بسم الله الرحمن الرحیم

دانشکده مهندسی برق

درس مبانی بلاک چین و رمز ارزها

استاد مربوطه : دکتر مداح علی

گزارش مقاله " Payment Networks as Creation Game "

تهیه کننده : علیرضا شیرزاد

شماره دانشجویی : 95101847

بهمن 1398

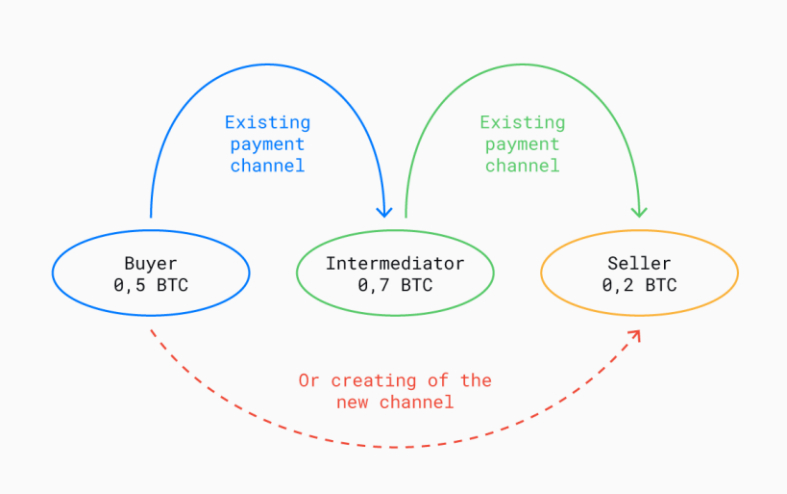
طرح مسئله :

همانگونه که در درس مطرح شد، یکی از مسائل مهم شبکه های Blockchain بحث Scalability و تعداد transactionها بر ثانیه است. مشاهده کردیم که یکی از راه حل های هوشمندانه، راه حل Lightning Network است. در این شبکه بین دو کاربر Channel هایی ساخته می شود که میتواند یک طرفه یا دو طرفه باشد. در این Channel مقداری پول به تعبیری سپرده می شود که از آن با نام Capital یاد می شود. با معماری Channel-Based امکان این فراهم می شود که اکثر تراکنش ها (که micropayment هستند) به صورت Off-Chain انجام بشوند بدین صورت که تنها یک تراکنش برای Channel Opening و یک تراکنش برای Channel Closing که تنها توزیع Capital را نشان می دهد روی Blockchain بنشیند و دیگر تراکنش ها به صورت خصوصی و Off-Chain بین دو node انجام بگیرد. از دیگر مزایای این شبکه توسعه ی Payment Channel Network(PCN) هاست. بدین صورت که در برای انتقال پولی به یک node در شبکه از Channel های موجود در شبکه استفاده بکنیم.

یکی از چالش های مهم برای node های موجود در این شبکه انتخاب راهی برای انتقال پول است که کمترین هزینه را برای Fee داشته باشد. هر سازنده ی Transaction دو انتخاب دارد:

- انتخاب مسیری در PCN و انتقال پول از طریق node های میانی
- ایجاد یک transaction یا باز کردن یک Channel به صورت مستقیم و On-Chain

هر کدام از انتخاب های بالا هزینه ای دارد که هر node با توجه به آن بهترین انتخاب را انجام می دهد. هزینه ی انتخاب اول transaction fee های متعددی است که باید برای Node های میانی پرداخت شود اما هزینه ی انتخاب دوم پرداخت یک transaction fee به مراتب بزرگ تر برای ثبت Transaction به صورت On-Chain است. در شکل1 نمای کلی این انتخاب به تصویر در آمده است.



شکل 1

در حالت کلی در هر transaction تعدادی node میانی مقداری fee را تصاحب میکنند و Node ابتدایی این Fee را از دست می دهد. پس سئوال اساسی اینجاست که هر Node با ورود به شبکه با چه node های دیگری Channel بسازد تا Cost Function خود را کمینه بسازد؟

در این مقاله مسئله ی ایجاد Channel ها با ادبیات Game Theory مدل شده و سعی شده که راه حلی برای این چالش ارائه شود که در ادامه میبینیم.

تعریف دقیق مسئله :

در این مقاله ابتدا کل مسئله ی ایجاد Channel ها به صورت یک Game مدل شده است. در این تعریف نویسنده تعدادی تعریف در نظر گرفته شده که باید به آن توجه داشت:

- استراتژی هر شرکت کننده به صورت مجموعه ی S_u در نظر گرفته شده که شامل Channel ها (و بالطبع transactionهای on-chain) است آن Node ایجاد می کند.
- هر Node از استراتژی همگان آگاه است و تمام استراتژ های قبل از issue شدن هر گونه transaction نهایی می شوند. در واقع هر Node از S^N آگاه است که ضرب دکارتی تمام S_u هاست و شامل تمام Channel های PCN است.
- مقدار fee برای تمام مسیرها یکسان و برابر f_0 است.
- هر Node برای تمام Node های دیگر kبار Transaction تولید میکند.

معیار این مقاله برای پایداری یک شبکه از دید Game Theory، تعادل نَش یا Nash equilibrium است. در ادامه به تعریف دقیق Nash Equilibrium می پردازیم:

تعادل نَش (Nash Equilibrium): در تئوری بازیها، تعادل نش (به نام جان فوربز نش، که آن را پیشنهاد کرد) راه حلی از تئوری بازی است که شامل دو یا چند بازیکن، که در آن فرض بر آگاهی هر بازیکن به استراتژی تعادل بازیکنان دیگر است و بدون هیچ بازیکنی که فقط برای کسب سود خودش با تغییر استراتژی یک جانبه عمل کند. اگر هر بازیکنی استراتژی را انتخاب کند هیچ بازیکنی نمی‌تواند با تغییر استراتژی خود در حالی که نفع بازیکن دیگر را بدون تغییر نگه داشته باشد عمل کند، سپس مجموعه انتخاب‌های استراتژی فعلی و بهره‌مندی مربوطه، تعادل نش را تشکیل می‌دهد. به بیان ساده، امی و فیل در تعادل نش است اگر امی در حال انجام بهترین تصمیم گیری که او می‌تواند با توجه به تصمیم‌گیری فیل داشته باشد و همچنین فیل بهترین تصمیمی که می‌تواند با توجه به تصمیم‌گیری امی داشته باشد. به همین ترتیب یک گروه از بازیکنان در تعادل نش است اگر هر یک در حال انجام بهترین تصمیم‌گیری باشند که آن‌ها

می‌تواند، با توجه به تصمیمات دیگران داشته باشند. با این حال، تعادلی که نش است لزوماً به معنای بهترین بهره‌وری کل برای همه بازیکنان مربوطه نمی‌باشد، در بسیاری از موارد ممکن است تمام بازیکنان بهره‌وری خود را بهبود بخشند در صورتی که چگونه بتوانند به توافق بر روی استراتژی‌های مختلف از تعادل نش برسند. (به عنوان نمونه، شرکت‌های تجاری رقابتی به منظور افزایش سود آن‌ها تشکیل کارتل می‌دهد). جنبه مهم تعادل نش این است که سود هر بازیکن نه تنها به استراتژی برگزیده خود بلکه به استراتژی برگزیده دیگر بازیکنان نیز ارتباط دارد.

حال سئوالی که این مقاله به آن حمله ور می شود این است که با چه توپولوژی ای از PCN و با چه مقادیری از fee شبکه ی ما به تعادل نَش می رسد. تابع هزینه های هر بازیکن شامل سه بخش است و تابعیت از استراتژی خود و دیگران دارد که به صورت زیر تعریف می شود:

$$c(\boldsymbol{\mu}, \mu_u) = \mu_u \cdot F_B + b_u \cdot F_B + \sum_{p \in \boldsymbol{P}: s(p) = u} f(x, p) - \sum_{p \in \boldsymbol{P}: u \in \boldsymbol{R}(x,p)} f_0$$

در عبارت بالا به تعریف چند نماد می پردازیم:

f_0 : مقدار fee پرداخت شده به صورت off-chain

μ_u : استراتژی بازیکن u

$\boldsymbol{\mu}$: استراتژی تمام بازیکنان

F_B : مقدار fee پرداخت شده به صورت on-chain

b_u : تعداد transaction های پرداخت شده به صورت on-chain

$\boldsymbol{P}$: مجموعه ی تمام transactionها

p : یک transaction به خصوص

$s(p)$: فرستنده ی *transaction*

همچنین با جمع تمام *cost* ها در شبکه ی PCN به مقدار social cost دست پیدا میکنیم که به صورت زیر تعریف می شود:

$$-W = \sum_{n \in \boldsymbol{N}} c(\boldsymbol{\mu}, \mu_u) = (\mu + b) \cdot F_B$$

طبق این گزاره برای کمینه کردن social cost باید تمام transaction ها را را off-chain انجام داد و از توپولوژی درختی برای PCN استفاده کرد. در این صورت داریم:

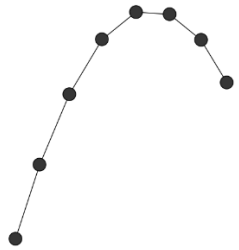
$$min(-W) = (N - 1) \cdot F_B$$

در ادامه مقاله به توپولوژی های مختلف شبکه ی PCN و استراتژی های مختلف برای ایجاد Payment Channel ها می پردازد و شروط برقراری تعادل نَش را در هر کدام از این ها بررسی میکند. به صورت به خصوص درباره توپولوژی های زیر شروط را تحقیق میکند:

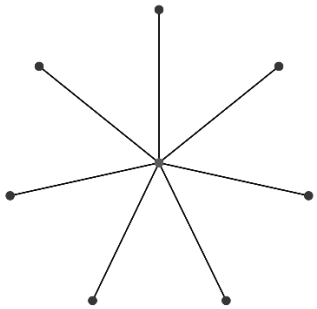
1) مسیر (path)
2) ستاره (star)
3) ستاره دو مرکزی (Star with two centers)
4) گراف کامل دو بخشی (Complete bipartite)
5) گروهک (Clique)

مسیر مقاله بسیار سرراست و دارای پترن خاصی است. در هر کدام از توپولوژی های بالا ابتدا مقدار social cost محسابه می شود. سپس روش های انحراف از استراتژی مطرح می شود و برای هر کدام شرط برقراری تعادل نَش بدست می آید. سپس در آخر اشتراک تمامی این شرط ها با هم گرفته می شود و به عنوان شرط نهایی تعادل نَش این توپولوژی اعلام می شود.

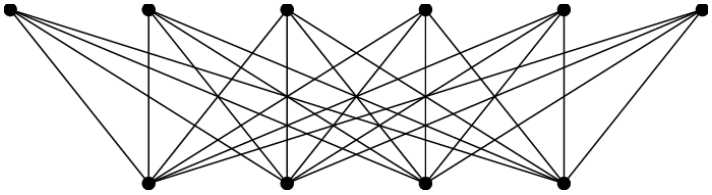
حال به طور خلاصه در جدول زیر به بررسی هر کدام از این توپولوژی ها می پردازیم:



شکل 2: گراف مسیر



شکل 3: گراف ستاره



شکل 4: گراف کامل دوبخشی

Topology	Conditions
Path	$f_0 = 0$
Star	$f_0 < \frac{F_B}{k} \cdot \frac{2}{N-1}$
Star (2 centers)	$\frac{F_B}{k} \cdot \frac{2}{N} < f_0 < \frac{F_B}{k} \cdot \frac{3}{N-1}$
Comp. Bipartite	$f_0 > \frac{F_B}{k} \cdot \frac{cN - c^2 - 2c}{N^2 - cN + N - 3c}$ $f_0 > \frac{F_B}{k} \cdot \frac{cN - c^2 - c}{N^2 - cN - N + c^2 - 2c}$ $f_0 < \frac{F_B}{k} \cdot \frac{c+1}{N-1}$
Clique	$f_0 > \frac{F_B}{k}$

همچنین در جدول زیر deviation های ممکن از استراتژی ها در هر Topology خلاصه شده است:

Topology	Deiviation
Path	first node can connect to a middle node on the path
Star	An outer node creates channels to $a \in [1; N - 2]$ other outer node
Star (2 centers)	A: A center node creates channels to $b \in [1; N - 3]$ outer nodes B: A center node creates channels to $b \in [0; N - 2]$ outer nodes and creates a channel to the other center node C: An outer node creates channels to $b\ 2$ $[1; N - 3]$ other outer nodes
Comp. Bipartite	A: A center node creates channels to only $b\ 2$ $[1; d - 1]$ outer nodes. B: A center node creates channels to $a \in [1; c - 1]$ center nodes and to $b = 0$ outer nodes. C: A center node creates channels to $a \in [1; c - 1]$ center nodes and to $b\ 2$ $[1; d]$ outer nodes D: An outer node creates channels to $b \in [1; d - 1]$ other outer nodes
Clique	A: The first node creates channels to only $a \in [1; N - 2]$ other nodes B: Node i (but not the first or last one) creates channels to only $a \in [0; N - i - 1]$ nodes from the set of nodes he would originally connect to (node $i + 1$ to node N)

پژوهش های مرتبط:

- ایده ی Payment Channel برای اولین بار در مقاله ی [1] مطرح شد. البته این طرح اولیه تنها Channel های یک طرفه بود که بین دو طرف بوجود می آید.
- سپس در مقالات زیادی ایده ی Channel های دوطرفه پیشنهاد شد [2,3,4,5].
- کنار هم گذاشتن تعداد زیادی از این Channel های دوطرفه ایده ی lightning network را در Bitcoin [3] و Raiden در Ethereum را پرورش داد. پژوهش انجام شده در این مقاله مستقل از نوع شبکه صورت گرفته و تنها به استراتژی ایجاد Channel می پردازد. لذا نتایج این مقاله می تواند در هر شبکه ای کاربرد داشته باشد.
- در [5] به این پرداخته شده که یک node مرکزی چگونه میتواند استراتژی ای انتخاب کند که برای آن optimum باشد. درواقع نگاه [5] یک نگاه بهینه سازی بود اما نگاه این مقاله به صورت تئوری بازی بود. اما با این همه تفاوت ها محصول نهایی مقاله ی [5] یک توپولوژِ ستاره بود که اتفاقا تعادل نَش را نیز به همراه داشت.
- ایده ی اولیه این مقاله در [7] آغاز شد. در این مقاله مدل سازی ایجاد شبکه با تئوری بازی برای سیستم ها توزیع شده انجام شد که نتایج آن برای رسیدن به تعادل نَش یک " درخت " بود که البته در [7] با آن مخالفت شد.

گسترش مقاله:

- در قدم اول باید قید ها و فرضیات بسیار سنگین و غیر واقعی این پژوهش از بین برود و مسئله با قیود آزادتری حل بشود. به عنوان مثال فرض استقلال fee از مقدار transact شده فرض بسیار بزرگی است که اکثر مواقع بر خلاف آن عمل می شود.
- در قدم بعدی به اعتقاد بنده باید شرطی روی درجه ی Connectivity گراف گذاشت تا از متمرکز شدن سیستم جلوگیری کرد. شبکه ی PCN نیز مانند شبکه ی اصلی (main chain) باید از خطر Centralization دور باشد تا از حملات احتمالی جلوگیری شود. با این منطق دیگر نباید توپولوژی ستاره و توپولوژی های شبیه به این را مطرح کرد.
- همچنین شبکه ی ما نباید از حالت همگن خارج بشود. یعنی تعدادی node هیچوقت موفق به دریافت fee نشوند و بعضی از node ها به عنوان گلوگاه شبکه مطرح بشوند که Fee های زیادی را برای خود کسب کنند. یکی از راه حل ها در شبکه های بلاکچین برای جلوگیری از این اتفاق، بوجود آمدن شبکه ی tangle است.
- یکی از مسیرهای گسترش این پژوهش، وارد کردن مدل های آماری برای مدل کردن محیط واقعی و Real time یک شبکه ی Blockchain است. در این پژوهش از ثابت k استفاده شده که نشان دهنده تعداد transaction های issue شده از سمت یک node به node دیگر است. اما در حالت واقعی باید بوجود آمدن transaction ها با فرآیند تصادفی Poisson مدل شود.

لیست مقالات مرتبط:

1. Spilman, Jeremy. "Anti dos for tx replacement." *2018-01-08]. https://lists. linuxfoundation. org/pipermail/bitcoin-dev/2013-April/002417. html* (2013).

2. Avarikioti, Georgia, Eleftherios Kokoris Kogias, and Roger Wattenhofer. "Brick: Asynchronous state channels." *arXiv preprint arXiv:1905.11360* (2019).

3. Decker, Christian, Rusty Russell, and Olaoluwa Osuntokun. "eltoo: A simple layer2 protocol for bitcoin." *White paper: https://blockstream. com/eltoo. pdf* (2018).

4. Decker, Christian, and Roger Wattenhofer. "A fast and scalable payment network with bitcoin duplex micropayment channels." *Symposium on Self-Stabilizing Systems*. Springer, Cham, 2015.

5. Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." (2016).

6. Valeriote, Frederick A., Thomas H. Corbett, and Laurence H. Baker, eds. *Cytotoxic Anticancer Drugs: Models and Concepts for Drug Discovery and Development: Proceedings of the Twenty-Second Annual Cancer Symposium Detroit, Michigan, USA—April 26–28, 1990*. Vol. 68. Springer Science & Business Media, 2012.

7. Albers, Susanne, et al. "On Nash equilibria for a network creation game." *ACM Transactions on Economics and Computation (TEAC)* 2.1 (2014): 1-27.