استفاده از نظریه بازی در طراحی سازوکار اجماع زنجیره بلوکی

مونا باباخانی[۱]، جابر کریم‌پور*[۲]، جواد حاجی‌پور[۳].

۱- دانشجوی دوره دکترای علوم کامپیوتر، دانشگاه تبریز، m.babakhani@tabrizu.ac.ir

۲- عضو هیات علمی گروه علوم کامپیوتر دانشگاه تبریز، karimpour@tabrizu.ac.ir

۳- عضو هیات علمی گروه علوم کامپیوتر دانشگاه تبریز، hajipour@tabrizu.ac.ir

چکیده

زنجیره بلوکی با عدم‌تمرکز و حذف عامل سوم، امکان ذخیره‌سازی امن، شفاف و قابل اعتماد داده‌ها را فراهم کرده است. این ویژگی باعث گسترش پژوهش‌ها و استفاده از زنجیره بلوکی در حوزه‌های متعددی شده است. حفظ عدم‌تمرکز در طول عمر یک زنجیره بلوکی دارای اهمیت فراوان است. اما زنجیره‌های بلوکی عمومی با گذشت زمان با مشکل متمرکزشدن روبه‌رو می‌شوند، به این معنی که بعد از مدتی شبکه زنجیره بلوکی تحت کنترل تعدادی از گره‌های شبکه قرار خواهد گرفت و این موضوع، امنیت و اعتبار شبکه زنجیره بلوکی را با مشکل روبه‌رو می‌کند. دلیل ایجاد این تمرکز، روش‌های مورد استفاده در سازوکار اجماع است. سازوکار اجماع به عنوان بخشی کلیدی از زنجیره بلوکی با حفظ عدم‌تمرکز، می‌تواند امنیت، اعتبار، پایداری و مقیاس‌پذیری زنجیره بلوکی را تحت تاثیر قرار دهد. در این مقاله، ابتدا دلایل ایجاد تمرکز در زنجیره بلوکی مورد بررسی قرار می‌گیرد و پس از آن، استفاده از نظریه بازی در طراحی سازوکار اجماع به‌عنوان راهکاری برای جلوگیری از ایجاد تمرکز در زنجیره بلوکی پیشنهاد شده است.

کلمات کلیدی: زنجیره بلوکی، سازوکار اجماع، عدم‌تمرکز، نظریه بازی

۱. مقدمه

زنجیره بلوکی به عنوان ابزاری برای رسیدن به یکپارچگی در سیستم‌های توزیع‌شده همتا به همتا و حفظ آن می‌تواند تمرکز را از بین ببرد، هزینه‌ها را کاهش دهد و سرعت و کارایی را افزایش دهد. به دلیل نبود مرکز، همه گره‌های شبکه، نسخه‌ای از زنجیره بلوکی را در اختیار دارند که خود باعث ایجاد شفافیت می‌شود. از طرفی به‌دلیل وجود چندین کپی، هر تغییری در دفتر کل ذخیره‌شده به سادگی قابل شناسایی است. داده‌های جدید به صورت بلوکی به انتهای زنجیره بلوکی اضافه می‌شوند؛ برای انجام این نوع ذخیره‌سازی از تکنیک‌های رمزنگاری استفاده می‌شود. بنابراین زنجیره بلوکی به تنهایی امن است. زنجیره بلوکی با وجود توانمندی‌هایش با مشکلاتی مانند متمرکزشدن، مقیاس‌پذیری، امنیت، تهدیدهای محاسبات کوانتومی و قابلیت استفاده روبه‌رو است [1]. مشکلات امنیتی موجود مربوط به پیاده‌سازی زنجیره بلوکی مانند سازوکار مورد

* **Corresponding author: عضو هیات علمی گروه علوم کامپیوتر دانشگاه تبریز**
Email: karimpour@tabrizu.ac.ir

استفاده برای افزودن بلوک جدید به زنجیره و کاربردهای آن مانند قراردادهای هوشمند و برنامه‌های توزیع‌شده مبتنی بر زنجیره بلوکی است.

عدم‌تمرکز به عنوان یکی از مهم‌ترین ویژگی‌های زنجیره بلوکی باعث گسترش استفاده از آن در حوزه‌های متعدد شده است. عدم‌تمرکز به این نکته اشاره دارد که در شبکه زنجیره بلوکی باید همه گره‌ها دارای قدرت حکمرانی یکسان باشند و زنجیره بلوکی تحت کنترل برخی از گره‌ها قرار نگیرد. این قدرت و کنترل به ایجاد و افزودن بلوک جدید به زنجیره بلوکی یعنی سازوکار اجماع مرتبط است. بنابراین سازوکار اجماع یکی از مهم‌ترین مولفه‌های فناوری زنجیره بلوکی در حفظ عدم‌تمرکز است. این اجماع در شبکه‌ای از شرکت‌کنندگان غیرقابل اعتماد که در آن نه هویت شرکت‌کنندگان معتمد و نه تعداد شرکت‌کنندگان غیرقابل اعتماد مشخص است باید صورت گیرد [2]. از طرفی سرعت و ارتباطات سازوکار اجماع نقش مهمی در کارایی، پایداری و مقیاس‌پذیری شبکه زنجیره بلوکی دارد. در طراحی و حتی انتخاب سازوکار اجماع برای یک شبکه زنجیره بلوکی علاوه‌بر کاربرد و اهداف شبکه باید به نکات متعددی توجه داشت. تاکنون سازوکارهای اجماع زیادی معرفی شده‌اند که هر یک در کنار اهداف اصلی یعنی توافق بر بلوک جدید و ترتیب بلوک‌های زنجیره، اهداف خاص دیگری از جمله هدف شبکه مدنظر، کاربردی خاص، رفع برخی از مشکلات امنیتی یا بهبود جنبه‌ای از مقیاس‌پذیری را دنبال می‌کند و هیچ یک به‌طور کامل و برای همه اهداف، انواع یا کاربردهای شبکه زنجیره بلوکی مناسب نیستند.

باتوجه به شباهت مفهوم بازی در نظریه بازی با شبکه زنجیره بلوکی، برخی محققین سعی کرده‌اند تا محیط شبکه زنجیره بلوکی را با هدف تجزیه و تحلیل بهتر توسط نظریه بازی مدل کنند [4] [3]. در کارهای معدودی نیز از نظریه بازی به‌طور مستقیم برای طراحی سازوکار اجماع استفاده شده است. در این مقاله برای حفظ عدم‌تمرکز و امنیت مربوط به آن در زنجیره‌های بلوکی عمومی، درکنار استفاده از نظریه بازی برای تعریف سیستم پاداش‌دهی مناسب، تعریف راهبردهای تنبیهی برای جلوگیری از تخلف مهاجمین و تنبیه ایشان با هدف پشتیبانی از انتخاب تصادفی شرکت‌کنندگان در سازوکار اجماع با حذف نیاز به استفاده از اعتبار برای انتخاب شرکت‌کنندگان مطرح شده است.

در بخش دوم، پیشینه کوتاهی از برخی از سازوکارهای موجود بیان شده است. شرح مختصری از زنجیره بلوکی و نظریه بازی در بخش‌های سه و چهار ذکر شده است. بخش پنجم به بیان مسئله اختصاص داده شده، راه حل پیشنهادی با بررسی جامع در بخش ششم مطرح شده و در نهایت در بخش هفتم پیشنهاداتی برای کارهای آینده بیان شده است.

۲. پیشینه تحقیق

امروزه سازوکارهای اجماع متعددی برای زنجیره بلوکی معرفی و استفاده می‌شوند. سازوکارهای اجماع را از منظرهای مختلفی می‌توان دسته‌بندی کرد. به‌عنوان نمونه می‌توان سازوکارهای اجماع را براساس تکنیک‌های مورد استفاده در سه دسته کلی قرار داد. **دسته اول**، سازوکارهایی که دارای ایده نو هستند. **دسته دوم**، سازوکارهایی که با توسعه سازوکارهای موجود سعی بر بهبود آن‌ها را دارند و **دسته سوم**، سازوکارهایی هستند که با ترکیب دو یا چند سازوکار موجود سعی بر معرفی سازوکارهای بهتر دارند. بر اساس دسته‌بندی مطرح‌شده، بیشتر سازوکارهای اجماع موجود از نوع دوم یا سوم هستند [5]. برخی از سازوکارهای اجماع برای کاربردی خاص و با بهره‌گیری از ویژگی‌های ذاتی کاربرد مورد نظر طراحی شده‌اند. سازوکار اجماع اثبات بازی[1] برای بازی‌های آنلاین توزیع‌شده مبتنی بر زنجیره بلوکی معرفی شده است [6]. باتوجه به جنبه سرگرمی بازی و اینکه بیشتر بازی‌ها خود دارای سیستم امتیازدهی هستند، این سازوکار فاقد سیستم پاداش‌دهی برای ایجاد انگیزه در گره‌ها برای شرکت در سازوکار اجماع است. برخی از سازوکارهای اجماع برای نوع خاصی از زنجیره‌های بلوکی و باتوجه‌به اولویت‌های آن نوع معرفی شده‌اند. به‌عنوان مثال زنجیره‌های بلوکی غیرعمومی، متمرکز هستند و از ویژگی‌های

[1] proof of play

دیگری مثل شفافیت و غیرقابل تغییربودن زنجیره بلوکی بهره می‌برند. برای این نوع از زنجیره‌های بلوکی مشکل متمرکزشدن و امنیت مربوط به آن موضوعیت ندارد. سازوکارهای اجماع تحمل خطای بیزانس[1] از جمله سازوکارهای اجماع مورد استفاده در زنجیره‌های بلوکی غیرعمومی هستند.

سازوکار اجماع اثبات کار[2] به عنوان پرکاربردترین سازوکار اجماع موجود در رمز ارز بیت‌کوین استفاده می‌شود [7]. این سازوکار اجماع از منابع محاسباتی برای گران‌کردن فرایند انتخاب شرکت‌کنندگان بهره می‌برد. اثبات کار مبتنی بر یک معمای ریاضی مبتنی بر توابع چکیده‌ساز[3] طراحی شده است. پیداکردن پاسخ معما دشوار است و تنها با جستجوی فراگیر و غیرهوشمندانه[4] ممکن است، اما تایید پاسخ آن بسیار ساده است. سختی معما، لزوم داشتن منابع محاسباتی قوی را برای شرکت در سازوکار اجماع تضمین می‌کند. از طرفی سختی معما و زمان‌بربودن حل آن، هزینه تخلف را برای گره‌ها بالا می‌برد. برای اطمینان از میزان سختی و زمان‌بربودن حل معما، سختی معما در بازه‌های زمانی مشخص براساس نرخ فعلی چکیده‌سازی شبکه تنظیم می‌شود. با افزایش قدرت محاسباتی گره‌های حاضر در شبکه و در نتیجه بیشترشدن سختی معما، زنجیره بلوکی بر گره‌هایی با منابع محاسباتی قوی و استخرهای استخراج[5] متمرکز می‌شود. بخش بزرگی از سازوکارهای موجود، مبتنی بر این سازوکار اجماع هستند. سازوکار اجماع اثبات کار و سازوکارهای اجماع مبتنی بر آن، امن و برای زنجیره‌های بلوکی عمومی مناسب هستند، اما با گذشت زمان به سمت متمرکزشدن پیش می‌روند و در مقیاس‌پذیری عملکرد خوبی ندارند.

سازوکار اثبات سهام[6] به‌عنوان دومین سازوکار اجماع شناخته شده در سال ۲۰۱۲ معرفی شده است . این سازوکار از سهام برای ایجاد محدودیت استفاده می‌کند. در این سازوکار، گره‌ها برای مشارکت در سازوکار اجماع، سهام خود را به وثیقه می‌گذارند. در نهایت گره‌های شرکت‌کننده به‌طور تصادفی انتخاب می‌شوند ولی نه با احتمال یکسان. احتمال انتخاب هر گره با میزان سهامی که به وثیقه‌گذاشته رابطه مستقیم دارد. از دست‌دادن سهام، مانع خوبی برای متخلفین است. اما این شیوه انتخاب، باعث سهام‌دارترشدن سهام‌داران عمده می‌شود. برخی از سازوکارهای مبتنی بر اثبات سهام، برای انتخاب اولیه نیز، مقدار حداقلی را درنظر می‌گیرند. این سازوکار اجماع به‌طور گسترده در طراحی سازوکارهای اجماع دیگر مورد استفاده قرار می‌گیرد. این سازوکار اجماع و سازوکارهای مبتنی بر آن نیز برای زنجیره‌های بلوکی عمومی مناسب هستند و در مقیاس‌پذیری عملکرد خوبی دارند، اما با گذشت زمان بر سهام‌داران عمده متمرکز می‌شوند.

در سازوکار اثبات اهمیت[7]، منظور از اهمیت، سودمندی گره برای زنجیره بلوکی است [8]. برای مشارکت در این اجماع هر گره باید حداقل مقدار مشخصی از ارز شبکه را دارا باشد. اهمیت هر گره با مولفه‌های متعددی مانند نقل و انتقالات خالص انجام‌شده و میزان فعالیت، محاسبه و ارزیابی می‌شود. این سازوکار محاسبات پیچیده‌ای ندارد، بنابراین نه به منابع محاسباتی قوی نیاز است و نه مصرف انرژی بالایی دارد اما همچنان با مشکل متمرکزشدن روبه‌رو است.

سازوکار اجماع معرفی شده در [9] مبتنی بر تندرمینت[8]، یکی از سازوکارهای تحمل خطای بیزانس، است. در این سازوکار سعی شده است با استفاده از نظریه بازی، عدم‌تمرکز حقیقی حاصل شود. هر دور اجماع در دو گام و دو نوع بازی مجزا انجام می‌شود. نمایه راهبردهای منجر به توافق در هر دو بازی، تعادل نش[9] هستند. باتوجه به مبتنی‌بودن این سازوکار

---

1 byzantine fault tolerance
2 proof of work
3 hash function
4 brute-force search
5 mining pool
6 proof of stake
7 proof of importance
8 Tendermint
9 Nash equilibrium

بر تندرمینت و نحوه نگاشت هر گره به رهبران و نگاشت هر رهبر با گره‌های زیرمجموعه‌اش، این سازوکار نیز برای شبکه‌های غیرعمومی یا کوچک مناسب است.

سازوکار اجماع معرفی‌شده در [10]، مبتنی بر اثبات فعالیت[1] و نظریه بازی است. اثبات فعالیت به دلیل استفاده از اثبات کار، نیاز به منابع محاسباتی قوی و مصرف انرژی بالایی دارد. در [10] سعی‌شده تا با استفاده از نظریه بازی، اثبات فعالیت به گونه‌ای اصلاح شود که بدون حل معمای سخت ریاضی، گره‌ها تمایلی به نقض سازوکار اجماع نداشته باشند. در نهایت نشان‌داده‌شده که حالت مطلوب طراح، تعادل نش بازی است و بازیکنان منطقی از آن پیروی خواهند کرد.

۳. شبکه زنجیره بلوکی

معرفی مفهوم زنجیره بلوکی به اواخر دهه ۸۰ میلادی برمی‌گردد [11] اما در سال ۲۰۰۸ شخصی با هویت مستعار ساتوشی ناکاموتو[2] با معرفی بیت‌کوین از زنجیره بلوکی به عنوان یک دفتر کل[3] توزیع‌شده استفاده کرد [7] . از آن زمان یکی از کاربردهای متداول زنجیره بلوکی را می‌توان دفتر کل توزیع‌شده در زمینه رمزارزها دانست.

زنجیره بلوکی ساختمان داده‌ای است که در آن داده‌ها به‌صورت بلوکی ذخیره می‌شوند و با استفاده از تکنیک‌های رمزنگاری از دست‌کاری حفاظت‌شده و یک زنجیره را تشکیل می‌دهند. داده‌های جدید، به صورت بلوکی به انتهای زنجیره اضافه می‌شوند. مالک هر داده، برای حفظ یکپارچگی داده‌ها، عدم‌انکار تایید خود و قابل تاییدبودن هویتش توسط گره‌های دیگر، به عنوان مالک داده آن را امضای دیجیتال می‌کند؛ دیگر گره‌ها با استفاده از کلید عمومی مالک داده می‌توانند ادعای او را تایید کنند. برای حفظ امنیت در زنجیره بلوکی از توابع چکیده‌ساز به‌طور گسترده استفاده می‌شود. این نحوه ذخیره‌سازی، هزینه دستکاری و جعل داده‌های ذخیره‌شده در زنجیره بلوکی را بالا می‌برد و غیرقابل تغییربودن و امنیت آن را تضمین می‌کند.

زنجیره بلوکی به‌عنوان ابزاری برای ذخیره‌سازی و نگهداری غیرمتمرکز و غیرقابل تغییر دفتر کل در شبکه‌های توزیع‌شده استفاده می‌شود. هر گره در شبکه زنجیره بلوکی دارای یک جفت کلید منحصربه‌فرد عمومی و خصوصی است. هر گره با کلید عمومی شناسایی می‌شود و از کلید خصوصی برای امضای دیجیتال استفاده می‌کند. به دلیل نبود مرکز، همه گره‌های شبکه، نسخه‌ای از زنجیره بلوکی را در اختیار دارند.

زنجیره‌های بلوکی را در سه دسته کلی عمومی، خصوصی و فدرال تقسیم می‌کنند. زنجیره‌های بلوکی عمومی کاملا غیرمتمرکز هستند. در مقابل زنجیره‌های بلوکی خصوصی دارای یک لایه کنترل دسترسی بر روی همه گره‌های شبکه و برای شرکت‌ها و سازمان‌های خصوصی مناسب هستند. زنجیره‌های بلوکی فدرال، بین دو نوع قبلی هستند و شبکه بر روی تعدادی از گره‌ها متمرکز است.

عدم‌تمرکز به عنوان یکی از مهم‌ترین ویژگی‌های زنجیره بلوکی باعث گسترش استفاده از آن در حوزه‌های متعدد شده است. حفظ عدم‌تمرکز و امنیت مربوط به آن می‌تواند اعتبار و قابلیت اعتماد کاربران به زنجیره بلوکی را بالا ببرد. بنابراین حفظ عدم‌تمرکز در طول عمر زنجیره بلوکی دارای اهمیت زیادی است. عدم‌تمرکز به این معنی است که در شبکه زنجیره بلوکی همه گره‌ها دارای قدرت یکسان باشند و زنجیره بلوکی تحت کنترل برخی از گره‌ها قرار نگیرد. این قدرت و کنترل به زمان ایجاد و افزودن بلوک جدید به زنجیره بلوکی برمی‌گردد.

[1] proof of activity
[2] Satoshi Nakamoto
[3] ledger

به فرایند ایجاد و افزودن بلوک جدید به زنجیره بلوکی سازوکار اجماع گفته می‌شود. همه سازوکارهای اجماع در نهایت به اهداف مشترک توافق بر بلوک جدید و ترتیب یکسان زنجیره بلوکی منتهی می‌شوند و در کنار اهداف اصلی، اهداف دیگری از جمله حفظ عدم‌تمرکز و امنیت در برابر حملات مربوطه را نیز دنبال می‌کنند. حقیقت این است که در زنجیره‌های بلوکی عمومی، سازوکارهای اجماع، شبکه را به مرور متمرکز می‌کنند. به‌عبارتی ابزاری که باید عدم‌تمرکز در زنجیره بلوکی را حفظ کند به‌دلیل ملاحظات امنیتی، خود باعث ایجاد تمرکز می‌شود. در بیشتر سازوکارهای اجماع برای مقابله با تهدیدهای امنیتی حاصل از انتخاب تصادفی شرکت‌کنندگان، راهکارهایی مورد استفاده قرار می‌گیرند که به مرور شبکه زنجیره بلوکی را متمرکز می‌کنند.

۴. نظریه بازی[1]

نخستین‌بار نظریه بازی در نوشته‌ای توسط جیمز والدگریو در سال ۱۷۱۳ مطرح شد. او در این نوشته، راهبردی خاص را به‌عنوان حل یکی از بازی‌های دو نفره ورق ارائه کرد. در سال ۱۹۲۸ جان فون نیومان نظریه بازی را به‌عنوان یک رشته مستقل معرفی کرد. در تمام این سال‌ها مطالعات در حوزه نظریه بازی گاهی به سرعت و گاهی آرام در حال گسترش بوده و تاکنون ادامه داشته است.

نظریه بازی به مطالعه مدل‌های ریاضی از تعارض و همکاری بین تصمیم‌گیرندگان عاقل[2] می‌پردازد و به‌عنوان روشی اصولی برای پیش‌بینی نتیجه تعامل بین تصمیم‌گیرندگان استفاده می‌شود. همه بازی‌ها ترکیبی از شانس، مهارت و راهبرد[3] به نسبت‌های مختلف هستند. راهبرد هر بازیکن یک برنامه حرکت کامل است که مشخص می‌کند بازیکن باید در هر مرحله و با هر تاریخچه‌ای چه حرکتی را انجام دهد. یک بازی شامل مجموعه‌ای از بازیکنان، اطلاعات، مجموعه‌هایی از حرکت‌ها[4]، راهبردها و نتیجه مشخصی برای هر ترکیب از راهبردهای ممکن می‌باشد. در بازی سود و زیان، هر فرد علاوه‌بر راهبرد خود او به راهبردهایی که دیگران انتخاب می‌کنند نیز بستگی دارد. بازیکنان عاقل و به دنبال بیشینه‌کردن عایدی[5] خود هستند.

هر نتیجه منطقی ممکن، ارزشی خاص برای بازیکن دارد؛ عقلانیت به این معنی است که هر بازیکن سعی می‌کند تا باتوجه‌به این ارزش‌ها به بهترین وجه منافع خود را تامین کند. نکته مهم این است که عاقل‌بودن بازیکن فقط به معنای پیگیری سیستم ارزشی خود بازیکن است. بنابراین، هنگام تجزیه و تحلیل باید هر بازیکن را در سیستم ارزشی یا ترجیحی خودش درنظر گرفت. برای ارزش‌های هر بازیکن یک مقیاس عددی کامل تخصیص داده می‌شود که با آن می‌توان تمام نتایج منطقی بازی را که با هر ترکیب ممکن از انتخاب راهبردهای همه بازیکنان مطابقت دارد، مقایسه کرد. عدد مربوط به هر نتیجه ممکن را عایدی آن بازیکن برای آن نتیجه می‌نامند. ترجیحات هر بازیکن با دیگران متفاوت است و با کمک عایدی‌ها مشخص می‌شود [12].

نتیجه تعامل بازیکنان منطقی در بازی تعادل[6] است. در نظریه بازی، تعادل‌ها حل بازی هستند. تعادل وضعیتی است که باتوجه‌به شرایط بازی، خود را بر بازیکنان تحمیل می‌کند. یک بازی ممکن است شامل چندین تعادل و یا حتی فاقد تعادل باشد.

[1] Game theory
[2] rational
[3] strategy
[4] actions
[5] payoff/utility
[6] equilibrium

طراحی سازوکار به نوعی مهندسی معکوس نظریه بازی است [13]. طراحی سازوکار، هنر طراحی بازی به‌گونه‌ای است که بازیکنان رفتار تعادلی مطلوب از خود نشان دهند. طراح سازوکار که از ترجیحات دقیق همه بازیکنان بی‌اطلاع است، باید بازی یا همان سازوکار را طوری طراحی کند که تعادل بازی همان انتخاب اجتماعی مطلوب باشد. اگر بازی با دقت طراحی شود در نهایت می‌توان توقع داشت که شرکت‌کنندگان در سازوکار، در انتخاب اجتماعی مطلوب به توافق برسند.

۵. انتخاب شرکت‌کنندگان سازوکار اجماع

همه سازوکارهای اجماع در نهایت به اهداف مشترک توافق بر بلوک جدید و ترتیب یکسان زنجیره بلوکی منتهی می‌شوند. هر سازوکار اجماع در کنار اهداف اصلی، اهداف دیگری از جمله حفظ عدم‌تمرکز و امنیت در برابر حملاتی خاص یا بهبود جنبه‌ای خاص از مقیاس‌پذیری را نیز دنبال می‌کند. حملات زیادی امنیت سازوکار اجماع را تهدید می‌کنند و راهبردهای متنوعی برای حفظ امنیت سازوکار اجماع استفاده می‌شوند.

مهم‌ترین ویژگی زنجیره‌های بلوکی، به‌خصوص در نوع عمومی آن، عدم‌تمرکز است. شبکه زنجیره بلوکی زمانی غیرمتمرکز است که همه گره‌ها دارای قدرت یکسان باشند. هر سازوکار اجماع باید بین سرعت به‌عنوان یکی از جنبه‌های مقیاس‌پذیری، عدم‌تمرکز و امنیت توازن ایجاد کند. سازوکارهای اجماع زیادی برای زنجیره‌های بلوکی عمومی با هدف حفظ عدم‌تمرکز در زنجیره بلوکی معرفی شده‌اند اما همچنان بسیاری از سازوکارهای موجود با مشکل متمرکزشدن روبه‌رو هستند و فقط ایجاد تمرکز را به‌تاخیر می‌اندازند. حفظ عدم‌تمرکز در زنجیره بلوکی رابطه مستقیم با نحوه انتخاب شرکت‌کنندگان سازوکار اجماع دارد. دو دیدگاه کلی در انتخاب شرکت‌کنندگان سازوکار اجماع وجود دارد. اول اینکه، شرکت‌کنندگان در اجماع، گروهی ثابت از گره‌ها باشند. این روش دارای مزایای امنیتی است که حاصل شناخته‌شده‌بودن گره‌های اجماع است، مانند انتخاب گره‌های معتمد. اما استفاده از گروه ثابتی از گره‌ها شبکه زنجیره بلوکی را متمرکز می‌کند و شبکه را با مشکلات حاصل از تمرکز مثل نفوذ، ترجیح نفع شخصی و درنهایت کاهش اعتماد روبه‌رو می‌کند. در مقابل، انتخاب تصادفی شرکت‌کنندگان، تضمین‌کننده عدم‌تمرکز در زنجیره‌های بلوکی عمومی است. اما این راهکار، مشکلات امنیتی ناشی از انتخاب تصادفی شرکت‌کنندگان را درپی خواهد داشت. سازوکار اجماعی که با هدف حفظ عدم‌تمرکز، شرکت‌کنندگان را به‌صورت تصادفی انتخاب می‌کند، باید در برابر خطرات این انتخاب مقاوم باشد.

باتوجه‌به دلیل ذکرشده، روش اول برای زنجیره‌های بلوکی غیرعمومی مناسب است. برای سازوکارهای اجماع زنجیره‌های بلوکی عمومی، سعی بر انتخاب تصادفی بازیکنان است. اولین موضوع برای دستیابی به این مهم، جذب همکاری گره‌های صادق شبکه است. سازوکارهای اجماع مربوط به زنجیره‌های بلوکی عمومی، برای جذب همکاری گره‌های صادق، نیازمند یک سازوکار تشویقی مناسب هستند. این سازوکار علاوه‌بر ایجاد انگیزه مشارکت، باعث افزایش اعتبار سیستم می‌شود. از این رو در تمام سازوکارهای اجماع مورد استفاده در زنجیره‌های بلوکی عمومی، نوعی سیستم پاداش‌دهی تعریف شده است. پاداش‌ها متنوعند. برخی از پاداش‌ها در ازای ساخت بلوک جدید داده می‌شوند. در برخی از سازوکارهای اجماع مانند سازوکار اثبات کار به‌عنوان پرکاربردترین سازوکار موجود و سازوکارهای مبتنی بر آن، گره‌ها با هدف دریافت پاداش تولید بلوک جدید، با یکدیگر رقابت می‌کنند. برخی دیگر مانند سازوکار اثبات اهمیت از پاداش‌ها به‌صورت درنظرگرفتن امتیازی به‌عنوان حُسن همکاری است. به‌این‌صورت که فعالیت‌های هر گره در شبکه ثبت و به ازای آن‌ها برای گره امتیازات مثبتی درنظر گرفته می‌شود.

دومین و مهم‌ترین مسئله که باید در انتخاب تصادفی بازیکنان به آن توجه داشت، حفظ امنیت است. انتخاب تصادفی شرکت‌کنندگان، احتمال حضور گره‌های متخلف در سازوکار اجماع را بالا می‌برد. حضور این گره‌ها و عدم‌برخورد مناسب با ایشان، می‌تواند با ازبین‌رفتن اعتماد گره‌های دیگر، به اعتبار سیستم خدشه وارد کند و به مرور از تعداد گره‌های شرکت‌کننده

در زنجیره بلوکی بکاهد. از این رو طراحان سازوکارهای اجماع برای حفاظت دربرابر خطرات امنیتی حاصل از انتخاب تصادفی شرکت‌کنندگان، مانند حمله سیبل، باتوجه‌به نوع و کاربرد شبکه زنجیره بلوکی، از دو راهبرد به‌طور همزمان استفاده می‌کنند. راهبرد اول که به شیوه انتخاب شرکت‌کنندگان برمی‌گردد، گران‌کردن شرکت در سازوکار اجماع یا استفاده از گره‌های معتبرتر است. طراحان سازوکار اجماع زنجیره بلوکی با این ایده، شرایطی مانند داشتن حداقل مقدار اعتبار یا ارز یا ایجاد رابطه مستقیم بین میزان اعتبار یا ارزِ گره با شانس انتخاب آن برای شرکت در اجماع را تنظیم کرده‌اند. اعتبار می‌تواند هر آن چیزی باشد که برای شبکه زنجیره بلوکی دارای اهمیت است. این راهکار علاوه‌بر تشویق گره‌ها به فعال‌بودن و همکاری، امنیت زنجیره بلوکی را با به‌کارگیری گره‌های معتبرتر که به نوعی ذی‌نفعان زنجیره بلوکی هستند، تضمین می‌کند. ایده اصلی این است که صاحبان اعتبار و سرمایه در زنجیره بلوکی ذی‌نفعان شبکه هستند که با به خطرافتادن اعتبار شبکه، متضرر خواهند شد، پس ایشان نیز سود خود را در همراهی و همکاری با زنجیره بلوکی می‌دانند. بنابراین سازوکارهای تشویقی علاوه‌بر ایجاد انگیزه، دارای مزیت امنیتی نیز هستند. اما وجود همین اعتبارها و امتیازها و چنین راهبردهای انتخابی به مرور باعث ایجاد تمرکز در شبکه می‌شوند.

شرکت‌کنندگان در سازوکار اثبات کار و سازوکارهای مبتنی بر آن، با هدف شرکت در سازوکار برای حل معمای ریاضی با میزان سختی مشخص، به منابع محاسباتی قوی نیاز دارند. در سازوکار اثبات سهام و سازوکارهای مبتنی برآن، شرکت‌کنندگان باید مقداری از سهام خود را به وثیقه بگذارند. شرکت‌کنندگانی که ارز بیشتری به وثیقه بگذارند، شانس بیشتری برای شرکت در سازوکار اجماع را پیدا می‌کنند. هر دو مثال مطرح‌شده با گران‌کردن شرکت در سازوکار اجماع می‌توانند در مقابل برخی حملات، به‌طور خاص حمله سیبل، مقاومت کنند. اما با گذشت زمان هر دو راهبرد باعث ایجاد تمرکز بر روی گروه خاصی از گره‌های شبکه می‌شوند. سازوکارهای مبتنی بر اثبات کار بر روی استخرهای استخراج و سازوکارهای مبتنی بر سهام بر سرمایه‌داران عمده متمرکز می‌شوند.

راهبرد دوم که مربوط به خود الگوریتم سازوکار اجماع می‌باشد، هزینه‌برکردن تخلف برای گره‌ها است. این کار باید به‌گونه‌ای انجام شود که هر گره‌ای تخلف را به ضرر خود و همکاری با سازوکار اجماع را به نفع خود بداند. در سازوکارهای موجود، این کار به طرق مختلفی انجام می‌شود. سازوکار اثبات کار و سازوکارهای مبتنی بر آن، با تنظیم سختی مسئله در بازه‌های زمانی مشخص، زمان‌بربودن حل مسئله را تضمین می‌کنند. هزینه تخلف در این نوع سازوکارها زمان و انرژی مورد استفاده برای دستکاری داده‌ها و سپس حل مسئله خواهد بود. گره در سازوکار اثبات سهام و سازوکارهای مبتنی بر آن، در صورت تخلف، سهام وثیقه گذاشته‌شده خود را از دست می‌دهد.

شیوه‌های مورد استفاده برای پیاده‌سازی راهبرد امنیتی اول، هرچند کُند اما به مرور شبکه را با تمرکز روبه‌رو می‌کنند. در این وضعیت همه گره‌های شبکه برای شرکت در سازوکار اجماع دارای شانس و احتمال برابر نیستند؛ درحالی‌که تعدادی شانس بیشتری برای انتخاب دارند برخی دارای احتمال انتخاب نزدیک به صفر هستند. این شیوه انتخاب زنجیره بلوکی را به سمت بی‌عدالتی و در نهایت متمرکزشدن پیش می‌برد. مهم‌ترین عامل ایجاد تمرکز، وابسته‌کردن فرایند انتخاب شرکت‌کنندگان در اجماع با اعتبار و سهام گره‌ها، به دلایل امنیتی است. بنابراین برای حفظ عدم‌تمرکز باید این وابستگی را از بین برد و از راهکار متفاوتی برای حفظ امنیت مربوط به انتخاب تصادفی شرکت‌کنندگان استفاده کرد.

۶. به سوی یک راه حل

در تمام سازوکارهای اجماع زنجیره‌های بلوکی عمومی سعی شده است تا با پشتیبانی از انتخاب تصادفی شرکت‌کنندگان سازوکار اجماع با متمرکزشدن زنجیره بلوکی و مسائل امنیتی حاصل از این نوع انتخاب مقابله کنند. همه از راهبردهای کلان مشابه یعنی تشویق گره‌ها برای مشارکت، گران‌کردن مشارکت و هزینه‌برکردن تخلف استفاده کرده‌اند اما با شیوه‌های متفاوت.

شبکه زنجیره بلوکی شبیه به مفهوم بازی در نظریه بازی است. در هر دو، مجموعه‌ای از عوامل غیرقابل اعتماد با یکدیگر در تعاملند. همانطور که بازیکنان با انگیزه به‌دست‌آوردن عایدی بازی می‌کنند، سازوکار اجماع زنجیره بلوکی نیز نیازمند یک سازوکار تشویقی برای جذب همکاری گره‌هاست. از طرفی طراحی سازوکار به معنی طراحی بازیی با هدف رسیدن به تعادل مطلوب یا همان انتخاب اجتماعی موردنظر طراحان سازوکار است. بنابراین با طراحی بازی مناسب با درنظرگرفتن تعاملات بازیکنان و با کمک تکنیک‌های نظریه بازی می‌توان سازوکار اجماع مناسبی را برای شبکه زنجیره بلوکی تعریف کرد. نظریه بازی می‌تواند به‌شیوه‌ای متفاوت امنیت سازوکار اجماع را تضمین کند.

این کار با تشخیص انگیزه گره‌های شبکه زنجیره بلوکی برای مشارکت در سازوکار اجماع شروع می‌شود. با فرض عمومی‌بودن زنجیره بلوکی و انتخاب تصادفی شرکت‌کنندگان سازوکار اجماع پیش از شروع هر دور اجماع، بیشتر گره‌ها با انگیزه دریافت پاداش از مشارکت استقبال می‌کنند و تعدادی نیز با انگیزه‌های مخرب قصد جعل داده یا برهم‌زدن اجماع را دارند. باید توجه داشت که تخلفات متنوعند و انگیزه‌های تخلف نیز در بازه‌ای گسترده قرار دارند. تخصیص مناسب توابع عایدی یا همان پاداش‌ها می‌تواند زمینه‌ساز خوبی برای مشارکت گره‌ها در سازوکار اجماع باشد. علاوه‌بر آن اگر پاداشی که گره در ازای مشارکت دریافت می‌کند، بیش از سود دریافتی او از تخلف باشد، آنگاه گره‌ها مشارکت را به تخلف ترجیح خواهند داد که خود مانع خوبی برای برخی تخلفات است، پس با دریافت پاداش بیشتر در ازای مشارکت، مشارکت در سازوکار اجماع برای تعداد زیادی از گره‌ها یک راهبرد غالب خواهد بود.

اما گاهی انگیزه مهاجم و دریافتی او از تخلف بیش از پاداش همکاری است. در این شرایط اتخاذ راهبردهای تنبیهی با کمک نظریه بازی می‌تواند کمک خوبی در حفظ امنیت باشد. راهبرد تنبیهی، راهبردی است که بازیکنان برای تنبیه بازیکن یا بازیکنانی خاص انتخاب می‌کنند و بر عایدی بازیکنان مورد تنبیه تاثیر منفی خواهد داشت، مانند تنبیه بازیکن خاطی با کمینه‌کردن مقداری که او قصد بیشینه‌کردنش را دارد. اگر سازوکار اجماع به صورت کاری جمعی که در آن امکان تشخیص تخلف و متخلف وجود داشته باشد تعریف شود آنگاه با تشخیص متخلفین در هر اجماع، گره‌های دیگر می‌توانند با اعمال راهبرد تنبیهی مشخص، متخلف را به شیوه‌ای متضرر کنند تا علاوه‌بر ضرر نهفته در تابع عایدی تعریف‌شده، ضرری بیشتر را بر ایشان تحمیل کنند.

برای افزودن هر بلوک جدید، سازوکار اجماع یک بار اجرا می‌شود. اعضای شرکت‌کننده در سازوکار اجماع همان گره‌های شبکه زنجیره بلوکی هستند. از دیدگاه نظریه بازی، سازوکار اجماع را می‌توان یک بازی مکرر[1] در نظر گرفت. این نوع بازی در مقابل بازی‌های یک‌باره[2] قرار دارد. در این نوع بازی، بازی به دفعات بین بازیکنانی ثابت انجام می‌شود. بازیکن فرصت کسب شهرت دارد و به همین منوال می‌تواند اطلاعاتی را از حریفان کسب کند. از طرفی بازیکنان می‌توانند در طول زمان برای رسیدن به سود، توافق یا برای مجازات یک متقلب در بازی‌های آینده با یکدیگر همکاری کنند. پس می‌توان برای تحمیل خسارتی بیشتر از تنبیه مبتنی بر عایدی موجود در راهبرد تنبیهی با هدف جلوگیری از وقوع تخلف، از ویژگی مکرربودن بازی نیز برای تنبیه متخلفین استفاده کرد.

با انتخاب راهبردی مناسب جهت تنبیه، هم می‌توان مانع از وقوع تخلف شد و هم در صورت وقوع می‌توان از اجرای مجدد آن در اجماع‌های بعدی جلوگیری کرد. ازاین‌رو راهبردهای تنبیهی نظریه بازی در کنار استفاده از ویژگی مکرربودن بازی بخشی دیگر از امنیت سازوکار اجماع را نیز تامین و غالب‌بودن راهبرد مشارکت در سازوکار اجماع را برای همه گره‌ها تضمین می‌کنند. بنابراین با تشخیص همه راهبردهای ممکن، انتخاب راهبردهای تنبیهی مناسب و استفاده از ویژگی مکرربودن بازی، می‌توان امنیت سازوکار اجماع را حفظ و از انتخاب تصادفی شرکت‌کنندگان پشتیبانی کرد.

[1] repeated game
[2] one-shot game

حال باید بازیی طراحی شود تا تمام شرایط مورد نظر را برآورده کند. همه انگیزه‌ها و ارزش‌گذاری‌ها را در قالب عایدی‌ها پوشش دهد و باتوجه به عایدی‌ها روند اجرای بازی به‌گونه‌ای پیش رود که برای همه بازیکنان راهبرد مشارکت در بازی، همان مشارکت در سازوکار اجماع، یک راهبرد غالب یا بهترین پاسخ هر بازیکن به راهبرد انتخابی بازیکنان دیگر باشد. در این صورت نمایه راهبردی که گویای مشارکت است، یک تعادل نش برای بازی خواهد بود که خود را بر بازیکنان تحمیل می‌کند و هیچ بازیکن عاقلی با انحراف از آن سود بیشتری به دست نخواهد آورد. به‌عبارتی نمایه راهبرد $s^* = (s_1^*, s_2^*, \dots, s_n^*)$ ، با مشارکت $\boldsymbol{s_i^*}$ به ازای $i = 1, \dots, n$ یک تعادل نش است اگر

$$u_i(s_i^*, \boldsymbol{s_{-i}^*}) \geq u_i(s_i, \boldsymbol{s_{-i}^*});\ \forall s_i \epsilon S_i, \forall i \in N \qquad (1)$$

که s_i راهبردی غیر از مشارکت برای بازیکن i ، u_i عایدی بازیکن i، $\boldsymbol{s_{-i}^*}$ نمایه راهبرد تعادل همه بازیکنان به جز بازیکن i و S_i مجموعه همه راهبردهای ممکن بازیکن i است.

ازاین‌رو نظریه بازی می‌تواند مزایای امنیتی موردنظر برای سازوکار اجماع را ایجاد کند. به این صورت که پاداش‌ها انگیزه لازم برای مشارکت و همکاری را ایجاد می‌کنند و ترس از اعمال راهبرد تنبیهی مانعی برای تخلف گره‌ها در شبکه می‌شود. بنابراین می‌توان بدون نیاز به انتخاب شرکت‌کنندگان سازوکار اجماع برمبنای اعتبارات و امتیازات، ایشان را به‌صورت کاملا تصادفی انتخاب کرد و نگران متمرکزشدن زنجیره بلوکی نبود.

۷. کارهای آینده

حفظ عدم‌تمرکز از مهم‌ترین ویژگی‌های زنجیره بلوکی است و اعتبار آن را تضمین می‌کند. انتخاب تصادفی و با شانس یکسان گره‌ها برای شرکت در سازوکار اجماع زنجیره بلوکی تنها راه حفاظت از عدم‌تمرکز است. راهکارهای مورد استفاده در سازوکارهای اجماع موجود برای مقابله با مسائل امنیتی مربوط به انتخاب تصادفی شرکت‌کنندگان، زنجیره‌های بلوکی عمومی را به مرور متمرکز می‌کنند. با کمک نظریه بازی می‌توان به شیوه‌ای متفاوت از سازوکار اجماع در برابر تهدیدهای امنیتی مربوط به انتخاب تصادفی شرکت‌کنندگان اجماع و در نتیجه عدم‌تمرکز زنجیره بلوکی محافظت کرد. تعریف توابع پاداش با کمک نظریه بازی انگیزه لازم برای شرکت در سازوکار اجماع را ایجاد می‌کند و راهبردهای تنبیهی لحاظ‌شده تمایل بازیکنان برای تخطی از انتخاب اجتماعی مطلوب یا همان تعادل بازی را از بین می‌برد.

حال دو مسئله وجود دارد. اول این که به دلیل بی‌اطلاعی از انگیزه‌ها و سیستم‌های ارزش‌گذاری واقعی بازیکنان، امکان وجود خطا در موارد تشخیص‌داده‌شده وجود دارد. بنابراین بازی طراحی‌شده باید بتواند با وجود مقدار کمی از خطا در تشخیص، عملکرد مناسب خود را حفظ کند و به عبارتی در برابر وقوع محدود برخی تخلفات تاب‌آوری داشته باشد. مسئله دوم، نحوه تشخیص به موقع متخلف در شبکه زنجیره بلوکی است. توجه به این نکته نیز ضروری است که حملات تشخیص‌داده‌شده مربوط به سازوکار اجماع متنوع هستند و با انگیزه‌های متعددی انجام می‌شوند. راهکارهایی جهت پاسخگویی به این مسائل در حال بررسی هستند که در کارهای آینده مطرح خواهند شد.

۸. منابع

[1] A. I. Sanka and M. Irfan and I. Huang and R.C. cheung, "A survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research," *Computer communications*, vol. 169, pp. 179-201, 2021.

[2] D. Drescher, Blockchain basics: a non-technical introduction in 25 steps., Apress, 2017.

[3] A. Lesham, W. Wang and D. Niyato and P. Wang and A., "Decentralized caching for content delivery based on blockchain: a game theoretic perspective," in *International conference on comminications (ICC), IEEE*, 2018.

[4] W. Wang and D. T. Hoang and P. Hu and Z. Xiong and D. Niyato and P. Wang and Y. Wen and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328-22370, 2019.

[5] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620-43652, 2021.

[6] H. Y. Yuen and F. Wu and W. Cai and H. C. Chan and Q. Yan and V. C. M. Leung, "Proof-of-Play: a novel consensus model for blockchain-based peer-to-peer gaming system," in *International symposium on blockchain and secure critical infrastructure, ACM*, 2019.

[7] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized business review*, pp. 21260-21269, 2008.

[8] NEM, "NEM technical reference," NEM, [Online]. Available: https://docs.nem.io/pages/Whitepapers/docs.en.html.

[9] N. Alzahrani and N. Bulusu, "Towards true decentralization: a blockchain consensus protocol based on game theory and randsomness," in *International conference on decision and game theory for security, Springer*, 2018.

[10] Z. Boreiri and A. N. Azad, "A novel consensus protocol in blockcahin network based on proof of activity protocol and game theory," in *International conference on web research (ICWR), IEEE*, 2022.

[11] W. S. Stornetta and S. Haber, "How to time-stamp a digital documnet," in *Conference on the theory and application of cryptography, Springer*, 1990.

[12] A. Dixit and S. Skeath and D. Reiley, Games of strategy, W. W. norton & company, 2015.

[13] Y. Narahari, Game theory and mechanism design, World scientific, 2014.

[14] Z. Liu and N. C. Luong and W. Wang and D. Niyatoand P. Wang and Y. C. Liang and D. I. Kim, "A survey on blockchain: a game theoretical perspective," *IEEE Access*, vol. 7, pp. 47615-47643, 2019.