دوفصلنامه محاسبات و سامانه های توزیع شده
سال ششم، شماره۱، شماره پیاپی۱۱، صفحه ۱۴ تا ۴۴، سال ۱۴۰۲

سامانه‌ی ثبت بازخورد غیرمتمرکز برای اعتبارسنجی سرویس‌های غیرمتمرکز

علی عبدالعظیمی[1]، لیلی محمدخانلی[2]، پدرام صالح‌پور[3]
[1,2,3]دانشکده مهندسی برق و کامپیوتر، دانشگاه تبریز، تبریز، ایران

چکیده

کاربران اغلب قبل از استفاده از یک سرویس، بازخوردهای کاربران دیگر را برای تصمیم‌گیری بهتر درباره‌ی آن سرویس می‌خوانند. از این رو سامانه‌هایی به وجود آمده‌اند که سیستم ثبت بازخورد را در اختیار کاربران قرار می‌دهند. تکنولوژی بلاک‌چین در سال‌های اخیر مورد توجه بسیاری از افراد قرار گرفته است. این امر با ویژگی‌های بلاک‌چین مانند شفافیت، تغییرناپذیری و حذف نهادهای واسط امکان‌پذیر شده است. با گسترش سامانه‌های غیرمتمرکز زمینه‌ی کلاهبرداری نیز فراهم می‌شود. کاربران برای اینکه بتوانند از سرویس‌های مطمئن‌تر استفاده کنند بازخوردهای کاربران دیگر را درباره‌ی آن سرویس می‌خوانند. این بررسی‌ها معیار قضاوتی در مورد اعتبار آن سرویس‌دهندگان است. سامانه‌های متمرکز موجود ثبت بازخورد آنلاین تحت کنترل یک نهاد مرکزی هستند که می‌توانند بازخوردهای کاربران را بر اساس منافع شخصی دستکاری کنند. این سامانه‌ها مستعد انواع تقلب در ثبت بازخوردها مانند ثبت بازخوردهای جعلی و غیرواقعی هستند. همچنین این سامانه‌ها در برابر حملات سیبل و تبانی آسیب پذیر می‌باشند که منجر به ثبت بازخوردهای غیرقابل اعتماد زیادی می‌شود. در این پایان‌نامه با بهره‌گیری از ویژگی‌های ذاتی بلاک‌چین، یک سامانه‌ی غیرمتمرکز جامع برای ثبت بازخوردهای کاربران به سرویس‌های غیرمتمرکز بر بستر بلاک‌چین پالیگان ارائه می‌دهیم که در آن هیچ نهاد واسطه‌ای امکان دستکاری بازخوردهای کاربران را ندارد. این راهکار با پیاده سازی مکانیزم شهرت و همچنین امکان ارزیابی بازخوردهای داده شده به یک سرویس توسط دیگر کاربرانی که از آن سرویس استفاده کرده‌اند، مقاوم در برابر ثبت نظرات جعلی و متعصبانه و همچنین حملات سیبل و تبانی است و باعث به وجود آمدن یک پایگاه داده‌ی قابل اعتماد و غیرقابل تغییر از بازخوردهای کاربران می‌شود.

کلمات کلیدی: مکانیزم شهرت، ثبت بازخورد غیرمتمرکز، قرارداد هوشمند

تاریخچه مقاله:
تاریخ ارسال: ۱۴۰۲/۰۳/۲۲
تاریخ اصلاحات: ۱۴۰۲/۰۵/۳۰
تاریخ پذیرش: ۱۴۰۲/۰۶/۲۸
تاریخ انتشار: ۱۴۰۲/۰۶/۳۰
ایمیل نویسنده مسئول: bdolazim010.ali@gmail.com

۱ – مقدمه و بیان مسئله

با پیشرفت فناوری سرویس‌های آنلاین رشد زیادی داشته‌اند وکاربران اغلب مایل به استفاده از خدمات آن سرویس‌ها هستند. کاربران معمولا قبل از استفاده از خدمات سرویس‌دهندگان، بازخوردهای دیگر کاربران را نسبت به آن سرویس‌دهنده می‌خوانند تا از خدمات و میزان قابل اعتماد بودن آن مطمئن شوند. از این رو سامانه‌های بازخوردی به وجود آمده‌اند که در آن کاربران می‌توانند به خدماتی که از یک پلتفرم گرفته‌اند بازخورد ثبت کنند و همچنین از این سامانه‌ها برای سنجش میزان قابل اعتماد بودن سرویس دهندگان استفاده کنند. به طور مثال این سامانه‌های ثبت بازخورد در پلتفرم‌های eBay، Amazon، Airbnb و ... استفاده می‌شوند. با توجه به [1] در خرید آنلاین بازخوردهای افرادی که از یک محصول استفاده کرده‌اند تاثیر بسیار زیادی بر انتخاب افراد دیگری که می‌خواهند از آن محصول استفاده کنند دارد. همچنین در ژوئن سال ۲۰۱۷ یک نظرسنجی در مورد رفتار مصرف‌کنندگان آنلاین ایالت متحده برگزار شد که در آن ۶۳٪ از کسانی که در نظرسنجی شرکت کرده بودند، خواندن بازخوردهای یک محصول را قبل از خرید آن بسیار مهم می‌دانستند[2]. بلاک‌چین در سال ۲۰۰۸ با بیت‌کوین معرفی شد [3] و از آن موقع تا الان با توجه به ویژگی‌های غیرقابل تغییر بودن داده‌ها، شفافیت، حذف نهادهای واسط و حریم‌خصوصی بالای کاربران توجه زیادی به خود جلب کرده است. با معرفی قراردادهای هوشمند توسط اتریوم، بلاک‌چین کاربردهای زیادی را پیدا کرد

و سامانه‌های غیرمتمرکز بسیاری به وجود آمدند که افراد در استفاده از آن‌ها نیاز به نهاد واسط مرکزی قابل اعتماد نداشتند [4]. با گسترش سامانه‌های غیرمتمرکز زمینه برای کلاهبرداری توسط افراد سودجو نیز فراهم شده است [5] و از این رو بررسی بازخوردهای دیگر کاربران، منجر به انتخاب سرویس‌هایی با درجه‌ی اطمینان بالاتر و تصمیمات مطمئن‌تر برای کاربران می‌شود.

با در نظر گرفتن اهمیت سامانه‌های بررسی در انتخاب خدمات، نیاز به سامانه‌ی ثبت بازخورد کاربران احساس می‌شود. از طرفی ما بر این باور هستیم که مشکل اصلی سامانه‌هایی که برای ثبت بازخورد وجود دارند معماری متمرکز آن‌هاست که آن‌ها را غیر قابل اعتماد می‌کند. در سامانه‌های ثبت بازخورد با معماری متمرکز یک نهاد مرکزی وجود دارد که کل سامانه را کنترل می‌کند و می‌تواند محتوای بازخوردها را به طور دلخواه تغییر دهد و یا حتی برخی از بازخوردها را حذف کند [6,7,8,9,10,11]. برای مثال همانطوری که در [11] گزارش شده است یک هتل زنجیره‌ای استرالیایی به دلیل حذف نظرات منفی در وب‌سایت TripAdvisor ۲/۲ میلیون دلار جریمه شده است و یا همانطوری که در [12] گزارش شده است سامانه‌ی Airbnb امتیاز یک کاربر به یک هتل را بدون رضایت او افزایش داده است. در سیستم‌های متمرکز فرآیند ثبت بازخوردها شفاف نمی‌باشد و ممکن است برخی بازخوردها از طرف افراد جعلی ثبت شوند و یا محتوای بازخوردها توسط سامانه تغییر یابد [12].

از طرف دیگر این سامانه‌ها مستعد انواع حملات ثبت بازخورد مانند حملات سیبل و تبانی هستند که در آن ممکن است یک فرد با چندین هویت جعلی اقدام به ثبت بازخورد نسبت به یک سرویس کند و یا گروهی از افراد نسبت به محصولات رقیب بازخورد منفی جعلی و یا نسبت به محصولات خود بازخورد مثبت جعلی ثبت کنند [13,14]. این سامانه‌ها همچنین با چالش‌هایی مانند ثبت نظرات جعلی و ثبت نظرات متعصبانه و همچنین غیرقابل اعتماد بودن بازخوردهای موجود رو به رو هستند. یعنی افراد ممکن است نسبت به محصولاتی که تجربه‌ی استفاده‌ی واقعی از آن را ندارند بازخورد ثبت کنند[15] و یا بازخوردهای متعصبانه و جهت‌دار نسبت به برخی سرویس‌ها ثبت کنند که غیرواقعی می‌باشند و تجربه‌ی واقعی کاربر از آن محصول نمی‌باشد [16,17].

مواردی که در بالا گفته شد باعث می‌شود که بازخوردهای موجود در چنین سامانه‌هایی غیرقابل اعتماد باشند و در نتیجه کاربران نتوانند به این بازخوردها در تصمیم‌گیری خود مبنی بر استفاده یا عدم استفاده از آن محصول اعتماد کنند.

در این پایان‌نامه با بهره‌گیری از ویژگی‌های شفافیت و تغییرناپذیری بلاک‌چین و امکان اجرای خودکار در قراردادهای هوشمند، یک سامانه‌ی غیرمتمرکز جامع برای ثبت بازخورد نسبت به سرویس‌های غیرمتمرکز ارائه می‌دهیم که در آن از مکانیزم شهرت برای اعتبارسنجی میزان قابل اعتماد بودن بازخوردها و کاربران استفاده می‌شود. از آنجایی که از قراردادهای هوشمند برای پیاده سازی فرآیند ثبت بازخورد استفاده می‌کنیم و همچنین بازخوردها در بلاک‌چین ذخیره می‌شوند، تمامی مراحل ثبت بازخورد در سامانه‌ی ما کاملا شفاف می‌باشد و بازخوردهای موجود قابل تایید و ردیابی توسط همه‌ی کاربران می‌باشند. از طرف دیگر معماری غیرمتمرکز سامانه‌ی ما تضمین می‌کند که هیچ نهاد واسطه‌ای نمی‌تواند بازخوردهای کاربران را حذف کند و یا محتوای آن را تغییر دهد و بازخوردها پس از ثبت در سامانه‌ی ما بدون تغییر خواهند ماند. کاربران برای ثبت بازخورد نسبت به یک سرویس در سامانه‌ی ما، باید خود را از طریق کیف پول بلاک‌چینی، ایمیل و توییتر احراز هویت کنند و حتما از خدمات سرویسی که می‌خواهند به آن بازخورد دهند استفاده کرده باشند. همچنین امتیاز شهرت کاربران بر اساس فعالیت‌هایشان و بازخوردهایی که از دیگران دریافت می‌کنند به روز رسانی می‌شود که این امتیاز رابطه‌ی مستقیم با میزان قابل اعتماد بودن یک کاربر و بازخوردهایی که می‌دهد دارد. استفاده از تکنولوژی بلاک‌چین و قراردادهای هوشمند و وجود احراز هویت ۳ مرحله‌ای و همچنین پیاده سازی مکانیزم شهرت، سامانه‌ی ما را در برابر حملات احتمالی ثبت بازخورد و چالش‌های مربوط به آن مقاوم می‌سازد.

در ادامه‌ی پایان‌نامه در بخش ۲ تکنولوژی‌های استفاده شده در سامانه و کارهای غیرمتمرکز انجام شده را مرور می‌کنیم و سپس در بخش ۳ سامانه‌ی پیشنهادی خود را ارائه می‌کنیم. در بخش ۴ عملکرد سامانه را ارزیابی می‌کنیم و همچنین در بخش ۵ نتیجه‌گیری و کارهای آینده را می‌آوریم.

۲ - کارهای پیشین

در این بخش در ۲-۱ به توضیح فناوری‌هایی که در این پایان‌نامه برای سامانه‌ی ثبت بازخورد غیرمتمرکز به کار رفته‌اند می‌پردازیم سپس در ۲-۲ به معرفی کارهای انجام شده در زمینه‌ی ثبت بازخورد با استفاده از تکنولوژی بلاک‌چین می‌پردازیم.

۲-۱ فناوری‌های استفاده شده

در این بخش به توضیح فناوری دفتر کل توزیع شده، بلاک‌چین، قراردادهای هوشمند، IPFS[1]، TheGraph و EIP712[2] می‌پردازیم.

۲-۱-۱ فناوری دفتر کل توزیع شده

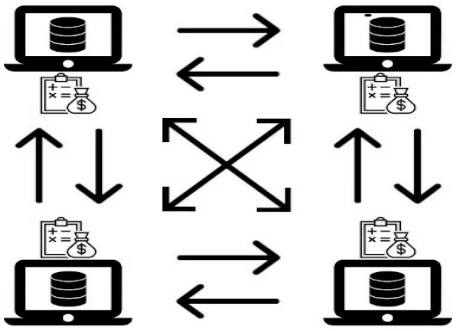
روش مرسوم فعلی برای ذخیره‌سازی داده‌ها استفاده از پایگاه داده‌های متمرکز است که داده‌ها در یک سرور منفرد قرار دارند. در حالی که این مدل متمرکز مدیریت کارآمد داده‌ها را تسهیل می‌کند اما آسیب‌پذیری‌هایی نیز دارد که در پایین آورده شده است:

- نقطه‌ی شکست منفرد: سرور مرکزی یک نقطه‌ی شکست منفرد را نشان می‌دهد که در صورت به وجود آمدن مشکل برای آن ممکن است کل سیستم به خطر بیفتد.
- آسیب‌پذیری در برابر حملات: سیستم‌های متمرکز به دلیل ماهیت متمرکز، بیشتر در معرض حملات سایبری هدفمند هستند.
- وابستگی به نهاد ثالث: کاربران در این رویکرد باید به نهاد مرکزی اعتماد کنند و این نهادهای مرکزی امکان دسترسی و تغییر داده‌های کاربران را دارند که این مسئله نگرانی‌هایی را در مورد دستکاری داده‌ها و یا دسترسی غیرمجاز ایجاد می‌کند.

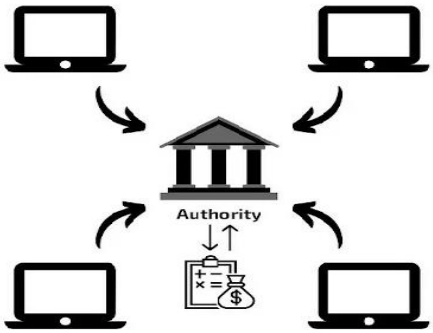
به عنوان مثال اطلاعات مربوط به تراکنش‌های بانکی در یک پایگاه داده مرکزی که در سرور بانک قرار دارد ذخیره می‌شوند. اگر این پایگاه داده مورد حمله قرار بگیرد، بانک می‌تواند از پایگاه داده‌ی پشتیبان اطلاعات را بازیابی کند. اما این امکان نیز وجود دارد که خود نسخه‌ی پشتیبان مورد حمله قرار بگیرد که در این صورت باید چند نسخه‌ی پشتیبان برای بازیابی داده‌ها وجود داشته باشد.

دفتر کل توزیع شده یک پایگاه داده است که در کل شبکه به اشتراک گذاشته می‌شود و این شبکه ممکن است چندین سایت، سازمان و مکان جغرافیایی را در بر گیرد. ماهیت توزیع شده‌ی دفتر کل با ارائه‌ی شاهدان عمومی به داده‌ها، سطح بالاتری از امنیت را معرفی می‌کند و حملات سایبری را برای عوامل مخرب چالش برانگیز می‌کند[18].

در هر گره از شبکه، شرکت‌کنندگان به سوابق مشترک دسترسی دارند و هر گره از این اطمینان دارد که دارای یک نسخه‌ی به روز از داده‌ها است. علاوه بر این هر تغییر، اصلاح و یا اضافه کردن اطلاعات به دفتر کل، ثبت می‌شود و در زمان کمی در دسترس همه‌ی شرکت کنندگان قرار می‌گیرد. این همگام‌سازی بلادرنگ یکپارچگی و شفافیت داده‌ها را در سراسر شبکه افزایش می‌دهد. در شکل ۲-۱ نحوه‌ی کارکرد دفتر کل غیرمتمرکز و در شکل ۲-۲ نحوه‌ی کارکرد دفتر کل متمرکز آورده شده است.



شکل ۲-۱. دفترکل غیرمتمرکز [19]



شکل ۲-۲. دفترکل متمرکز[19]

بلاک‌چین که در آن داده‌ها اندازه‌گیری شده و سپس در بلاک‌های به هم پیوسته ذخیره می‌کنند [20].

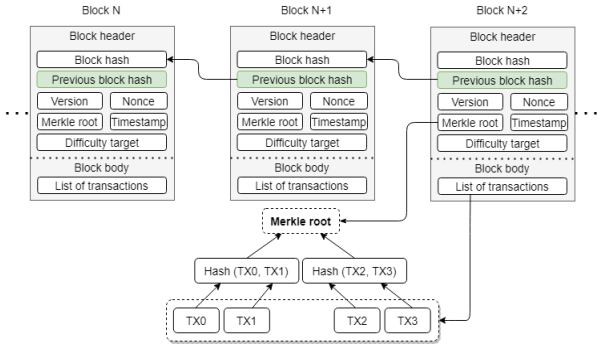
۲-۱-۲ بلاک‌چین

تکنولوژی بلاک‌چین یک پیاده سازی از دفتر کل غیرمتمرکز است [21] و از مجموعه‌ای از بلاک‌های متصل به هم تشکیل شده است [22]. در بلاک‌چین از یک تابع هش برای ارتباط بین

[1] InterPlanetary File System

[2] Ethereum Improvement Proposals 712

بلاک‌ها استفاده می‌شود، به این صورت که هش بلاک قبلی در بلاک فعلی ذخیره می‌شود و این باعث می‌شود که تغییر یک بلاک وابسطه به تغییر بلاک‌های قبلی شود که باعث سخت‌تر شدن دستکاری داده‌ها در بلاک‌چین می‌شود. همانطوری که در شکل۳-۲ مشخص است یک بلاک در بلاک‌چین از ۲ بخش کلی تشکیل می‌شود [23]:



شکل۳-۲. ساختار بلاک در بلاک‌چین [23]

- هدر بلاک: که شامل ۷ بخش زیر است:
  - هش بلاک: هش اطلاعات بلاک فعلی را نشان می‌دهد.
  - هش بلاک قبلی: یک هش ۲۵۶ بیتی که به هش بلاک قبلی اشاره می‌کند.
  - ورژن بلاک: قوانینی که در تایید بلاک باید در نظر گرفته شود را مشخص می‌کند.
  - نانس: از صفر شروع می‌شود و هر بار که یک هش محاسبه شد یک واحد افزایش پیدا می‌کند.
  - هش ریشه‌ی درخت مرکل: مقدار هش تمام تراکنش‌های داخل بلاک است.
  - مهر زمانی: زمان فعلی به واحد ثانیه بعد از تاریخ ۱۹۷۰/۰۱/۰۱ می‌باشد.
  - سختی بلاک: یک حد آستانه است که بلاک‌هایی که تولید می‌شوند باید تا آن حد از یک الگوی خاص پیروی کنند.
- بدنه بلاک: شامل تاریخچه‌ی تراکنش‌های ذخیره شده در شبکه است.

بلاک‌چین را به لحاظ دسترسی به داده‌ها می‌توان به شکل‌های مختلف دسته‌بندی کرد که در زیر آورده شده است:

- با مجوز یا بدون مجوز: این مورد بلاک‌چین‌ها را از لحاظ دسترسی به شرکت در فرآیند اجماع بررسی می‌کند. در بلاک‌چین‌های بدون مجوز مانند بیتکوین هیچ محدودیتی برای شرکت کردن افراد در فرآیند اجماع وجود ندارد و همه می‌توانند در مکانیزم اجماعی که برای اعتبارسنجی تراکنش‌ها انجام می‌شود شرکت کنند اما در بلاک‌چین‌های بامجوز مانند ریپل، یک زیرمجموعه‌ی از پیش تعریف شده می‌توانند در فرآیند اجماع شرکت کنند [24].
- عمومی یا خصوصی: این مورد بلاک‌چین‌ها را از این لحاظ که چه کسی می‌تواند داده‌ها را از بلاک‌چین بخواند و یا امکان نوشتن داده بر روی بلاک‌چین را دارد بررسی می‌کند [25] . در بلاک‌چین‌های عمومی مانند اتریوم و بیتکوین همه می‌توانند داده‌ها را از بلاک‌چین بخوانند و بر روی آن داده بنویسند اما در بلاک‌چین‌های خصوصی فقط به یک زیرمجموعه‌ی از پیش تعریف شده مانند یک سازمان خاص اجازه خواندن داده از روی بلاک‌چین و نوشتن داده بر روی آن داده می‌شود.

بلاک‌چین به عنوان یک دفتر کل توزیع شده همانند سایر سیستم‌های توزیع شده با چالش بین گره‌های شبکه‌ی خود برای اطمینان از سازگاری پایگاه داده خود مواجه است و گره‌ها باید بین خود تصمیم بگیرند که کدام بلاک به بلاک‌چین اضافه شود. به همین خاطر بلاک‌چین‌های مختلف از مکانیزم‌های اجماع مختلفی برای اضافه کردن بلاک‌ها به بلاک‌چین استفاده می‌کنند که در زیر ۲ نمونه از معروف‌ترین آن‌ها یعنی اثبات کار (pow[3]) و اثبات سهام (pos[4]) آورده شده است:

- اثبات کار: اثبات کار یک نوع مکانیزم اجماع است [25,26] که برای جلوگیری از حملات انکار سرویس توزیع شده (DDOS) و هرزنامه کردن شبکه طراحی شده است[27]. در اثبات کار قاعده بر این است که زنجیره‌ی بلاکی که بیشترین محاسبات را انجام داده است حفظ شود. در واقع میزان کار انجام شده معیاری از اعتماد در سیستم می‌باشد بنابراین بلاکی که بیشترین مقدار محاسبات را انجام داده باشد به بلاک‌چین اضافه

[3] Proof Of Work

[4] Proof Of Stake

می‌شود. ماینرها نهادهایی هستند که این محاسبات را از طریق حل یک پازل محاسباتی انجام می‌دهند و با دیگر ماینرها برای حل کردن این پازل رقابت می‌کنند. هر ماینری که موفق به اضافه کردن بلاک به بلاک‌چین شود یک جایزه که از قبل مشخص شده است را دریافت می‌کند. از آنجایی که ماینرها برای اعتبارسنجی جوابی که پیدا کرده‌اند آن را در کل شبکه به اشتراک می‌گذارند تا دیگر ماینرها درستی آن را بررسی کنند، این فرآیند برخلاف حل کردن پازل که بخاطر امنیت شبکه فرآیندی زمان‌بر است، باید سریع اتفاق بیفتد و دیگر ماینرها بتوانند به سرعت درستی پاسخ را اعتبارسنجی کنند. همچنین میزان سختی حل کردن این پازل با توجه به قدرت محاسباتی شبکه به روز رسانی می‌شود تا میانگین زمان تولید هر بلاک را ثابت نگه دارد.

- اثبات سهام: این نوع مکانیزم اجماع از میزان سهامی که افراد در سیستم دارند به عنوان یک معیار اندازه‌گیری اعتماد استفاده می‌کند [28] و باور بر این است که کسانی که سهم بیشتری (معمولا پول) در سیستم دارند تمایل کمتری به رفتار اشتباه دارند و میزان سهام هر کس متناسب با میزان قدرت او در تصمیم‌گیری برای اجماع می‌باشد.

بلاک‌چین با گذشت زمان با توجه به ویژگی‌هایی مانند شفافیت، تغییرناپذیری و امنیت بالا علاوه بر بحث رمزارزها در زمینه‌های مختلفی مانند سرویس‌های الکترونیکی حاکمیتی، حوزه‌ی سلامت و ... مورد استفاده قرار گرفته است. برای مثال در [29,30] یک راه حل برای شفاف کردن فرآیند رای‌گیری به طوری که حکومت‌ها نتوانند رای‌هایی که افراد می‌دهند را تغییر دهند ارائه شده است و با کاربردی شدن بیشتر آن انتظار می‌رود که در زمینه‌های گسترده‌ای مورد استفاده قرار گیرد.

۳-۱-۲ قرارداد هوشمند

مفهوم قرارداد هوشمند در سال ۱۹۹۶ توسط Nick Szabo معرفی شد [31]. قراردادهای هوشمند، قراردادهایی هستند که به صورت خودکار اجرا می‌شوند و در آن شرایط توافق به طور مستقیم در کد گنجانده شده است. این قراردادها مبتنی بر فناوری بلاک‌چین هستند که به عنوان یک دفترکل توزیع شده و غیرمتمرکز عمل می‌کند. قراردادهای هوشمند نیاز به وجود واسطه را حذف می‌کنند و شفافیت، امنیت و خودکارسازی در اجرای تعهداتی که در متن قرارداد هستند و در بلاک‌چین ذخیره می‌شوند را تضمین می‌کنند.

مقاله اصلی Nick Szabo در مورد قراردادهای هوشمند یک پروتکل دیجیتالی بود که می‌توانست فرآیند نوشتن و یا اجرای یک قرارداد را تسهیل کند و این امکان را بدهد که این قراردادها به صورت خودکار اجرا شوند و قابل تایید باشند [31].

با این حال با ظهور اتریوم در سال ۲۰۱۵، قراردادهای هوشمند به صورت عملی پیاده سازی شدند [32]. اتریوم به رهبری Vitalik Buterin، یک زبان برنامه نویسی تورینگ کامل به نام Solidity را معرفی کرد که به طور خاص برای ایجاد قراردادهای هوشمند طراحی شده است.

قراردادهای هوشمند بر روی شبکه بلاک‌چین قرار می‌گیرند که از شبکه‌ای از گره‌های توزیع شده در سراسر جهان تشکیل شده است. این گره‌ها یک کپی از کل بلاک‌چین را نگه می‌دارند و از یک مکانیزم اجماع که اغلب اثبات کار یا اثبات سهام است برای اعتبارسنجی و افزودن تراکنش‌های جدید به بلاک‌چین استفاده می‌کنند. قراردادهای هوشمند شامل چندین جزء کلیدی هستند که در زیر آورده شده است:

- کد قرارداد هوشمند: کدهای قراردادهای هوشمند با استفاده از زبان برنامه نویسی مخصوص نوشتن قراردادهای هوشمند مانند Solidity نوشته می‌شوند و این کدها شامل قوانین، شرایط و منطقی است که شرایط قرارداد هوشمند را مشخص می‌کند.
- تورینگ کامل بودن: زبان‌های برنامه نویسی قراردادهای هوشمند اغلب تورینگ کامل هستند. به این معنی که می‌توانند هر محاسباتی که بتوان به صورت الگوریتمی بیان کرد را انجام دهند. این امر باعث انعطاف‌پذیری بیشتر در اجرای قراردادها می‌شود.
- تغییرناپذیری: زمانی که قراردادهای هوشمند در بلاک‌چین قرار داده شد امکان تغییر آن‌ها وجود ندارد. تغییر ناپذیری تضمین می‌کند که شرایط قرارداد پس از استقرار کامل قابل تغییر یا دستکاری نیست و یک محیط امن را تضمین می‌کند.

- دفتر کل غیرمتمرکز: قراردادهای هوشمند بر روی یک شبکه‌ی بلاک‌چین غیرمتمرکز قرار می‌گیرند. این شبکه شامل گره‌هایی است که در سراسر جهان توزیع شده‌اند و هر کدام یک کپی از بلاک‌چین را نگه‌داری می‌کنند و این ماهیت غیرمتمرکز امنیت و شفافیت را تضمین می‌کند.
- شفاف و قابل تایید بودن: هر شرکت کننده در شبکه‌ی بلاک‌چین به کد قرارداد هوشمند و تاریخچه‌ی اجرای آن دسترسی دارد. این شفافیت تضمین می‌کند که همه‌ی طرف‌های درگیر می‌توانند به طور مستقل تراکنش‌ها را تایید کنند.
- تاریخچه‌ی تراکنش‌ها: بلاک‌چین یک رکورد شفاف و تغییرناپذیر از تمام تراکنش‌ها و تعاملات با قراردادهای هوشمند را نگه‌داری می‌کند. این سوابق به عنوان یک دفتر کل عمومی است که می‌تواند حسابرسی و تایید شود.
- اجرای بدون نیاز به اعتماد: در قراردادهای هوشمند شرکت کنندگان می‌توانند بدون نیاز به اعتماد به یکدیگر در معاملات شرکت کنند و این اعتماد از طریق ویژگی‌های امنیتی ذاتی بلاک‌چین و ماهیت اجرای خودکار قرارداد هوشمند ایجاد می‌شود.
- قابلیت اجرای خودکار: قراردادهای هوشمند به گونه‌ای طراحی شده‌اند که در صورت تحقق شرایط از پیش تعیین شده، اقدامات مشخصی به صورت خودکار اجرا می‌شوند و نیاز به یک شخص یا نهاد واسطه برای اجرای این قراردادها نیست.

قراردادهای هوشمند پذیرش گسترده‌ای در حوزه‌های مختلف داشته‌اند و فرآیندهای سنتی را متحول کرده‌اند. در بخش مالی، پلتفرم‌های مالی غیرمتمرکز (DeFi[5]) از قراردادهای هوشمند برای وام‌دهی خودکار و تجارت بدون واسطه‌های سنتی استفاده می‌کنند. مدیریت زنجیره‌ی تامین از شفافیت ارائه شده توسط قراردادهای هوشمند، خودکارسازی و اعتبارسنجی جریان کالاها، کاهش تقلب و افزایش کارایی سیستم سود می‌برد. قراردادهای هوشمند همچنین نقش مهمی در ایجاد سیستم‌های رای‌گیری ثبت بازخورد ایمن دارند. با استفاده از دفترکل تغییرناپذیر بلاک‌چین، قراردادهای هوشمند یکپارچگی فرآیند رای‌گیری و ثبت بازخورد را تضمین می‌کنند و نگرانی‌های مربوط به تقلب و دستکاری را کاهش می‌دهند[33]. در نتیجه در قراردادهای هوشمند کد قانون است و شرایط نوشته شده در قراردادهای هوشمند به صورت خودکار و غیرقابل برگشت اجرا می‌شوند که این امر نیاز به واسطه را از بین می‌برد و خطر تقلب را کاهش می‌دهد.

۴-۱-۲ پروتکل IPFS

IPFS یک پروتکل برای ایجاد سیستم فایل غیرمتمرکز و توزیع شده است. مفهوم اصلی IPFS شامل آدرس دهی محتوا است که در آن به هر داده یک هش رمزنگاری شده منحصر به فرد اختصاص داده می‌شود که این موضوع بازیابی کارآمد داده‌ها و تایید آن‌ها را تضمین می‌کند [34].

IPFS به طور ذاتی غیرمتمرکز است و آسیب‌پذیری‌های مرتبط با نقطه‌ی شکست منفرد را از بین می‌برد و یک مدل همتا به همتا برای اشتراک‌گذاری فایل‌ها معرفی می‌کند [34,35].

شبکه‌ی IPFS مبتنی بر ۳ اصل زیر می‌باشد:

- غیرمتمرکز بودن: در پروتکل IPFS افراد از تمامی مکان‌های جغرافیایی بدون اینکه داده‌ها توسط یک سازمان تحت نظارت و کنترل باشد می‌توانند به آن دسترسی داشته باشند.
- آدرس دهی محتوایی: آدرس‌دهی سنتی در فضای وب بر اساس محل ذخیره‌سازی آن است. محدودیت این نوع آدرس‌دهی وقتی که داده‌ها در چند مکان وجود داشته باشد خودش را نشان می‌دهد. این در صورتی است که IPFS از محتوای فایل برای آدرس‌دهی آن استفاده می‌کند که به آن شناسه‌ی محتوایی (Content Id) گفته می‌شود. شناسه‌ی محتوایی هر داده هش رمزنگاری شده‌ی محتوای آن می‌باشد.
- مشارکت اعضا: اینترنت فعلی بر ۲ پایه اساسی مالکیت و دسترسی بنا شده است که در آن محتوا از طرف مالک به شخصی که می‌تواند به آن دسترسی داشته باشد، داده می‌شود در حالی که در IPFS افراد زیادی فایل‌های یکدیگر را در اختیار خواهند داشت و با مشارکت با یکدیگر از در دسترس بودن آن اطمینان حاصل می‌کنند.

[5] Decentralized Finance

IPFS همچنین تغییرناپذیری داده‌ها را تضمین می‌کند و از طریق نسخه‌سازی داده‌ها امکان ردیابی تاریخچه‌ی داده‌ها را به ما می‌دهد.

۲-۱-۵ پروتکل TheGraph

TheGraph یک پروتکل نمایه سازی (Indexing) برای جست و جوی داده‌ها از بلاک‌چین است. TheGraph که برای تقویت برنامه‌های غیرمتمرکز و تعامل آن‌ها با داده‌های بلاک‌چین توسعه یافته است، یک شبکه‌ی پرس و جوی غیرمتمرکز را ارائه می‌دهد که کارایی دسترسی به داده‌های ذخیره شده بر روی بلاک‌چین را افزایش می‌دهد [36]. TheGraph واسط‌های برنامه نویسی کاربردی (API[6]) عمومی را که به subgraph معروف است در اختیار توسعه دهندگان قرار می‌دهد و این امکان را به آن‌ها می‌دهد تا داده‌ها را در بلاک‌چین‌های مختلف به صورت یکپارچه جست و جو کنند. ماهیت غیرمتمرکز TheGraph مقاومت در برابر سانسور و قابلیت اطمینان را در شبکه‌های مختلف بلاک‌چینی تضمین می‌کند.

در هسته‌ی عملکرد TheGraph مفهوم subgraph نهفته است [37] که توسط توسعه دهندگان نوشته می‌شوند تا داده‌ها را از قراردادهای هوشمند خاصی که توسعه دهندگان مشخص کرده‌اند در بلاک‌چین بازیابی کنند.

این رویکرد غیرمتمرکز برای پرس و جو به توسعه دهندگان اجازه می‌دهد تا به صورت کارآمد داده‌ها را از بلاک‌چین بازیابی کنند و بازیابی غیرضروری داده‌ها را به حداقل می‌رساند.

پروتکل TheGraph با ارائه‌ی یک جایگزین غیرمتمرکز به چالش‌های مرتبط با خدمات نمایه‌سازی مانند سانسورکردن می‌پردازد و همچنین استفاده از آن دسترسی بلادرنگ و قابل اطمینان به داده‌های بلاک‌چینی را تضمین می‌کند که TheGraph را برای برنامه‌های کاربردی غیرمتمرکز بسیار کارآمد می‌کند [36].

۲-۱-۶ استاندارد EIP712

EIP712 یک نوع استاندارد پیشنهاد بهبود اتریوم است که برای هش کردن داده‌های ساخت یافته و تایید امضایی که کاربر با کلید خصوصی خود تولید می‌کند بر روی بلاک چین به کار می‌رود. EIP712 که توسط توسعه دهندگان اتریوم پیشنهاد شده است، با ارائه‌ی یک روش استاندارد برای رمزگذاری و امضای داده‌های ساختار یافته، امنیت و قابلیت استفاده‌ی برنامه‌های کاربردی مبتنی بر اتریوم را افزایش می‌دهد. از طریق این استاندارد پلتفرم‌های غیرمتمرکز می‌توانند این امکان را به کاربران خود بدهند که بدون نیاز به اجرای تراکنش توسط کاربر بر روی بلاک‌چین و پرداخت هزینه‌ی تراکنش، از طریق کلید خصوصی خود تراکنشی که می‌خواهند بر روی بلاک‌چین اجرا شود را امضا کنند و هرکسی که این امضا را دارد می‌تواند آن تراکنش را با شرایطی که در محتوای امضا مشخص است و کاربر آن را امضا کرده است بر روی بلاک‌چین اجرا کند [38].

هنگام اجرا شدن تراکنش، امضایی که کاربر با کلید خصوصی خود آن را ایجاد کرده است در سطح قرارداد هوشمند بررسی می‌شود و اگر تغییری در محتوایی که کاربر آن را امضا کرده است اتفاق نیفتاده باشد این تراکنش اجرا خواهد شد.

ساختار EIP712 از ۳ بخش اصلی زیر تشکیل شده است[38]:

- پیشوند EIP712: در اول پیام از پیشوند \x19\x01 استفاده می‌شود که بیانگر این است که استاندارد پیام EIP712 است.
- دامنه: دارای ۴ بخش اصلی است که در زیر مشخص است:
  - نام: نام قرارداد هوشمند
  - ورژن: ورژن قرارداد هوشمند
  - شناسه شبکه: شناسه‌ی شبکه‌ی بلاک‌چینی که این امضا در آن می‌تواند اجرا شود.
  - آدرس قرارداد هوشمند: آدرس قرارداد هوشمند که این امضا در آن اجرا می‌شود.

استفاده از دامنه در متن پیام‌هایی که کاربر امضا می‌کند برای جلوگیری از سواستفاده از امضای کاربر می‌باشد. برای مثال کاربر با امضا کردن پیامی حاوی اطلاعات یک قرارداد خاص در یک شبکه‌ی خاص می‌تواند مطمئن باشد که این امضا در شبکه‌های دیگر نامعتبر خواهد بود و کسی نمی‌تواند از این امضا در یک قرارداد هوشمند دیگر استفاده کند.

- پیام اصلی: محتوای پیام اصلی بر حسب تابعی که کاربر آن را امضا می‌کند مشخص می‌شود. نوع داده این پیام از نوع ساختمان است که در آن بر حسب

[6] Application Programming Interface

ورودی تابعی که کاربر آن را امضا می‌کند ممکن است انواع داده‌های ممکن وجود داشته باشد.

یکی از ویژگی های اصلی EIP712 توانایی آن در هش کردن داده‌های ساختار یافته به روش قطعی و استاندارد است. EIP712 برخلاف روش‌های سنتی، فرمت تعریف شده‌ای برای رمزگذاری و هش کردن داده‌های ساختار یافته ارائه می‌کند و اطمینان می‌دهد که در سطح قرارداد هوشمند نیز داده‌ها به این فرمت هش می‌شوند.

به طور خلاصه EIP712 به چالش‌های مربوط به احرازهویت پیام در قراردادهای هوشمند می‌پردازد و یک استاندارد مشترک برای امضای پیام‌ها ایجاد می‌کند. از EIP712 به طور گسترده در برنامه‌های مبتنی بر بلاک‌چین به ویژه برنامه‌هایی که به احراز هویت امن و قابل تایید پیام‌های خارج از زنجیره نیاز دارند استفاده می‌شود که در آن کاربران داده‌های ساختار یافته را با کلید خصوصی خود امضا می‌کنند و این امضاها قابلیت تایید توسط قراردادهای هوشمند بر روی شبکه‌ی بلاک‌چین را دارند.

۲-۲ کارهای انجام شده

[39] یک سامانه‌ی غیرمتمرکز مبتنی بر بلاک‌چین را برای تجارت الکترونیک و خرید آنلاین معرفی می‌کند. این سامانه از بلاک‌چین اتریوم، IPFS و قراردادهای هوشمند برای بالا بردن امنیت و شفافیت ذخیره‌ی اطلاعات محصول و محاسبات مربوط به امتیاز شهرت استفاده می‌کند. این سامانه دارای ۶ نقش محوری از جمله فروشندگان، خریداران، رابط کاربری، IPFS، قراردادهای هوشمند و بلاک‌چین است که با همدیگر برای ایجاد یک اکوسیستم خرید آنلاین و غیرمتمرکز در ارتباط هستند.

این سامانه دارای ۲ مرحله‌ی کلی تراکنش و ارزیابی است. در مرحله‌ی تراکنش فروشندگان اطلاعات محصول خود شامل نام، قیمت و ... را در IPFS از طریق رابط کاربری ذخیره می‌کنند و IPFS هش اطلاعات را بازمی‌گرداند و این هش در بلاک‌چین به عنوان اطلاعات محصول ذخیره می‌شود. سپس خریداران می‌توانند یک محصول را برای خرید انتخاب کرده و دستور خرید را به بلاک‌چین ارسال کنند. مرحله‌ی بعد مرحله‌ی ارزیابی می‌باشد که در آن فروشندگان و خریداران می‌توانند نسبت به هم امتیاز بدهند. خریداران بعد از تکمیل خرید، امتیاز خود نسبت به محصول و فروشنده را در IPFS ذخیره می‌کنند و IPFS هش مربوط به اطلاعات را بازمی‌گرداند سپس این مقدار هش در بلاک‌چین ذخیره می‌شود و جایزه‌ای در قالب رمزارز از طرف فروشنده به خریدار به عنوان مشوق داده می‌شود. فروشنده نیز امتیاز خود نسبت به خریدار را در IPFS ذخیره می‌کند و IPFS هش اطلاعات ذخیره شده را بازمی‌گرداند و این هش در بلاک‌چین ذخیره می‌شود. پس از اینکه هر ۲ طرف نسبت به همدیگر امتیاز ثبت کردند، از طریق قرارداد هوشمند و به صورت خودکار محاسبات مربوط به امتیاز شهرت انجام می‌شود و امتیاز شهرت کاربران به روز رسانی می‌شود. در محاسبات مربوط به امتیاز شهرت و مشوق‌هایی که به خریداران داده می‌شود ۳ فاکتور اصلی وجود دارد:

- زمان بین تراکنش‌ها: فاصله‌ی زمانی بین خرید قبلی کاربر با خرید فعلی را نشان می‌دهد که هرچقدر این مقدار بیشتر باشد امتیازی که کاربر می‌دهد قابل اعتمادتر است.
- مقدار تراکنش: مقدار پولی که کاربر برای تراکنش فعلی می‌دهد و هرچقدر این مقدار بیشتر باشد امتیازی که کاربر می‌دهد قابل اعتمادتر است.
- میزان شهرت قبلی کاربر: هرچقدر کاربر امتیاز شهرت بیشتری داشته باشد به آن میزان قابل اعتمادتر است.

این سامانه با در نظر گرفتن مشوق‌هایی برای کاربران سعی در ترغیب آن‌ها نسبت به ثبت بازخورد کرده است در حالی که هیچ صحبتی از کاربرد این مشوق‌ها نکرده است و از آنجایی که خود کاربر هزینه‌ی ثبت بازخورد را می‌دهد این مورد که مشوق‌ها هزینه‌ی تراکنش ثبت بازخورد را پوشش می‌دهد یا نه مشخص نیست. از طرف دیگر این سامانه هزینه‌های خود در شبکه‌ی تستی را در بخش ارزیابی آورده است و مقدار قیمت گس را عدد ۱ در نظر گرفته است در حالی که با توجه به بررسی‌های ما از مقدار قیمت گس شبکه‌ی اتریوم در ۶ ماه اخیر حتی با در نظر گرفتن عدد ۱۰ برای قیمت گس که یک مقدار خوشبینانه می‌باشد، هزینه‌ی فرآیندهای ثبت بازخورد و محاسبات مربوط به امتیاز شهرت این سامانه ۱۰ برابر بیشتر از مقادیری است که توسط این کار گزارش داده شده است و بالا بودن این هزینه‌ها باعث می‌شود که این سامانه انتخاب مقرون به صرفه‌ای برای کاربران نباشد. همچنین در مکانیزم شهرت استفاده شده در این سامانه، ارزیابی امتیازات داده شده توسط دیگران که یکی از عوامل مهم در جلوگیری از ثبت نظرات متعصبانه و غیرواقعی است لحاظ نشده است و این سامانه را در برابر بازخوردهای

غیرواقعی آسیب‌پذیر می‌کند و امکان ثبت اینگونه بازخوردها، قابلیت اعتماد سامانه را پایین می آورد.

[40] یک سامانه‌ی رتبه‌بندی غیرمتمرکز را برای سیستم‌های توصیه‌گر با هدف غلبه بر چالش‌های موجود در سیستم‌های متمرکز با استفاده از فناوری بلاک‌چین معرفی می‌کند. این سامانه با استفاده از قراردادهای هوشمند و همچنین ذخیره‌سازی داده‌های مربوط به امتیازات در بلاک‌چین، شفافیت فرآیندهای رتبه‌بندی را افزایش می‌دهد و تضمین می‌کند که یک نهاد مرکزی قدرت تغییر رتبه‌بندی‌های کاربران را ندارد. در این سامانه سرویس‌ها و خدماتی که امکان ثبت بازخورد به آن‌ها وجود دارد شامل ویژگی‌هایی هستند که هرکدام از آن‌ها مربوط به یک مهارت می‌شوند. کاربران در این سامانه فقط به سرویس‌هایی که از آن استفاده کرده‌اند می‌توانند امتیاز بدهند. فرآیند صدور مجوز برای ثبت امتیاز به این صورت است که اگر کاربران از طریق ارز دیجیتال و سامانه اقدام به پرداخت هزینه کنند به صورت خودکار به آن‌ها مجوز ثبت امتیاز صادر می‌شود ولی در صورتی که از طریق پول رایج اقدام به پرداخت هزینه کنند این مجوز باید از طریق صاحبان سرویس صادر شود. در این سامانه این امکان به صاحبان سرویس داده شده است که به هر کاربری که می‌خواهند، مجوز ثبت امتیاز نسبت به خود را بدهند. کاربران بعد از صدور مجوز می‌توانند نسبت به یک سرویس امتیاز ثبت کنند و پس از ثبت امتیاز نسبت به یک سرویس، ویژگی‌های آن را به عنوان مهارت دریافت می‌کنند. در این سامانه مفهوم توکن محلی برای پاداش دادن به کسانی که نسبت به یک سرویس امتیاز ثبت می‌کنند معرفی شده است. این توکن‌ها توسط صاحبان سرویس ساخته و ارزش‌گذاری می‌شوند و استفاده از توکن‌های محلی باعث می‌شود که صاحبان سرویس کنترل بیشتری بر اقتصاد توکن خود داشته باشند. در این سامانه از امتیاز شهرت برای نشان دادن تجربه‌ی کاربران در یک مهارت استفاده می‌شود و مقدار آن بعد از ثبت بازخورد نسبت به یک سرویس افزایش می‌یابد. کاربران در این سامانه متناسب با میزان امتیاز شهرت خود پاداش دریافت می‌کنند و پیاده سازی چنین مکانیزم پاداشی باعث افزایش مشارکت و همکاری کاربران در فرآیند امتیازدهی می‌شود.

این سامانه با استفاده از بلاک‌چین و قراردادهای هوشمند فرآیند رتبه بندی سیستم‌های توصیه‌گر را شفاف‌تر می‌کند و مانع از تغییر امتیازهای کاربران می‌شود. با این حال مکانیزم شهرت پیاده سازی شده در برابر چالش‌هایی مانند ثبت نظرات متعصبانه و غیرواقعی آسیب‌پذیر است و این امتیازات توسط دیگر کاربران ارزیابی نمی‌شوند. این سامانه همچنین در برابر حملات ثبت بازخورد مانند حمله‌ی سیبل، تبانی و ثبت بازخورد جعلی آسیب‌پذیر است و صاحبان سرویس می‌توانند به افرادی که از یک سرویس استفاده نکرده‌اند مجوز ثبت امتیاز بدهند که باعث افزایش امتیازهای جعلی می‌شود. همچنین این امکان وجود دارد صاحبان سرویس افراد با امتیاز شهرت بالا را به ثبت بازخوردهای مثبت یا منفی جعلی ترغیب کنند که این موارد باعث غیرقابل اعتماد شدن رتبه بندی‌های ارائه شده توسط این سامانه می‌شود.

در [41] هدف اصلی ارائه‌ی یک راهکار غیرمتمرکز در برابر فعالیت‌های متقلبانه در ثبت بازخورد با استفاده از بلاک‌چین و قراردادهای هوشمند است که در آن سامانه به جای تکیه کردن به تصمیمات یک نهاد مرکزی، به جامعه‌ی کاربر متکی است. در سیستم ۳ نقش اساسی شامل مشتری، فروشنده و نهاد ثالث وجود دارد که در آن مشتری‌ها می‌توانند به محصولات و کیفیت آن‌ها بر اساس بازخوردهایی که به آن محصول ثبت شده است دسترسی داشته باشند. فرآیند خرید محصول در این سامانه به این صورت است مشتری اقدام به خرید یک محصول می‌کند سپس درخواست خرید آن توسط صاحب محصول داده می‌شود و شناسه‌ی درخواست به همراه قیمت محصول به مشتری ارسال می‌شود. خرید محصول و فرآیند ثبت بازخورد توسط این شناسه انجام می‌شود. مشتریانی که در سامانه محصول خود را برای فروش بارگذاری می‌کنند تبدیل به فروشنده می‌شوند و این یک فرآیند یک طرفه می‌باشد یعنی فروشندگان امکان تبدیل شدن به مشتری را ندارند و همچنین نمی‌توانند یک محصول را بخرند و یا نسبت به آن بازخورد ثبت کنند. در این سامانه نهادهای ثالث شرکت‌های خارجی هستند که بر اساس داده‌های موجود در سامانه سیستم پیشنهادگر ارائه می‌کنند.

فرآیند ثبت بازخورد در این سامانه به این گونه است که مشتریان پس از خرید محصول با قفل کردن مقداری پول در قرارداد هوشمند که نشان‌دهنده‌ی میزان اعتماد آن‌ها به بازخوردی که می‌دهند است، نسبت به یک محصول بازخورد ثبت می‌کنند. این پول پس از ثبت بازخورد قابل برداشت توسط مشتری می‌باشد. از طرف دیگر مشتریان می‌توانند یک بازخورد را با قفل کردن پول در قرارداد هوشمند به چالش بکشند و

همچنین افراد دیگر نیز می‌توانند با قفل کردن پول، نظر موافق یا مخالف خود را نسبت به آن چالش اعلام کنند. میزان پول قفل شده متناسب با میزان رای مشتریان می‌باشد. پس از پایان چالش و رای‌گیری، هر گروهی که رای بیشتری داشته باشد برنده می‌شود و پول قفل شده توسط مشتریان بازنده بین آن‌ها تقسیم می‌شود. این سامانه با بررسی کردن استفاده‌ی مشتریان از یک محصول و با به چالش کشیدن بازخوردهای ثبت شده، جلوی ثبت نظرات جعلی و متعصبانه و همچنین حمله‌ی تبانی را می‌گیرد. اما از آنجایی که فروشنده می‌تواند هنگام تعریف کردن محصول قیمت آن را برای گروهی خاص رایگان تنظیم کند این امکان وجود دارد که کاربران با ساخت حساب‌های متعدد و فقط پرداخت کردن هزینه‌ی تراکنش حمله‌ی سیبل انجام دهند. پس مکانیزم دفاعی این سامانه در برابر این حمله کامل و قوی نیست. از طرف دیگر در مکانیزم ارزیابی بازخوردی که این سامانه در نظر گرفته است این امکان وجود دارد که با به چالش کشیدن بازخوردهای کاربر دارایی‌های آن‌ها به خطر بیفتد و این امر ممکن است تمایل افراد را به ثبت بازخورد از بین ببرد و مانع از مشارکت کاربران در فرآیند ثبت بازخورد شود.

در [42] یک سیستم بررسی محصولات آنلاین بر بستر بلاک‌چین اتریوم ارائه شده است که هدف آن کاهش تقلب‌های رتبه‌بندی ممکن می‌باشد. این سامانه فرآیند خرید محصول را با ثبت بازخورد یکپارچه می‌کند و تنها در صورتی به خریداران مجوز بررسی می‌دهد که حتما یک محصول را خریده باشند.

۴ نقش اصلی در این سامانه وجود دارد:

- فروشندگان: کسانی که محصول را می‌فروشند.
- خریداران: کسانی که محصول را خریداری می‌کنند.
- بازخورد دهندگان: خریدارانی که نسبت به یک محصول بازخورد ثبت می‌کنند.
- تاییدکنندگان: گروهی از بازخورد دهندگان صادق که قبلا در فرآیند ثبت بازخوردها رفتار صادقانه داشته‌اند و در هر بار ثبت بازخورد برای تایید یا رد کردن بازخوردها انتخاب می‌شوند.

در این سامانه فروشندگان و خریداران باید خود را از طریق کارت اعتباری احراز هویت کنند و هر آدرس کیف پول بلاک‌چینی به یک کارت اعتباری منحصر به فرد متصل است. فرآیند تعریف محصول توسط فروشندگان به این گونه است که مقداری اتریوم هنگام تعریف کردن محصول به قرارداد هوشمند برای پوشش هزینه‌ی تراکنش واریز می‌کنند. سامانه به خریداران پس از خرید محصول یک توکن PRAT به عنوان مجوز ثبت بازخورد اختصاص می‌دهد و در صورتی که کاربر بازخورد خود را ثبت کند این توکن PRAT که معادل ۰/۰۱ اتریوم می‌باشد به عنوان هزینه‌ی تراکنش به بازخورد دهنده انتقال داده می‌شود. تاییدکنندگان به بازخوردهایی که ثبت می‌شود رای موافق یا مخالف می‌دهند. بازخوردهایی که میزان رای موافق آن‌ها بیشتر از مخالف بود نشان معتبر بودن دریافت می‌کنند و بازخوردهایی که میزان رای مخالف آن‌ها بیشتر باشد نشان جعلی دریافت می‌کنند. بازخورد دهندگانی که نشان معتبر دریافت می‌کنند به لیست تاییدکنندگان اضافه می‌شوند و ۶۰٪ از کسانی که بیشترین نشان معتبر را گرفته‌اند به عنوان تاییدکنندگان بعدی انتخاب می‌شوند و کسانی که نشان جعلی دریافت کرده‌اند به لیست جریمه اضافه می‌شوند و از بین این لیست کاربرانی که بیش از یک آستانه نشان نامعتبر داشته باشند به لیست سیاه اضافه می‌شوند و از سامانه حذف می‌شوند. این سامانه امکان ثبت بازخورد را فقط برای محصولات خود فراهم می‌کند و یک سامانه‌ی جامع که کاربران بتوانند نسبت به سرویس‌های دیگران بازخورد ثبت کنند را در اختیار آن‌ها قرار نمی‌دهد.

ما در این پایان‌نامه یک سامانه‌ی جامع مبتنی بر بلاک‌چین برای ثبت بازخورد نسبت به سرویس‌های غیرمتمرکز ارائه می‌دهیم که در برابر حملات و تقلب‌های ثبت بازخورد مقاوم است و بازخوردهایی قابل اعتماد برای کاربران فراهم می‌کند.

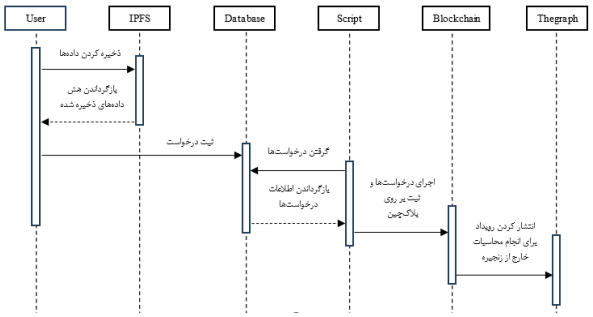
۳ - سامانه‌ی پیشنهادی

در این پایان‌نامه ما یک سامانه‌ی ثبت بازخورد به صورت غیرمتمرکز برای محصولات مبتنی بر بلاک‌چین ارائه می‌دهیم که هدف آن ایجاد یک مکانیزم قوی و شفاف برای ثبت بازخورد کاربران، ارزیابی کیفیت خدمات یک سرویس و محاسبه‌ی شهرت کاربران در یک چهارچوب غیرمتمرکز است که تقلب در ثبت بازخوردها را کاهش می‌دهد.در این پایان‌نامه ما به عنوان یک سامانه‌ی مستقل بستری را برای کاربرانی که از یک سرویس

استفاده کرده‌اند فراهم می‌کنیم تا بتوانند بازخوردهای خود را نسبت به آن سرویس ثبت کنند. همچنین این امکان وجود دارد که افراد دیگر در صورت استفاده از یک سرویس بازخوردهای خود را نسبت به بازخوردهای دیگران که به آن سرویس داده شده است، ثبت کنند و بر اساس این فعالیت‌های کاربران میزان شهرت آن‌ها که معیاری از قابل اطمینان بودن بازخوردهایشان می‌باشد، محاسبه شود.

شکل۱-۳ معماری کلی سیستم را نشان می‌دهد و جزئیات اجزای کلیدی و ارتباطات و فرآیندهای پایان‌نامه به شرح زیر می‌باشد:

در ۳-۱ نقش‌هایی که در سیستم وجود دارد را معرفی می‌کنیم، در ۳-۲ فرآیندهایی که در سیستم توسط این نقش‌ها انجام می‌شود را توضیح می‌دهیم، در ۳-۳ درباره‌ی استاندارد EIP712و استفاده از آن در فرآیندهای ثبت اطلاعات در بلاک‌چین توضیح می‌دهیم و در ۳-۴ نیز محاسبات مربوط به مکانیزم شهرت را می‌آوریم.



شکل۱-۳. معماری کلی سیستم

۳-۱ نقش های موجود در سیستم

به طور کلی ۲ نقش در سامانه وجود دارد:

- کاربر (user)
- اسکریپت (script)

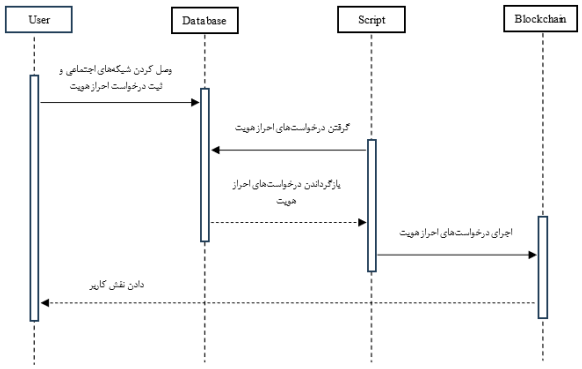
نقش کاربر هم شامل صاحبان سرویس می‌شود که سرویس غیرمتمرکز خود را در سامانه ثبت می‌کنند و هم شامل بازخورد دهندگان می‌شود که بازخوردهای خود را نسبت به سرویس‌های موجود در سامانه ثبت می‌کنند. نقش اسکریپت وظیفه‌ی اجرای خودکار تراکنش‌های مربوط به درخواست‌های اضافه کردن سرویس به پلتفرم و ثبت بازخوردها را دارد.

عملیات مختلفی که توسط هر یک از نقش های بالا انجام می‌شود در ۳-۲ توضیح داده شده است.

۳-۲ فرآیند ها و عملیات سیستم

افراد قبل از انجام هر کاری باید خود را احراز هویت کرده و نقش کاربر را از سامانه‌ی ما دریافت کنند و فقط کسانی که نقش کاربر را دارند می‌توانند از سامانه استفاده کنند. این کار باعث می‌شود که ساخت حساب‌های جعلی کاهش یابد و همچنین باعث کاهش رفتار متقلبانه در سیستم می‌شود. همچنین دیگر کاربران اعتماد بیشتری به سامانه و بازخوردهای ثبت شده در آن می‌کنند.

افراد برای گرفتن نقش کاربر ابتدا باید از طریق کیف پول بلاک‌چینی خود وارد سیستم شوند. پس از وصل کردن کیف پول، برای تکمیل کردن احراز هویت خود باید حساب کاربری توییتر و ایمیل خود را که باید منحصر به فرد بوده و قبلا توسط کاربران دیگر استفاده نشده باشد به سامانه متصل کنند. پس از تکمیل کردن این ۳ مرحله می‌توانند درخواست خود را برای گرفتن نقش کاربر همانطوری که در شکل۲-۳ نیز مشخص است ثبت کنند. ثبت این درخواست از طریق کیف پول بلاک‌چینی کاربران می‌باشد که درخواست خود را برای گرفتن نقش کاربر ثبت می‌کنند و این درخواست‌ها توسط نقش اسکریپت اجرا می‌شوند و درصورتی که کاربران ۳ مرحله احراز هویت را تکمیل کرده باشند از طریق قرارداد هوشمند AccessRestriction که وظیفه‌ی تخصیص و بررسی نقش‌ها را دارد، نقش کاربر به فرد داده می‌شود. این اطلاعات در بلاک‌چین ذخیره می‌شود و بعدا در استفاده‌ی کاربر از سامانه، برای مثال اضافه کردن یک سرویس به سامانه یا ثبت کردن بازخورد نسبت به یک سرویس مورد استفاده قرار می‌گیرد و از طریق قرارداد هوشمند AccessRestriction بررسی می‌شود که فقط افرادی که نقش کاربر را دارند بتوانند عملیات مربوط به افزودن سرویس به سامانه یا ثبت بازخورد را اجرا کنند.



شکل۲-۳. احراز هویت کاربر و گرفتن نقش کاربر

احراز هویت فوق خطرات ناشی از ساخت اکانت‌های جعلی را کاهش می‌دهد و این اطمینان را می‌دهد که فقط افراد واقعی بتوانند از سامانه استفاده کنند و به تبع آن حملات سیبل را در ثبت بازخوردها کاهش می‌دهد.

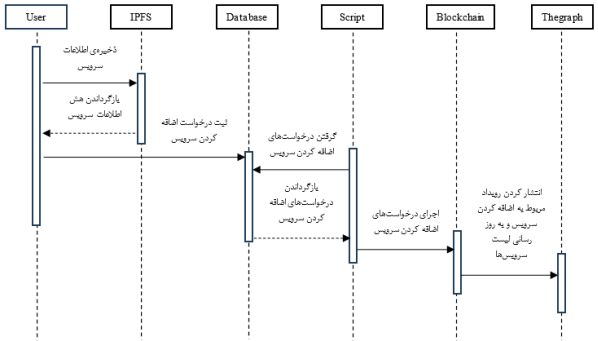
افرادی که نقش کاربر را دریافت کرده‌اند می‌توانند عملیاتی که در جدول۱-۳ آورده شده است را انجام دهند که جزییات آن به شرح زیر می‌باشد:

جدول۱-۳. عملیات کاربر

عنوان	توضیحات
اضافه کردن سرویس غیرمتمرکز برای ثبت بازخورد	افرادی که نقش کاربر را دارند می‌توانند سرویس خود را برای گرفتن بازخورد از دیگران ثبت کنند.
ثبت بازخورد نسبت به یک سرویس	افرادی که نقش کاربر را دارند می‌توانند در صورت استفاده از یک سرویس بازخورد خود را نسبت به آن ثبت کنند.
ثبت بازخورد نسبت به بازخوردهای ثبت شده به یک سرویس	افرادی که نقش کاربر را دارند می‌توانند بازخورد خود را نسبت به بازخوردهایی که دیگران به یک سرویس داده‌اند، در صورت استفاده از آن ثبت کنند.

۳-۲-۱ اضافه کردن سرویس غیرمتمرکز برای ثبت بازخورد

کاربران از طریق واسط کاربری که برای تعامل کاربران با سامانه طراحی شده است می‌توانند اطلاعات سرویس خود را وارد کنند. همانطوری که در شکل۳-۳ مشخص است این اطلاعات در IPFS ذخیره می‌شوند. IPFS برای اطلاعات ذخیره شده یک هش که یکتا می‌باشد را بازمی‌گرداند و این هش نمایانگر اطلاعات سرویس می‌باشد. سپس کاربر از طریق کیف پول خود و با استاندارد EIP712 که در ۳-۳ توضیح داده خواهد شد پیامی را که شامل هش اطلاعات سرویس است امضا می‌کند و درخواست اضافه شدن سرویس به سامانه را ثبت می‌کند. این درخواست‌ها به صورت خودکار و توسط نقش اسکریپت اجرا می‌شوند و در سطح قرارداد هوشمند بررسی می‌شوند که حتما محتوا و فرستنده‌ی درخواست‌ها تغییر نکرده باشد. نقش اسکریپت در صورتی که این محتوا تغییر نکرده باشد و کسی که درخواست ثبت سرویس را دارد دارای نقش کاربر باشد، اطلاعات سرویس را در بلاک‌چین ذخیره می‌کند و یک رویداد ثبت سرویس در شبکه‌ی بلاک‌چین منتشر می‌شود و داده‌های مربوط به این رویداد در TheGraph ذخیره می‌شوند. شکل۳-۳ فرآیند ثبت سرویس توسط کاربر را نشان می‌دهد.

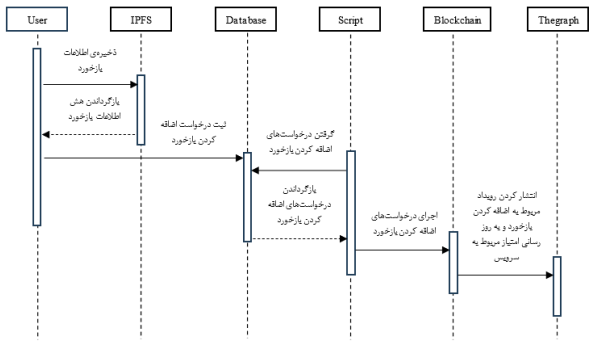


شکل۳-۳. ثبت سرویس توسط کاربر

۳-۲-۲ ثبت بازخورد نسبت به یک سرویس

کاربرانی که از یک سرویس استفاده کرده‌اند می‌توانند بازخورد خود را نسبت به آن سرویس ثبت کنند. این کار از طریق واسط کاربری که برای تعامل کاربر با سامانه در نظر گرفته شده است صورت می‌گیرد و کاربران بازخوردهای خود شامل متن بازخورد و یک عدد در بازه‌ی ۰ تا ۱۰۰ که نمایانگر میزان رضایت از آن سرویس می‌باشد را نسبت به آن سرویس ثبت می‌کنند. از آنجایی که تاریخچه‌ی تراکنش‌های کاربر که با کیف پول بلاک‌چینی خود آن‌ها را انجام داده است به صورت شفاف در بلاک‌چین وجود دارد و قابل تایید و ردیابی توسط همه می‌باشد، سامانه‌ی ما از طریق APIهای پالیگان اسکن [43] می‌تواند تمامی تراکنش‌های کاربر را قبل از ثبت بازخورد بازیابی کند و استفاده کردن کاربر از آن سرویس را بررسی کند و سپس اجازه‌ی اضافه کردن بازخورد نسبت به آن سرویس را بدهد. همانطوری که در شکل۴-۳ مشخص است کاربر اطلاعات بازخورد را در IPFS ذخیره می‌کند و IPFS برای اطلاعات

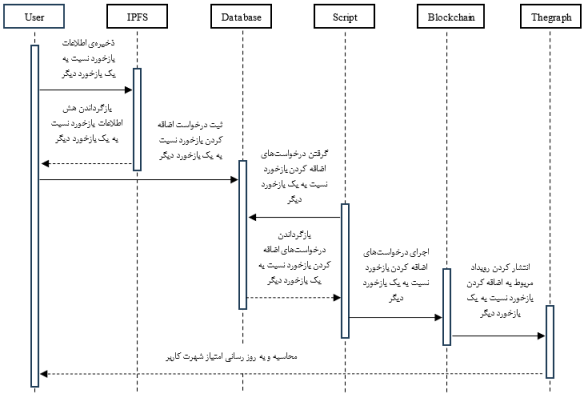
ذخیره شده یک هش که یکتا می‌باشد را بازمی‌گرداند و این هش نمایانگر اطلاعات بازخورد می‌باشد. سپس کاربر از طریق کیف پول خود و با استاندارد EIP712 پیامی را که شامل هش اطلاعات بازخورد است، امضا می‌کند و درخواست اضافه شدن بازخورد به سرویس را ثبت می‌کند. این درخواست‌ها به صورت خودکار و توسط نقش اسکریپت اجرا می‌شوند و در سطح قرارداد هوشمند بررسی می‌شوند که حتما محتوا و فرستنده‌ی درخواست‌ها تغییر نکرده باشد. نقش اسکریپت در صورتی که این محتوا تغییر نکرده باشد و کسی که درخواست ثبت بازخورد را دارد دارای نقش کاربر بوده و قبلا نیز نسبت به آن سرویس بازخورد ثبت نکرده باشد، اطلاعات بازخورد را در بلاک‌چین ذخیره می‌کند و یک رویداد ثبت بازخورد در شبکه‌ی بلاک‌چین منتشر می‌شود و داده‌های مربوط به این رویداد در TheGraph که یک رویکرد غیرمتمرکز برای بازیابی داده‌ها از بلاک‌چین است ذخیره می‌شوند. شکل۴-۳ فرآیند ثبت بازخورد توسط کاربر نسبت به یک سرویس را نشان می‌دهد.



شکل۴-۳. فرآیند ثبت بازخورد

۳-۲-۳ ثبت بازخورد نسبت به بازخوردهای ثبت شده به یک سرویس

کاربران در صورت استفاده از یک سرویس می‌توانند نظرات خود را نسبت به بازخوردهای داده شده به آن ثبت کنند. کاربران همانند ثبت بازخورد به یک سرویس، فقط یکبار می‌توانند بازخورد خود را نسبت به بازخوردی که به یک سرویس داده شده است، ثبت کنند و همچنین برای اینکار حتما باید از آن سرویس استفاده کرده باشند. در این مرحله نیز از طریق واسط کاربری که برای تعامل کاربران با سامانه در نظر گرفته شده است، می‌توانند بازخورد خود شامل متن بازخورد و یک عدد در بازه‌ی ۰ تا ۱۰۰ که نمایانگر میزان موافقت کاربر با بازخورد ثبت شده می‌باشد را نسبت به آن بازخورد ثبت کنند. از آنجایی که تاریخچه‌ی تراکنش‌های کاربر که با کیف پول بلاک‌چینی خود آن‌ها را انجام داده است به صورت شفاف در بلاک‌چین وجود دارد و قابل تایید و ردیابی توسط همه می‌باشد، سامانه‌ی ما از طریق API های پالیگان اسکن [43] می‌تواند تمامی تراکنش‌های کاربر را قبل از ثبت بازخورد نسبت به یک بازخورد دیگر بازیابی کند و استفاده کردن کاربر از آن سرویس را بررسی کند و سپس اجازه‌ی اضافه کردن بازخورد نسبت به بازخوردی که به آن سرویس داده شده است را بدهد. همانطوری که در شکل۵-۳ مشخص است کاربر اطلاعات بازخورد را در IPFS ذخیره می‌کند و IPFS برای اطلاعات ذخیره شده یک هش که یکتا می‌باشد را بازمی‌گرداند و این هش نمایانگر اطلاعات بازخورد کاربر نسبت به بازخورد ثبت شده توسط کاربر دیگر می‌باشد. سپس کاربر از طریق کیف پول خود و با استاندارد EIP712 پیامی را که شامل هش اطلاعات بازخورد خود است، امضا می‌کند و درخواست اضافه شدن بازخورد به یک بازخورد دیگر را ثبت می‌کند. این درخواست‌ها به صورت خودکار و توسط نقش اسکریپت اجرا می‌شوند و در سطح قرارداد هوشمند بررسی می‌شوند که حتما محتوا و فرستنده‌ی درخواست‌ها تغییر نکرده باشد. نقش اسکریپت در صورتی که این محتوا تغییر نکرده باشد و کسی که درخواست ثبت بازخورد را دارد دارای نقش کاربر باشد و همچنین قبلا نسبت به آن بازخورد، بازخوردی ثبت نکرده باشد، اطلاعات بازخورد را در بلاک‌چین ذخیره می‌کند و یک رویداد ثبت بازخورد نسبت به یک بازخورد در شبکه‌ی بلاک‌چین منتشر می‌شود و داده‌های مربوط به این رویداد در TheGraph ذخیره می‌شوند که از این طریق شهرت کاربران و میزان قابل اعتماد بودن بازخوردهایشان محاسبه می‌شود. شکل۵-۳ فرآیند ثبت بازخورد نسبت به بازخوردی که کاربر دیگر به یک سرویس داده است را نشان می‌دهد.



شکل۵-۳. فرآیند ثبت بازخورد نسبت به یک بازخورد

۳-۳ استفاده از EIP712 برای ثبت بازخورد کاربران

انجام تراکنش بر روی شبکه‌ی بلاک‌چین برای کاربران هزینه دارد و آن‌ها باید ارز دیجیتال مخصوص هر شبکه‌ای را که در آن می‌خواهند تراکنش انجام دهند در کیف پول خود داشته باشند و هنگام انجام تراکنش یک مقدار از آن ارز دیجیتال به عنوان سوخت انجام تراکنش از حساب آن‌ها کم شود. این هزینه ممکن است باعث کاهش انگیزه کاربران برای ثبت بازخوردهایشان شود.

در سامانه‌ی پیشنهادی ما برای افزایش انگیزه کاربران برای ثبت بازخورد، امکان ثبت بازخورد بدون هزینه را از طریق EIP712 برای آن‌ها فراهم کرده‌ایم. به این صورت که کاربران محتوای تراکنش خود را امضا می‌کنند و این درخواست‌ها به صورت خودکار توسط نقش اسکریپت اجرا می‌شوند. از طرفی استاندارد EIP712 این اطمینان را به کاربر می‌دهد که محتوای پیامی که آن‌ها امضا کرده‌اند هنگام اضافه شدن به بلاک‌چین تغییر نخواهد کرد. برای اینکار کاربران از طریق کیف پول خود و با استفاده از کلید خصوصی خود یک پیام را که از استاندارد EIP712 پیروی می‌کند امضا می‌کنند. پیامی که کاربر امضا می‌کند از ۲ قسمت دامنه و پیام اصلی تشکیل شده است که در بخش ۲-۱-۶ در مورد آن‌ها توضیح داده شد. دامنه‌ی پیامی که کاربر امضا می‌کند در این سامانه ثابت می‌باشد اما داده‌های پیام اصلی وابسته به تابعی که کاربر می‌خواهد آن را امضا کند متفاوت است که در زیر انواع مختلف توابعی که کاربر در سامانه‌ی ما امضا می‌کند به همراه داده‌های مربوط به آن آورده شده است:

۳-۳-۱ اضافه کردن سرویس به سامانه

در این تابع پیام اصلی که کاربر امضا می‌کند به شرح زیر است:

- نانس افزودن سرویس: یک عدد است که مقدار آن بعد از هر امضای کاربر برای افزودن سرویس یک واحد افزایش می‌یابد و برای اطمینان از اینکه فقط یکبار امکان استفاده از آن امضا وجود دارد در پیام اصلی استفاده می‌شود.
- هش اطلاعات: هش اطلاعات مربوط به یک سرویس می‌باشد.
- آدرس بلاک‌چینی سرویس: آدرس بلاک‌چینی سرویسی است که کاربر اضافه می‌کند.

۳-۳-۲ ثبت بازخورد نسبت به یک سرویس

در این تابع پیام اصلی که کاربر امضا می‌کند به شرح زیر است:

- نانس ثبت بازخورد نسبت به یک سرویس: یک عدد است که مقدار آن بعد از هر امضای کاربر برای ثبت بازخورد نسبت به یک سرویس یک واحد افزایش می‌یابد و برای اطمینان از اینکه فقط یکبار امکان استفاده از آن امضا وجود دارد در پیام اصلی استفاده می‌شود.
- امتیاز: یک عدد بین ۰ تا ۱۰۰ است که نشان دهنده‌ی امتیاز کاربر نسبت به یک سرویس می‌باشد.
- هش اطلاعات: هش اطلاعات مربوط به بازخورد می‌باشد.
- آدرس بلاک‌چینی سرویس: آدرس بلاک‌چینی سرویسی است که کاربر نسبت به آن بازخورد ثبت می‌کند.

۳-۳-۳ ثبت بازخورد نسبت به یک بازخورد

در این تابع پیام اصلی که کاربر امضا می‌کند به شرح زیر است:

- نانس ثبت بازخورد نسبت به یک بازخورد: یک عدد است که مقدار آن بعد از هر امضای کاربر برای ثبت بازخورد نسبت به یک بازخورد یک واحد افزایش می‌یابد و برای اطمینان از اینکه فقط یکبار امکان استفاده از آن امضا وجود دارد در پیام اصلی استفاده می‌شود.

- امتیاز: یک عدد بین ۰ تا ۱۰۰ است که نشان دهنده‌ی امتیاز کاربر نسبت به یک بازخورد می‌باشد.
- هش اطلاعات: هش اطلاعات مربوط به یک بازخورد می‌باشد.
- بازخورد دهنده‌ی قبلی: آدرس بلاک‌چینی بازخورد دهنده‌ی قبلی می‌باشد.
- آدرس بلاک‌چینی سرویس: آدرس بلاک‌چینی سرویسی است که کاربر نسبت به بازخوردی که به آن ثبت شده، بازخورد ثبت می‌کند.

پس از امضا کردن پیام توسط کاربر این امضا به همراه اطلاعات محتوایی که کاربر امضا کرده است به قرارداد هوشمند فرستاده می‌شود و در سطح قرارداد هوشمند این امضا رمزگشایی می‌شود. اگر تغییری در محتوای پیام صورت نگرفته باشد نتیجه‌ی رمزگشایی امضا برابر کسی که پیام را امضا کرده است خواهد بود و در صورت کوچک‌ترین تغییر در محتوا، نتیجه‌ی رمزگشایی امضا مقدار متفاوتی خواهد بود و این تراکنش بر روی بلاک‌چین ثبت نخواهد شد. پس EIP712 این اطمینان را به کاربران می‌دهد که بازخوردهای آن‌ها هنگام ثبت شدن در بلاک‌چین تغییر نخواهند کرد و به کمک آن ما در پلتفرم خود امکان ثبت بازخورد به صورت خارج از زنجیره را برای کاربران فراهم می‌کنیم. ثبت کردن تراکنش‌های کاربران به این صورت در بلاک‌چین این امکان را می‌دهد که آن‌ها بدون اینکه هزینه‌ای پرداخت کنند تراکنش خود را در شبکه ثبت کنند و مطمئن باشند که تغییری در تراکنش آن‌ها صورت نخواهد گرفت.

۳-۴ محاسبات مربوط به مکانیزم شهرت

سیستم شهرت به عنوان یک مولفه‌ی مهم برای اطمینان از اعتبار، قابلیت اطمینان و قابل اعتماد بودن بازخوردهای کاربران تلقی می‌شود و یک معیار مهم برای قابل اعتماد بودن مشارکت کنندگان سیستم محسوب می‌شود. بالا بودن امتیاز شهرت قابلیت اطمینان بازخوردهای ثبت شده توسط یک کاربر را بالا می‌برد یعنی افراد به بازخوردهای کسانی که شهرت بیشتری دارند نسبت به کسانی که امتیاز شهرت آن‌ها کم است بیشتر اعتماد می‌کنند.

از آنجایی که در سامانه‌ی ما امکان ارزیابی بازخوردهایی که کاربران ثبت می‌کنند توسط کاربران دیگر وجود دارد و با رفتار مخرب و ثبت بازخوردهای جعلی و غیرواقعی امتیاز شهرت آن‌ها کاهش می‌یابد و باعث می‌شود که افراد دیگر به بازخوردهای آن‌ها اعتماد کمتری کنند و آن‌ها را به عنوان کاربر مخرب در سامانه بشناسند، پس کاربران با ثبت بازخوردهای واقعی و درست در راستای افزایش امتیاز شهرت خود تلاش می‌کنند. دخیل کردن میزان شهرت بازخورد دهنده‌ها در میزان قابل اعتماد بودن بازخوردهای آن‌ها باعث کاهش حملات سیبل می‌شود و افراد تمایل کمتری به ثبت بازخورد با هویت‌های جعلی و متعدد پیدا می‌کنند و با ثبت بازخوردهای سازنده کیفیت کلی اطلاعات سیستم را افزایش می‌دهند.

در سامانه‌ی ما کاربران می‌توانند نسبت به یک سرویس یا نسبت به بازخوردهای دیگران که به یک سرویس داده شده است بازخورد ثبت کنند. این بازخوردها شامل متن بازخورد و یک عدد بین ۰ تا ۱۰۰ می‌باشند که نمایانگر میزان قابل اعتماد بودن یک سرویس یا یک بازخورد است. پس از ثبت این بازخوردها یک رویداد در شبکه‌ی بلاک‌چین منتشر می‌شود و اطلاعات این رویداد در TheGraph ذخیره می‌شود. مقدار اولیه‌ی شهرت کاربران که در قابل اعتماد بودن بازخوردهایی که ثبت می‌کنند موثر است پس از ثبت نام ۰ می‌باشد و بر حسب بازخوردی که از دیگر کاربران دریافت می‌کنند مقدار آن به روز رسانی می‌شود.

در این سامانه هم برای سرویس‌های غیرمتمرکز و هم برای کاربران میزان قابل اطمینان بودن را محاسبه می‌کنیم. میزان قابل اطمینان بودن سرویس‌ها به صورت وزن دار از بازخوردهایی که کاربران به آن‌ها می‌دهند محاسبه می‌شود و میزان قابل اطمینان بودن کاربران یا همان امتیاز شهرت کاربران نیز به صورت وزن دار از بازخوردهایی که دیگر کاربران به بازخوردهای آن‌ها می‌دهند محاسبه می‌شود. این وزن به میزان امتیاز شهرت کاربران بستگی دارد یعنی بازخورد کاربران با امتیاز شهرت بالا به نسبت کاربران با امتیاز شهرت پایین تاثیر بیشتری بر امتیاز شهرت یک سرویس یا یک کاربر دارد.

در صورتی که کاربر هیچ بازخوردی دریافت نکرده باشد وزن شهرت کاربر در بازخوردهایی که می‌دهد تاثیرگذار نخواهد بود و به صورت موقت بیشترین مقدار ممکن برای وزن که ۱ می‌باشد در نظر گرفته می‌شود. در صورتی که یک کاربر

اولین بازخورد را از کاربران دیگر دریافت کند و فرآیند به روز رسانی شهرت برای او آغاز شود امتیاز شهرت محاسبه شده برای او که یک عدد بین ۰ و ۱ می‌باشد به عنوان وزن کاربر در نظر گرفته می‌شود.

به طور خلاصه در سامانه‌ی ما میزان وزن کاربر به صورت زیرمحاسبه می‌شود:

```
if (userFeedbackTaken == 0) {
  userWeight = 1;
} else {
  userWeight = userReputation;
}
```

میزان امتیاز شهرت یک کاربر همانطوری که اشاره شد در ابتدا ۰ می‌باشد و وقتی که از کاربران دیگر بازخورد دریافت می‌کند از طریق فرمول زیر محاسبه و به روز رسانی می‌شود:

$$userReputation += (feedback - userReputation)/totalFeedBack * userWeight \quad (۱)$$

پارامترهای فرمول ۱ به شکل زیر می‌باشند:

userReputation: امتیاز شهرت کاربری که نسبت به او بازخورد ثبت شده است.

feedback: امتیاز بازخورد ثبت شده نسبت به یک کاربر که عددی بین ۰ و ۱۰۰ می‌باشد.

totalFeedBack: تعداد کل بازخورد ثبت شده نسبت به یک کاربر.

userWeight: وزن کاربری که بازخورد ثبت می‌کند.

میزان قابل اعتماد بودن یک سرویس نیز همانند امتیاز شهرت کاربر در ابتدا مقدار ۰ می‌باشد و با گرفتن بازخورد از کاربران میزان قابل اعتماد بودن سرویس از طریق فرمول زیر محاسبه و به روز رسانی می‌شود:

$$serviceRate += (feedback - serviceRate)/totalFeedBack * userWeight \quad (۲)$$

پارامترهای فرمول ۲ به شکل زیر می‌باشند:

serviceRate: امتیاز سرویسی که نسبت به آن بازخورد ثبت شده است.

feedback: امتیاز بازخورد ثبت شده نسبت به یک سرویس که عددی بین ۰ و ۱۰۰ می‌باشد.

totalFeedBack: تعداد کل بازخورد ثبت شده نسبت به یک سرویس.

userWeight: وزن کاربری که بازخورد ثبت می‌کند.

همان طور که در فرمول‌های ۱ و ۲ آورده شده است بازخوردهای کاربران نسبت به یک سرویس یا بازخوردهای آن‌ها نسبت به بازخوردهای دیگران که به یک سرویس ثبت شده است به صورت وزن دار و متناسب با میزان شهرت کاربر بر شهرت فرد یا سرویس تاثیر می‌گذارد.

ذخیره کردن محتوای بازخوردها در بلاک‌چین و انتشار رویدادهای مربوط به تراکنش‌ها بر روی بلاک‌چین و همچنین ذخیره سازی اطلاعات رویدادها خارج از زنجیره‌ی بلاک‌چین و در TheGraph علاوه بر اینکه شفافیت و تغییر ناپذیری داده‌ها به دلیل اینکه داده‌ها همچنان در بلاک‌چین ذخیره هستند و قابل تایید توسط همه می‌باشند را تضمین می‌کند، علاوه بر آن به دلیل خارج کردن محاسبات مربوط به مکانیزم شهرت از بلاک‌چین و انجام محاسبات خارج از زنجیره بلاک‌چین باعث افزایش مقیاس‌پذیری می‌شود.

TheGraph یک پروتکل غیرمتمرکز است که از آن برای نمایه‌سازی و بازیابی داده‌های بلاک‌چین استفاده می‌شود. این پروتکل به گونه‌ای طراحی شده است که بازیابی و استفاده از داده‌های بلاک‌چین را در برنامه‌های غیرمتمرکز برای توسعه دهندگان آسان‌تر می‌کند. پروتکل TheGraph علاوه بر اینکه فرآیند دسترسی به داده‌های بلاک‌چین را ساده‌تر می‌کند و ساخت برنامه‌های غیرمتمرکز را برای توسعه دهندگان آسان‌تر می‌کند، ماهیت غیرمتمرکز پروتکل را نیز تضمین می‌کند که دسترسی به داده‌ها قابل اعتماد و مقاوم در برابر سانسور و تغییر باقی می‌ماند. با افزایش حجم بازخوردها و تعاملات کاربران، محاسبات خارج از زنجیره به نسبت محاسبات بر روی زنجیره آسان‌تر انجام می‌شوند و قابل دسترس‌تر می‌باشند. همچنین سیستم‌های شهرت اغلب شامل الگوریتم‌های پیچیده می‌باشند که محاسبات خارج از زنجیره انعطاف پذیری بیشتری را برای پیاده سازی آن‌ها فراهم می‌کند و از لحاظ هزینه نیز برای

سیستم بهینه می‌باشد چون انجام محاسبات بر روی شبکه بلاک‌چین نیازمند هزینه می‌باشد در حالی که خارج از شبکه بلاک‌چین نیازی به پرداخت هزینه نیست و در عین حال از همان شفافیت و مزایای بلاک‌چین بهره مند است و نتایج حاصل از محاسبات قابل تایید توسط افراد دیگر می‌باشد. پس محاسبات خارج از زنجیره در سامانه‌ی ما در عین این که این اطمینان را می‌دهد که اطلاعات سامانه قابل اعتماد و هماهنگ با اطلاعات روی بلاک‌چین است، باعث کاهش هزینه‌ی محاسبات مقادیر امتیاز شهرت می‌شود و مقیاس‌پذیری سیستم را افزایش می‌دهد.

۴- ارزیابی

در این بخش ابتدا در ۴-۱ انواع سناریوهای مربوط به حملات و چالش‌های سیستم ثبت بازخورد را بررسی می‌کنیم. سپس در ۴-۲ عملکرد سیستم را در برابر مواردی که در ۴-۱ آورده شده است، بررسی می‌کنیم و در انتها در ۴-۳ به تجزیه و تحلیل عملکرد هزینه‌ای سامانه می‌پردازیم.

۴-۱ چالش‌ها و حملات مرتبط با سیستم ثبت بازخورد

در این بخش ما انواع حملات و چالش‌های مربوط به سیستم ثبت بازخورد و اهمیت پرداختن به آن‌ها را بررسی می‌کنیم. بیشتر حملات و چالش‌های رایج مانند حمله‌ی تبانی، حمله‌ی سیبل و ... همانطوری که توسط [15,16,17,44,45] توضیح داده شده است، در زیر فهرست شده اند.

۴-۱-۱ ثبت نظرات جعلی

این نوع تقلب شامل ارائه‌ی بازخورد به یک سرویس بدون استفاده‌ی واقعی از آن‌ها است. این کار می‌تواند به شکل بازخوردهای مثبت یا منفی ساختگی باشد که اغلب به دلیل به دست آوردن مزیت رقابتی، تبلیغات بیشتر و انگیزه‌های مالی می‌باشد. بررسی این نوع تقلب‌ها به دلیل تاثیر قابل توجه آن در یکپارچگی سیستم‌های ثبت بازخورد آنلاین بسیار مهم است. بازخوردهای تقلبی ممکن است مصرف کنندگان را گمراه کند و به تصمیمات آن‌ها تاثیر بگذارد. همچنین ثبت بازخورد توسط کسانی که تجربه‌ی استفاده از یک محصول را ندارند باعث می‌شود که بازخوردهای موجود در سیستم غیرقابل اعتماد شوند و اعتبار کلی سیستم را کاهش دهد.

۴-۱-۲ حمله‌ی تبانی در ثبت بازخورد

در این نوع حمله چندین کاربر به صورت هماهنگ اقدام به دستکاری و مخدوش کردن یکپارچگی و اعتبار سامانه می‌کنند و باعث می‌شوند که صحت بازخوردهای موجود در سامانه و قابلیت اطمینان آن‌ها کاهش یابد که این اتفاق باعث کاهش اعتبار کلی سیستم می‌شود. در حمله‌ی تبانی کاربران با همکاری یکدیگر و با هدف ایجاد تصویری تحریف شده از یک سرویس، بازخوردهای مغرضانه و متقلبانه به یک سرویس می‌دهند. حملات تبانی می‌توانند به صورت نظرات مصنوعی مثبت و منفی درباره‌ی یک سرویس و یا سرکوب نظرات مثبت یا منفی درباره‌ی یک سرویس اتفاق بیفتد که اعتبار کل سامانه‌ی ثبت بازخورد را به خطر می‌اندازد. این حملات تهدیدی جدی برای سامانه‌های ثبت بازخورد آنلاین می‌باشند که خود را مرجعی برای راهنمایی کاربران معرفی می‌کنند چون این حملات می‌تواند کاربران را گمراه کند و آن‌ها را به سمت انتخاب‌های مبتنی بر اطلاعات نادرست و دستکاری شده سوق دهد.

۴-۱-۳ حمله‌ی سیبل در ثبت نظرات

در حمله‌ی سیبل یک کاربر با ایجاد حساب‌های کاربری جعلی متعدد، یکپارچگی سامانه را به هم می‌ریزد. این استراتژی چهره‌ای از کاربران متنوع و قانونی ایجاد می‌کند درحالی که در واقعیت، همه‌ی این کاربران از یک منبع مخرب واحد سرچشمه می‌گیرند. همچنین کاربران می‌توانند با ایجاد هویت‌های متنوع انواع حملات ثبت بازخورد مانند حمله‌ی تبانی را انجام دهند. حمله‌ی سیبل مانند دیگر حملات قابلیت اعتماد سامانه را کاهش می‌دهد و باعث می‌شود که بازخوردهایی که در سامانه ثبت شده است نامعتبر باشد و کاربران دیگر نتوانند آن‌ها را مبنای تصمیم‌گیری قرار دهند.

۴-۱-۴ دستکاری داده‌ها یا حذف نظرات منفی

یکی از مشکلات موجود در پلتفرم‌های ثبت بازخورد آنلاین، دستکاری محتوای بازخورد توسط سامانه‌های ثبت بازخورد است که به موضوعی رایج و نگران کننده تبدیل شده است. دستکاری بازخوردهای کاربران باعث ایجاد تردید در صحت و اعتبار بازخوردهای تولید شده توسط کاربران می‌شود. این عمل شامل تلاش‌های عمدی توسط خود سامانه برای تغییر یا تحریف بازخوردهای سرویس‌ها، خدمات و یا کسب وکارها می‌باشد که باعث ایجاد درک نادرستی از کیفیت و شهرت آن‌ها می‌شود. سامانه‌های ثبت بازخورد ممکن است از روش‌های مختلف مانند

نمایش انتخابی نظرات مثبت و سرکوب نظرات منفی، تغییر محتوای بازخورد ثبت شده توسط کاربر و ارائه‌ی بازخورد دلخواه و یا حذف کردن بازخوردهای کاربران برای این منظور استفاده کنند. این دستکاری‌ها اعتماد کاربران به سیستم‌های بررسی آنلاین را از بین می‌برد و آن‌ها نمی‌توانند از این بازخوردها در تصمیم‌گیری‌های خود مبنی بر استفاده یا عدم استفاده از یک سرویس استفاده کنند و همچنین باعث کاهش قابلیت اطمینان اطلاعات سامانه می‌شود. در نتیجه قابلیت اعتماد کلی سامانه نیز کاهش می‌یابد و کاربران نمی‌توانند به بازخوردهای موجود در چنین سامانه‌ای اعتماد کنند.

۴-۱-۵ ثبت نظرات متعصبانه و جهت دار

در این حالت کاربران با اینکه واقعا از یک سرویس استفاد کرده‌اند ولی ممکن است به دلیل انگیزه‌ها و وابستگی‌های شخصی، ارزیابی نادرستی را به سرویس‌ها ارائه کنند که ممکن است ماهیت واقعی آن سرویس را به درستی منعکس نکند. این جانبداری می‌تواند به صورت نظرات بسیار مثبت یا منفی، تحت تاثیر عوامل غیرمرتبط با تجربه‌ی واقعی کاربر ظاهر شود. این نوع بازخوردها به صورت حمایت‌های شدید یا مخالفت‌های کورکورانه که اغلب ناشی از عقاید شخصی و افراطی افراد است نمایان می‌شود. بازخوردهای متعصبانه و جهت‌دار باعث انحراف اکوسیستم ثبت بازخورد می‌شود و مانع از توانایی سایر کاربران برای تصمیم‌گیری عینی و آگاهانه می‌شود و باعث می‌شود که اعتبار و قابلیت اطمینان بازخوردهای ثبت شده کاهش یابد که این امر منجر به کاهش اعتماد کاربران به بازخوردهای ثبت شده در چنین سامانه‌ای می‌شود و همچنین باعث می‌شود که قابلیت اعتماد کلی سیستم کاهش یابد.

۴-۱-۶ قابلیت اعتماد بازخوردهای ثبت شده

یکی از مهم‌ترین چالش‌هایی که در سامانه‌های ثبت بازخورد آنلاین وجود دارد بحث قابل اعتماد بودن بازخوردهای ثبت شده در سامانه است. مشکلاتی مانند دستکاری محتوای بازخوردها، ثبت بازخوردهای جعلی و غیرواقعی، آسیب‌پذیری سامانه در برابر حملات ثبت بازخورد مانند حملات سیبل و تبانی و همچنین شفاف نبودن فرآیند ثبت بازخورد باعث می‌شود که بازخوردهای موجود در یک سامانه غیرقابل اعتماد شوند و چون کاربران نمی‌توانند به صورت شفاف مراحل ثبت بازخورد را ببینند و حتی نمی‌توانند از اصیل بودن یک بازخورد اطمینان حاصل کنند پس نتوانند این بازخوردها را معیاری برای تصمیم‌گیری خود قرار دهند چون ممکن است این بازخوردها دستکاری شده باشد و یا محتوای آن‌ها غیرواقعی و جعلی باشد. به همین دلیل قابلیت اطمینان بازخوردها یکی از مهم‌ترین چالش‌های چنین سامانه‌هایی می‌باشد و این سامانه‌ها برای جلب اعتماد کاربران و اطمینان خاطر دادن به آن‌ها از اینکه یک بازخورد معتبر و بدون دستکاری و شفاف است، باید تمرکز ویژه‌ای روی افزایش قابلیت اطمینان بازخوردها داشته باشند.

جدول۱-۴. حملات و چالش‌های مربوط به ثبت بازخورد و مکانیزم دفاعی سامانه‌ی ثبت بازخورد ما در برابر آن‌ها

عنوان حمله یا چالش	مکانیزم دفاعی
ثبت نظرات جعلی	۱- بررسی کردن استفاده‌ی کاربران از یک سرویس قبل از ثبت بازخورد ۲- امکان ثبت بازخورد فقط از طریق کلید خصوصی کیف پول بلاک‌چینی کاربر
حمله‌ی تبانی در ثبت بازخورد	۱- هزینه دار بودن ثبت بازخورد نسبت به یک سرویس به دلیل الزام استفاده‌ی کاربر از آن سرویس قبل از ثبت بازخورد ۲- امکان ارزیابی بازخوردهای ثبت شده نسبت به یک سرویس توسط دیگر کاربران که از آن استفاده کرده‌اند ۳- وجود مکانیزم شهرت
حمله‌ی سیبل در ثبت بازخورد	۱- وجود احراز هویت ۳ مرحله‌ای ۲- بررسی کردن استفاده‌ی کاربران از یک سرویس قبل از ثبت بازخورد نسبت به آن
دستکاری داده‌ها یا حذف نظرات منفی	۱- استفاده از فناوری بلاک‌چین برای ذخیره‌سازی بازخوردها ۲- استفاده از قراردادهای هوشمند برای ثبت بازخوردها
ثبت نظرات متعصبانه و غیرواقعی	۱- امکان ارزیابی بازخوردهای ثبت شده نسبت به یک سرویس توسط دیگر کاربرانی که از آن استفاده کرده‌اند ۲- وجود مکانیزم شهرت
قابلیت اعتماد بازخوردهای ثبت شده	۱- ثبت شدن بازخوردها بر روی بلاک‌چین ۲- مقاوم بودن سامانه در برابر حملات احتمالی ۳- وجود سیستم ارزیابی بازخوردهای ثبت شده

۴-۲ تجزیه و تحلیل عملکرد سیستم در برابر حملات ثبت بازخورد

در این بخش به تجزیه و تحلیل عملکرد سامانه‌ی خود در برابر حملات و چالش‌هایی که در ۴-۱ توضیح داده شد می‌پردازیم. در جدول۱-۴ خلاصه‌ای از حملات و چالش‌های سامانه‌های ثبت بازخورد و مکانیزم‌های دفاعی سامانه‌ی خود در برابر آن‌ها آورده شده است. سامانه‌ی ما با قدرت گرفتن از قابلیت ردیابی در بلاک‌چین، با بررسی تاریخچه‌ی تراکنش‌های یک کاربر فقط به کسانی که از یک سرویس استفاده کرده‌اند، اجازه‌ی ثبت بازخورد به آن سرویس را می‌دهد و همچنین با پیاده سازی مکانیزم شهرت و یک سیستم احرازهویت ۳ مرحله‌ای از طریق کیف پول بلاک‌چینی، ایمیل و توییتر در برابر تقلب‌های ثبت بازخورد مقاوم می‌شود. سامانه‌ی ما با تمرکززدایی، نهاد واسط را از فرآیند ثبت بازخورد حذف می‌کند و این باعث می‌شود که بازخوردها پس از ثبت شدن در سامانه‌ی ما غیرقابل تغییر شوند و امکان دستکاری آن‌ها وجود نداشته باشد. همچنین در سامانه‌ی ما کاربران دیگر می‌توانند بازخوردهایی که به یک سرویس داده شده است را ارزیابی کنند.

در زیر به طور جداگانه عملکرد سامانه‌ی خود را در کنار دیگر سامانه‌هایی که در بخش ۲-۲ آورده شده است، در برابر حملات و چالش‌های مطرح شده بررسی می‌کنیم.

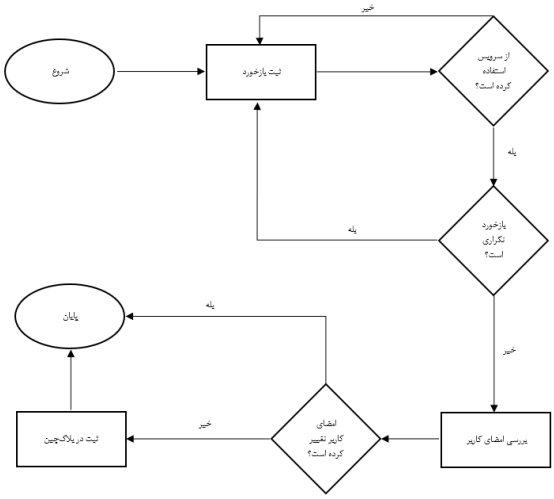
۱-۲-۴ ثبت نظرات جعلی

ما ابتدا عملکرد سامانه‌ی خود و سپس عملکرد کارهای آورده شده در بخش ۲-۲ را در برابر این حمله بررسی می‌کنیم.

سامانه‌ی ما به کمک فناوری بلاک‌چین از ثبت بازخوردهای جعلی جلوگیری می‌کند. در سامانه‌ی ما کاربران از طریق کیف پول بلاک‌چینی خود برای سرویس‌های مختلف بازخورد ثبت می‌کنند و اساس فعالیت بر حسب آدرس کیف پول بلاک‌چینی می‌باشد. از آنجایی که تاریخچه‌ی فعالیت‌های کاربر از ابتدای ساخت کیف پول در بلاک‌چین وجود دارد و قابل ردیابی است، سامانه‌ی ما این امکان را دارد که بررسی کند یک کاربر حتما از سرویسی که می‌خواهد به آن بازخورد دهد استفاده کرده باشد. ما قبل از اینکه به کاربر اجازه‌ی ثبت بازخورد بدهیم تاریخچه‌ی تراکنش‌های کیف پول بازخورد دهنده را بررسی می‌کنیم که حتما از آن سرویس استفاده کرده باشد و از این طریق مطمئن می‌شویم افرادی که واقعا از یک سرویس استفاده کرده‌اند نسبت به آن بازخورد ثبت می‌کنند و کسانی که از یک سرویس استفاده نکرده‌اند حق ثبت بازخورد نسبت به آن را ندارند.

در سامانه‌ی ما به دلیل شفاف بودن فرآیند ثبت بازخورد و استفاده از قراردادهای هوشمند، افرادی که از یک سرویس استفاده کرده‌اند این امکان را ندارند که از طرف دیگر افراد اقدام به ثبت بازخورد کنند به این دلیل که در سطح قرارداد هوشمند سامانه‌ی ثبت بازخورد، بررسی می‌شود که محتوای بازخورد حتما با کلید خصوصی کسی که بازخورد را ثبت می‌کند امضا شده باشد و در صورت مغایرت این بازخورد در بلاک‌چین ثبت نمی‌شود. پس کسانی که از یک سرویس استفاده نکرده‌اند و همچنین دیگر کاربرانی که از یک سرویس استفاده کرده اند به جای یک کاربر نمی‌توانند در سامانه‌ی ما بازخورد ثبت کنند و فقط خود کاربر در صورت استفاده از یک سرویس می‌تواند نسبت به آن بازخورد ثبت کند که این عمل سامانه‌ی ما را در برابر ثبت بازخوردهای جعلی مقاوم می‌کند. شکل۱-۴ فلوچارت ثبت بازخورد توسط کاربر را در سامانه‌ی ما نشان می‌دهد.

در اینجا به بررسی عملکرد کارهای مطرح شده در بخش ۲-۲ در برابر ثبت نظرات جعلی می‌پردازیم. در [37] سامانه قبل از اینکه اجازه ثبت بازخورد به کاربر را بدهد، استفاده کردن کاربر از یک محصول را بررسی می‌کند و فقط به کاربرانی که از یک محصول استفاده کرده‌اند، اجازه‌ی ثبت بازخورد می‌دهد و به همین دلیل است که در برابر ثبت نظرات جعلی مقاوم می‌باشد. در [40] صاحبان سرویس می‌توانند به کاربران مجوز ثبت بازخورد نسبت به محصولات خود را بدهند و کسانی که این مجوز را داشته باشند می‌توانند نسبت به آن محصول بدون اینکه از آن استفاده کرده باشند بازخورد ثبت کنند که این سامانه را در برابر ثبت بازخوردهای جعلی آسیب‌پذیر می‌کند. [41] از طریق شناسه‌ی سفارش فقط به کسانی که یک محصول را خریده باشند اجازه‌ی ثبت بازخورد می‌دهد که این سامانه را در برابر ثبت نظرات جعلی مقاوم می‌کند. همچنین در [42] از طریق توکن PRAT فقط به کسانی که یک محصول را خریداری کرده‌اند امکان ثبت بازخورد داده می‌شود که باعث می‌شود این سامانه در برابر ثبت نظرات جعلی مقاوم باشد.



شکل۱-۴. فلوچارت بررسی استفاده کاربر از یک سرویس قبل از ثبت بازخورد

۴-۲-۲ حمله‌ی تبانی در ثبت بازخورد

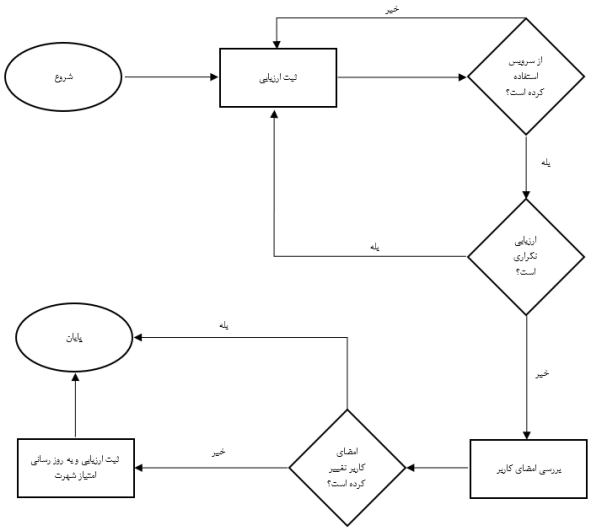
ما ابتدا عملکرد سامانه‌ی خود و سپس عملکرد کارهای آورده شده در بخش ۲-۲ را در برابر این حمله بررسی می‌کنیم.

برای این حمله ما ۲ سناریوی ممکن را بررسی می‌کنیم. در سناریوی اول کاربرانی را در نظر می‌گیریم که به صورت گروهی می‌خواهند به یک سرویس رقیب بازخورد منفی ثبت کنند. در سامانه‌ی ما کاربران برای اینکه بتوانند نسبت به یک سرویس بازخورد ثبت کنند همانطوری که در شکل۱-۴ نیز نشان داده شده است حتما باید از آن سرویس استفاده کرده باشند. به همین دلیل این کاربران باید ۲ نوع هزینه برای ثبت بازخورد نسبت به آن سرویس پرداخت کنند. هزینه‌ی اول مربوط به استفاده از خدمات آن کسب و کار است و از آنجایی که کاربر برای انجام تراکنش بر روی شبکه‌ی بلاک‌چین باید مقداری هزینه به عنوان کارمزد پرداخت کند، هزینه دوم مربوط به کارمزد تراکنش برای استفاده از آن سرویس می‌باشد. استفاده از سرویس رقیب علاوه بر اینکه باعث افزایش درآمد رقیب می‌شود، هزینه‌هایی را نیز برای کسی که می‌خواهد بازخوردهای منفی به آن سرویس ثبت کند به همراه دارد که این مورد را انتخاب اقتصادی برای آن‌ها نمی‌کند. با این حال اگر کسی مایل به پرداخت این هزینه بود می‌تواند نسبت به آن سرویس بازخورد ثبت کند اما همانطوری که در فلوچارت مربوط به ارزیابی در شکل۲-۴ نشان داده شده است این امکان وجود دارد که اعتبار این بازخوردها توسط کاربران دیگر که از آن سرویس استفاده کرده‌اند ارزیابی شود و آن‌ها می‌توانند به این بازخوردها امتیاز بدهند که این امتیازها نشان‌دهنده‌ی میزان قابل اعتماد بودن آن بازخورد است و بر اساس آن امتیاز شهرت کاربر به روز رسانی می‌شود. از طرفی میزان شهرت کاربران به صورت وزن دار بر روی بازخوردی که می‌دهند تاثیر دارد یعنی بازخورد افراد با میزان شهرت بالاتر از قابلیت اعتماد بیشتری نسبت به افراد با میزان شهرت پایین‌تر برخوردار است به همین دلیل این ارزیابی‌ها در صورت رفتار مخرب ممکن است با کاهش امتیاز شهرت تاثیر بازخوردهایی که یک کاربر می‌دهد را کاهش دهد.

در سناریوی دوم افرادی را در نظر می‌گیریم که می‌خواهند به سرویس خود یا یک سرویس دیگر بازخورد مثبت ثبت کنند. در این مورد هزینه‌ی استفاده از آن خدمت ممکن است به نوعی به کاربران بازگشت داده شود اما در این حالت نیز دیگر کاربرانی که از آن سرویس استفاده کرده‌اند می‌توانند این بازخوردها را ارزیابی کنند و آن‌ها کنترلی بر این فرآیند ندارند و این ارزیابی‌ها همانطوری که توضیح داده شد تاثیر مستقیم بر روی امتیاز شهرت افراد دارد. سامانه‌ی ما از طرفی با پیاده سازی مکانیزم شهرت و امکان ارزیابی بازخوردها توسط دیگر کاربران و از طرف دیگر با الزام استفاده از سرویس توسط کاربر قبل از ثبت بازخورد تا حد زیادی مانع از حمله‌ی تبانی می‌شود و در صورتی که این حمله اتفاق بیفتد به مرور زمان و با کمک مکانیزم شهرت تاثیر بازخوردهای کسانی که حمله‌ی تبانی انجام داده‌اند را کاهش می‌دهد و آن‌ها را تبدیل به افراد غیرقابل اعتماد بین دیگر کاربران می‌کند که یک عامل بازدارنده برای حمله‌ی تبانی توسط کاربران می‌باشد.

در اینجا به بررسی عملکرد کارهای مطرح شده در بخش ۲-۲ در برابر ثبت نظرات جعلی می‌پردازیم. در [39] کاربران برای ثبت بازخورد نسبت به یک محصول باید از قبل آن را خریده باشند. این مورد با بالا بردن هزینه‌ی ثبت بازخورد برای کسانی که می‌خواهند به محصولات رقیب بازخورد منفی جعلی ثبت کنند، مانع از حمله‌ی تبانی می‌شود اما در مورد کسانی که می‌خواهند نسبت به سامانه‌ی خود بازخوردهای مثبت جعلی ثبت کنند آسیب پذیر است. در این حالت چون کاربران از محصولات خود استفاده می‌کنند خرید یک محصول هزینه ثبت بازخورد را افزایش نمی‌دهد. از طرف دیگر به دلیل اینکه بازخوردهایی که یک کاربر ثبت می‌کند توسط دیگران ارزیابی نمی‌شود، افرادی که بازخوردهای جعلی مثبت ثبت می‌کنند امتیاز شهرتشان کاهش پیدا نمی‌کند. پس افراد می‌توانند

بازخوردهای جعلی مثبت در این سامانه ثبت کنند و این سامانه در برابر حمله‌ی تبانی آسیب پذیر است. در [40] از آنجایی که صاحبان سرویس می‌توانند به کاربران بدون اینکه از محصولاتشان استفاده کنند مجوز ثبت بازخورد بدهند این امکان وجود دارد که گروهی از کاربران به دلیل انگیزه‌های مالی، نسبت به یک سامانه بازخورد جعلی مثبت ثبت کنند و همچنین چون مکانیزم شهرت به گونه‌ای نیست که با ارزیابی‌های دیگر کاربران این بازخوردهای جعلی مشخص شده و غیرقابل اعتماد شناخته شوند، این سامانه امکان حمله‌ی تبانی را برای کاربران فراهم می‌کند. وجود مکانیزم ارزیابی در [41,42] به همراه بررسی کردن استفاده‌ی کاربر از یک محصول قبل از ثبت بازخورد نسبت به آن، این ۲ سامانه را در برابر حمله‌ی تبانی مقاوم می‌کند.



شکل۲-۴. فلوچارت ثبت بازخورد نسبت به یک بازخورد دیگر

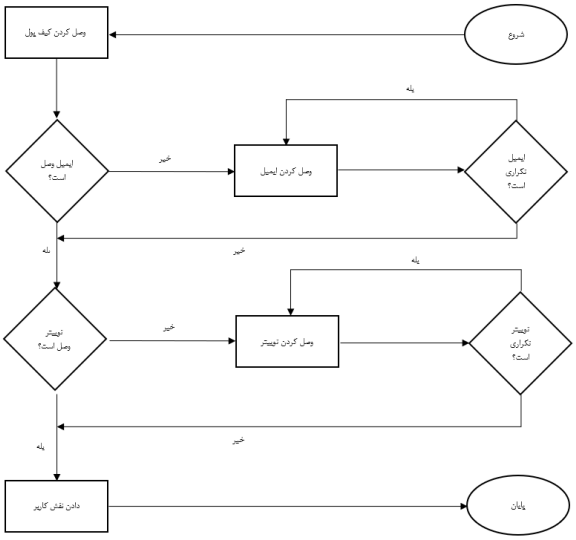
۳-۲-۴ حمله‌ی سیبل در ثبت نظرات

ما ابتدا عملکرد سامانه‌ی خود و سپس عملکرد کارهای آورده شده در بخش ۲-۲ را در برابر این حمله بررسی می‌کنیم.

در سامانه‌ی ما کسانی حق ثبت بازخورد دارند که نقش کاربر را دریافت کرده باشند. افراد برای گرفتن نقش کاربر باید احرازهویت ۳ مرحله‌ای را پشت سر بگذارند. همانطوری که در شکل۳-۴ نیز مشخص است آن‌ها ابتدا باید از طریق کیف پول بلاک‌چینی خود در سامانه ثبت نام کنند و سپس باید یک ایمیل معتبر که به آن دسترسی دارند را به سامانه‌ی ما متصل کنند و پس از آن نیز باید با حساب کاربری توییتر خود احراز هویت کنند. متصل کردن توییتر و ایمیل توسط کاربر به ما این اطمینان را می‌دهد که این فرد صاحب اصلی آن حساب کاربری توییتر و ایمیل می‌باشد. از آنجایی که ساخت حساب توییتر با شماره‌ی تلفن می‌باشد و هر شماره تلفن فقط یک حساب کاربری می‌تواند داشته باشد در صورتی که فرد بخواهد حساب‌های متعدد در سامانه‌ی ما ایجاد کند باید به تعداد حساب‌هایی که می‌خواهد باز کند ایمیل و حساب توییتر داشته باشد که آن هم مستلزم داشتن چندین شماره تلفن منحصر به فرد است و این هزینه‌ی حمله‌ی سیبل را برای یک کاربر مخرب بالا می‌برد. از طرف دیگر همانطور که قبلا توضیح داده شد در سامانه‌ی ما کاربران برای اینکه بتوانند نسبت به یک سرویس بازخورد ثبت کنند حتما باید از آن استفاده کرده باشند. برای مثال اگر یک کاربر مخرب بخواهد با ۱۰۰ حساب کاربری مختلف نسبت به یک سرویس بازخورد ثبت کند باید از طریق ۱۰۰ آدرس کیف پول که به ۱۰۰ ایمیل و حساب توییتر منحصر به فرد متصل است در سامانه‌ی ما ثبت نام کند. از طرف دیگر حتی اگر این کاربر مرحله‌ی احراز هویت را نیز پشت سر بگذارد برای اینکه بتواند به آن سرویس بازخورد ثبت کند باید با هرکدام از این حساب‌های کاربری از آن سرویس استفاده کرده باشد که این نیز برای کاربر مخرب هزینه‌بر می‌باشد. البته یک کاربر مخرب می‌تواند با پشت سر گذاشتن این مراحل در نهایت حمله‌ی سیبل انجام دهد و سامانه‌ی ما به صورت قطعی جلوی حمله‌ی سیبل را نمی‌گیرد ولی با پیاده سازی یک احرازهویت قوی و بررسی استفاده‌ی کاربر از یک سرویس قبل از ثبت بازخورد نسبت به آن هزینه‌ی حملات سیبل را برای کاربران مخرب بالا می‌برد و باعث کاهش حملات سیبل در سامانه می‌شود.

در اینجا به بررسی عملکرد کارهای مطرح شده در بخش ۲-۲ در برابر ثبت نظرات جعلی می‌پردازیم. [39] استفاده کردن کاربران از یک محصول را بررسی می‌کند و فقط به کسانی که از آن استفاده کرده‌اند اجازه‌ی ثبت بازخورد می‌دهد ولی از آنجایی که سیستم احراز هویت برای کاربران وجود ندارد، یک کاربر به راحتی و بدون نیاز به احراز هویت می‌تواند حساب‌های متعددی ایجاد کند که باعث می‌شود این سامانه در برابر حمله‌ی سیبل آسیب پذیر باشد. در [40] از آنجایی که ساخت حساب‌های کاربری نیاز به احراز هویت ندارد یک کاربر می‌تواند حساب‌های کاربری متعددی را بدون پرداختن هزینه‌ای ایجاد

کند و همچنین این امکان وجود دارد که افراد بدون استفاده از یک محصول به آن بازخورد ثبت کنند. پس این سامانه در برابر حمله‌ی سیبل آسیب پذیر است. [41] نیز به دلیل نبودن فرآیند احراز هویت در برابر حمله‌ی سیبل آسیب پذیر است و در آن این امکان وجود دارد که کاربران با ساخت حساب‌های کاربری متعدد حمله‌ی سیبل انجام دهند. [42] به دلیل استفاده از سیستم احراز هویت به وسیله‌ی کارت اعتباری منحصر به فرد و بررسی استفاده کردن کاربر از یک محصول قبل از ثبت بازخورد در برابر حمله‌ی سیبل مقاوم می‌باشد.



شکل۳-۴. فلوچارت احراز هویت

۴-۲-۴ دستکاری داده‌ها یا حذف نظرات منفی

ما ابتدا عملکرد سامانه‌ی خود و سپس عملکرد کارهای آورده شده در بخش ۲-۲ را در برابر این حمله بررسی می‌کنیم.

سامانه‌ی ما از فناوری بلاک‌چین که یک دفترکل تغییرناپذیر وشفاف است برای نگه‌داری بازخوردهای خود استفاده می‌کند. فرآیند ثبت بازخورد از طریق قراردادهای هوشمند می‌باشد و در نهایت بازخوردهای کاربران در بلاک‌چین پالیگان ذخیره می‌شود و سامانه‌ی ما این تضمین را می‌دهد که بازخوردهای کاربران پس از ثبت تغییر نخواهند یافت. همچنین معماری غیرمتمرکز سامانه‌ی ما این اطمینان را می‌دهد که یک شخص یا نهاد خاص اجازه‌ی کنترل سامانه را ندارد و نمی‌تواند بازخوردهای کاربران را دستکاری کند. همچنین به دلیل ثبت شدن قراردادهای هوشمند بر روی بلاک‌چین پالیگان همه‌ی افراد به منطق کد قراردادهای هوشمند دسترسی دارند و این کدها قابل تایید توسط همه می‌باشد.کاربران می‌توانند اطمینان حاصل کنند که سامانه امکان به روز رسانی کد قراردادهای هوشمند را ندارد و در آینده نمی‌تواند منطقی را پیاده سازی و جایگزین کند که در آن امکان حذف بازخورد وجود داشته باشد. در نتیجه به دلیل غیرقابل تغییر بودن قراردادهای هوشمند و ذخیره شدن بازخوردهای کاربران در بلاک‌چین پالیگان، امکان تغییر محتوای بازخوردهای کاربران وجود ندارد و هر بازخوردی که ثبت می‌شود، توسط همه قابل تایید و ردیابی می‌باشد. در نتیجه سامانه‌ی ما امکان دستکاری محتوای بازخوردهای کاربران و یا حذف بازخوردهای آن‌ها را ندارد.

در اینجا به بررسی عملکرد کارهای مطرح شده در بخش ۲-۲ در برابر ثبت نظرات جعلی می‌پردازیم. در [39,40,41,42] تمامی بازخوردهای کاربران در بلاک‌چین که یک دفتر کل توزیع شده و تغییرناپذیر است ذخیره می‌شود و کسی نمی‌تواند محتوای بازخوردهای کاربران را تغییر دهد و یا یک بازخورد را حذف کند به همین دلیل این سامانه‌ها در برابر حذف و یا تغییر محتوای بازخوردها مقاوم هستند.

۵-۲-۴ ثبت نظرات متعصبانه و جهت دار

ما ابتدا عملکرد سامانه‌ی خود و سپس عملکرد کارهای آورده شده در بخش ۲-۲ را در برابر این حمله بررسی می‌کنیم.

در سامانه‌ی ما همانطوری که در شکل۲-۴ نیز آورده شده است کاربرانی که از یک سرویس استفاده کرده‌اند می‌توانند بازخوردهایی که نسبت به آن سرویس داده شده است را ارزیابی کنند و در صورتی که یک بازخورد به دور از واقعیت بود به آن بازخورد امتیاز منفی بدهند. این قابلیت در سیستم ما به عنوان یک سیستم ارزیابی و گزارش‌دهی غیرمتمرکز عمل می‌کند و در آن کاربران می‌توانند نظرات خود را نسبت به بازخوردهای یک سرویس که از آن استفاده کرده اند ثبت کنند. بازخوردهایی که یک کاربر از دیگران می‌گیرد به میزان امتیاز شهرتش تاثیر می‌گذارد و این میزان شهرت نیز رابطه‌ی وزن دار با میزان قابل اعتماد بودن خود کاربر و بازخوردهایی که ثبت می‌کند دارد. کاربر مخربی را فرض کنید که در سیستم ما بازخوردهای متعصبانه ثبت می‌کند و یا کاربری که به دلیل عصبانیت، نسبت به یک سرویس بازخورد مغرضانه ثبت می‌کند. در این صورت دیگر کسانی که از آن سرویس استفاده کرده‌اند می‌توانند بازخوردهای کاربر مخرب را ارزیابی کنند و در صورتی که بازخوردهای او را به دور از واقعیت ارزیابی کردند به آن کاربر

مخرب امتیاز منفی بدهند که این امتیاز منفی باعث می‌شود امتیاز شهرتش کاهش یابد و در نتیجه باعث کاهش تاثیر بازخوردهایی که او نسبت به دیگر سرویس‌ها می‌دهد بشود.

در سامانه‌ی ما تمامی فعالیت‌های کاربران قابل ردیابی و تایید توسط دیگران می‌باشد و همچنین یک کاربر بر دیگر کاربرانی که از یک سرویس استفاده کرده‌اند کنترل ندارد. به همین دلیل افراد در جهت بالا بردن امتیاز شهرت خود تمایل به رفتار صادقانه دارند. برای مثال حالتی را در نظر بگیرید که یک کاربر در ارزیابی خود رفتار صادقانه‌ای نداشته باشد و بخواهد نسبت به یک بازخورد که یک فرد مخرب از روی تعصب یا عصبانیت ثبت کرده است و واقعیت ندارد، ارزیابی مثبت داشته باشد. از آنجایی که این ارزیابی توسط دیگر افراد قابل مشاهده است و او می‌داند که دیگران می‌توانند با رفتار صادقانه او را تبدیل به یک فرد مخرب در سیستم کنند و باعث پایین آمدن امتیاز شهرت او شوند، تمایل کمتری به رفتار مخرب پیدا می‌کند. به همین دلیل افراد در سامانه‌ی ما در جهت بالا بردن امتیاز شهرت خود تمایل به رفتار صادقانه دارند و این باعث می‌شود که تا حد امکان ارزیابی‌های درست و از همه مهم‌تر بازخوردهای مبتنی بر واقعیت و به دور از تعصب ثبت کنند و قابلیت اعتماد بازخوردهایی که در سامانه ثبت می‌شود بالا برود.

در اینجا به بررسی عملکرد کارهای مطرح شده در بخش ۲-۲ در برابر ثبت نظرات جعلی می‌پردازیم. در [39] کاربران نمی‌توانند بازخوردهایی که به یک محصول داده می‌شود را ارزیابی کنند و در آن افراد می‌توانند بازخوردهای متعصبانه به یک محصول بدهند و امکان به چالش کشیدن میزان واقعی بودن این بازخوردها و اعمال کردن نتیجه‌ی آن در امتیاز شهرت وجود ندارد که این سامانه را در برابر ثبت بازخوردهای متعصبانه آسیب‌پذیر می‌کند. در [40] نیز به دلیل اینکه امکان ارزیابی بازخوردهای کاربران وجود ندارد و مکانیزم شهرت به گونه‌ای نیست که ثبت بازخوردهای غیرواقعی و متعصبانه باعث کاهش امتیاز شهرت کاربران شود، این سامانه نیز در برابر ثبت بازخوردهای غیرواقعی و متعصبانه آسیب‌پذیر می‌باشد. [41] با پیاده سازی امکان به چالش کشیدن بازخوردهای یک کاربر جلوی ثبت بازخوردهای متعصبانه و غیرواقعی را می‌گیرد همچنین [42] نیز با ارزیابی بازخوردهای ثبت‌شده توسط گروهی از تاییدکنندگان و همچنین داشتن مکانیزم شهرت که در آن کاربران مخرب نشان جعلی دریافت کرده و از سامانه حذف می‌شوند، جلوی ثبت بازخوردهای جعلی را می‌گیرد.

۶-۲-۴ قابلیت اعتماد بازخوردهای ثبت شده

در این بخش ما میزان قابل اعتماد بودن بازخوردهای سامانه‌ی خود را در کنار کارهای آورده شده در بخش ۲-۲ بررسی می‌کنیم.

در سامانه‌ی ما تمامی بازخوردهای کاربران بر روی بلاک‌چین ذخیره می‌شوند و این اطمینان به کاربران داده می‌شود که محتوای بازخوردهای آن‌ها تغییر داده نخواهد شد و همچنین بازخوردهای آن‌ها پس از ثبت شدن در بلاک‌چین قابل حذف نخواهند بود. معماری غیرمتمرکز در سامانه‌ی ما، نهاد واسط مرکزی را از فرآیندهای سامانه‌ی ثبت بازخورد حذف می‌کند و یک نهاد مرکزی قابلیت کنترل سامانه، حذف و یا تغییر محتوای بازخوردهای کاربران را ندارد. از طرف دیگر همانطور که در بخش‌های قبلی توضیح داده شد سامانه‌ی ما مقاوم در برابر ثبت نظرات جعلی و حملات ثبت بازخورد می‌باشد و این اطمینان به کاربر داده می‌شود که بازخوردها از طرف افراد واقعی که از یک سرویس استفاده کرده‌اند ثبت شده است و همچنین با پیاده سازی مکانیزم شهرت تا حد زیادی اطمینان پیدا می‌کنند که بازخوردهایی که از طرف کاربران با امتیاز شهرت بالا ثبت شده‌اند، بازخودهای قابل اعتمادی هستند و می‌توانند این بازخوردها را مبنای تصمیم‌گیری خود بر استفاده یا عدم استفاده از یک سرویس قرار دهند. همچنین شفاف بودن مراحل ثبت بازخورد یکی از دلایلی است که کاربران از قابل اعتماد بودن سامانه‌ی ما می‌توانند اطمینان داشته باشند. در سامانه‌ی ما تمامی فرآیندها به صورت قطعی و غیرقابل بازگشت و تغییرناپذیر اتفاق می‌افتد و تمامی محاسبات امتیاز شهرت بر اساس داده‌هایی که بر روی بلاک‌چین ذخیره می‌شود صورت می‌گیرد و هرکسی قابلیت تایید این محاسبات و نتایج امتیاز شهرت را دارد و می‌تواند از امتیاز شهرت کاربران اطمینان حاصل کند.

مواردی که در بالا بحث شد باعث می‌شود که سامانه‌ی ما و بازخوردهایی که در آن ثبت شده اند برای کابران قابل اعتماد باشد و بتوانند از آن‌ها در تصمیم‌گیری های خود استفاده کنند. بازخوردهایی که در [39] ثبت می‌شوند به دلیل آسیب پذیر بودن این سامانه در برابر حمله‌ی سیبل و تبانی و همچنین امکان ثبت نظرات غیرواقعی، از میزان قابلیت اعتماد بالایی

برخوردار نیستند همچنین در [40] امکان حمله‌ی سیبل و تبانی و ثبت بازخوردهای جعلی و متعصبانه وجود دارد که باعث می‌شود بازخوردهای این سامانه نیز غیرقابل اعتماد باشند. آسیب پذیر بودن[41] در برابر حمله‌ی سیبل، بازخوردهایی که در این سامانه ثبت می‌شود را غیرقابل اعتماد می‌کند این در حالی است که [42] در مقایسه با کارهای دیگر با مقابله با حملات و چالش‌های مطرح شده از میزان قابلیت اعتماد بیشتری برخوردار است.

۴-۳ ارزیابی عملکرد هزینه‌ای

در این بخش ما به بررسی و تجزیه و تحلیل هزینه‌ی فرآیندهای ثبت بازخورد سامانه می‌پردازیم. در بلاک‌چین برای پردازش تراکنش‌ها کاربران باید مقداری هزینه به عنوان کارمزد بدهند. در بلاک‌چین پالیگان این هزینه گس نام دارد و برای اجرای قراردادهای هوشمند مورد استفاده قرار می‌گیرد. هر کد دستوری در قرارداد هوشمند به توان پردازشی و در نتیجه هزینه نیاز دارد که با گس اندازه‌گیری می‌شود و در قالب ارز بومی شبکه که متیک است پرداخت می‌شود. هزینه‌ی گس از حاصل‌ضرب گس لیمیت (GasLimit) و قیمت گس (GasPrice) به دست می‌آید که در زیر هرکدام از آن‌ها توضیح داده شده است.

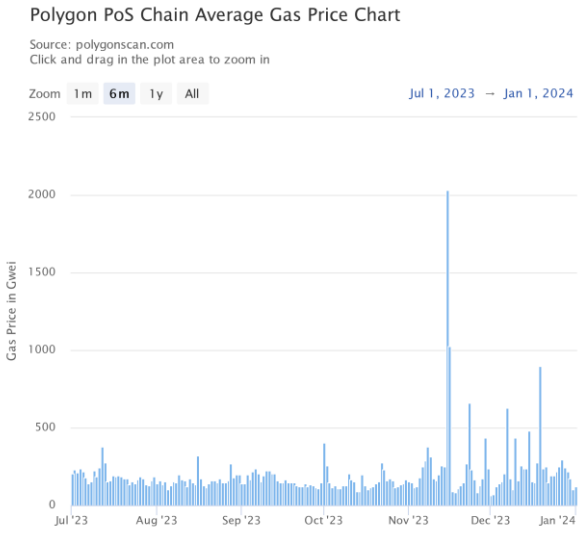
گس لیمیت

هر کد دستوری در پالیگان گس لیمیت ثابت و از پیش تعیین‌شده‌ای دارد و به دلیل جلوگیری از حملات هرزنامه کردن شبکه وجود دارد که مانع از ارسال تراکنش‌های زیاد برای مختل کردن شبکه می‌شود. این فاکتور حداکثر میزان گس را نشان می‌دهد که کاربران برای انجام کارهای مختلف باید پرداخت کنند. انواع مختلف تراکنش‌ها بر روی بلاک‌چین پالیگان هزینه‌های گس لیمیت متفاوتی دارند. برای مثال ارسال متیک گس لیمیت برابر با ۲۱۰۰۰ واحد دارد. در واقع گس لیمیت بر اساس نوع قرارداد هوشمند و حجم کدهای مندرج در آن تعیین می‌شود.

قیمت گس

هزینه‌ای است که یک کاربر تمایل دارد به ازای هر واحد گس پرداخت کند. واحد قیمت گس جیوی (Gwei) است که برابر با $۱۰^{۹}$ (wei) می‌باشد. Wei کوچکترین واحد شمارش در متیک می‌باشد و یک متیک برابر با $۱۰^{۱۸}$ (wei) می‌باشد.

کیف پول‌های بلاک‌چینی معمولا و به صورت خودکار یک قیمت منطقی برای قیمت گس در نظر می‌گیرند که قابل تغییر توسط خود کاربر می‌باشد. قیمت گس بر اساس عرضه و تقاضا تعیین می‌شود و ماینرها تراکنش‌ها را بر اساس قیمت گس اجرا می‌کنند، یعنی هر تراکنشی را که قیمت گس بیشتری تعیین کرده باشد زودتر اجرا می‌کنند. تعیین کردن قیمت گس بالاتر از میانگین قیمت فعلی که تراکنش‌ها با آن انجام می‌شوند باعث می‌شود که تراکنش‌ها سریع‌تر در شبکه اجرا شوند و در صورت تعیین کردن قیمت گس پایین‌تر از میانگین، تراکنش یا انجام نمی‌شود و یا زمان زیادی طول می‌کشد که انجام شود.



شکل۴-۴. قیمت گس از تاریخ ۲۰۲۳/۷/۱ تا ۲۰۲۴/۱/۱ در شبکه‌ی پالیگان

شکل۵-۴. قیمت متیک از تاریخ ۲۰۲۳/۷/۱ تا ۲۰۲۴/۱/۱

به منظور ارزیابی هزینه‌ی فرآیندها ما قراردادهای هوشمند خود را در شبکه‌ی تستی Mumbai دیپلوی کردیم که دقیقا شبیه شبکه‌ی اصلی می‌باشد با این تفاوت که در آن از متیک تستی که رایگان است به جای متیک واقعی استفاده می‌شود و با هدف تست کردن پروژه قبل از دیپلوی کردن به شبکه‌ی اصلی به وجود آمده است. همچنین به دلیل ازدحام کمتر شبکه‌ی تستی قیمت گس در آن پایین تر از شبکه‌ی اصلی می‌باشد. ما برای تعیین کردن قیمت گس در شبکه‌ی اصلی داده‌های مربوط به قیمت گس را در ۶ ماه گذشته همانطوری که در شکل۴-۴ مشخص است بررسی کرده و میانگین قیمت گس را در این ۶ ماه که عدد ۲۰۰ می‌باشد به عنوان قیمت گس مورد استفاده در سامانه در نظر می‌گیریم و تمامی تراکنش‌های سامانه‌ی ما با این قیمت گس اجرا می‌شوند و برای ارزیابی هزینه‌ی بخش‌های مختلف سامانه از این عدد استفاده می‌کنیم. همچنین برای تعیین قیمت متیک برای استفاده در محاسبات، قیمت آن را در ۶ ماه گذشته همانطوری که در شکل۵-۴ مشخص است بررسی کرده و میانگین قیمت متیک را در این ۶ ماه که برابر ۰/۶۸ دلار است برای استفاده در محاسبات مربوط به هزینه‌ی سامانه در نظر می‌گیریم:

جدول۲-۴. هزینه عملیات سامانه در شبکه‌ی تستی برای ۱ کاربر

نام عملیات	گس لیمیت	قیمت گس (GWEI)	هزینه‌ی کل (متیک)	هزینه‌ی کل (دلار)
دادن نقش کاربر به ۱ نفر	۲۶۴۹۵	۱/۵	۰/۰۰۰۳	۰/۰۰۰۲
افزودن ۱ سرویس به سامانه	۱۱۴۰۹۹	۱/۵	۰/۰۰۱۷	۰/۰۰۰۱۱
ثبت بازخورد نسبت به ۱ سرویس	۱۱۴۶۵۸	۱/۵	۰/۰۰۱۷	۰/۰۰۰۱۱
ثبت بازخورد نسبت به ۱ بازخورد	۱۱۵۵۲۴	۱/۵	۰/۰۰۱۷	۰/۰۰۰۱۱

جدول۳-۴. هزینه عملیات سامانه در شبکه‌ی اصلی برای ۱ کاربر

نام عملیات	گس لیمیت	قیمت گس (GWEI)	هزینه‌ی کل (متیک)	هزینه‌ی کل (دلار)
دادن نقش کاربر به ۱ نفر	۲۶۴۹۵	۲۰۰	۰/۰۰۵	۰/۰۰۳
افزودن ۱ سرویس به سامانه	۱۱۴۰۹۹	۲۰۰	۰/۰۲۲	۰/۰۱۴
ثبت بازخورد نسبت به ۱ سرویس	۱۱۴۶۵۸	۲۰۰	۰/۰۲۲	۰/۰۱۴
ثبت بازخورد نسبت به ۱ بازخورد	۱۱۵۵۲۴	۲۰۰	۰/۰۲۳	۰/۰۱۵

جدول۴-۴. هزینه عملیات سامانه در شبکه‌ی تستی برای ۱۰ کاربر

نام عملیات	گس لیمیت	قیمت گس (GWEI)	هزینه‌ی کل (متیک)	هزینه‌ی کل (دلار)
دادن نقش کاربر به ۱۰ نفر	۲۶۴۹۵۰	۱/۵	۰/۰۰۰۳	۰/۰۰۰۲
افزودن ۱۰ سرویس به سامانه	۸۰۶۷۹۰	۱/۵	۰/۰۰۱۲	۰/۰۰۰۸
ثبت بازخورد نسبت به ۱۰ سرویس	۸۱۲۳۲۲	۱/۵	۰/۰۰۱۲	۰/۰۰۰۸
ثبت بازخورد نسبت به ۱۰ بازخورد	۸۳۸۱۰۷	۱/۵	۰/۰۰۱۲	۰/۰۰۰۸

جدول۵-۴. هزینه عملیات سامانه در شبکه‌ی اصلی برای ۱۰ کاربر

نام عملیات	گس لیمیت	قیمت گس (GWEI)	هزینه‌ی کل (متیک)	هزینه‌ی کل (دلار)
دادن نقش کاربر به ۱۰ نفر	۲۶۴۹۵۰	۲۰۰	۰/۰۵۲	۰/۰۳۵
افزودن ۱۰ سرویس به سامانه	۸۰۶۷۹۰	۲۰۰	۰/۱۶۱	۰/۱۰۹
ثبت بازخورد نسبت به ۱۰ سرویس	۸۱۲۳۲۲	۲۰۰	۰/۱۶۲	۰/۱۱۰
ثبت بازخورد نسبت به ۱۰ بازخورد	۸۳۸۱۰۷	۲۰۰	۰/۱۶۷	۰/۱۱۳

در سامانه‌ی ما ۴ بخش کلی شامل تخصیص نقش کاربر به یک فرد، افزودن سرویس، دادن بازخورد نسبت به یک سرویس و ثبت بازخورد نسبت به یک بازخورد وجود دارد که در آن تراکنش‌های بلاک‌چینی ثبت می‌شود. ما در این بخش در ۲ حالت هزینه‌ی هرکدام از این عملیات را بررسی می‌کنیم. حالت اول مربوط به انجام این عملیات برای ۱ کاربر و حالت دوم مربوط به انجام این عملیات برای ۱۰ کاربر می‌باشد. جدول۲-۴ و۳-۴ به طور خلاصه هزینه‌ی این عملیات را برای حالت اول در هر ۲ شبکه‌ی تستی و اصلی نشان می‌دهد و همچنین جدول۴-۴ و۵-۴ هزینه‌ی این عملیات را برای حالت دوم در آن ۲ شبکه نشان می‌دهد. در زیر به صورت جزیی هزینه‌ی هرکدام از این عملیات را بررسی می‌کنیم:

۴-۳-۱ تخصیص نقش کاربر به یک فرد

این عملیات به گونه‌ای است که در هر بار اجرا به یک فرد نقش کاربر داده می‌شود و برای دادن نقش کاربر به ۱۰ نفر باید ۱۰ بار این عملیات انجام شود. همانطوری که در شکل۶-۴ مشخص است این تابع دارای گس لیمیت ۲۶۴۹۵ برای دادن نقش کاربر به یک فرد می‌باشد. در حالت اول برای محاسبه‌ی هزینه‌ی تخصیص نقش کاربر به ۱ نفر با در نظر گرفتن عدد ۱/۵ برای قیمت گس در شبکه‌ی تستی این عملیات ۰/۰۰۰۳ متیک هزینه دارد. این عملیات در شبکه‌ی اصلی و با در نظر گرفتن عدد ۲۰۰ برای قیمت گس، ۰/۰۰۵ متیک هزینه دارد که معادل ۰/۰۰۳ دلار است. در حالت دوم برای محاسبه‌ی هزینه‌ی تخصیص نقش کاربر به ۱۰ نفر، از آنجایی که این تابع برای هرکدام از افراد به صورت جداگانه اجرا می‌شود پس گس لیمیت ۲۶۴۹۵۰ می‌شود که در شبکه‌ی تستی با در نظر گرفتن عدد ۱/۵ برای قیمت گس، ۰/۰۰۰۳ متیک و در شبکه‌ی اصلی با در نظر گرفتن عدد ۲۰۰ برای قیمت گس، ۰/۰۵۲ متیک هزینه دارد که معادل ۰/۰۳۵ دلار می‌باشد.

شکل۶-۴. تراکنش مربوط به تخصیص نقش کاربر به ۱ نفر

۴-۳-۲ اضافه کردن سرویس

در این عملیات امکان فرستادن تراکنش‌ها به صورت گروهی وجود دارد یعنی برای افزودن ۱۰ سرویس به سامانه نیاز نیست که هرکدام از این تراکنش‌ها به صورت جداگانه ارسال شود و با یک تراکنش امکان اضافه کردن بیش از ۱ سرویس به سامانه وجود دارد. در حالت اول و برای اضافه کردن یک سرویس به سامانه همانطوری که در شکل۷-۴ مشخص است این عملیات دارای گس لیمیت ۱۱۴۰۹۹ می‌باشد. برای محاسبه‌ی هزینه با در نظر گرفتن عدد ۱/۵ برای قیمت گس در شبکه‌ی تستی، هزینه‌ی این عملیات ۰/۰۰۰۱۷ متیک می‌شود. این هزینه در شبکه‌ی اصلی و با در نظر گرفتن عدد ۲۰۰ برای قیمت گس ۰/۰۲۲ متیک می‌شود که معادل ۰/۰۱۴ دلار است. در حالت دوم و برای اضافه کردن ۱۰ سرویس به صورت گروهی به سامانه همانطوری که در شکل۸-۴ مشخص است این عملیات دارای گس لیمیت ۸۰۶۷۹۰ می‌باشد. برای محاسبه‌ی هزینه با در نظر گرفتن عدد ۱/۵ برای قیمت گس در شبکه‌ی تستی، هزینه‌ی این عملیات ۰/۰۰۱۲ متیک می‌شود. این هزینه در شبکه‌ی

اصلی و با در نظر گرفتن عدد ۲۰۰ برای قیمت گس ۰/۱۶۱ متیک می‌شود که معادل ۰/۱۰۹ دلار است.

شکل۷-۴. تراکنش مربوط به افزودن ۱ سرویس به سامانه

شکل۸-۴. تراکنش مربوط به افزودن ۱۰ سرویس به سامانه

۴-۳-۳ ثبت بازخورد نسبت به یک سرویس

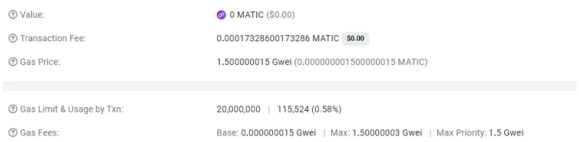
در این عملیات امکان فرستادن تراکنش‌ها به صورت گروهی وجود دارد یعنی برای ثبت کردن ۱۰ بازخورد نیاز نیست که هرکدام از این تراکنش‌ها به صورت جداگانه ارسال شود و با یک تراکنش امکان ثبت کردن بیش از ۱ بازخورد وجود دارد. در حالت اول و برای ثبت کردن ۱ بازخورد همانطوری که در شکل۹-۴ مشخص است این عملیات دارای گس لیمیت ۱۱۴۶۵۸ می‌باشد. برای محاسبه‌ی هزینه با در نظر گرفتن عدد ۱/۵ برای قیمت گس در شبکه‌ی تستی، هزینه‌ی این عملیات ۰/۰۰۰۱۷ متیک می‌شود. این هزینه در شبکه‌ی اصلی و با در نظر گرفتن عدد ۲۰۰ برای قیمت گس ۰/۰۲۲ متیک می‌شود که معادل ۰/۰۱۴ دلار است. در حالت دوم و برای ثبت کردن ۱۰ بازخورد به صورت گروهی همانطوری که در شکل۱۰-۴ مشخص است این عملیات دارای گس لیمیت ۸۱۲۳۲۲ می‌باشد. برای محاسبه‌ی هزینه با در نظر گرفتن عدد ۱/۵ برای قیمت گس در شبکه‌ی تستی، هزینه‌ی این عملیات ۰/۰۰۱۲ متیک می‌شود. این هزینه در شبکه‌ی اصلی و با در نظر گرفتن عدد ۲۰۰ برای قیمت گس ۰/۱۶۲ متیک می‌شود که معادل ۰/۱۱۰ دلار است.

شکل۹-۴. تراکنش مربوط به ثبت کردن ۱ بازخورد نسبت به سرویس

شکل۱۰-۴. تراکنش مربوط به ثبت کردن ۱۰ بازخورد نسبت به سرویس

۴-۳-۴ ثبت بازخورد نسبت به یک بازخورد

در این عملیات امکان فرستادن تراکنش‌ها به صورت گروهی وجود دارد یعنی برای ثبت کردن ۱۰ بازخورد نیاز نیست که هرکدام از این تراکنش‌ها به صورت جداگانه ارسال شود و با یک تراکنش امکان ثبت کردن بیش از ۱ بازخورد وجود دارد. در حالت اول و برای ثبت کردن ۱ بازخورد همانطوری که در شکل۱۱-۴ مشخص است این عملیات دارای گس لیمیت ۱۱۵۵۲۴ می‌باشد. برای محاسبه‌ی هزینه با در نظر گرفتن عدد ۱/۵ برای قیمت گس در شبکه‌ی تستی، هزینه‌ی این عملیات ۰/۰۰۰۱۷ متیک می‌شود. این هزینه در شبکه‌ی اصلی و با در نظر گرفتن عدد ۲۰۰ برای قیمت گس ۰/۰۲۳ متیک می‌شود که معادل ۰/۰۱۵ دلار است. در حالت دوم و برای ثبت کردن ۱۰ بازخورد به صورت گروهی همانطوری که در شکل۱۲-۴ مشخص است این عملیات دارای گس لیمیت ۸۳۸۱۰۷ می‌باشد. برای محاسبه‌ی هزینه با در نظر گرفتن عدد ۱/۵ برای قیمت گس در شبکه‌ی تستی، هزینه‌ی این عملیات ۰/۰۰۱۲ متیک می‌شود. این هزینه در شبکه‌ی اصلی و با در نظر گرفتن عدد ۲۰۰ برای قیمت گس ۰/۱۶۷ متیک می‌شود که معادل ۰/۱۱۳ دلار است.



شکل۱۱-۴. تراکنش مربوط به ثبت کردن ۱ بازخورد نسبت به بازخورد

شکل۱۲-۴. تراکنش مربوط به ثبت کردن ۱۰ بازخورد نسبت به بازخورد

نتایج بدست آمده برای هزینه‌های سامانه نشان می‌دهد که سیستم ما به دلیل بهبود فرآیندهای ثبت بازخورد و همچنین ارائه‌ی راهکار خارج از زنجیره برای محاسبات مربوط به مکانیزم شهرت عملکرد بهتری نسبت به [39,40,42] دارد. از آنجایی که در [41] گزارشی از هزینه‌های سامانه وجود ندارد ما امکان مقایسه هزینه‌های سامانه‌ی خود با این کار را نداریم.

۵- نتیجه‌گیری و کارهای آینده

۵-۱ نتیجه‌گیری

در این پایان نامه یک سامانه‌ی ثبت بازخورد غیرمتمرکز جامع برای سرویس‌های مبتنی بر بلاک‌چین ارائه کردیم که به چالش‌های مرتبط با سیستم‌های متمرکز، مانند تقلب در ثبت بازخورد و دستکاری محتوای بازخوردها می‌پردازد. این سامانه مکانیزم شفافی را برای ثبت بازخورد کاربر، ارزیابی کیفیت خدمات و محاسبه شهرت کاربر در چارچوب غیرمتمرکز معرفی می‌کند.

این سامانه با استفاده از فناوری بلاک‌چین و قراردادهای هوشمند، شفافیت فرآیندهای ثبت بازخورد را افزایش می‌دهد و همچنین تغییر ناپذیری بازخوردهای ثبت شده را تضمین می‌کند. استفاده کردن از محاسبات خارج از زنجیره برای مکانیزم شهرت مقیاس‌پذیری سامانه را افزایش می‌دهد. فرآیند احراز هویت استفاده شده در این سامانه مشروعیت کاربران را تضمین می‌کند و خطر فعالیت‌های تقلبی را کاهش می‌دهد. همچنین استفاده کردن از فناوری‌هایی مانند IPFS برای ذخیره‌سازی غیرمتمرکز اطلاعات سرویس‌ها و بازخوردها، EIP712 برای ثبت بازخوردهای خارج از زنجیره و رایگان برای کاربران و TheGraph برای محاسبات مربوط به امتیازات شهرت کاربران به صورت غیرمتمرکز قابلیت اعتماد سامانه را بالا می‌برد و این اطمینان را می‌دهد که داده‌ها غیرقابل تغییر و قابل تایید توسط همه می‌باشند. این سامانه‌ی غیرمتمرکز ثبت بازخورد در کنار پرداختن به محدودیت‌های سیستم‌های موجود، راهکاری مقیاس‌پذیر برای ثبت بازخورد به صورت امن و شفاف و کاربر محور معرفی می‌کند که در برابر حملات و چالش‌های ثبت بازخورد مقاوم است و هیچ نهادی قابلیت دستکاری بازخوردها را ندارد و کاربران می‌توانند این بازخوردها را مبنای تصمیم‌گیری خود برای استفاده یا عدم استفاده از یک سرویس قرار دهند.

۵-۲ کارهای آینده

در حالی که این پایان نامه یک سامانه‌ی ثبت بازخورد غیرمتمرکز جامع و مقاوم در برابر تقلب‌ها و حملات ثبت بازخورد را معرفی می‌کند، چندین کار برای تحقیق و توسعه‌ی آینده وجود دارد:

۱. ایجاد مکانیزم‌های تشویقی اضافی برای کاربران مانند پاداش‌های رمزارزی که باعث می‌شود کاربران به ارائه‌ی بازخوردهای صادقانه و سازنده تشویق شوند.

۲. بررسی و اجرای مکانیزم‌های حکمرانی غیرمتمرکز (DAO) که به جامعه اجازه می‌دهد در فرآیندهای مربوط به تصمیم‌گیری سامانه مشارکت کنند. برای مثال نقش اسکریپت می‌تواند به DAO داده شود که افراد فعال در سامانه در تصمیم‌گیری‌های مربوط به نقش اسکریپت مشارکت کنند.

۳. استقرار سامانه در شبکه‌های بلاک‌چینی مختلف که کاربران بتوانند در شبکه‌های مختلف بازخوردهایشان را ثبت کنند.

۴. بررسی امکان ادغام سامانه‌ی ثبت بازخورد غیرمتمرکز با سرویس‌ها و خدمات آنلاین

۵. بررسی راهکارهایی که در آن حریم خصوصی کاربر در عین حفظ شفافیت و تغییرناپذیری داده‌ها افزایش می‌یابد.

۵- منابع

[1] Chatterjee, Patrali (2001), “Online Reviews Do Consumers Use Them?" ACR 2001Proceedings,eds. M. C. Gilly and J. Myers-Levy,Provo, UT:Association for Consumer Research, 129-134.
[2] Statista.com, For each of the following circumstances, how important is it to read online reviews before purchasing a product or selecting a service provider? 2017. URL:https://www.statista.com/statistics/713258/online-review-importance-circumstances-usa/.
[3] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[4] Khan, S., Loukil, F., Ghedira-Guegan, C.,Benkhelifa, E., & Bani-Hani, A.(2021).Blockchain smart contracts: Applications, challenges, and future trends.Peer-to-Peer Networking and Applications, 14(5), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0
[5] Hetler, A. (2023, December 18). 10 common cryptocurrency scams in 2023:TechTarget. WhatIs.https://www.techtarget.com/whatis/feature /Common-cryptocurrency-scams
[6] T. Doukoupil, "TripAdvisor accused of deleting reviews that raised red flags". CBS News. November 2nd 2017. [Online]Available: https://www.cbsnews.com/news/tripadvisor-accused-of-deletingreviews-that-raised-red-flags/[Accessed: 8 August 2018].
[7] S. Fenton, "TripAdvisor denies rating system is flawed, after fake restaurant tops rankings in Italy". The Independent. London. June 30th 2015 [Online] Available: https://www.independent.co.uk/tech/tripadvisor-denies-rating-system-is-flawed-after-fake-restaurant-tops-rankings-in-italy-10354818.html. [Accessed: 8- Aug-2018].
[8] D. Lewis, "Meriton allegedly prevents guests from giving negative reviews, bribes them to improve ratings on TripAdvisor". ABC News,October 21st 2015. [Online] Available:http://www.abc.net.au/news/2015-10-21/meriton-apartments-allegedly-cheating-tripadvisorsystem /6870256. [Accessed: 8-Aug-2018].
[9] BBC, "Trip Advisor rebuked over 'trust' claims by ASA". BBC News – Tech, March 8th 2012[Online] Available:https://www.bbc.com/news/technology-16823012. [Accessed: 8-August2018].
[10] Mail Online, “TripAdvisor removes 'reviews you can trust' slogan from its website", London: Daily Mail.co.uk, September 13th 2011. [Online] Available: http://www.dailymail.co.uk/travel/article2036846/Trip Advisor -removes-reviews-trust-slogan-website.html [Accessed: 8-Aug-2018].
[11] D. Williams, “Australian hotel chain fined$2.2 million for manipulating TripAdvisorreviews” August 1st 2018. [Online] Available: https://edition.cnn.com/travel/article/australia-tripadvisor-hotel-fined-trnd/index.html [Accessed: 8-Aug-2018].
[12] "Airbnb Rating System Deceives Guests andHosts", Airbnb Hell, March 18th, 2017. [Online]. Available:https://www.airbnbhell.com/airbnbratig-system-deceives-guests-hosts/. [Accessed: 8-Aug-2018].
[13] Hu, N., Liu, L., & Sambamurthy, V. (2011). Fraud detection in online consumer reviews. Decision Support Systems, 50(3), 614–626.https://doi.org/10.1016/j.dss.2010.08.012
[14] Y. Cai, D. Zhu, Fraud detections for online businesses: a perspective from blockchaintechnology, Financial Innovation 2 (2016) 20. doi:10.1186/s40854-016-0039-4.
[15] Bulchand-Gidumal, J., & González, S. M. (2023). Fighting fake reviews with blockchain enabled consumer-generated reviews. Current Issues in Tourism, 1–15.https://doi.org/10.1080/13683500.2023.2173054
[16] Fradkin, A., Grewal, E., Holtz, D., & Pearson, M. (2015). Bias and Reciprocity in Online Reviews. Proceedings of the Sixteenth ACM Conference on Economics and Computation - EC ’15. https://doi.org/10.1145/2764468.2764528
[17] Dellarocas, C. (2000). Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. Proceedings of the 2nd ACM Conference on Electronic Commerce – EC ’00. https://doi.org/10.1145/352871.352889
[18] Saad, A., and Park, S. Y. (2019, May). Decentralized Directed acyclic graph based DLT Network. In Proceedings of the International Conference on Omni-Layer Intelligent Systems (pp. 158–163).
[19] Isler, M. (2023, December 26). DLT Demistyfied: How distributed ledger technology works. iMi Blockchain. https://imiblockchain.com/dlt-distributed-ledger-technology/
[20] Liu, X., Farahani, B., & Firouzi, F. (2020). Distributed ledger technology. In Springer eBooks (pp. 393–431). https://doi.org/10.1007/978-3-030-30367-9_8
[21] BASHIR, I. Mastering blockchain. PacktPublishing Ltd, 2017.
[22] GARZIK, J. Public versus private blockchains. BitFury Group, San Francisco, USA, White Paper 1 (2015).
[23] Iqbal, M., & Matulevičius, R. (2021).Exploring Sybil and Double-Spending Risks in Blockchain Systems. IEEE Access, 9,7615376177.https://doi.org/10.1109/access.2021.3081998 24] Jani, S. (2018). An Overview of Ripple Technology & its Comparison with Bitcoin Technology. ResearchGate. https://www.researchgate.net/publication/322436263_

[39] Zhou, Z., Wang, M., Yang, C. N., Fu, Z., Sun, X., & Wu, Q. J. (2021). Blockchain-based decentralized reputation system in E-commerce environment.Future Generation Computer Systems, 124, 155–167. https://doi.org/10.
1016/j.future.2021.05.035
[40] Lisi, A., De Salve, A., Mori, P., Ricci, L., & Fabrizi, S. (2021b). Rewarding reviews with tokens:An Ethereum-based approach. Future Generation Computer Systems, 120, 36–54.
https://doi.org/10.1016/j.future.2021.02.003
[41] Karode, T., & Werapun, W. (2021).Robustness against fraudulent activities of a blockchain-based online review system. Peer-to-Peer Networking and Applications, 15(1), 92–106. https://doi.org/10.1007/s12083-021-01225-z
[42] Zulfiqar, M., Tariq, F., Janjua, M. U., Mian, A. N., Qayyum, A., Qadir, J., Sher, F., & Hassan, M. (2021). EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds. Computers &Amp; Security, 100, 102094.https://doi.org/10.1016/j.cose.2020.102094
[43] https://docs.polygonscan.com/api-endpoints/stats
[44] Irissappane, A. A., Jiang, S., & Zhang, J.(2012). Towards a Comprehensive Testbed toEvaluate the Robustness of Reputation Systemsagainst Unfair Rating Attacks.
ResearchGate.https://www.researchgate.net/publication
/232318207_Towards_a_Comprehensive_Testbed_to_
Evaluate_the_Robustness_of_Reputation_Systems_aga
inst_Unfair_Rating_Attacks
[45] Hu, N., Bose, I., Koh, N. S., & Liu, L. (2012). Manipulation of online reviews: An analysis of ratings, readability, and sentiments. Decision Support Systems, 52(3), 674–
684. https://doi.org/10.1016/j.dss.2011.11.002
An_Overview_of_Ripple_Technology_its_Comparison
_with_Bitcoin_Technology
[25] ZHENG, Z., XIE, S., DAI, H., CHEN, X., AND WANG, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (Honolulu, HI,
USA, June 2017), IEEE, pp. 557–564.
[26] Jakobsson, M., & Juels, A. (1999). Proofs of Work and Bread Pudding Protocols(Extended Abstract). In Springer eBooks (pp. 258–272). https://doi.org/10.1007/978-0-387-35568-9_18.
[27] Back, A. (2002). Hashcash - a denial of service Counter-
Measure.ResearchGate.https://www.researchgate.net/p
ublication/2482110_Hashcash_-
_A_Denial_of_Service_Counter-
Measure
[28] Mahmood, W., & Wahab, A. (2018). Survey of consensus protocols. Social Science ResearchNetwork. https://doi.org/10.2139/ssrn.3556482
[29] SUN, J., YAN, J., AND ZHANG, K. Z. K.Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation 2, 1 (Dec. 2016).
[30] QING, S., OKAMOTO, T., AND ZHOU, J.Information and communications security. Springer, 2001.
[31] Nick Szabo - Smart Contracts: Building Blocks for Digital
Markets.(n.d.). https://www.fon.hum.uva.nl/rob/Course
s/InformationInSpeech/CDROM/Literature/LOTwinter
school2006/szabo.best.vwh.net/smart_contracts_2.html
[32] V. Buterin. A next-generation smart contract and decentralized application platform. white paper, 2014
[33] Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J., & Imran, M. (2020).An overview on smart contracts: Challenges, advances andplatforms. Future Generation Computer Systems,105, 475–
491.https://doi.org/10.1016/j.future.2019.12.019
[34] Benet, J. (2014, July 14). IPFS-Content Addressed, Versioned, P2P File system. arXiv.org. https://arxiv.org/abs/1407.3561
[35] Ghodsi, A. (2006). Distributed k-ary System: Algorithms for Distributed Hash Tables.DIVA.https://www.divaportal.org/smash/record
.jsf?pid=diva2%3A11131&dswid=8596
[36] Yaniv Tal, Brandon Ramirez, Jannis Pohlmann. The Graph: A Decentralized Query Protocol for Blockchains. white paper, (March, 2018)
[37] Building Subgraphs with Subgraph Studio. (n.d.). The Graph. https://thegraph.com/blog/building-with-subgraph-studio
[38] Ethereum. (n.d.-a). EIPs/EIPS/eip-712.md at master · ethereum/EIPs. GitHub. https://github.com/ethereum/EIPs/blob/master/EIPS/eip
-
712.md

Decentralized Review Registration System For Validation Of Decentralized Services

Ali Abdolazimi Davari[1], Leyli Mohammad Khanli[2], Pedram Salehpour[3]
[1,2,3] Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Abstract

Users often read the feedback of other users before using a service to make better decisions about that service. Consequently, systems have been created that provide users with a feedback registration system. Blockchain technology has gained a lot of attention in recent years. This has been made possible by blockchain features such as transparency, immutability, and the elimination of intermediary entities. With the expansion of decentralized systems, the potential for fraud is also provided. Users read feedback from other users to use more reliable services. These reviews are a judgment criterion for the credibility of service providers. Existing centralized feedback registration systems are under the control of a central authority that can manipulate user feedback based on personal interests. These systems are susceptible to various types of fraud in registering feedback, such as registering fake and unreal feedback. They are also vulnerable to Sybil and collusion attacks, leading to the registration of unreliable feedback. In this thesis, using the inherent features of blockchain, we present a comprehensive decentralized system for registering user feedback to decentralized services on the Polygon blockchain platform, where no intermediary can manipulate user feedback. This solution, by implementing a reputation mechanism and the ability to evaluate feedback given to a service by other users who have used that service, is resistant to registering fake and biased opinions as well as Sybil and collusion attacks. It also creates a reliable and unchangeable database of user feedback.

Keywords: Reputation Mechanism, Decentralized Feedback Registration, Smart Contract

علی عبدالعظیمی داوری مدرک کارشناسی خود را در رشته مهندسی کامپیوتر و مدرک کارشناسی ارشد خود را در رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه تبریز اخذ کرده است.
نشانه رایانامه ایشان عبارتند از:
abdolazim010.ali@gmail.com

لیلی محمد خانلی استاد گروه مهندسی کامپیوتر دانشگاه تبریز، از سال ۱۳۸۶ در دانشگاه تبریز مشغول به کار است. حوزه‌های تحقیقاتی ایشان سیستم‌های توزیع شده، رایانش ابری و سیستم‌های پیچیده می‌باشد.
نشانه رایانامه ایشان عبارتند از:
L-khanli@tabrizu.ac.ir

پدرام صالح پور مدرک کارشناسی و کارشناسی ارشد خود را در رشته علوم کامپیوتر و دکتری در رشته مهندسی برق الکترونیک از دانشگاه تبریز اخذ کرده است. ایشان در حال حاضر به عنوان استادیار گروه فناوری اطلاعات دانشگاه تبریز مشغول به کار هستند.
نشانه رایانامه ایشان عبارتند از:
Psalehpoor@tabrizu.ac.ir

روش ارجاع: ع.عبدالعظیمی، ل.محمدخانلی، پ.صالح‌پور، سامانه‌ی ثبت بازخورد غیرمتمرکز برای اعتبارسنجی سرویس‌های غیرمتمرکز. فصلنامه محاسبات و سامانه های توزیع شده ،سال ششم، شماره ۲، شماره پیاپی۱۱، صفحه ۱۴ تا ۴۴، سال ۱۴۰۲

How to cite: A.Abdolazimi Davari, L. Mohammad Khanli, P. Salehpour[3], Decentralized Review Registration System For Validation Of Decentralized Services, Journal of Distributed Computing and Systems(JDCS), Vol 6 Issue 2, Page 14-44, 2024.