7th International Conference on Web Research
May 19-20, 2021; Tehran, IRAN ICWR2021

Improving The Performance of Blockchain-Based Recommender Systems

Sahar Bahrampour[1], Zahra Movahedi[2,*], Amir Hossein Kayhanipour[2]

[1]Master student in Information Technology Engineering,
Department of Computer Engineering, School of Engineering, College of Farabi, University of Tehran, Iran
sahar.bahrampour@ut.ac.ir

[2] Assistant Professor,
Department of Computer Engineering, Faculty of Engineering, College of Farabi, University of Tehran, Iran
{zmovahedi, keyhanipour}@ut.ac.ir

Abstract

Blockchain has recently raised significant attention among many scientists as a promising technology in the field of distributed systems. The main properties of blockchain that make it popular are decentralization, transparency, and immutability. The novelty of blockchain technology poses many challenges in this area. One of these challenges is managing data in blockchain and providing data that is appropriate to the user's interests. This challenge in current centralized systems is addressed through recommender systems. Implementing recommender systems within smart contracts increases transaction costs and inaccurate recommendations due to the lack of complex computational capabilities of machine learning algorithms in smart contract programming languages.

This paper proposes a method to improve data-based blockchain recommendation systems. In this method, data is stored in a blockchain structure that is defined in smart contract. This data is then provided to recommender system out of blockchain through the public key of the smart contract to be processed for providing the appropriate recommendations to the user. The results are then stored in blockchain through a transaction to be presented to the user. The results of the present study and comparison with previous works show that performing complex off-chain calculations reduces the transaction cost in terms of Gas consumption for the smart contract deployment as well as the execution of recommendation function defined in smart contract. In consequence, we can achieve more scalability in blockchain-based recommender systems.

Keywords: Blockchain, Business Process Management, Smart Contracts, Recommender System

7th International Conference on Web Research
May 19-20, 2021; Tehran, IRAN ICWR2021

بهبود عملکرد سیستم‌های توصیه‌گر مبتنی بر تکنولوژی بلاک‌چین

سحر بهرام‌پور[۱]، زهرا موحدی[۲,*]، امیر حسین کیهانی‌پور[۲]

[۱] دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، گروه مهندسی کامپیوتر، دانشکده‌ی مهندسی، پردیس فارابی، دانشگاه تهران
Sahar.bahrampour@ut.ac.com

[۲] استادیار، گروه مهندسی کامپیوتر، دانشکده‌ی مهندسی، پردیس فارابی، دانشگاه تهران
{zmovahedi, keyhanipour}@ut.ac.ir

چکیده

تکنولوژی بلاک‌چین در سال‌های اخیر، به عنوان یک فناوری امیدوارکننده در زمینه‌ی سیستم‌های توزیع‌شده، مورد توجه بسیاری از دانشمندان قرار گرفته است. این امر با ویژگی‌های بلاک‌چین مانند شفافیت و تغییرناپذیری امکان‌پذیر شده است. جدید بودن تکنولوژی بلاک‌چین باعث چالش‌های بسیاری در این زمینه است. یکی از این چالش‌ها مدیریت داده‌ها در بلاک‌چین و ارائه داده مناسب با علایق کاربر می‌باشد. این چالش در سیستم‌های متمرکز کنونی از طریق سیستم‌های توصیه‌گر برطرف می‌شود. پیاده‌سازی سیستم‌های توصیه‌گر در قراردادهای هوشمند بلاک‌چین علاوه بر بالا بردن هزینه تراکنش، موجب دقیق نبودن توصیه‌ها به دلیل عدم امکانات محاسبه پیچیده الگوریتم‌های یادگیری ماشین در زبان‌های برنامه‌نویسی قراردادهای هوشمند می‌شود.

در این مقاله، روشی برای بهبود سیستم‌های توصیه‌گر مبتنی بر داده‌های بلاک‌چین ارائه شده است. در این روش، داده‌ها بر اساس ساختاری در بلاک‌چین ذخیره می‌شوند که در قرارداد هوشمند تعریف شده است. این داده‌ها از طریق کلید عمومی قرارداد هوشمند در اختیار سیستم توصیه‌گر خارج از زنجیره قرار می‌گیرند تا پردازش لازم برای ارائه توصیه مناسب به کاربر انجام گیرد. سپس نتایج طی یک تراکنش در بلاک‌چین ذخیره می‌شود تا به کاربر ارائه شود. نتایج به‌دست‌آمده از تحقیق پیش رو و مقایسه با کارهای پیشین نشان می‌دهد که انجام محاسبات پیچیده خارج از زنجیره، علاوه بر کاهش هزینه تراکنش استقرار قرارداد هوشمند، موجب کاهش هزینه تراکنش مرتبط با توصیه‌گر در سیستم پیشنهادی از نظر گس مصرفی می‌شود، که حاصل آن افزایش مقیاس‌پذیری است.

کلمات کلیدی

مدیریت فرآیندهای کسب‌وکار، بلاک‌چین، قراردادهای هوشمند، سیستم‌های توصیه‌گر

۱- مقدمه

در سال‌های اخیر، تکنولوژی بلاک‌چین به یکی از مهمترین تحولات در دنیای دیجیتال امروزی تبدیل شده است. بلاک‌چین زنجیره‌ای از بلاک‌هاست که لیست کاملی از تراکنش‌های انجام شده را در بدنه خود دارد. بعضی از این تراکنش‌ها مالی و بعضی دیگر تنها کار ثبت داده را انجام می‌دهند. هر بلاک در بلاک‌چین شامل هدر و بدنه است و هش بلاک قبلی (بلاک والد) را در خود ذخیره می‌کند. اولین بلاک در زنجیره بلاک‌ها، بلاک مولد نام دارد که والدی ندارد. یکی دیگر از امکاناتی که بلاک‌چین ارائه می‌دهد، استقرار قراردادهای هوشمند است[1]. قراردادهای هوشمند، کدهایی هستند که توافق

نامه‌های قراردادی دنیای واقعی را در حوزه سایبر رمزگذاری و رمزگشایی می‌کنند. در واقع، قرارداد هوشمند، یک شکل دیجیتالی از قرارداد حقوقی سنتی است که شامل مجموعه‌ای از پروتکل‌ها می‌باشد که با استفاده از یک کلید عمومی در دسترس عموم قرار دارد. این قراردادها توسط شرکت‌کنندگان در بلاک‌چین قابل استفاده می‌باشند و قبل از پیاده‌سازی قرارداد هوشمند، شرکت‌کنندگان آن باید در مورد پروتکل استفاده شده به توافق برسند، زیرا بعد از پیاده‌سازی دیگر قادر به تغییر قوانین تعریف شده نیستند. در دسترس بودن کد قرارداد هوشمند با استفاده از کلید عمومی در بلاک‌چین، موجب تغییر ناپذیری و در نتیجه ایجاد اعتماد در افراد شرکت‌کننده می‌شود و اجرای خودکار این قرارداد نیاز به شخص ثالث را از بین می‌برد. برای مثال فرض کنید که چند سازمان جهت خرید و فروش محصولی با هم همکاری دارند. توافق‌ها و قوانین موجود بین این سازمان‌ها از طریق کدهای قرارداد هوشمند در بلاک‌چین وارد می‌شود و تمام داده‌ها و تراکنش‌های مربوط به محصول، به صورت شفاف و تغییرناپذیر، در دسترس تمام سازمان‌های مرتبط قرار می‌گیرد. از این رو امکان دستکاری در داده‌ها وجود ندارد و در صورت برزو مشکل میان سازمان‌ها، با بررسی لیست تراکنش‌ها می‌توان عامل خطا را شناسایی کرد[5]–[2].

چالش‌های زیادی در بلاک‌چین مورد توجه است. یکی از این چالش‌ها مدیریت و بازیابی داده‌ها بعد از پیاده‌سازی قرارداد هوشمند می‌باشد. در بلاک‌چین تمام داده‌های مربوط به قراردادها و تراکنش‌ها ذخیره می‌شوند؛ در این میان پیدا کردن اطلاعات مناسب مثلا خرید یک محصول متناسب باعلاقه‌ی کاربر، کاری دشوار خواهد بود. در سیستم‌های جا افتاده امروزی برای این که کاربر بتواند اطلاعات مورد علاقه خود را پیدا کند از سیستم‌های توصیه‌گر[6] اغلب متمرکز استفاده می‌شود[7]. در این سیستم‌ها، یک مرجع مرکزی وجود دارد که کلیه‌ی اطلاعات و داده‌های کاربران را در اختیار داشته و با استفاده از الگوریتم‌های مختلف هوش مصنوعی، اقدام به توصیه به کاربران می‌کند. برای مثال سیستم‌های توصیه‌گر فیلتر مشارکتی مبتنی بر شباهت کاربران، از طریق شباهت سنجی بین سوابق کاربران، کاربران شبیه به هم را پیدا کرده و علایق آن‌ها را به هم توصیه می‌کنند. این شباهت از روش‌های مختلفی مثل ضریب همبستگی پیرسون (که بین یک و منفی یک است) محاسبه می‌شود و همبستگی کاربران در یک ماتریس تشابه ذخیره می‌شود و هر چه کاربران به هم شبیه‌تر باشند مولفه تشابه آن‌ها به یک نزدیک‌تر است.

در سیستم‌های توصیه‌گر متمرکز، کاربر فقط نتیجه را دریافت می‌کند و از داده‌ها و توابع استفاده شده برای ارائه این پیشنهادات مطلع نیست؛ بنابراین درجه اعتماد کاربر به پیشنهادات ارائه شده از طریق سازمان‌های مختلف کم است. در همین راستا، توسعه‌ی سیستم‌های توصیه‌گر با استفاده از داده‌های بلاک‌چین، اعتماد را به داده‌های متناسب با سلایق کاربران حین دریافت توصیه برمی‌گرداند[7]. در این پژوهش هدف، ارائه راه‌حلی کارآمد با استفاده از قراردادهای هوشمند در DApp® های مورد استفاده برای کسب‌وکارهاست. در این روش، سیستم توصیه‌گر توزیعی مبتنی بر داده‌های به‌دست آمده از تراکنش‌های بین سازمان‌ها تحت یک قرارداد هوشمند در بستر بلاک‌چین، پیشنهاد شده‌است، تا بتوان به کاربران محصولات مناسب با علایق آن‌ها پیشنهاد کرد. در این سیستم با توجه به این که تمامی توابع و داده‌های استفاده شده توسط کاربر در دسترس هستند، کاملا شفاف بوده و توصیه‌ها دقیقی را به کاربر ارائه می‌دهد. علاوه بر این کاربران می‌توانند به آن اعتماد داشته باشند، زیرا می‌دانند که این پیشنهادات بر اساس چه داده‌ها و توابعی به آن‌ها ارائه شده است. همچنین داده‌ها و توابع رتبه‌دهی غیر قابل دستکاری بوده و از طریق نهاد خاصی کنترل نمی‌شوند. برای رسیدن به این هدف، قرارداد هوشمند پس از استقرار در شبکه بلاک‌چین در دسترس رابط کاربری و سیستم توصیه‌گر قرار می‌گیرد. رابط کاربری با اتصال به قرارداد هوشمند طی تراکنش‌هایی داده‌های وارد شده از طریق کاربران را در ساختارهای تعریف شده توسط قرارداد روی بلاک‌چین ذخیره می‌کند. در ادامه داده‌های ذخیره شده در بلاک‌چین توسط سیستم توصیه‌گر استخراج شده و پس از پردازش لازم، نتایج طی یک تراکنش در بلاک‌چین ذخیره می‌شود، تا در رابط کاربری نمایش داده شود. نتایج پیاده‌سازی با روش‌های مشابه مقایسه و ارزیابی شده است.

ساختار مقاله به‌این صورت است: در بخش دوم، ادبیات کارهای انجام شده بررسی می‌شود. توصیف روش پیشنهادی در بخش سوم آورده شده است. بخش چهارم، پیاده‌سازی روش پیشنهادی و ارزیابی نتایج آن و مقایسه با کارهای پیشین می‌باشد. در بخش پنجم، نتیجه‌گیری و کارهای آینده مورد بحث قرار گرفته است.

۲- مرور ادبیات

امروزه، بلاک‌چین در حوزه‌های مختلفی مانند اینترنت اشیا[8]، زنجیره تامین[9]، مدیریت فرآیندهای کسب‌وکار[5]، محاسبات ابری[10] و غیره کاربرد دارد. با گسترش استفاده از تکنولوژی بلاک‌چین و قراردادهای هوشمند تحقیقات بسیاری در زمینه مفاهیم و چالش‌های موجود ارائه شد. یکی از مهم‌ترین تحقیقات در این زمینه مقاله ژنگ و همکارانش[1] است. آن‌ها در تحقیق خود به بررسی دقیق مفاهیم بلاک‌چین پرداختند و چالش‌های موجود در این زمینه را بررسی کردند. لی و همکارانش[11] بررسی سیستماتیک در زمینه مسائل امنیتی بلاک‌چین و حفظ حریم خصوصی در آن انجام دادند. ژنگ و همکارانش در تحقیقی دیگر[3]، به بررسی قراردادهای هوشمند، پلتفرم‌های مورد استفاده و چالش‌های آن پرداختند.

ادغام سیستم‌های توصیه‌گر و بلاک‌چین موضوع جدیدی است که در سال‌های اخیر مورد توجه محققان قرار گرفته است. لیسی و همکارانش[7] در سال ۲۰۱۹ روشی را برای ساخت سیستم توصیه‌گر مبتنی بر بلاک‌چین ارائه دادند، که استراتژی امتیازدهی شفاف و غیرمتمرکز را به کاربران ارائه می‌دهد. در سیستم آن‌ها، هیچ مرجع مرکزی برای نظارت وجود ندارد. آن‌ها چارچوبی را در این زمینه پیشنهاد دادند که سیستم توصیه‌گر ویژگی‌های بلاک‌چین مانند شفافیت، عمومی، ضد دستکاری و ماندگاری را به ارث می‌برد. آن‌ها

برای ایجاد سیستم خود از چندین قرارداد هوشمند به زبان Solidity استفاده می‌کنند، و آن را تحت یوزکیس رتبه‌دهی محصولات در شبکه آزمایشی Ropsten اتریوم مستقر کردند. در این مدل از توابع ریاضی ساده در قرارداد هوشمند، یعنی میانگین وزنی و روش‌های میانگین ساده، برای به دست آوردن رتبه توصیه شده برای یک آیتم استفاده می‌شود، که به توصیه‌های نادرست منجر خواهد شد. منظور از توصیه نادرست این است که سیستم توصیه‌گر بارها مورد مشابه را برای همه کاربران توصیه می‌کند. همچنین ممکن است به دلیل بررسی‌های منفی گسترده و فروش هدف از شرکت‌های رقابتی، این امتیازات جعلی باشد، در ضمن ظرفیت سیستم آن‌ها تنها ۴۰۰۰ رکورد داده رتبه‌بندی به دلیل محدودیت گس تخمین زده شده است.

یه و همکارانش[12] برای غلبه بر معایب کار لیسی و همکارانش، الگوریتم توصیه‌گر مشارکتی را با استفاده از فناوری بلاکچین توسعه دادند. برای محاسبه امتیاز توصیه شده برای آیتم‌ها از ماتریس تشابه در قرارداد هوشمند استفاده کردند. این ماتریس، شباهت رابطه بین هر کاربر را نشان می‌دهد، به گونه‌ای که شباهت بالاتر منجر به تأثیر قابل توجهی در امتیازات توصیه می‌شود. سیستم رتبه‌بندی پیشنهادی آن‌ها، براساس مشخصات کاربر در مورد آیتم‌ها مناسب‌ترین توصیه را به کاربران ارائه می‌دهد. در روش پیشنهادی آن‌ها اولویت‌های هر کاربر در نظر گرفته و بهترین پیشنهاد به او ارائه می‌شود. این سیستم آدرس‌های جدید بلاک‌چین را محاسبه می‌کند، اعلان‌هایی را برای شرکت ارسال می‌کند، به طور خودکار از فیلتر مشارکتی برای پردازش داده‌ها برای ارائه توصیه استفاده می‌کند و در نهایت تجسم توصیه‌ها توسط کاربر و سازمان بهبود می‌یابد. همچنین این روش اجازه می‌دهد تا کل جنبه مشخصات مشتری از امنیت بیشتری برخوردار باشد. همچنین، این امکان را برای مصرف‌کنندگان فراهم می‌کند تا به صورت ناشناس فعالیت کنند، این محرمانه بودن با بلاکچین تضمین می‌شود. یه وهمکارنش نتایج ارزیابی خود را بر روی دیتاست Movielens و Netflix ارائه کردند، لازم به ذکر است که آن‌ها به دلیل محدودیت گس در قراردادهای هوشمند به زبان Solidity روی بلاکچین اتریوم، دیتاست‌ها را برای ۱۰ کاربر و فقط ۲۰۰ فیلم فیلتر کردند. با بررسی نتایج آن‌ها می توان دریافت، به دلیل استفاده از ماتریس تشابه در داخل قرارداد هزینه پیاده‌سازی و اجرای قرارداد آن‌ها بالاست. با این که آن‌ها از محاسبات خارج از زنجیره بلاک‌چین نیز استفاده کرده‌اند ولی نتیجه‌ای که در ارزیابی آن‌ها به دست آمده است هنوز بالاتر از نتیجه کار لیسی و همکارانش است. این افزایش هزینه منجر شد، سیستم آن‌ها نتواند مقیاس‌پذیری خوبی داشته باشد.

دو روش قبل به دلیل دقیق نبودن، هزینه بالا و مقیاس‌پذیری کم، کارا نیستند. هدف این مقاله، ارائه روشی است که با کاهش هزینه تراکنش‌ها مقیاس‌پذیری سیستم را بالا ببرد، علاوه بر آن بتواند توصیه مناسبی را به کاربر ارائه دهد. جدول (۱)، خلاصه‌ای از مقایسه رویکرد پیشنهادی با دو رویکرد مشابه می‌باشد.

جدول (۱) : مقایسه دو رویکرد ارائه شده سیستم توصیه‌گر در بلاک‌چین با روش پیشنهادی

محقق	لیسی و همکاران[7]	یه و همکاران [12]	روش پیشنهادی
روش توصیه‌گر	استفاده از میانگین رتبه‌ها و میانگین وزن رتبه‌ها	استفاده از پالایش مشارکتی و ایجاد ماتریس تشابه در قرارداد هوشمند	استفاده از توصیه‌گر مشارکتی خارج از زنجیره و استفاده از داده‌های بلاک‌چین
یوزکیس استفاده شده	امتیاز دهی محصولات	امتیاز دهی فیلم	فروش فیلم
دیتاست	ذکر نشده	MovieLen و Netflix	MovieLen
مقیاس‌پذیری	حداکثر ۴۰۰۰ رکورد	۱۰ کاربر، ۲۰۰ فیلم	۲۰۰ کاربر، ۱۰۰۰ فیلم، ۹۱۰۲ رکورد رتبه‌دهی
قرارداد هوشمند	Solidity	Solidity	Solidity
بلاک‌چین	اتریوم	اتریوم	اتریوم
مزایا	تمام پروسه‌ها در قرارداد پیاده‌سازی شده است	توصیه‌های دقیق‌تر از روش قبل برای کاربر	کاهش هزینه و افزایش مقیاس‌پذیری نسبت به روش‌های قبل
معایب	توصیه‌های نادرست به‌علت استفاده از توابع محاسباتی ساده	هزینه‌ی بالا به‌علت استفاده از ماتریس تشابه داخل زنجیره	نمایش تنها یک رکورد برتر در رابط کاربری

۳- روش پیشنهادی

در این بخش، معماری سیستم پیشنهادی توصیف شده است. همانطور که در شکل (۱) نشان داده شده، سیستم پیشنهادی دارای بخش‌های زیر می‌باشد:

۱- بلاک‌چین: قراردادهای هوشمند تعریف شده در این قسمت روی بلاک‌چین مستقر می‌شوند.

۲- رابط کاربری: با اتصال به قرارداد هوشمند، کاربر می‌تواند با بلاک‌چین به ارسال و دریافت داده بپردازد. این داده‌ها تحت ساختارهایی که در قرارداد هوشمند تعریف شده است در بلاک‌چین ذخیره و در دسترس عموم قرار می‌گیرند.

۳- سیستم‌های توصیه‌گر: داده‌های ذخیره شده در قرارداد هوشمند را برای توصیه مناسب در خارج از بلاک‌چین پردازش کرده و نتایج را طی یک تراکنش در ساختار تعریف شده در بلاک‌چین ذخیره می‌کند تا برای کاربر نمایش داده شود.

در روش پیشنهادی، از یک سیستم توصیه‌گر مشارکتی مبتنی بر مدل و داده‌های بلاک‌چین استفاده شده است. در این روش سیستم رتبه‌دهی بر اساس قرارداد هوشمند ایجاد شده و داده‌های رتبه‌دهی، به خارج از زنجیره

بلاک‌چین منتقل می‌شود، تا محاسبات پیچیده سیستم توصیه‌گر روی آن انجام شود. در آخر پس از پایان پردازش توصیه‌گر، نتایج توصیه در قالب یک تراکنش در بلاک‌چین می‌شود. این تراکنش، اجرای یک تابع در قرارداد هوشمند است. در آخر، نتایج در رابط کاربری نمایش داده می‌شود.

در بخش سیستم‌های توصیه‌گر از روش پالایش مشارکتی مبتنی بر مدل و الگوریتم SVD برای پیش‌بینی محصولات مورد علاقه کاربر فعال استفاده شده است. در روش پالایش مشارکتی از ماتریسی تحت عنوان ماتریس رتبه‌دهی به عنوان ورودی توصیه‌گر استفاده می‌شود. این ماتریس یک ماتریس عددی شامل امتیازات هر کاربر به هر آیتم است. عدد صفر در این ماتریس نمایانگر این است، کاربر، آیتم را مشاهده نکرده است. این ماتریس، یک ماتریس تنک است، زیرا کاربر بسیاری از آیتم‌ها را مشاهده نکرده است. در سیستم‌توصیه‌گر رتبه‌بندی آیتم‌های دیده نشده توسط کاربر با استفاده از الگوریتم‌های مختلف یادگیری ماشین مانند SVD پیش‌بینی می‌شود. از نظر ریاضی SVD روشی است که یک ماتریس را به سه ماتریس تجزیه می‌کند که حاصل ضرب آن‌ها همان ماتریس اولیه خواهد بود. برای مثال ماتریس A را می‌توان به صورت فرمول (۱) تجزیه کرد:

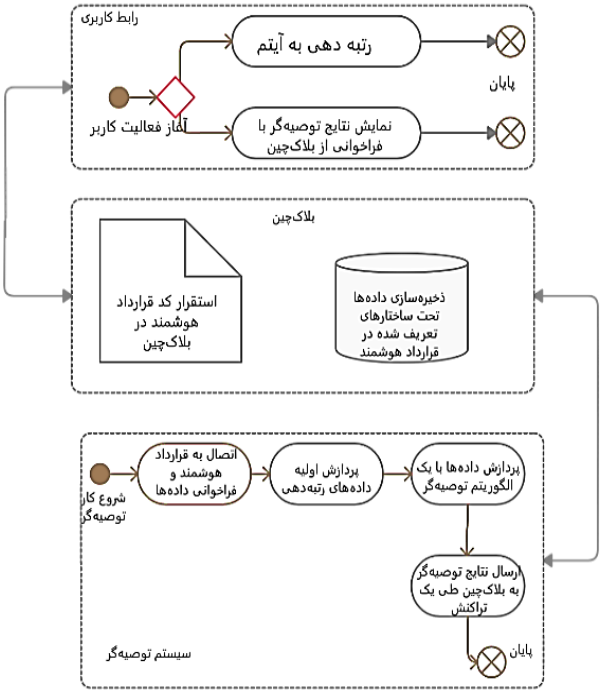
$$SVD(A) = USV^T \qquad (۱)$$

که در اینجا A یک ماتریس $m \times n$، ماتریس S یک ماتریس قطری است که فقط r ورودی غیر صفر دارد، که ابعاد موثر این سه ماتریس U، S و V را به ترتیب m × r، r × r و r × n می سازد. U و V دو ماتریس متعامد و S ماتریسی قطری است که ماتریس مقادیر منفرد نامیده می‌شود که در فرمول (۲) نشان داده شده است.

$$\begin{bmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mn} \end{bmatrix}_{m\times n} = \begin{bmatrix} u_{11} & \cdots & u_{1r} \\ \vdots & \ddots & \vdots \\ u_{m1} & \cdots & u_{mr} \end{bmatrix}_{m\times r} \qquad (۲)$$

$$\times \begin{bmatrix} s_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & s_{rr} \end{bmatrix}_{r\times r} \times \begin{bmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{r1} & \cdots & v_{rn} \end{bmatrix}_{r\times n}$$

ورودی‌های ماتریس قطری S $(s_1, s_2, \dots, s_r)$ به صورت $s_i > 0$ و $s_1 \geq s_2 \geq \cdots \geq s_r$ هستند. r ستون اول U و V به ترتیب بردارهای ویژه متعامد مرتبط با r ارزش غیر صفر AA^T و A^TA را نشان می‌دهند. به عبارت دیگر، r ستون U مقادیر منفرد غیر صفر در



شکل(۱): معماری سیستم پیشنهادی

فضای ستونی و r ستون V فضای سطری ماتریس A را در بر می‌گیرد. به U و V به ترتیب بردارهای منفرد چپ و راست نامیده می‌شوند. SVD بهترین تقریب خطی با رتبه کم از ماتریس اصلی A را ارائه می دهد. این ویژگی از طریق نگه داشتن مقادیر منفرد $k \ll r$ با حذف مقادیر دیگر امکان پذیر می‌شود. این ماتریس جدید که مقادیر آن کاهش یافته است، S_k نامیده می‌شود. در اینجا r تعداد اولیه عناصر غیر صفر و ابعاد S و k فاکتور کاهش ابعاد است. به خاطر این که ورودی‌های S به صورت $s_1 \geq s_2 \geq \cdots \geq s_k$ ذخیره می‌شوند، فرآیند کاهش با حفظ k اولین مقادیر منفرد انجام می‌شود. ماتریس‌های U و V نیز با کاهش مقادیر به ترتیب به ماتریس‌های U_k و V_k تبدیل می‌شوند. بنابراین برای تولید پیش‌بینی با استفاده از SVD، ابتدا ماتریس رتبه‌بندی A با ابعاد $m \times n$ تجزیه و با توجه به سه ماتریس مولفه SVD، U_k، S_k و V_k با k ویژگی کاهش می‌یابد، که حاصلضرب آن یک تخمین ثانویه از ماتریس رتبه‌دهی A است. سپس پیش‌بینی را می‌توان از طریق محاسبه شباهت از روش‌های مختلفی مانند cosine (ضرب نقطه‌ای) میان m شبه مشتری $U_k.\sqrt{S_k}^T$ و n شبه محصول $\sqrt{S_k}V_k^T$ انجام داد. در کل، پیش‌بینی امتیاز $P_{i,j}$ برای iامین مشتری و jامین محصول با اضافه کردن میانگین رتبه‌بندی‌های انجام شده توسط کاربر i $(\overline{r_i})$ و شباهت تولید می‌شود و فرمول آن به صورت فرمول (۳) خواهد بود:

$$P_{i,j} = \overline{r_i} + U_k.\sqrt{S_k}^T(i).\sqrt{S_k}V_k^T(j) \quad (۳)$$

هنگامی که تجزیه SVD انجام شد، فرایند تولید پیش بینی فقط شامل یک محاسبه ضرب نقطه‌ای است که پیچیدگی زمانی آن O(1) است، زیرا k یک ثابت است. در آخر از میان رتبه‌های پیش‌بینی شده، آیتم‌های که رتبه بالایی دارند به کاربر توصیه می‌شوند[13].

٤- ارزیابی و نتایج

برای پیاده‌سازی و ارزیابی روش پیشنهادی، شبکه‌آزمایشی عمومی اتریوم[14] به نام Rinkeby و شبکه‌آزمایشی شخصی Ganache به کار رفته است. از شبکه Ganache به دلیل محدود بودن تعداد کاربران برای آزمایش‌های اولیه و از شبکه Rinkeby برای آزمایش‌ها در مقیاس بزرگ‌تر استفاده شده است. همچنین از زبان solidity برای نوشتن قرارداد هوشمند، از ابزار Truffle برای کامپایل قرارداد هوشمند در محیط ویندوز، از remix IDE برای استقرار قرارداد روی شبکه Rinkeby و کیف پول MetaMask برای مدیریت حساب‌ها استفاده شده است. در این پژوهش، از دیتاست MovieLen برای آزمایش عملکرد سیستم استفاده و تاکنون داده‌های رتبه‌دهی ۲۰۰ کاربر برای ۱۰۰۰ فیلم وارد شده است. در نتیجه ۱۰۰۰ رکورد برای فیلم‌ها و حدود ۹۱۰۲ رکورد برای رتبه‌دهی و نتایج توصیه‌گر نیز برای ۲۰۰ کاربر در آن ذخیره شده است، ولی تاکنون قرارداد هوشمند به محدودیت گس خود نرسیده و همچنان کاربر قابلیت انجام تراکنش با آن را داراست. در این سیستم با توجه به این‌که داده‌ها در بستر بلاک‌چین و تنها با کد هش کاربران ذخیره شده‌اند، حریم خصوصی کاربران به خوبی حفظ شده است. علاوه بر این توصیه‌گر می‌تواند با بروزرسانی اطلاعات در بستر بلاک‌چین بروز شده و توصیه‌های بهتری با افزایش داده‌ها در طول زمان انجام دهد. در این سیستم برای کاهش هزینه، با وجود این‌که سیستم توصیه‌گر قابلیت پیش‌بینی n آیتم برتر را دارد، تنها گزینه اول به کاربر در رابط کاربری نمایش داده می‌شود. در اینجا منظور از هزینه، هزینه‌ی هر تراکنش با توجه به اتر و گس مصرفی است، که در ادامه مفاهیم آن ذکر شده است.

در شبکه اتریوم در ازای اجرای تراکنش‌ها باید هزینه پرداخت شود. این هزینه به صورت گس[15] پرداخت می‌شود. در واقع گس، سوخت اتریوم برای انجام تراکنش‌ها می‌باشد. برای تراکنش استقرار قراردادهای هوشمند در شبکه، مقدار گس پرداختی بستگی به حجم برنامه و داده‌های ذخیره شده دارد. برای تراکنش اجرای تابع‌های درون قرارداد هوشمند، مقدار گس پرداختی بستگی به نوع عملیات و حجم داده‌های ذخیره شده به وسیله تابع دارد. گس قیمت واحد ندارد، در واقع قیمت گس با پیشنهاد فرستنده تراکنش بر حسب اتر مشخص می‌شود. سرعت انجام تراکنش با قیمت گس نسبت مستقیم دارد، یعنی با افزایش قیمت گس، سرعت انجام تراکنش نیز بالا می‌رود. مقدار گس هر تراکنش در نهایت به عنوان پاداش ماینینگ به حساب صاحب ماینر تراکنش ارسال می‌شود. کوچکترین مقیاس اندازه‌گیری در شبکه اتریوم وِی نام دارد که برای تبدیل اتر به وی می‌توان از فرمول (۴) استفاده کرد:

$$1\ Ether = 10^{18}\ \text{Wei} \quad (۴)$$

حداقل مقداری که می‌توان برای گس در نظر گرفت درفرمول (۵) نشان داده شده است:

$$1\ GAS \geq 1\ GWei = 10^{9}\ Wei = 10^{-9}\ Ether \quad (۵)$$

در هر تراکنش، فرستنده باید حداکثر گس مصرفی در آن تراکنش را تعیین کند، که به آن محدودیت گس گفته می‌شود. در صورت رسیدن گس مصرفی به محدودیت تعیین شده برنامه به صورت خودکار متوقف می‌شود. در بعضی از موارد تراکنش‌های برگشتی نیز گس مصرف می‌کند که این بستگی به روش برنامه‌نویسی قرارداد آن تراکنش دارد. هزینه هر تراکنش، هزینه‌ای است که با توجه به قیمت و محدودیت گس تعیین شده توسط فرستنده برای قرارداد هوشمند تغییر می‌کند[17] ,[16] ,[14]. برای مقایسه دقیق، ابتدا هزینه تراکنش استقرار قرارداد هوشمند با قیمت‌ها و محدودیت‌های گس مختلف در جدول (۲) آورده شده است و در نمودار شکل (۲) روند افزایش هزینه تراکنش استقرار با دو پارامتر محدودیت گس و هزینه گس نشان داده شده است.

هزینه تراکنش استقرار متناسب با قیمت و محدودیت گس کارهای قبلی در مقایسه با روش پیشنهادی در جدول (۳) آورده و در نمودار شکل (۳) نشان داده شده است. با توجه به نتایج، روش پیشنهادی هزینه تراکنش استقرار کمتری نسبت به روش‌های قبلی دارد در نتیجه می‌تواند با محدودیت گس مشابه از داده‌های بیشتری پشتیبانی کند. با داده‌های بیشتر و استخراج آن توسط توصیه‌گر، می‌توان به نتایج دقیق‌تری برای توصیه رسید. علاوه برای این با افزایش داده‌ها هزینه‌ی تراکنش‌های قرارداد تغییر نکرده و ثابت می‌ماند در نتیجه به محدودیت گس نمی رسد از این نظر مقیاس‌پذیری سیستم نسبت به سیستم‌های قبل که با افزایش داده به محدودیت گس می‌رسید، بالاتر است.

در طرح پیشنهادی هدف این است که هزینه تراکنش‌ها کاهش داده شود. در روش‌های قبلی به دلیل انجام محاسبات در داخل زنجیره به صورت دوره‌ای و هنگام اجرای هر بار قرارداد هوشمند، قرارداد خیلی زود به محدودیت گس تعریف شده می‌رسید و دیگر قادر به اجرا شدن نبود. در کارهای قبلی برای تعداد دفعات بیشتر اجرا محدودیت گس را بالا می‌بردند، که باعث بالا رفتن هزینه استقرار قرارداد هوشمند در بلاک‌چین می‌شد. در این پژوهش، برای رفع این مشکل و بالا بردن مقیاس‌پذیری قرارداد کلیه محاسبات پیچیده، با توجه

توابع دقیق و کتابخانه‌های پایتون در خارج از زنجیره منتقل شد. با این روش، علاوه بر کاهش هزینه‌های استقرار قرارداد، هزینه اجرا و ارائه توصیه به کاربر کاهش یافت. بنابراین در روش پیشنهادی، قرارداد هوشمند می‌تواند با محدودیت گس کمتر تعداد دفعات بیشتری اجرا شود. در جدول (۴) متوسط هزینه‌های اجرای توابع اصلی قرارداد هوشمند پیشنهادی آورده شده است.

علاوه بر همه این موارد استفاده از solidity برای نوشتن توصیه‌گر با توجه به نداشتن کتابخانه‌های مناسب و عدم پشتیبانی از داده‌های شناور، نتایج دقیقی برای توصیه‌گر به همراه ندارد. در این پژوهش از کتابخانه‌ی surprise و تابع SVD در پایتون برای ارائه سیستم توصیه‌گر استفاده شد تا توصیه مناسب به کاربر ارائه شود.

جدول(۲): هزینه تراکنش استقرار قرارداده هوشمند پیشنهادی در بلاک‌چین با محدودیت و قیمت گس مختلف

هزینه ها	محدودیت گس	هزینه گس به GWEI	هزینه هر تراکنش به اتر یا ETH
هزینه تراکنش استقرار	۲۷۶۴۲۶۲	۱	۰.۰۰۲۷۶۴
	۲۷۶۴۲۶۲	۱۵	۰.۰۴۱۴۶۴
	۲۷۶۴۲۶۲	۲۰	۰.۰۵۵۲۸۵
	۴۷۰۰۰۰۰	۱	۰.۰۰۴۷
	۴۷۰۰۰۰۰	۵	۰.۰۲۳۵
	۴۷۰۰۰۰۰	۱۵	۰.۰۷۰۵
	۴۷۰۰۰۰۰	۲۰	۰.۰۹۴
	۸۹۰۰۰۰۰	۲۰	۰.۱۷۸
	۸۹۰۰۰۰۰	۱	۰.۰۰۸۹
	۸۹۰۰۰۰۰	۱۵	۰.۱۳۳۵

جدول (۳) : مقایسه هزینه‌های استقرار قرارداد روش پیشنهادی با دو روش قبلی

روش‌ها	هزینه گس به GWei	محدودیت گس	هزینه هر تراکنش به اتر
لیسی و همکارانش	۱۵	۴۷۰۰۰۰۰	۰.۰۷۱۲
روش پیشنهادی	۱۵	۴۷۰۰۰۰۰	۰.۰۷۰۵
یه و همکارانش	۲۰	۸۹۰۰۰۰۰	۱.۲۵
روش پیشنهادی	۲۰	۸۹۰۰۰۰۰	۰.۱۷۸
روش‌ها	**هزینه گس به GWei**	**محدودیت گس**	**هزینه هر تراکنش به اتر**
لیسی و همکارانش	۱۵	۴۷۰۰۰۰۰	۰.۰۷۱۲
روش پیشنهادی	۱۵	۴۷۰۰۰۰۰	۰.۰۷۰۵
یه و همکارانش	۲۰	۸۹۰۰۰۰۰	۱.۲۵
روش پیشنهادی	۲۰	۸۹۰۰۰۰۰	۰.۱۷۸

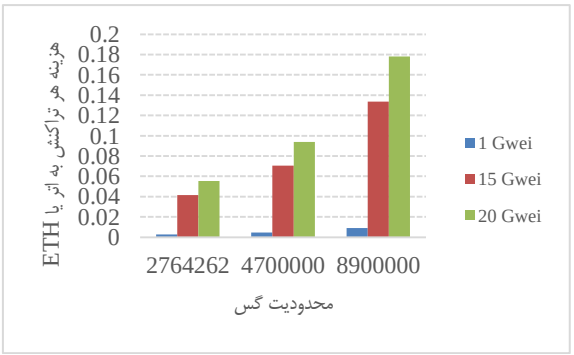
جدول(٤): متوسط هزینه‌های اجرای توابع اصلی قرارداد هوشمند

نام تابع	هزینه گس GWEI	محدودیت گس	هزینه هر تراکنش به اتر
AddMovie	۲۰	۱۳۹۱۳۱	۰.۰۰۲۷۸۳
addRate	۲۰	۳۳۸۲۸۰	۰.۰۰۶۷۶۶
Recommendation	۲۰	۱۰۹۶۱۹	۰.۰۰۲۱۹۲

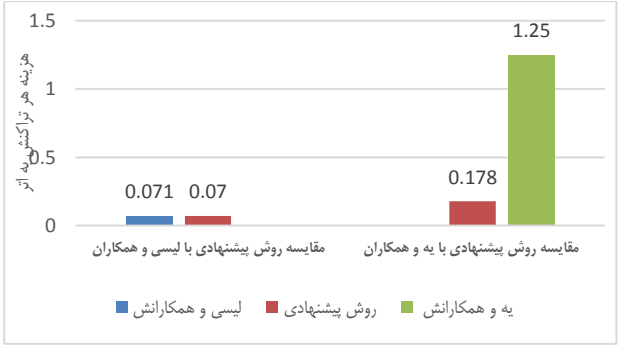
۵- نتیجه‌گیری و کارهای آینده

هدف این مقاله، افزایش امکانات استفاده از بلاک‌چین و قراردادهای هوشمند بود. برای این امر، ابتدا روش‌های موجود در این زمینه بررسی شد. با این بررسی می‌توان دریافت که اجرای الگوریتم‌ها با پیچیدگی زمانی غیر خطی موجب افزایش هزینه اجرا و خاتمه یافتن زودتر قرارداد هوشمند به دلیل محدودیت گس می‌شود. بدین منظور روشی پیشنهاد داده شد، تا با انتقال اطلاعات قرارداد به خارج از زنجیره و انجام الگوریتم SVD، توصیه مناسب برای هر کاربر را پیش‌بینی کرده و این توصیه را در قالب یک تراکنش به قرارداد منتقل کند. با ارزیابی‌های صورت گرفته، می‌توان نتیجه گرفت که روش پیشنهادی هزینه‌های اتر و گس تراکنش اجرای توابع قرارداد هوشمند را کاهش داده و باعث می‌شود قرارداد بتواند تعداد دفعات بیشتری اجرا شده و مقیاس‌پذیری بیشتری داشته باشد. علاوه بر این، از مزایای سیستم‌های توصیه‌گر موجود بهره برده و توصیه دقیق‌تری را به کاربر ارائه دهد. امروزه، بلاک‌چین در حوزه‌های مختلفی مانند اینترنت اشیا کاربرد دارد.

در کارهای آینده بررسی می‌شود که با توجه به این که سوابق هر کاربر با کد هش کاربر در بلاک‌چین در دسترس است، آیا می‌توان توصیه‌گری طراحی و



شکل(۲):نمودار هزینه‌های استقرار قرارداد هوشمند پیشنهادی در بلاک‌چین با محدودیت و قیمت گس مختلف



شکل(۳): مقایسه هزینه‌های استقرار قرارداد هوشمند روش پیشنهادی با دو روش قبل

اجرا کرد که بتواند از طریق استخراج کل سوابق تراکنش‌های کاربر از بلاک‌چین تحت قراردادهای هوشمند مشابه توصیه دقیق‌تری در اختیار کاربر قرار داد. آیا این روش می‌تواند برای مشکل شروع سرد توصیه‌گرهای پالایش مشارکتی موثر واقع شود و این که این روش تا چه حد می‌تواند مقیاس‌پذیر باشد. علاوه بر این، باید سیستم پیشنهادی را برای آسیب‌پذیری‌های موجود مورد تجزیه و تحلیل قرار داد.

مراجع

[1] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, 'Blockchain challenges and opportunities: A survey', *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] D. Macrinici, C. Cartofeanu, and S. Gao, 'Smart contract applications within blockchain technology: A systematic mapping study', *Telematics and Informatics*, vol. 35, no. 8, pp. 2337–2354, 2018.

[3] Z. Zheng *et al.*, 'An overview on smart contracts: Challenges, advances and platforms', *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.

[4] S. Dhaiouir and S. Assar, 'A systematic literature review of Blockchain-enabled smart contracts: platforms, languages, consensus, applications and choice criteria', in *International Conference on Research Challenges in Information Science held in Limassol, Cyprus*, 2020.

[5] J. A. Garcia-Garcia, N. Sánchez-Gómez, D. Lizcano, M. J. Escalona, and T. Wojdyński, 'Using blockchain to improve collaborative business process management: Systematic literature review', *IEEE Access*, vol. 8, pp. 142312–142336, 2020.

[6] J. Lu, D. Wu, M. Mao, W. Wang, and G. Zhang, 'Recommender system application developments: a survey', *Decision Support Systems*, vol. 74, pp. 12–32, 2015.

[7] A. Lisi, A. De Salve, P. Mori, and L. Ricci, 'A Smart Contract Based Recommender System', in *International Conference on the Economics of Grids, Clouds, Systems, and Services held in , Leeds, UK*, 2019.

[8] A. M. Saghiri, M. Vahdati, K. Gholizadeh, M. R. Meybodi, M. Dehghan, and H. Rashidi, 'A framework for cognitive Internet of Things based on blockchain', in *2018 4th International Conference on Web Research (ICWR)*, 2018.

[9] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, 'Blockchain technology and its relationships to sustainable supply chain management', *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[10] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, 'Blockchain for cloud exchange: A survey', *Computers & Electrical Engineering*, vol. 81, p. 106526, Jan. 2020, doi: 10.1016/j.compeleceng.2019.106526.

[11] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, 'A survey on the security of blockchain systems', *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[12] T.-Y. Yeh and R. Kashef, 'Trust-Based Collaborative Filtering Recommendation Systems on the Blockchain', *Advances in Internet of Things*, vol. 10, no. 4, pp. 37–56, 2020.

[13] D. Bokde, S. Girase, and D. Mukhopadhyay, 'Matrix factorization model in collaborative filtering algorithms: A survey', *Procedia Computer Science*, vol. 49, pp. 136–146, 2015.

[14] V. Buterin, 'A next-generation smart contract and decentralized application platform', *white paper*, vol. 3, no. 37, 2014.

[15] G. A. Pierro and H. Rocha, 'The influence factors on ethereum transaction fees', in *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB) held in Montreal, QC, Canada* , 2019.

[16] D. Vujičić, D. Jagodić, and S. Ran\djić, 'Blockchain technology, bitcoin, and Ethereum: A brief overview', in *2018 17th international symposium infoteh-jahorina (infoteh)held in Bosnia and Herzegovina*, 2018.

[17] R. Böhme, N. Christin, B. Edelman, and T. Moore, 'Bitcoin: Economics, technology, and governance', *Journal of economic Perspectives*, vol. 29, no. 2, pp. 213–38, 2015.

زیرنویس

* Decentralized application – برنامه غیر متمرکز