
بسم الله الرحمن الرحيم

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

تحلیل شبکه پیچیده از شبکه تراکنش بیت‌کوین [۱]

گزارش پایانی درس ارائه مطلب

مسیح تنورساز

استاد درس

دکتر محمدحسین منشئی

۱۴۰۲

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

گزارش پایانی درس ارائه مطلب – آقای مسیح تنورساز

تحت عنوان

تحلیل شبکه پیچیده از شبکه تراکنش بیت‌کوین

تشکر و قدردانی

پروردگار منّان را سپاسگزارم .....

فهرست مطالب

فهرست تصاویر

فهرست جداول

چکیده

تحلیل شبکه‌های پیچیده[1] به عنوان یکی از شاخه‌های نوین علم شبکه‌ها، به بررسی ساختار و پویایی شبکه‌های پیچیده می‌پردازد. شبکه تراکنش بیت‌کوین[2] به عنوان یکی از بزرگترین و مهم‌ترین شبکه‌های مالی دیجیتال، نمونه‌ای بارز از یک شبکه پیچیده است که تحلیل آن می‌تواند دیدگاه‌های ارزشمندی در مورد رفتار کاربران و ساختار کلان این شبکه فراهم کند. در این پژوهش، به بررسی شبکه تراکنش بیت‌کوین از جایگاه تحلیل شبکه‌های پیچیده پرداخته شده است.

در این مقاله، شبکه‌ی پیچیده‌ی تراکنش‌های بیت‌کوین را مورد بررسی و تحلیل قرار می‌دهیم. به‌طور خاص، یک روش نمونه‌گیری جدید به نام پیمایش تصادفی با بازگشت[3] معرفی می‌شود تا نمونه‌گیری داده‌ها به‌طور موثرتری انجام شود. سپس، تحلیل جامعی از شبکه بلاکچین[4] بیت‌کوین از نظر توزیع درجه، ضریب خوشه‌بندی، طول کوتاه‌ترین مسیر، مولفه‌های متصل، مرکزیت، خودهمبستگی، و ضریب باشگاه ثروتمندان انجام می‌دهیم. پس از تحلیل، شاهد چندین نتیجه‌گیری جالب و حیرت انگیز مانند پدیده دنیای کوچک، وضعیت چند مرکزی، اتصال ترجیحی، و عدم تاثیر باشگاه ثروتمندان در شبکه فعلی خواهیم بود.

واژه‌های کلیدی: ۱- بیت‌کوین، ۲- بلاکچین، ۳- شبکه پیچیده، ۴ـ تحلیل شبکه.

[1] Complex Network
[2] Bitcoin Transaction Network
[3] Random Walk With Flying-Back (RWFB)
[4] Blockchain

فصل اول

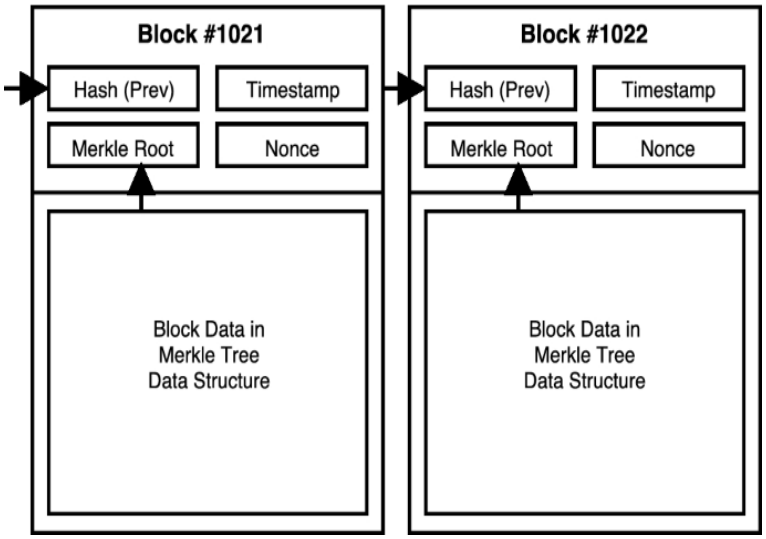
مقدمه

در سال‌های اخیر، بیت‌کوین [۲] به عنوان یکی از برجسته‌ترین ارزهای دیجیتال از زمان پیدایش آن در سال ۲۰۰۹ توسط ساتوشی ناکاموتو[1] مورد توجه قرار گرفته است. ویژگی‌های نوآورانه‌ای نظیر ناشناس بودن، کارمزد پایین تراکنش، عدم تمرکز و دسترسی دائمی به خدمات، بیت‌کوین را به موضوعی پرطرفدار در سال‌های گذشته تبدیل کرده است. با این حال، تحقیقات محدودی در زمینه تحلیل شبکه بیت‌کوین انجام شده است. تحلیل ساختار شبکه تراکنش‌های بیت‌کوین از منظر شبکه‌های پیچیده بسیار مهم است زیرا می‌تواند رازهای سیستم‌های بلاکچین موجود را آشکار کند.

مهمترین مشارکت‌های این پژوهش به شرح زیر خلاصه می‌شود:

یک روش نمونه‌گیری جدید به نام پیمایش تصادفی با بازگشت برای تحلیل داده‌های تراکنش بیت‌کوین معرفی می‌گردد. روش بیان شده در حالی که پیچیدگی محاسباتی کمتری نسبت به روش های متعارف دارد، نمونه برداری[2] دقیق‌تری از شبکه پیچیده بیت‌کوین ارائه می‌دهد و ویژگی‌های شبکه اصلی بیت‌کوین را حفظ می‌کند. سپس با استفاده از روش معرفی شده، از شبکه نمونه برداری کرده و به تحلیل آن میپردازیم. با تحلیل این شبکه پیچیده چندین مشاهده جدید از عملکرد کاربران و ساختار شبکه

[1] Satoshi Nakamoto
[2] Sampling



شکل ۱ - ۱: ساختار کلی بلاکچین

فعلی بیت‌کوین به دست می‌آوریم.

مشاهدات جدید درک عمیقی از ساختار شبکه بلاکچین بیت‌کوین ارائه می‌دهند و می‌توانند به بهبود امنیت و کارایی شبکه‌های بلاکچین ارزهای دیجیتال کمک کنند.

۱ - ۱ مقدمه‌ای بر بلاکچین

بلاکچین یک فناوری انقلابی است که به عنوان پایه‌ای برای بیت‌کوین و سایر ارزهای دیجیتال[1] عمل می‌کند. در ساده‌ترین شکل، بلاکچین یک دفتر کل[2] توزیع شده و تغییرناپذیر است که تراکنش‌ها را به صورت امن و شفاف ذخیره می‌کند [۳].

۱ - ۱ - ۱ مفهوم بلاکچین

همانطور که در شکل ۱ - ۱ قابل مشاهده است، ساختار بلاکچین شامل تعدادی بلاک می‌باشد که اطلاعات تراکنش‌ها رو درون خود جای داده اند و به کمک زنجیره‌ای به یکدیگر متصل شده اند. هر بلاک شامل اطلاعات زیر است:

- **اطلاعات تراکنش‌ها:** لیستی از تراکنش‌های انجام شده.
- **هش[3] بلاک قبلی:** یک رشته منحصر به فرد که به بلاک قبلی اشاره می‌کند و بلاک‌ها را به یکدیگر متصل می‌سازد.

[1] Cryptocurrency
[2] Ledger
[3] Hash

- **هش بلاک فعلی:** یک رشته منحصر به فرد که به محتوای بلاک اشاره دارد و با استفاده از الگوریتم‌های رمزنگاری ایجاد می‌شود.

۱-۱-۲ نحوه کار بلاکچین

بلاکچین یک سیستم توزیع‌شده و غیرمتمرکز است که امکان ثبت و ذخیره‌سازی امن و شفاف اطلاعات را بدون نیاز به یک نهاد مرکزی فراهم می‌کند. در این بخش، نحوه کار بلاکچین را با جزئیات بیشتری بررسی می‌کنیم.

تراکنش‌ها

افراد تراکنش‌های خود را از طریق یک شبکه توزیع‌شده ارسال می‌کنند. هر تراکنش شامل اطلاعاتی نظیر فرستنده، گیرنده و مقدار ارز منتقل شده است. این تراکنش‌ها در شبکه منتشر می‌شوند تا توسط گره‌های[1] موجود در شبکه بررسی و تایید شوند.

تایید تراکنش‌ها

تراکنش‌ها توسط گره‌های شبکه تایید می‌شوند. گره‌ها دستگاه‌هایی هستند که بلاکچین را پشتیبانی می‌کنند و مسئولیت تایید صحت تراکنش‌ها را بر عهده دارند. برای تایید تراکنش‌ها، گره‌ها از الگوریتم‌های رمزنگاری استفاده می‌کنند تا اطمینان حاصل کنند که فرستنده تراکنش واقعاً مالک ارز دیجیتال مورد نظر است.

ایجاد بلاک جدید

پس از تایید تراکنش‌ها، این تراکنش‌ها به یک بلاک جدید اضافه می‌شوند. هر بلاک شامل مجموعه‌ای از تراکنش‌های تایید شده است که به همراه یک شناسه یکتا (هش بلاک) و هش بلاک قبلی به بلاکچین اضافه می‌شود. فرآیند ایجاد بلاک جدید معمولاً توسط استخراج‌کنندگان[2] انجام می‌شود که از قدرت محاسباتی خود برای حل مسائل پیچیده ریاضی استفاده می‌کنند.

افزودن به زنجیره

بلاک جدید به زنجیره بلاک‌های قبلی متصل می‌شود. این اتصال با استفاده از هش بلاک قبلی و هش بلاک جدید انجام می‌شود. هش بلاک جدید باید به گونه‌ای محاسبه شود که با معیارهای مشخصی سازگار باشد، که این امر به تضمین امنیت و یکپارچگی بلاکچین کمک می‌کند.

---
[1] Node
[2] Miners

توزیع بلاکچین

نسخه جدید بلاکچین به تمام گره‌های شبکه ارسال می‌شود. پس از تایید و صحت سنجی بلاک، آنها نسخه‌های خود را به‌روزرسانی می‌کنند. این فرآیند به گره‌های موجود در شبکه اجازه می‌دهد تا از یک نسخه مشترک و به‌روز بلاکچین استفاده کنند. این امر باعث شفافیت شبکه و همچنین غیرمتمرکز بودن آن می‌شود.

۱-۱-۳ مزایای بلاکچین

بلاکچین به عنوان یک فناوری نوآورانه دارای مزایا و کاربردهای فراوانی است که بهبودهای قابل توجهی در مقایسه با سیستم‌های سنتی ارائه می‌دهد. در این بخش، برخی از مهم‌ترین مزایای بلاکچین شرح داده می‌شوند.

توزیع شدگی

بلاکچین به صورت توزیع شده عمل می‌کند، به این معنا که داده‌ها در شبکه‌ای از گره‌ها ذخیره می‌شوند و هیچ نقطه متمرکزی برای حمله وجود ندارد. این ویژگی باعث افزایش مقاومت شبکه در برابر حملات سایبری و کاهش خطر از دست رفتن داده‌ها می‌شود.

شفافیت

یکی از ویژگی‌های بارز بلاکچین، شفافیت آن است. تمامی تراکنش‌ها در بلاکچین عمومی هستند و هر کسی می‌تواند آنها را مشاهده کند. این شفافیت موجب افزایش اعتماد کاربران و کاهش احتمال تقلب می‌شود. هرچند که امروزه سیستم‌های خصوصی مبتنی بر بلاکچین نیز در حال گسترش و تولید اند.

تغییرناپذیری

تراکنش‌های ذخیره شده در بلاکچین قابل تغییر یا حذف نیستند. هر بلاک شامل هش بلاک قبلی است و این اتصال به زنجیره‌ای از بلاک‌ها منجر به تغییرناپذیری داده‌ها می‌شود. این ویژگی، از تغییرات غیرمجاز و دستکاری در داده‌ها جلوگیری می‌کند.

امنیت

بلاکچین از الگوریتم‌های رمزنگاری پیچیده برای ایجاد هش استفاده می‌کند که امنیت داده‌ها را تضمین می‌کند. هر تراکنش و بلاک توسط الگوریتم‌های رمزنگاری محافظت می‌شوند و این امر مانع از دسترسی غیرمجاز و هک شدن داده‌ها می‌شود.

۱-۲ مقدمه‌ای بر شبکه‌های پیچیده

شبکه‌های پیچیده، به عنوان یک زیرشاخه مهم در علم شبکه‌ها، ساختارها و رفتارهای پیچیده‌ای را مدل‌سازی و بررسی می‌کنند. به دلیل پیچیدگی بالای موجود در اینگونه شبکه‌ها، تحلیل و مطالعه خواصشان نیازمند روش‌ها و تکنیک‌های منحصربه‌فرد می‌باشد. این شبکه‌ها معمولاً از عناصر متعدد و پیچیده‌ای مانند گره‌ها (نقاط) و پیوندها (لبه‌ها) تشکیل شده‌اند که با هم به شکل‌دهی ساختارهای غیرمنظم و پویایی منجر می‌شوند. این ساختار پیچیده با استفاده از گراف‌ها مدل می‌شود. از این رو تئوری گراف و بررسی ساختار شبکه‌های پیچیده، بسیار شباهت دارند.

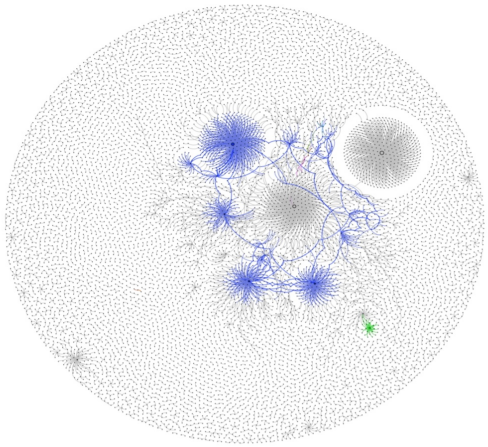
شبکه‌های پیچیده در زندگی مدرن امروزی نقش مهمی ایفا می‌کنند. همچنین شاهد حضور پررنگ شبکه‌های پیچیده در زندگی روزمره انسان هستیم. یکی از این شبکه‌های پیچیده؛ شبکه تراکنش‌های بیت‌کوین، به عنوان یک رمزارز مورد استفاده توسط مردم می‌باشد.

۱-۲-۱ ویژگی‌های شبکه‌های پیچیده

برای بررسی و آشنایی با شبکه‌های پیچیده، نیازمند شناخت ویژگی‌ها و خصوصیات اینگونه شبکه‌ها می‌باشیم.

در ادامه به بررسی اجمالی ویژگی‌های یک شبکه پیچیده می‌پردازیم.

- **تعداد زیاد گره‌ها و پیوندها:** شبکه‌های پیچیده معمولاً شامل تعداد زیادی گره و پیوند هستند. به عنوان مثال، در شبکه‌های اجتماعی، گره‌ها نماینده افراد و پیوندها نماینده روابط اجتماعی بین آن‌ها هستند و یا در شبکه پیچیده بیت‌کوین، آدرس‌های تراکنش نماینده گره‌ها و تراکنش انجام شده میان آدرس مبدا و آدرس مقصد نمایانگر پیوند جهت‌دار و وزن‌دار میان دو گره می‌باشد.
- **ساختار غیرمنظم:** شبکه‌های پیچیده دارای ساختاری غیرمنظم و پیچیده هستند. این ساختار به دلیل تعداد بالای پیوندها و پویایی شبکه، به صورت مرتب و منظم نیست. به عبارت دیگر، الگوی خاصی برای چگونگی اتصال گره‌ها به یکدیگر وجود ندارد و شبکه‌ها به صورت تصادفی و پویا تغییر می‌کنند.
- **همبستگی و ساختارهای سلسله‌مراتبی:** شبکه‌های پیچیده ممکن است دارای همبستگی‌ها و ساختارهای سلسله‌مراتبی باشند. این به این معناست که برخی از گره‌ها به عنوان گره‌های اصلی یا مرکزی عمل می‌کنند و بسیاری از گره‌های دیگر به این گره‌های مرکزی متصل می‌شوند.



شکل ۱-۲: نمایی از شبکه تراکنش بیت‌کوین با ۱۰،۰۰۰ گره منتخب [۱]

۱-۳ ساختار شبکه بیت‌کوین[1]

این مقاله به بررسی تراکنش‌های بیت‌کوین پرداخته است که در آن، هر تراکنش می‌تواند چندین آدرس ورودی و چندین آدرس خروجی داشته باشد. به عنوان مثال، یک تراکنش از x آدرس ورودی و y آدرس خروجی استخراج می‌شود و به صورت $x \times y$ نمایش داده می‌شود. سپس، هر گره نماینده یک آدرس بیت‌کوین خواهد بود، همچنین هر لبه جهت‌دار نشان‌دهنده جهت انجام آن تراکنش است و وزن لبه متناسب با ارزش تراکنش مشخص می‌شود.

مقاله یک شبکه تراکنش بیت‌کوین را به یک گراف جهت‌دار وزنی تبدیل می‌کند که با $G = (V, E, W)$ نشان داده می‌شود، جایی که V مجموعه گره‌ها، E مجموعه لبه‌ها و W مجموعه وزن‌ها است. هر لبه به صورت $e_{ij} = (i, j, w_{ij})$ نمایش داده می‌شود. مجموعه E با N گره می‌تواند به صورت یک ماتریس $N \times N$ نمایش داده شود که اساساً یک ماتریس مجاورت است و با A نشان داده می‌شود. برای هر عنصر a_{ij} در A، داریم:

$$a_{ij} = \begin{cases} w_{ij} & \text{اگر } e_{ij} \text{ تعریف شده باشد} \\ 0 & \text{در غیر این صورت} \end{cases}$$

[1] Bitcoin Network Construction

داده‌های مورد استفاده در این مقاله؛ از تراکنش‌ها و آدرس تراکنش‌های موجود در پایگاه داده پروژه بیت‌کوین، از ژانویه ۲۰۱۷ تا ژانویه ۲۰۱۸ بدست آمده اند که شامل بیش از ۱۴۸،۰۰۰،۰۰۰ گره و ۸۷۰،۰۰۰،۰۰۰ لبه می‌باشند. شکل ۱-۲ نمایی از شبکه تراکنش بیت‌کوین با ۱۰،۰۰۰ گره منتخب را نشان می‌دهد.

۱-۴ نمونه‌برداری از شبکه بیت‌کوین

شبکه تراکنش بیت‌کوین یک گراف بسیار بزرگ با میلیون‌ها گره است، بنابراین لازم است که یک شبکه نمونه، نماینده، برای ساده‌سازی تحلیل‌ها بدست آوریم. برخی از مطالعات قبلی نشان داده‌اند که روش‌های نمونه‌برداری مبتنی بر پیاده‌روی تصادفی[1] می‌توانند خواص ساختاری شبکه بلاکچین مقیاس آزاد[2] را به خوبی حفظ کنند. بنابراین، در این مقاله نیز یک روش نمونه‌برداری گراف، مبتنی بر پیاده‌روی تصادفی، برای نمایندگی شبکه بلاکچین بیت‌کوین طراحی معرفی می‌گردد.

۱-۴-۱ روش نمونه برداری RWFB

در روش‌های سنتی پیاده‌روی تصادفی، گره بعدی j به صورت تصادفی از همسایگان گره فعلی i انتخاب می‌شود. با این حال، این روش‌ها نمی‌توانند به دقت شبکه بیت‌کوین را نمونه‌برداری کنند. برای رفع این مشکل، روش ابداعی با نام پیاده روی تصادفی با بازگشت به عقب طراحی و معرفی می‌گردد.

به طور خاص، پیاده روی تصادفی با بازگشت به عقب هنگام نمونه‌برداری از شبکه، احتمال بازگشت به گره فعلی را نیز در نظر می‌گیرد. در هر گام از پیاده‌روی تصادفی جهت‌دار، RWFB با احتمال بازگشت p به گره فعلی یعنی i بازمی‌گردد؛ و با احتمال $1-p$ یک همسایه تصادفی از میان k_i همسایه‌های خود را انتخاب می‌کند، بنابراین هر کدام دارای احتمالی برابر با $(1-p)/k_i$ هستند. احتمال RWFB را که با P_{RWFB_i} نشان داده می‌شود، به صورت زیر تعریف می‌کنیم:

$$P_{RWFB_i} = \begin{cases} p & \text{بازگشت به گره } i \\ \frac{1-p}{k_i} & \text{انتقال به همسایه } j \text{ از گره } i \end{cases}$$

پیاده‌روی همیشه از یک گره تصادفی شروع می‌شود. علاوه بر این، اگر در طول پیاده‌روی به بن‌بست برخورد کند، یک گره تصادفی دیگر برای ادامه انتخاب می‌شود تا زمانی که اندازه نمونه‌برداری به مقدار دلخواه و موردنیازمان برسد.

[1] Random Walk(RW)
[2] Scale-Free

Sampling Method	Degree	Clustering	Betweenness	Closeness	Average
RWFB	0.120	0.045	0.091	0.429	**0.171**
RWS	0.293	0.046	0.536	0.618	0.373
RN	0.895	0.053	0.151	0.433	0.383
RE	0.275	1.000	0.067	0.549	0.473
FF	0.187	1.000	0.075	0.669	0.483
SB	0.409	0.025	0.583	0.645	0.415

جدول ۱-۱: مقایسه روش‌های نمونه‌برداری با استفاده از K-S D-statistic

حال پس از اتمام نمونه‌برداری نیاز به تعریف گراف جدید داریم. گراف نمونه‌برداری شده با تابع بازگشت را به عنوان $G_{RWFB} = (V_i, E_{i,j}, w_{i,j})$ دوباره تعریف می‌کنیم. در این گراف جهت‌دار و وزن‌دار، گره‌ها همان رئوس پیموده شده هستند و لبه‌ها همان گام‌هایی اند که پیموده ایم.

۱-۴-۲ ارزیابی روش نمونه‌برداری RWFB

جدول ۱-۱، مقایسه روش‌های نمونه‌برداری با استفاده از آماره K-S D-statistic را نشان می‌دهد. این آماره مشخص می‌کند که ورودی هایش در معیارهای مختلف چه‌قدر متفاوت اند. هرچه تفاوت دو ورودی اش، که گراف نیز می‌باشند، بیشتر باشد عدد حاصل به یک نزدیکتر است. هرچه عدد حاصل به صفر نزدیکتر باشد یعنی تفاوت میان گراف نمونه[۱] و گراف اصلی[۲] کمتر بوده است.

مطابق با جدول ۱-۱ می‌توان نتیجه گرفت؛ روش ابداعی عملکرد بهتری را نسبت به سایر روش‌های سنتی داشته است، گراف اصلی را بهتر نمونه‌برداری کرده و دارای خواص نسبتا مشابه با آن می‌باشد.

[1] $G_{RWFB} = (V_i, E_{i,j}, w_{i,j})$
[2] $G = (V, E, W)$

فصل دوم

تحلیل شبکه‌های پیچیده

۲-۱ توزیع درجه[1]

بررسی توزیع درجه گره‌ها در شبکه بیت‌کوین بسیار حائز اهمیت است. درجه یک گره که با k نشان داده می‌شود، تعداد یال‌های مجاور آن گره را مشخص می‌کند. در شبکه تراکنش‌های بیت‌کوین، درجه k برای هر آدرس بیت‌کوین با مجموع تعداد تراکنش‌ها محاسبه می‌شود. تعداد تراکنش‌های ورودی (دریافت بیت‌کوین) به عنوان درجه ورودی و تعداد تراکنش‌های خروجی (پرداخت بیت‌کوین) به عنوان درجه خروجی شناخته می‌شود. توزیع درجه که با $P(k)$ نشان داده می‌شود، احتمال این است که یک گره انتخابی به صورت تصادفی دارای درجه برابر با k باشد. اگر درجه k از قانون توان تبعیت کند، آنگاه $P(k) \propto k^{-\alpha}$ است، که α پارامتر مقیاس توزیع قانون توان است.

نتایج نشان می‌دهند که تمامی توزیع‌های درجه از قانون توان با دنباله‌های سنگین تبعیت می‌کنند. این نشان می‌دهد که شبکه بیت‌کوین یک شبکه مقیاس آزاد است که در آن تنها تعداد کمی از گره‌ها دارای تعداد زیادی اتصالات هستند در حالی که بیشتر گره‌ها دارای درجه‌های کم و اتصالات کمتری هستند. این یافته‌ها با نتایج تحقیقاتی که با داده‌های واقعی شبکه به دست آمده‌اند، سازگار است.

[1] Degree distribution

۲-۲ ضریب خوشه‌بندی و طول کوتاه‌ترین مسیر[1]

ضریب خوشه‌بندی و طول کوتاه‌ترین مسیر می‌توانند شبکه را از دیدگاه هندسی مورد ارزیابی قرار دهند. ضریب خوشه‌بندی متوسط شبکه با C نشان داده می‌شود که به صورت زیر تعریف می‌شود:

$$C = \frac{1}{N} \sum_{i \in V(G)} \frac{\Delta_i}{k_i(k_i-1)/2},$$

که در آن N تعداد گره‌ها، Δ_i تعداد مثلث‌های کامل و k_i درجه گره i را نشان می‌دهند.

از سوی دیگر، طول متوسط کوتاه‌ترین مسیر با L نشان داده می‌شود که به صورت زیر تعریف می‌شود:

$$L = \sum_{i,j \in V(G)} \frac{l(i,j)}{N(N-1)},$$

که در آن $V(G)$ مجموعه گره‌های گراف G و $l(i,j)$ طول کوتاه‌ترین مسیر بین i و j است. برای گراف تراکنش بیت‌کوین، ضریب خوشه‌بندی $C_{Bitcoin} = 0.0071$ و طول کوتاه‌ترین مسیر $L_{Bitcoin} = 3.833$ می‌باشد که نشان‌دهنده تعداد زیاد تراکنش‌های غیرمستقیم است.

۲-۲-۱ اثر جهان کوچک در شبکه بیت‌کوین[2]

اثر جهان کوچک یک ویژگی در شبکه‌های پیچیده است که نشان می‌دهد چگونه هر دو گره در یک شبکه بزرگ می‌توانند با تعداد کمی یال به یکدیگر متصل شوند. دو ویژگی اصلی شبکه‌های جهان کوچک عبارتند از:

- **ضریب خوشه‌بندی بالا:** ضریب خوشه‌بندی نشان می‌دهد که چقدر احتمال دارد که دو گره همسایه یک گره دیگر نیز با هم متصل باشند. ضریب خوشه‌بندی بالا نشان‌دهنده وجود خوشه‌های محکم از گره‌ها است.
- **میانگین طول کوتاه‌ترین مسیر کم:** این ویژگی نشان می‌دهد که به طور میانگین، چند یال باید طی شود تا از یک گره به هر گره دیگر در شبکه رسید. در شبکه‌های جهان کوچک، این میانگین طول کوتاه است.

در شبکه بیت‌کوین، ضریب خوشه‌بندی و طول کوتاه‌ترین مسیر به صورت زیر محاسبه شده است:

$$L_{\text{Bitcoin}} = 3.833 \quad \text{و} \quad C_{\text{Bitcoin}} = 0.0071$$

[1] Clustering coefficient and the shortest-path length
[2] Small-world effect

این مقادیر نشان‌دهنده این است که شبکه بیت‌کوین دارای خوشه‌های محکم از گره‌ها و همچنین مسیرهای کوتاه بین گره‌ها است. بنابراین در شبکه پیچیده بیت‌کوین شاهد اثر جهان کوچک می‌باشیم. این اثر به این معناست که توکن‌های بیت‌کوین[۱] می‌توانند در چند مرحله به اکثر گره‌ها منتقل شوند.

۲-۳ مولفه‌های متصل[۲]

با توجه به اینکه شبکه بلاکچین بیت‌کوین یک شبکه جهان کوچک است، تحلیل اتصال‌پذیری آن اهمیت زیادی دارد. در یک شبکه پیچیده، اگر هر جفت گره در یک زیرگراف حداقل یک مسیر متصل داشته باشد، آن زیرگراف را یک مولفه متصل می‌نامیم. در شبکه‌های جهت‌دار، مولفه‌های قویاً متصل[۳] به زیرگراف‌هایی اشاره دارد که هر جفت گره (i, j) دارای مسیری جهت‌دار از i به j و از j به i به‌طور همزمان هستند. به‌طور مشابه، مولفه‌های ضعیفاً متصل[۴] به مولفه‌های متصل بدون جهت اشاره دارد.

نتایج حاصل از این تحلیل نشان می‌دهند که گراف شبکه پیچیده بیت‌کوین یک گراف نسبتا متصل است. همچنین احتمالاً گره‌های رابط، تعداد بسیاری از گره‌های جدا شده و منفرد را به شبکه متصل می‌کنند. در واقعیت، چنین گره‌های رابطی ممکن است صرافی‌ها، موسسات تجاری یا سازمان‌های مالی باشند. همچنین می‌توان نتیجه گرفت که بسیاری از تراکنش‌ها در این گراف تنها یک‌طرفه هستند. به عبارت دیگر، اکثر گره‌ها به‌طور مکرر تراکنش‌های دوطرفه (ورودی و خروجی) انجام نمی‌دهند و فقط بیت‌کوین پرداخت می‌کنند یا دریافت می‌کنند.

۲-۴ مرکزیّت[۵]

تحلیل مولفه‌های متصل باعث شد به وجود گره‌های رابط پی ببریم. برای تأیید این فرضیه، مرکزیّت شبکه را تحلیل می‌کنیم.

---

[1] Bitcoin tokens
[2] Connected component
[3] Strongly Connected Component(SCC)
[4] Weakly Connected Component(WCC)
[5] Centrality

۲-۴-۱ مرکزیّت شبکه

مرکزیّت شبکه مفهومی است که برای اندازه‌گیری اهمیت نسبی گره‌ها در یک شبکه استفاده می‌شود. این مفهوم به ما کمک می‌کند تا بفهمیم کدام گره‌ها نقش کلیدی‌تری در ساختار شبکه ایفا می‌کنند. در ادامه به بررسی چند نوع مرکزیّت در شبکه‌های پیچیده می‌پردازیم.

مرکزیّت نزدیکی[1]

مرکزیّت نزدیکی معیاری است که نشان می‌دهد یک گره چقدر به سایر گره‌های شبکه نزدیک است. این معیار بر اساس طول کوتاه‌ترین مسیرها از یک گره به سایر گره‌ها محاسبه می‌شود. فرمول مرکزیّت نزدیکی یک گره i به صورت زیر است:

$$O(i) = \frac{n-1}{\sum_{j=1}^{n-1} d(i,j)}$$

که در آن n تعداد گره‌های قابل دسترس گره i و $d(j,i)$ فاصله کوتاه‌ترین مسیر بین گره j و گره i است. این معیار نشان می‌دهد که یک گره چقدر سریع می‌تواند به سایر گره‌ها دسترسی پیدا کند.

مرکزیّت بینابینی[2]

مرکزیّت بینابینی نشان می‌دهد که یک گره چقدر در مسیرهای کوتاه بین سایر گره‌ها قرار دارد. این معیار نشان می‌دهد که یک گره چقدر در انتقال اطلاعات بین سایر گره‌ها نقش دارد. فرمول مرکزیّت بینابینی یک گره i به صورت زیر است:

$$B(i) = \sum_{u,v \in V} \frac{\sigma(u,v|i)}{\sigma(u,v)}$$

که در آن $\sigma(u,v)$ تعداد کل مسیرهای کوتاه بین گره‌های u و v و $\sigma(u,v|i)$ تعداد مسیرهایی است که از گره i عبور می‌کنند. این معیار نشان می‌دهد که یک گره چقدر در اتصال سایر گره‌ها به هم نقش دارد.

مطابق با یافته‌های این مقاله، مرکزیّت بینابینی با افزایش درجه گره افزایش می‌یابد. اگر تعداد زیادی از گره‌ها دارای مقادیر بالای بینابینی باشند، تعداد زیادی از گره‌های رابط در گراف ظاهر می‌شوند که باعث شکنندگی گراف می‌شود. این نتایج نشان می‌دهد که تعداد زیادی از گره‌های رابط در شبکه بیت‌کوین وجود ندارد و این شبکه در مقابل حذف گره‌ها مقاوم است. بیشتر گره‌ها دارای مقادیر نسبتاً کم نزدیکی و بینابینی هستند که نشان می‌دهد تعداد کمی گره‌های مرکزی وجود دارند. بنابراین، ما یک

[1] Closeness centrality
[2] Betweenness centrality

گراف چندمرکزی مشاهده می‌کنیم که در آن برخی از گره‌های مرکزی مستقیماً با تعداد زیادی از گره‌ها بدون واسطه متصل هستند. دلیل چندمرکزی و مقاومت عالی را می‌توان به توزیع ناهمگن گره‌ها نسبت داد که در بخش‌های بعدی مورد بررسی قرار می‌گیرد.

۲-۵ عدم تناسب[1]

در این تحلیل تمایلات اتصالات شبکه بیت‌کوین مورد بررسی قرار گرفته است. محققان از ضریب همبستگی پیرسون[2] با نماد ρ برای مشخص کردن تناسب شبکه استفاده کرده‌اند.

نتیجه به‌دست آمده برای ضریب همبستگی پیرسون $\rho = -0.023$ بوده که نشان‌دهنده این است که شبکه دارای خاصیت عدم تناسب است. مطالعات قبلی بر روی ساختار شبکه بیت‌کوین نیز این موضوع را تایید می‌کنند.

درنهایت می‌توان نتیجه گرفت که گره‌های با درجه بالا ترجیح می‌دهند به گره‌های با درجه کمتر متصل شوند، درحالی‌که گره‌های با درجه پایین نیز ترجیح دارند به گره‌های با درجه بالاتر متصل شوند. به عنوان مثال، گره‌های تازه وارد ترجیح می‌دهند با گره‌های درجه بالا (که احتمالا صرافی ها و غیره می‌باشند) متصل شوند.

۲-۶ ضریب باشگاه ثروت‌مندان

تنها پایه به طوری که گره‌های پایین درجه به گره‌های درجه بالا وصل می‌شوند. در همین حال، از نیازمندی به بررسی اتصالات بین گره‌های درجه بالا نیز خبره می‌دهد. در یک شبکه پیچیده، باشگاه ثروتمند به پدیده اتصال فشرده بین گره‌های درجه بالا اطلاق می‌شود. به عبارت دیگر، گره‌های با درجه بالاتر به عنوان گره‌های ثروتمند شناخته می‌شوند که با احتمال بیشتری به باشگاه‌ها (یعنی زیرگراف‌ها) جمع می‌شوند در مقایسه با آن گره‌هایی که دارای یال کمتری هستند.

ضریب باشگاه ثروتمند با $\phi(k)$ نشان داده می‌شود و به صورت زیر تعریف می‌شود [؟]:

$$\phi(k) = \frac{2E > k}{N > k(N > k-1)}, \qquad (۱-۲)$$

که در آن $N > k$ تعداد کل گره‌هایی است که درجه آن‌ها بیشتر از k است و $E > k$ تعداد یال‌های بین گره‌های $N > k$ است. $N > k(N > k-1)/2$ حداکثر یال‌های ممکن بین تمام گره‌های $N > k$ است.

[1] Disassortativity
[2] Pearson correlation coefficient

نمودار شکل **؟؟** نتایج را نشان می‌دهد. از شکل **؟؟**(a) می‌بینیم که ضریب باشگاه ثروت‌مند با افزایش k به طور یکنواخت افزایش نمی‌یابد، که نشان‌دهنده عدم پدیده واضح باشگاه ثروت‌مند است. برای ارزیابی دقیق‌تر، از ضریب باشگاه ثروت‌مند نرمال‌شده $\phi_{\text{norm}}(k)$ استفاده می‌کنیم که به صورت زیر تعریف می‌شود [؟]:

$$\phi_{\text{norm}}(k) = \frac{\phi(k)}{\phi_{\text{rand}}(k)}, \tag{۲-۲}$$

که در آن $\phi_{\text{rand}}(k)$ ضریب باشگاه ثروت‌مند شبکه تصادفی با توزیع درجه مشابه است. نمودار شکل **؟؟**(b) نتایج را نشان می‌دهد، و چیدمان واقعی باشگاه ثروت‌مند به وابستگی $\phi_{\text{norm}}(k) > 1$ است. نتایج نشان می‌دهد که در اکثر ارزش‌های k، چیدمان باشگاه ثروت‌مند وجود ندارد.

در کل، شبکه بیت‌کوین پدیده عدم وجود باشگاه ثروت‌مند را از خود نشان می‌دهد، که نشان‌دهنده آن است که گره‌های مرکزی با درجه بالا در این شبکه تمایل به اتصال با یکدیگر ندارند و در زیرگراف‌های متصل مختلف پخش می‌شوند. این اثر می‌تواند توسط واقعیت توضیح داده شود که گره‌های مرکزی احتمالاً تبادلات متداولی را انجام می‌دهند. در نتیجه، گره‌های ثروتمند در شبکه بیت‌کوین به طور مستقیم با یکدیگر ارتباط ندارند.

پیوست اول

روش K-S D-statistic

یکی از روش‌های گسسته‌سازی یک سیستم زمان‌پیوسته روش تبدیل دوخطی است. این روش که به روش توستین[1] نیز معروف است، یک روش انتگرال‌گیری عددی به کمک تقریب ذوزنقه‌ای است. سیستمی با ورودی $u(t)$، خروجی $y(t)$ و تابع تبدیل $\frac{1}{s}$ در نظر بگیرید. رابطه

$$y(t) = \int_{-\infty}^{t} u(\tau)d\tau \qquad (آ-۱)$$

بین ورودی و خروجی سیستم برقرار است. با گسسته‌سازی آ-۱ به رابطه

$$y[(k+1)h] = y(kh) + \int_{kh}^{(k+1)h} u(\tau)d\tau \qquad (آ-۲)$$

می‌رسیم. اگر از تقریب ذوزنقه‌ای برای محاسبه انتگرال استفاده کنیم، آ-۲ به صورت

$$y[(k+1)h] \simeq y(kh) + \frac{h}{2}\left(u(kh) + u[(k+1)h]\right) \qquad (آ-۳)$$

در می‌آید. از رابطه تقریبی آ-۳ می‌توان برای تبدیل یک سیستم زمان‌پیوسته به یک سیستم زمان‌گسسته استفاده کرد.

[1] Tustin

سیستم زمان‌پیوسته خطی و تغییرناپذیر با زمان $G = (A, B, C, D)$ را در نظر بگیرید. اگر این سیستم را با دوره تناوب h گسسته‌سازی کنیم، مدل فضای حالت $G_d = (A_d, B_d, C_d, D_d)$ به دست می‌آید که در آن

$$A_d = (I - \frac{h}{2}A)^{-1}(I + \frac{h}{2}A)$$

$$B_d = \frac{h}{2}(I - \frac{h}{2}A)^{-1}B)$$

$$C_d = C(I + A_d)$$

$$D_d = D + CB_d$$

است.

مراجع

[1] B. Tao, H. -N. Dai, J. Wu, I. W. -H. Ho, Z. Zheng and C. F. Cheang, ”Complex Network Analysis of the Bitcoin Transaction Network,” in IEEE Transactions on Circuits and Systems II: Express Briefs., vol. 69, no. 3, pp. 1009-1013, March. 2022

[2] S. Nakamoto, “Bitcoin: a Peer-to-Peer Electronic Cash System,” Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, ”An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564.

Complex Network Analysis of the Bitcoin Transaction Network

Masih Tanoursaz
m.tanoursaz@ec.iut.ac.ir

June 15, 2024

Department of Electrical and Computer Engineering
Isfahan University of Technology, Isfahan 84156-83111, Iran
Degree: B.Sc. Language: Farsi

Supervisor: Prof. Bahram Borzou (bahram.borzou@cc.iut.ac.ir)

Abstract

In most applications, because of numerous advantages it offers, digital technology (computer, PLC, microcontroller etc.) is used to control industrial plants. These types of systems, where the process under control is continuous-time but the controller is digitally implemented, are called sampled-data systems. Faults can occur in sampled-data systems like any other control system. In order to prevent performance degradation, physical damage or failure, faults should be promptly detected. In this thesis fault diagnosis in sampled-data systems is studied. The sampled-data design can be carried out using direct or indirect design approaches. Direct design, emphasized in this research, does not involve any approximations.

Normally, to design a robust fault detection and isolation (FDI) scheme, a performance index which is a measure of the sensitivity of the FDI to faults and its robustness to unknown inputs and disturbances is defined and optimized. Different performance indices based on norms are considered. Using the direct design approach and the so-called norm invariant transformation, it is shown that a sampled-data FDI problem can be converted to an equivalent discrete-time problem. This will form the foundation of a unifying framework for optimal sampled-data residual generator design.

Multirate systems are also abundant in industry. Here, several methods of residual generation based on multirate sampled data are developed. The key feature of such residual generators is that they operate at a fast rate for prompt fault detection. The lifting technique is used to convert the multirate problem into an equivalent single-rate discrete-time problem with causality constraints.

It is generally believed that the optimal multirate design performs better than the optimal slow-rate and worse than the optimal fast-rate designs. This conjecture is theoretically proved in this thesis for general multirate control systems with norms of the closed-loop system as performance indices. However, it is shown that the common performance indices in FDI design do not satisfy this property. To resolve this, an alternative performance index is defined after formulating the FDI problem as a standard control problem.

Key Words: Fault Detection, Wind Turbine Control, Fault Accomodation, Unknown Input Observers

Isfahan University of Technology

Department of Electrical and Computer Engineering

Increasing Efficiency in Low-Efficiency Systems

A Thesis

Submitted in partial fulfillment of the requirements

for the degree of Master of Science

by

Azin Azadeh

Evaluated and Approved by the Thesis Committee, on March 21, 2015

1. Bahram Borzou, Prof. (Supervisor)
2. Poorya Parniani, Assoc. Prof. (Advisor)
3. Tahamtan Trabi, Prof. (Examiner)
4. Soraya Sanaei, Assist. Prof (Examiner)

Jamshid Jahangir, Department Graduate Coordinator