانه این الگوریتم، توانایی آن در شناسایی و حل اختلافات به‌صورت خودکار است. مراحل اصلی این بخش شامل موارد زیر است.

۱. پایش تراکنش‌ها: کانال‌های فعال به‌طور مستمر از نظر صحت تراکنش‌ها و توازن مالی پایش می‌شوند.

۲. شناسایی اختلاف: در صورت مشاهده مغایرت (مانند اختلاف در تاریخچه تراکنش‌ها یا موجودی)، سازوکار حل اختلاف فعال می‌شود.

۳. حل اختلاف: اگر بازیکن اعتراضی داشته باشد، سرویس‌دهنده موظف است مدارک معتبر ارائه دهد. در صورت معتبر بودن مدارک سرویس‌دهنده، اختلاف به نفع سرویس‌دهنده حل می‌شود؛ در غیر این صورت، کانال بسته شده و اختلاف به نفع بازیکن خاتمه می‌یابد.

۴. بستن کانال: در پایان چرخه کانال، وضعیت نهایی تراکنش‌ها و موجودی به زنجیره بلوکی ثبت می‌شود تا تسویه نهایی انجام شود.

در آخر نیز به بررسی خروجی الگوریتم می‌پردازیم. خروجی این الگوریتم مجموعه‌ای از کانال‌های پرداخت فعال و وضعیت نهایی آنها است که نشان‌دهنده کارایی و امنیت سیستم است. این الگوریتم از طریق بهینه‌سازی

است که تراکنش‌ها به‌صورت خارج از زنجیره در کانال پرداخت انجام می‌شوند. در پایان، زمانی که بازیکن یا سرویس‌دهنده تصمیم به بستن کانال می‌گیرد، نتایج نهایی (تغییرات نهایی و وضعیت کل تراکنش‌ها) به‌عنوان یک بلوک واحد بر روی زنجیره بلوکی ثبت می‌شود. در این مرحله، وضعیت نهایی کانال، شامل مجموع تراکنش‌ها و توازن مالی، به‌عنوان برچسب یال ذخیره می‌شود. در نهایت، یک گراف داده شامل ویژگی‌های گره‌ها، یال‌ها و برچسب‌ها ایجاد شده و به مجموعه داده‌های گرافی اضافه می‌شود. خروجی این الگوریتم یک مجموعه داده گرافی است که می‌توان از آن برای تحلیل سیستم کانال‌های پرداخت و بهینه‌سازی عملکرد آن استفاده کرد. این ساختار گرافی به‌ویژه برای پیاده‌سازی الگوریتم‌های یادگیری ماشین و تحلیل‌های پیشرفته در سیستم‌های پرداخت زنجیره بلوکی مناسب است و امکان ارتقای کارایی و امنیت سیستم را فراهم می‌آورد.

۴-۴- مدیریت کانال‌های پرداخت

الگوریتم ارائه شده در این پژوهش که در شکل ۴ قابل مشاهده است، به‌منظور مدیریت بهینه کانال‌های پرداخت در بازی‌های مبتنی بر زنجیره بلوکی طراحی شده است. این الگوریتم شامل دو بخش اصلی است: ایجاد کانال‌های پرداخت با بهینه‌سازی هزینه‌ها و حل اختلافات به‌صورت خودکار. هدف اصلی این الگوریتم کاهش هزینه‌های تراکنش، افزایش سرعت پردازش، و بهبود اعتماد و امنیت کاربران است. در ادامه به شرح بخش‌های مختلف این الگوریتم می‌پردازیم. در ابتدا بخش ۱ را که ایجاد کانال پرداخت با بهینه‌سازی هزینه‌ها است مورد بررسی قرار می‌دهیم. در این بخش، الگوریتم شرایطی را فراهم می‌کند که هر بازیکن بتواند با کمترین هزینه یک کانال پرداخت با سرویس‌دهنده بازی ایجاد کند. در ادامه به توضیح مراحل اصلی این بخش می‌پردازیم.

۱. بررسی شرایط اولیه: بازیکن درخواست ایجاد کانال

آتی، این مدل خطی می‌تواند با مدل‌های غیرخطی یا تطبیقی که پارامترهای خود را بر اساس ترافیک لحظه‌ای شبکه تنظیم می‌کند، جایگزین شود، بدون آن که نیاز به تغییر در معماری اصلی سیستم باشد. این پژوهش، چالش قفل شدن سرمایه در طول فرایندهای حل اختلاف را به‌عنوان یک ریسک اقتصادی کلیدی برای کاربران شناسایی کرده است. در سازوکارهای رایج، بازگشت وجه صرفاً اصل دارایی مورد مناقشه را مسترد می‌کند. این رویکرد، هزینه فرصت ناشی از عدم دسترسی کاربر به آن دارایی در طول بازه زمانی اختلاف را نادیده می‌گیرد و منجر به عدم جبران خسارت کامل می‌شود. راه‌حل عملیاتی ارائه شده در این مدل، یک روش اقتصادی مبتنی بر وثیقه‌گذاری اجباری برای سرویس‌دهنده است که میزان آن به‌صورت پویا و بر اساس پارامترهای ریسک کانال مانند حجم تراکنش‌ها و مدت زمان، محاسبه می‌شود. این وثیقه، فراتر از یک ضمانت ساده، به‌عنوان یک روش هم‌راستاسازی انگیزه عمل می‌کند. در صورت بروز اختلاف و اثبات قصور سرویس‌دهنده توسط قرارداد هوشمند، فرآیند تسویه به صورت خودکار فعال می‌شود. در این فرایند، کاربر نه‌تنها دارایی اصلی خود را بازپس می‌گیرد، بلکه مبلغ جریمه‌ای نیز از محل وثیقه کسر و به وی پرداخت می‌گردد. این پرداخت اضافی به‌طور خاص برای جبران هزینه فرصت سرمایه قفل‌شده و اصطکاک ناشی از فرآیند داوری طراحی شده‌است و رفتار صادقانه سرویس‌دهنده را به لحاظ اقتصادی تضمین می‌کند.

۴-۵-۱- منطق استخراج و انتخاب مدل خطی

فرمول‌های پیشنهادی برای کارمزد و وثیقه، مدل‌های اکتشافی هستند که بر اساس تحلیل عوامل اصلی هزینه در یک سامانه کانال پرداخت طراحی شده‌اند. انتخاب یک مدل خطی یک تصمیم مهندسی آگاهانه بوده و دلایل زیر را دارد:

۱. قابلیت تفسیرپذیری بالا: مدل‌های خطی به سادگی قابل درک هستند. تأثیر هر متغیر (مانند افزایش یک روز به

Algorithm 1: Constructing Payment Channels for Blockchain Transactions

Input: (1) Set of players P , each requiring blockchain transactions.
(2) A single server S acting as the intermediary for opening and closing payment channels.

Output: (1) Graph dataset G_i with nodes representing players and the server, and edges representing payment channels.

```

1
2 PROCEDURE:
3   Part 1: Payment Channel Creation
4   Initialize an empty dataset  $D$ .
5   Define a single server  $S$  as a central node.
6   for each player  $p \in P$  do
7     Define a node for player  $p$ .
8     Create an edge  $E$  between player  $p$  and server  $S$  when a
       payment channel is opened.
9   Initialize node feature matrix  $X$  and edge index list.
10  for each player  $p \in P$  do
11    Encode player characteristics (e.g., balance, transaction count)
      into feature vectors.
12    Append to node feature matrix  $X$ .
13  for each payment channel opened do
14    Record source and target nodes (player and server) in the edge
      index list.
15    Store off-chain transaction data temporarily in the channel.
16  if a player or server decides to close the channel then
17    Record the total transaction history.
18    Submit the final state (aggregated results and changes) to the
      blockchain as a single batch.
19    Encode the final state of the channel closure as an edge label  $Y$ .
20  Create a graph data object  $G_i = (X, E, Y)$  with features, edges, and
      labels.
21  Add  $G_i$  to dataset  $D$ .
22  return dataset  $D$  for payment channel analysis.

```

شکل ۳: الگوریتم ساخت کانال‌های پرداخت برای بازی‌های زنجیره بلوکی

هزینه‌ها و ایجاد سازوکارهای حل اختلاف خودکار، علاوه بر کاهش هزینه‌های مالی کاربران، بهبود قابل‌توجهی در امنیت و اعتماد به سیستم پرداخت بازی‌های زنجیره بلوکی ایجاد می‌کند.

۴-۵- مدل‌سازی اقتصادی و بهینه‌سازی

برای افزایش بار علمی و شفافیت مدل، در این بخش به تشریح منطق استخراج فرمول‌ها و سازوکارهای اقتصادی آن می‌پردازیم، همچنین انتخاب مدل خطی برای بهینه‌سازی هزینه‌ها، آگاهانه و با هدف اولویت‌دهی به شفافیت و کارایی محاسباتی در این چارچوب پایه انجام شده است. این مدل به ما اجازه می‌دهد تا تأثیر هر پارامتر (مانند هر تراکنش اضافی یا هر روز باز بودن کانال) را به وضوح تحلیل کنیم. با این حال، اذعان داریم که این مدل یک تقریب از سناریوی واقعی است. این چارچوب به گونه‌ای طراحی شده که تابع هزینه قابل جایگزینی است. در توسعه‌های

کانال (هزینه فرصت سرمایه قفل شده)، N تعداد تراکنش‌ها (بار محاسباتی) و G وثیقه گرو گذاشته شده توسط سرویس‌دهنده (عامل ریسک) است. ضرایب k وزن هر عامل را مشخص می‌کنند که از طریق تحلیل رگرسیون بر روی داده‌های شبیه‌سازی شده به دست آمده‌اند.

Algorithm 1: Managing Payment Channels with Automatic Dispute Resolution

Input: (1) Set of players P and server S .
(2) Set of initial conditions for opening payment channels, including server fees and cost optimization for users.
(3) Set of conditions for resolving disputes between players and server.
Output: (1) Successful creation of payment channels.
(2) Resolution of disputes, if any, during the payment channel lifecycle.

```

1
2 PROCEDURE:
3 Part 1: Payment Channel Creation with Fee Optimization
4 Initialize an empty set of active channels  $C$ .
5 for each player  $p \in P$  do
6   Player  $p$  sends a request to server  $S$  to open a payment channel.
7   Server  $S$  verifies the conditions for opening the channel,
   including initial server fees.
8   if conditions are met (including agreement on server fees) then
9     Create a new payment channel  $c$  between player  $p$  and server  $S$ .
10    Record the starting balance of the player and server.
11    Add  $c$  to the set of active channels  $C$ .
12    Calculate optimized transaction fees for the player, ensuring
    that the cost of transactions within the channel is lower
    than direct blockchain transactions.
13    Player  $p$  can now send multiple transactions through the
    payment channel, with each transaction being cost-optimized
    and lower than the blockchain fees.
14 Part 2: Automatic Dispute Resolution
15 for each active channel  $c \in C$  do
16   Monitor the transactions between player  $p$  and server  $S$ .
17   if a dispute arises (e.g., inconsistency in transaction history or
    balance) then
18     Automatically trigger the dispute resolution mechanism.
19     Check the dispute conditions (e.g., balance, transaction
    count, and proof of transactions).
20     if player  $p$  challenges the server then
21       Server  $S$  must provide proof of valid transactions.
22       Player  $p$  can request that the server stakes an additional
       collateral to ensure fairness.
23       if proof is valid then
24         Dispute is resolved in favor of server  $S$ .
25       else
26         Dispute is resolved in favor of player  $p$ , and the
         channel may be closed.
27   If no disputes occur, the channel continues to function as normal.
28 for each closed channel  $c$  do
29   Submit the final state of the payment channel (total
   transactions, balances) to the blockchain for final settlement.
30   Remove  $c$  from the set of active channels  $C$ .
31 return The set of active channels and their states.

```

شکل ۴: الگوریتم مدیریت کانال‌های پرداخت برای بازی‌های زنجیره بلوکی

۴-۵-۴- سازوکار وثیقه و تمایز آن با بازپرداخت

در سیستم‌های سنتی، بازپرداخت تنها مبلغ اصلی تراکنش را باز می‌گرداند. این روش، خسارت ناشی از زمان از دست رفته کاربر و تجربه کاربری منفی را جبران نمی‌کند. سازوکار وثیقه پیشنهادی در این پژوهش، یک سیستم جریمه و جبران خسارت است. سرویس‌دهنده

عمر کانال) بر هزینه نهایی کاملاً شفاف است.

۲. کارایی محاسباتی: این مدل‌ها از نظر محاسباتی بسیار سبک هستند و سربار کمی ایجاد می‌کنند که برای یک سیستم بیدرنگ ضروری است.

۳. کفایت برای هدف اصلی: هدف این پژوهش، نشان دادن بهبود قابل توجه نسبت به روش‌های سنتی است. یک مدل خطی به خوبی می‌تواند روابط اصلی را شناسایی کرده و به این هدف دست یابد. این مدل به عنوان یک پایه قوی عمل می‌کند که در کارهای آتی می‌توان آن را با مدل‌های پیچیده‌تر مانند یادگیری ماشین جایگزین کرد.

۴-۵-۲- مدل‌سازی هزینه کل سامانه

هزینه کل برای یک کانال پرداخت از دیدگاه کاربر، مجموعه‌ای از هزینه‌های مختلف است که توسط فرمول (۱-۴) تجمیع شده‌اند:

$$C_{total} = C_{collateral} + \sum_b C_{blockchain} + \sum_s C_{server} - 1) + \sum_i C_{dispute} + \sum_i C_{open} + \sum_i C_{close}$$

که در آن C_{open} و C_{close} هزینه باز و بسته کردن کانال، $C_{dispute}$ هزینه احتمالی فرایند حل اختلاف، C_{server} کارمزد پرداختی به سرویس‌دهنده و $C_{blockchain}$ هزینه نهایی ثبت تراکنش بر روی زنجیره بلوکی است. هدف اصلی مدل، کمینه کردن C_{total} از طریق بهینه‌سازی مؤلفه‌های آن است.

۴-۵-۳- بهینه‌سازی کارمزد سرویس‌دهنده

کارمزد دریافتی توسط سرویس‌دهنده باید منعکس‌کننده منابع مصرفی و ریسک پذیرفته شده باشد. این کارمزد توسط فرمول (۲-۴) مدل‌سازی شده است:

$$C_{server} = B + K_1 D + k_r N + K_r G \quad (2-4)$$

در این رابطه، B کارمزد پایه، D مدت زمان باز بودن

اجرای شبیه‌سازی‌ها و تحلیل نتایج به‌کار رفت. ضمن تأیید اهمیت ارزیابی مدل در یک محیط عملیاتی واقعی با کاربران نهایی، لازم به توضیح است که در این پژوهش، قدم‌های اساسی برای اعتبارسنجی فراتر از شبیه‌سازی نظری برداشته شده است. برای اطمینان از استحکام و کارایی مدل در مواجهه با شرایط واقعی شبکه، ارزیابی‌ها بر روی شبکه‌های آزمایشی عمومی انجام پذیرفت که بالاترین سطح شباهت به شبکه‌های اصلی را دارند. در ابتدا، استفاده از ابزارهای شبیه‌سازی کاملاً محلی مانند Ganache، به دلیل ارائه زمان‌های پردازش غیرواقعی و عدم لحاظ کردن تأخیر واقعی شبکه، کنار گذاشته شد. به‌منظور دستیابی به نتایج دقیق و قابل اتکا، مدل با استفاده از بُن‌سازهٔ اینفورا مستقیماً بر روی شبکه‌های آزمایشی سپولیا و Polygon Mumbai پیاده‌سازی گردید. این شبکه‌ها از زیرساخت و الگوریتم‌های اجماع مشابه با زنجیره‌های اصلی بهره می‌برند و نتایج آن‌ها بازتاب دقیقی از عملکرد مدل در مواجهه با تأخیر واقعی شبکه و فرآیندهای تأیید بلوک است. با این حال، پذیرفته شده است که ارزیابی نهایی و بررسی چالش‌های مقیاس‌پذیری در مواجهه با کاربران انسانی، نیازمند پیاده‌سازی در یک بازی واقعی است. این قابلیت بازتولیدپذیری، شبیه‌سازی‌ها با مشخصات دقیق زیر انجام شدند:

۱. محیط شبکه: برای جلوگیری از نتایج غیرواقعی شبکه‌های محلی (مانند Ganache)، از بُن‌سازهٔ اینفورا برای اتصال به شبکه‌های آزمایشی عمومی سپولیا (اتریوم) و Polygon Mumbai استفاده شد.
۲. توزیع داده‌ها: مجموعه داده تحلیل هزینه شامل ۱۰۰۰ کانال شبیه‌سازی شده بود. پارامتر مدت زمان باز بودن کانال (D) به‌صورت تصادفی بین ۱ تا ۳۰ روز و تعداد تراکنش‌ها (N) به‌صورت تصادفی بین ۱ تا ۱۰۰۰ تراکنش نمونه‌برداری شد.
- در حالی که مدل پیشنهادی از مفهوم بنیادین کانال پرداخت مشابه شبکه لایتنینگ بهره می‌برد، نوآوری و

موظف است وثیقه‌ای را گرو بگذارد که به‌عنوان یک ضمانت اقتصادی برای رفتار صحیح عمل می‌کند. مقدار این وثیقه بر اساس ریسک کانال و با استفاده از فرمول (۳-۴) محاسبه می‌شود:

(۳-۴)

$$C_{collateral} = \gamma + D_{channel} \beta + \alpha \sum_{i=1}^n T_i$$

در این رابطه، γ وثیقه پایه، D مدت زمان و $\sum_{i=1}^n T_i$ حجم کل تراکنش‌ها در کانال است. در صورت بروز اختلاف و اثبات قصور سرویس‌دهنده، بخشی از این وثیقه به‌عنوان جریمه به بازیکن پرداخت می‌شود. این سازوکار، علاوه بر بازگرداندن مبلغ اصلی، خسارت کاربر را نیز جبران کرده و یک عامل بازدارنده قوی در برابر رفتار متقلبانه ایجاد می‌کند.

۵- ارزیابی و نتایج

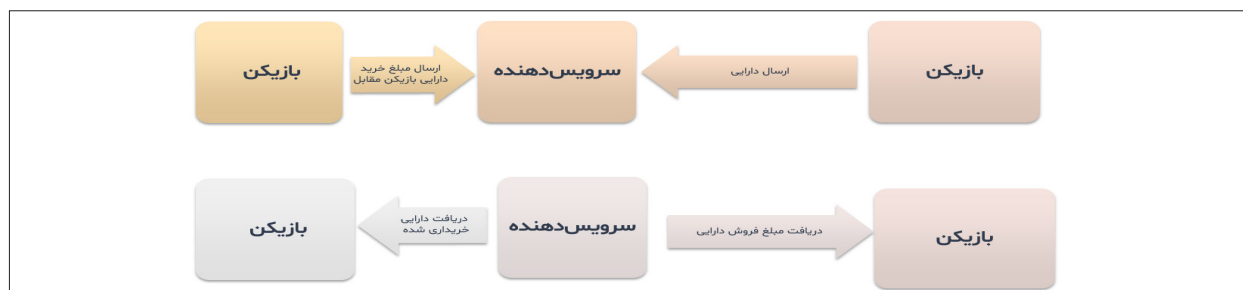
برای ارزیابی عملکرد مدل پیشنهادی، یک محیط شبیه‌سازی جامع طراحی و پیاده‌سازی شد. در این بخش، ابتدا به تشریح محیط و ابزارهای مورد استفاده پرداخته، سپس سناریوهای ارزیابی و نتایج حاصل از آن‌ها به تفصیل تحلیل می‌شوند.

۵-۱- محیط و ابزارهای پیاده‌سازی

برای اطمینان از نزدیکی نتایج به شرایط واقعی، از ابزارهای استاندارد استفاده شد. شبیه‌سازی تراکنش‌ها بر روی شبکه‌های اتریوم و پالیگان با استفاده از سکوی اینفورا^{۱۱} انجام گرفت که امکان تعامل مستقیم با شبکه‌های آزمایشی عمومی را فراهم می‌کند. شبکه آزمایشی سپولیا^{۱۲} برای اتریوم انتخاب شد تا محیطی مشابه با شبکه اصلی شبیه‌سازی شود. زبان برنامه‌نویسی پایتون به دلیل کتابخانه‌های غنی در تحلیل داده، برای اسکریپت‌نویسی،

11- Infura

12- Sepolia



شکل ۱: مراحل انجام تراکنش در کانال پرداخت

۵-۲-۱- نتایج آزمایش و تحلیل

در این بخش به بررسی نتایج آزمایش و تحلیل داده‌ها می‌پردازیم.

۵-۲-۲- تحلیل عملکرد سرعت

نتایج شبیه‌سازی نشان داد که زمان میانگین برای یک تراکنش مستقیم بر روی شبکه اتریوم ۱۵ ثانیه و بر روی شبکه پالیگان ۲ ثانیه است. در مقابل، زمان هر تراکنش خارج از زنجیره در مدل پیشنهادی ۱/۲ ثانیه محاسبه شد. این زمان بر اساس کار یو و همکاران [۴۱] و با در نظر گرفتن یک فرایند چهار مرحله‌ای برای هر تراکنش درون کانال (ارسال درخواست، تأیید، به‌روزرسانی وضعیت و ارسال پاسخ) به‌دست آمده است. هر یک از این مراحل به‌طور میانگین ۰/۳ ثانیه زمان می‌برد که مجموعاً ۱/۲ ثانیه برای تکمیل یک تراکنش کامل در کانال لازم است. که جزئیات این فرایند را می‌توان در شکل ۱ مشاهده کرد. با در نظر گرفتن این زمان پایه و هزینه ثابت باز و بسته کردن کانال، با توجه به جدول ۱، عملکرد کلی مدل با افزایش تعداد تراکنش‌ها به‌طور چشمگیری بهبود می‌یابد.

جدول ۱: خروجی نتایج شبیه‌سازی

تراکنش	زمان عادی در شبکه اتریوم	زمان عادی در شبکه پالیگان	زمان کانال پرداخت در شبکه پالیگان	زمان کانال پرداخت در شبکه اتریوم
۱	۱۵	۲	۳,۲	۱۶,۲
۲	۳۰	۴	۴,۴	۱۷,۴
۳	۴۵	۶	۵,۶	۱۸,۶
۱۰	۱۵۰	۲۰	۱۴	۲۷
۲۰	۳۰۰	۴۰	۲۶	۳۹
۳۰	۴۵۰	۶۰	۳۸	۵۱

تمایز آن در سه جنبه اساسی است:

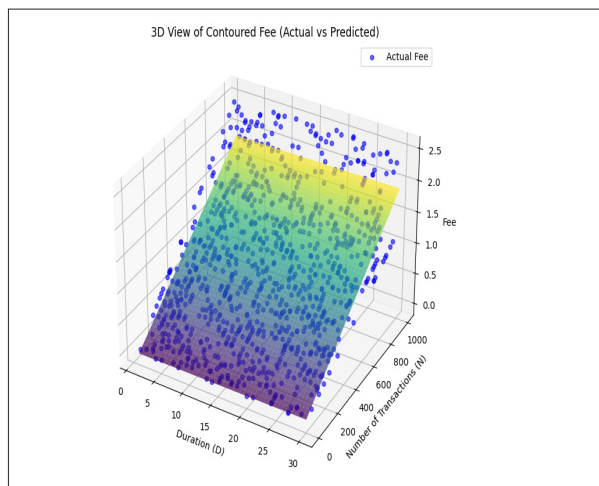
۱. همبندی: لایتنینگ برای یک شبکه توری غیرمتمرکز و مسیریابی چندمرحله‌ای طراحی شده است. مدل ما به‌طور خاص برای همبندی ستاره بازی‌ها بهینه شده است.
۲. مدل اعتماد: در لایتنینگ اعتماد کاملاً توزیع شده است. مدل ما از یک رویکرد ترکیبی استفاده می‌کند: هماهنگ‌کننده (سرویس‌دهنده) بر کارایی متمرکز است. اما اعتماد نهایی توسط قراردادهای هوشمند روی زنجیره (برای حل اختلاف و وثیقه) تضمین می‌شود.
۳. هدف: هدف لایتنینگ پرداخت‌های عمومی است. هدف این مدل، یک راهکار جامع برای بازی‌ها، شامل مدیریت تراکنش‌های خرد درون بازی و تضمین امنیت آن‌ها از طریق سازوکار وثیقه است.

۵-۲-۳- سناریوهای ارزیابی

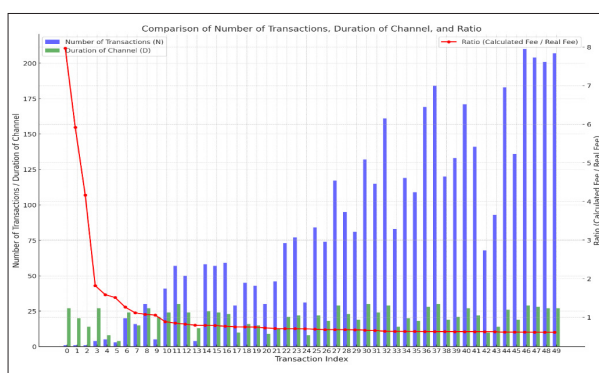
دو سناریوی اصلی برای ارزیابی مدل تعریف شد:

۱. ارزیابی سرعت تراکنش: در این سناریو، زمان کل موردنیاز برای انجام تعداد مختلفی از تراکنش‌ها (از ۱ تا ۳۰) در مدل پیشنهادی با زمان لازم برای ثبت همان تعداد تراکنش به‌صورت مستقیم بر روی شبکه‌های اتریوم و پالیگان مقایسه شد.

۲. ارزیابی هزینه کارمزد گس: در این سناریو، میزان کاهش هزینه گس با استفاده از مدل کانال پرداخت در مقایسه با روش سنتی (ثبت هر تراکنش روی زنجیره) مورد سنجش قرار گرفت.



شکل ۲: نقشه کانتور رگرسیون انجام شده



شکل ۳: نمودار نتیجه‌گیری نهایی رابطی بین تعداد تراکنش‌ها، مدت زمان باز بودن کانال و نسبت کارمزد محاسبه شده به واقعی

۵-۳-۱- مقایسه در بهبود سرعت تراکنش‌ها

در مقایسه با راهکارهای لایه اول مانند شاردرینگ که توسط شاتاهای باکر و همکاران [۷] ارائه شده و به سرعت ۱/۷ ثانیه دست یافته‌اند، یا راهکارهای مبتنی بر اثبات سهام که توسط طارق و همکاران [۶] با سرعت ۰/۲۵ ثانیه پیاده‌سازی شده‌اند، مدل پیشنهادی با سرعت ۱/۲ ثانیه عملکردی رقابتی ارائه می‌دهد. همان‌طور که در جدول ۲ آمده است، مزیت اصلی مدل ما این است که برخلاف راهکارهای لایه اول که با افزایش پیچیدگی یا تعداد کاربران دچار افت عملکرد می‌شوند، سرعت آن مستقل از وضعیت کلی شبکه اصلی است.

۵-۳-۲- مقایسه در کاهش هزینه گس

در زمینه کاهش هزینه، با توجه به جدول ۳ مدل پیشنهادی با کاهش بیش از ۵۰ درصد، عملکردی بسیار

۵-۲-۳- تحلیل عملکرد هزینه گس

برای تحلیل هزینه، یک مجموعه داده مصنوعی با ۱۰۰۰ کانال شبیه‌سازی شد که در آن تعداد تراکنش‌ها (N) (بین ۱ تا ۱۰۰۰) و مدت زمان باز بودن کانال (D) (بین ۱ تا ۳۰ روز) متغیر بود. با استفاده از رگرسیون خطی بر روی این داده‌ها، ضرایب بهینه برای فرمول (۲-۴) استخراج شد. نتایج نشان داد که مدل پیشنهادی با جمع تراکنش‌ها، هزینه گس را به‌طور میانگین بیش از ۵۰ درصد در حالت عادی و بیش از ۴۰ درصد در حالت وجود وثیقه کاهش می‌دهد. نقشه کانتور رگرسیون انجام شده در شکل ۲ قابل مشاهده است. تحلیل‌های انجام شده بر روی شکل ۳ نیز نشان داد که کارایی مدل در کاهش هزینه، زمانی به حداکثر می‌رسد که تعداد تراکنش‌ها بالا و مدت زمان باز بودن کانال منطقی باشد. با این حال، تحلیل حساسیت بر روی این پارامترها، محدودیت‌های عملیاتی مدل را آشکار می‌سازد. در شرایطی که تعداد تراکنش‌ها بسیار کم و مدت زمان باز بودن کانال طولانی باشد، هزینه فرصت سرمایه قفل‌شده و هزینه ثابت کانال، این روش را غیراقتصادی می‌کند. برای مثال، در یک سناریوی شبیه‌سازی شده با تنها یک تراکنش (N=1) و کانال باز به مدت ۲۷ روز (D=27)، مشاهده شد که نسبت هزینه محاسبه شده به هزینه واقعی به حدود ۸ برابر افزایش یافت. دلیل این امر آن است که هزینه‌های ثابت باز کردن و بستن کانال، در این حالت بر تعداد تراکنش‌های بسیار کمی سرشکن می‌شود. این یافته تأیید می‌کند که مدل پیشنهادی برای کاربردهای با حجم تراکنش بالا و مکرر بهینه است، اما برای تراکنش‌های پراکنده و تکی توصیه نمی‌شود.

۵-۳-۳- مقایسه با پژوهش‌های مرتبط

برای ارزیابی جایگاه مدل پیشنهادی در میان پژوهش‌های اخیر، عملکرد آن با چندین راهکار دیگر در زمینه بهبود سرعت و کاهش هزینه مقایسه شده است.

جدول ۲: جدول مقایسه کارهای مرتبط در بهبود سرعت تراکنش‌ها

نام مقاله	شبکه زنجیره‌بلوکی و محیط آزمایش	سرعت تراکنش (تغییرات)	توضیحات	مشکلات
مقاله [۱۵]: Yunifa et al., 2024	شبکه آزمایشی Mumbai	کمتر از ۱۵ ثانیه	استفاده از محدودیت گس برای بهبود سرعت	افزایش هزینه گس با افزایش سرعت
مقاله [۷]: Baker et al., 2023	شبکه آزمایشی	۱/۷ ثانیه (سطح دشواری ۶)، ۸۱/۷ ثانیه (سطح دشواری ۷)	استفاده از Sharding و کاهش زمان استخراج با تقسیم کار	افزایش زمان با افزایش سطح دشواری (۷ به ۸۱/۷ ثانیه)
مقاله [۶]: Tariq et al., 2023	اتریوم و Aurora Testnet	۰/۲۵ ثانیه (۱۰ کاربر)، ۱/۲۳ ثانیه (۱۰۰۰ کاربر)	استفاده از PoS و الگوریتم‌های بهینه‌سازی در شبکه خصوصی	محدودیت مقیاس‌پذیری؛ افزایش زمان با افزایش کاربران، PoS برخلاف PoW در اتریوم
مقاله [۱۴]: Ciprian et al., 2022	Hyperledger Fabric	۱/۰۳ ثانیه	قراردادهای هوشمند و استفاده از Hyperledger برای تراکنش‌های سریع	محدودیت در تعداد کاربران؛ زمان به شدت افزایش می‌یابد
کار پیشنهادی	تمامی شبکه‌ها و محیط آزمایشی بُن‌سازه اینفورا	۱/۲ ثانیه	بهینه‌سازی کانال پرداخت و کاهش کارمزد گس	عملکرد بهینه در تعداد زیاد

جدول ۳: جدول مقایسه کارهای مرتبط در کاهش کارمزد گس.

نام مقاله	توضیحات	شبکه زنجیره‌بلوکی	کاهش کارمزد گس	مشکلات
مقاله [۹]: Fangxiao et al., 2020	پیش‌بینی قیمت گس با استفاده از مدل MLR-XGB، با معیارهای پیچیدگی شبکه و قیمت اتر	شبکه عمومی اتریوم	۶۴/۶ درصد	وابستگی به داده‌های تاریخی، تغییرات ناگهانی پیچیدگی شبکه، محدودیت در داده و منابع محاسباتی
مقاله [۱۰]: Farokhnia et al., 2023	انتقال محاسبات به خارج از زنجیره و استفاده از قراردادهای Wrapper	شبکه عمومی اتریوم	۴۰/۰۹ درصد	نیاز به اعتماد به محاسبات خارج از زنجیره و پیچیدگی هماهنگی
مقاله [۱۱]: Suhyeon et al., 2024	بهینه‌سازی عملکرد EVM در Pietrzak VDF	شبکه عمومی اتریوم	۵۰ درصد	پیچیدگی زیاد محاسبات و مدیریت داده‌ها
مقاله [۱۲]: Hukkinen et al., 2023	کاهش مصرف گس از طریق بهینه‌سازی توابع قرارداد	شبکه عمومی اتریوم	۱۱ درصد	کاهش محدود و نیاز به تغییرات ریشه‌ای‌تر در منطق بازار
مقاله [۱۳]: Bo et al., 2021	شناسایی و حذف کدهای اضافی با ابزار sOptimize	شبکه عمومی اتریوم	۲ درصد	شناسایی ناکامل کدهای اضافی و نیاز به مدیریت دقیق
کار پیشنهادی	بهینه‌سازی سامانه و کانال‌های پرداخت	تمامی شبکه‌ها	بیش از ۵۰ درصد	عملکرد بهینه در تعداد زیاد

خارج از زنجیره، پتانسیل بیشتری برای کاهش هزینه در مقیاس بزرگ دارد. بر اساس نتایج ارائه شده، مدل پیشنهادی یک تعادل بهینه میان سرعت، هزینه ارائه می‌دهد. در حالی که برخی راهکارها ممکن است در یک معیار خاص (مانند سرعت خالص در اثبات سهام) برتری جزئی داشته باشند، مدل ما یک راهکار جامع است که به‌طور خاص برای معماری ستاره‌ای بازی‌های آنلاین طراحی شده و با افزودن لایه‌های امنیتی مانند حل اختلاف و وثیقه، راه حلی عملی‌تر و قابل اعتمادتر ارائه می‌دهد.

مطلوب دارد. در مقایسه با ابزارهای پیش‌بینی قیمت گس که توسط فانگیانو و همکاران [۹] توسعه داده شده و به کاهش ۶۴/۳ درصد دست یافته‌اند، مدل ما یک راهکار ساختاری ارائه می‌دهد که هزینه را به‌طور ذاتی کاهش می‌دهد، نه این که صرفاً زمان بهتری برای تراکنش پیشنهاد دهد. همچنین، در مقایسه با روش‌های بهینه‌سازی قراردادهای هوشمند که توسط فرخ‌نیا و همکاران [۱۰] یا سوهیون و همکاران [۱۱] ارائه شده و کاهش‌هایی در حدود ۴۰ درصد تا ۵۰ درصد گزارش کرده‌اند، مدل ما با انتقال کامل عملیات به

۶- نتیجه‌گیری

بررسی کارهای مرتبط نشان می‌دهد که اکثر راهکارهای کانال پرداخت موجود (مانند شبکه لایتنینگ یا پروتکل‌های مسیریابی) روی تراکنش‌های چندمرحله‌ای تمرکز دارند. نوآوری کلیدی این پژوهش، ارائه یک راه‌حل یکپارچه و بهینه شده برای معماری ستاره‌ای است که مشخصه اصلی بازی‌های برخط (رابطه بازیکن با سرویس‌دهنده) است. این مدل، برخلاف کارهای پیشین، صرفاً یک کانال پرداخت نیست، بلکه یک معماری سرویس‌گرا ارائه می‌دهد که سازوکارهای حیاتی حل اختلاف خودکار و مدیریت وثیقه را برای تضمین اعتماد در این ساختار متمرکز، مستقیماً با بهینه‌سازی هزینه‌ها ترکیب می‌کند. مقیاس‌پذیری کارآمد، یکی از چالش‌های اساسی در مسیر پذیرش گسترده بازی‌های مبتنی بر زنجیره بلوکی است. روش‌های سنتی که بر ثبت مستقیم تراکنش‌ها بر روی زنجیره اصلی تکیه دارند، با محدودیت‌هایی جدی در زمینه سرعت و هزینه مواجه هستند. این پژوهش برای غلبه بر این چالش‌ها، یک مدل جامع مبتنی بر کانال‌های پرداخت را با معماری سرویس‌گرای بهینه برای بازی‌های دیجیتال ارائه کرد. این مدل با انتقال تراکنش‌ها به خارج از زنجیره و افزودن سازوکارهای امنیتی مانند حل خودکار اختلافات و مدیریت وثیقه، راهکاری عملی و کارآمد فراهم می‌آورد. نتایج تجربی نشان داد که سیستم پیشنهادی در مقایسه با روش‌های پایه، بهبود چشمگیری در عملکرد دارد. زمان تراکنش به‌طور میانگین به ۱/۲ ثانیه کاهش یافت و هزینه کارمزد گس نیز بیش از ۵۰ درصد بهینه شد. این دستاوردها نشان می‌دهد که مدل پیشنهادی می‌تواند نقشی کلیدی در کاهش هزینه‌های عملیاتی و افزایش کیفیت سرویس در بازی‌های زنجیره بلوکی ایفا کند. انتخاب مدل رگرسیون خطی برای بهینه‌سازی کارمزدها، یک انتخاب آگاهانه برای این مرحله از پژوهش بود که بر اساس چهار مزیت کلیدی صورت گرفت که اولین بخش

آن، تفسیرپذیری است که مدل خطی یک رابطه شفاف و قابل درک میان متغیرهای ورودی (مانند تعداد تراکنش و مدت زمان) و هزینه نهایی ارائه می‌دهد. همچنین، این مدل بسیار سبک است و سربار محاسباتی ناچیزی در یک سیستم بیدرنگ ایجاد می‌کند. مزیت بعدی تناسب با داده‌ها است که روابط اصلی هزینه در این سناریو به خوبی توسط یک مدل خطی قابل تقریب هستند. برای کارهای آتی، پیشنهاد می‌شود پژوهش در مسیرهای زیر گسترش یابد:

۱. استفاده از مدل‌های یادگیری ماشین: می‌توان از مدل‌های یادگیری عمیق برای پیش‌بینی پویای کارمزدها و زمان بهینه برای باز و بسته کردن کانال‌ها استفاده کرد.
۲. پیاده‌سازی در محیط واقعی: آزمایش مدل در یک بازی واقعی با حجم بالای کاربران برای ارزیابی عملکرد در مقیاس بزرگ.
۳. طراحی سازوکارهای تشویقی: افزودن سیستم‌های پاداش‌دهی برای تشویق کاربران به استفاده بهینه از کانال‌ها.

اگرچه این پژوهش بر بهینه‌سازی مدل برای معماری ستاره‌ای متمرکز است که ساختار رایج در بازی‌های برخط است، معماری نرم‌افزاری پیشنهادی قابلیت تعمیم‌پذیری دارد. مدل ارائه شده بر پایه یک معماری سرویس‌گرا بنا شده است که مؤلفه‌های اصلی آن مانند مدیریت کانال، حل اختلافات و مدیریت وثیقه را از یکدیگر مستقل می‌کند. در یک معماری غیرمتمرکزتر مانند مش، نقش گره مرکزی می‌تواند توسط چندین گره هماهنگ‌کننده توزیع شود. در حالی که منطق مسیریابی تراکنش‌ها تغییر خواهد کرد، هسته اصلی نوآوری ارائه شده- یعنی قراردادهای هوشمند روی زنجیره بلوکی برای تضمین تسویه نهایی، حل اختلاف خودکار، و مدیریت وثیقه- مستقل از همبندی شبکه عمل می‌کند و در سایر معماری‌ها نیز قابل پیاده‌سازی است. ما اذعان داریم که در شرایط پویای شبکه، مدل‌های پیشرفته‌تر می‌توانند کارایی را افزایش دهند. در همین

electricity Market application,” in Proceedings of the 2019 Annual Hawaii International Conference on System Sciences, Jan-2019, Hawaii, USA, pp. 6875-6884.

[13] Gao, B., Shen, S., Shi, L. & Li, J. (2021). “Verification assisted gas reduction for smart contracts,” in Proceedings of 2021 28th Asia-Pacific Software Engineering Conference (APSEC), December -2021, Taipei, Taiwan, pp. 264-274

[14] Paduraru, C., Rares, C. & Stefanescu, A. (2022). “Enhancing the security of gaming transactions using blockchain technology,” in Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering, October 2022, Rochester, MI, USA, pp. 1-8.

[15] Arif, Y. M., Imron, M. K. A., Hanani, A., Nurhayati, H., Karami, A. F. & Hariyadi, M. A. (2024). “Blockchain as a learning tool: Analyzing transaction speeds at various gas limits in computer assembly simulations,” International Journal of Intelligent Engineering and Systems, vol. 17, no. 2, pp. 728--739, 2024.

راستا و در توسعه‌های آتی، استفاده از یادگیری عمیق برای پیش‌بینی پویای کارمزدها و بهینه‌سازی زمان باز و بسته کردن کانال‌ها در دستور کار قرار دارد.

۷- مراجع

[1] Min, T., Wang, H., Guo, T., & Cai, W. (2019). “Blockchain games: A survey,” in Proceedings of the 2019 IEEE Conference on Games (CoG), August-2019, London, UK, pp. 1-8.

[2] Avarikioti, Z., Lizurej, T., Michalak, T. & Yeo, M. (2023). “Lightning creation games,” in Proceedings of IEEE 43rd International Conference on Distributed Computing Systems (ICDCS), July-2023, Hong Kong, Hong Kong, pp. 1-11.

[3] Papadis, N., & Tassiulas, L. (2020). “Blockchain-based payment channel networks: Challenges and recent advances,” IEEE Access, vol. 8, pp. 227596--227609.

[4] Ru, H., Shiqin, Z., Zhihao, W., Jiajia, Sh., Wei, Ch., Tao, H., Shuo, W., Richard, Y.F. & Yunjie, L. (2020). “A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges,” IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 88-122.

[5] Far, S.B., Rad, A.I., & Asaar, M.R. (2023). “Blockchain and its derived technologies shape the future generation of digital businesses: a focus on decentralized finance and the Metaverse,” Data Science and Management, vol. 6, no. 3, pp. 183-197.

[6] Khanzada, T. J., Shahid, M. F., Mutahhar, A. & Aslam, M. A. (2023). “Authenticity, and Approval Framework for Bus Transportation Based on Blockchain 2.0 Technology,” Applied Sciences, vol. 13, no. 20, p. 11323.

[7] Baker, S. A., & Nori, A. S. (2023). “A secure proof of work to enhance scalability and transaction speed in blockchain technology for IoT,” in Proceedings of the 2023 AIP Conference Proceedings, Jul 2023, Cimadur, Bayah, Banten, Indonesia.

[8] Suat, M., Enes, E. & Kemal, A. (2021). “Improving transaction success rate in cryptocurrency payment channel networks,” Computer Communications, vol. 166, pp. 196-207.

[9] Fangxiao, L., Xingya, W., & Zixin, L. (2020). “Effective gas price prediction for carrying out economical ethereum transaction,” in Proceedings of the 2019 6th International Conference on Dependable Systems and Their Applications (DSA), January 2020, Harbin, China, pp. 329-334.

[10] Farokhnia, S., & Kafshdar Goharshady, A. (2023). “Reducing the gas usage of Ethereum smart contracts without a sidechain,” in Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), May-2023, Dubai, United Arab Emirates, pp. 1-3.

[11] Lee, S., Gee, E. & Lee, J. (2024). “Implementation Study of Cost-Effective Verification for Pietrzak’s Verifiable Delay Function in Ethereum Smart Contracts,” arXiv preprint, 2024.

[12] Jussi, H., Jur, M., Kari, S. & Timo, S. (2019). “Skimping on gas--reducing ethereum transaction costs in a blockchain