دانشگاه صنعتی شریف
دانشکده‌ی مهندسی برق

گزارش شماره دو پایان نامه ارشد برای طرح گرنت همراه اول
مهندسی برق

عنوان:

طراحی الگوریتم آنلاین برای مدیریت هزینه در شبکه کانال های پرداخت

نگارش:

مهسا باستان خواه

استاد راهنما:

دکتر محمد علی مداح علی

آبان ۱۴۰۱


بسم الله الرحمن الرحیم

چکیده

امروزه استفاده از شبکه کانال های پرداخت[۱] مبتنی بر بلاکچین به عنوان یکی از عملی ترین راه حل های مشکل عدم مقیاس پذیری بلاکچین بسیار مورد توجه قرار گرفته است. کاربران با استفاده از شبکه کانال های پرداخت برای تراکنش های روزمره،در عین اینکه از تمام تضمین های امنیتی و محرمانگی بلاکچین بهره مند میشوند، میتوانند از پرداخت کارمزد های سرسام آور بلاکچین خودداری کنند.

نحوه کار کانال پرداخت به صورت خلاصه به شرح زیر است. دو نفر برای ایجاد یک کانال پرداخت باید با فرستادن تراکنش مخصوصی به بلاکچین، مقداری سپرده برای کانال خود ذخیره کنند. بعد از ایجاد کانال دو نفر میتوانند تا سقف سپرده خود تراکنش برون بلاکچینی [۲] برای هم بفرستند و چون این تراکنش ها به صورت محلی[۳] و بدون مراجعه به بلاکچین انجام میشوند بسیار سریع هستند و کارمزد آن ها ناچیز است. در انتها وقتی طرفین تصمیم به بستن کانال خود میگیرند با ارسال تراکنش دیگری به بلاکچین میتوانند سپرده خود را آزاد کنند. بدین ترتیب با تنها دو تراکنش درون بلاکچینی[۴] یکی برای ایجاد کانال و دیگری برای بستن کانال، امکان ارسال صدها تراکنش برون بلاکچینی فراهم میشود.

یکی از مهم ترین محدودیت های کانال پرداخت این است که افراد امکان اضافه کردن سپرده به کانال را فقط و فقط در هنگام ایجاد کانال دارند و اگر بعدا تصمیم به افزایش سپرده خود بگیرند باید کانال را بسته و کانال جدیدی ایجاد کنند که امری هزینه بر است. بنابراین کاربران تمایل دارند مقدار سپرده کافی در کانال از همان ابتدا قرار دهند اما از طرف دیگر نباید بیش از اندازه هم در کانال پول بگذارند زیرا امکان استفاده از این پول را تا بستن کانال نخواهند داشت. در نتیجه کاربران هنگام ایجاد کانال با یک مسأله تصمیم گیری آنلاین روبرو هستند. اما در عمل مساله از این هم پیچیده تر است زیرا میلیون ها کاربر با کانال پرداخت های دو به دویی که تشکیل میدهند، شبکه عظیمی از کانال های پرداخت [۵] را تشکیل میدهند. در این شبکه هر دو نودی که که یک کانال پرداخت مشترک دارند میتوانند بی واسطه برای هم تراکنش بفرستند اما نود هایی که کانال مستقیم با هم ندارند باید با استفاده از سایر نود های شبکه به عنوان واسطه، تراکنش خود را در شبکه مسیریابی و ارسال کنند. به طور مثال شبکه ای به صورت A-B-C را در نظر بگیرید که در آن نود های A و C کانال پرداخت مشترک ندارند اما هر دو با

[۱] payment channel
[۲] بدون مراجعه به بلاکچین off-chain transaction
[۳] local
[۴] on-chain
[۵] payment channel networks

B کانال مشترک دارند؛ در این شبکه A میتواند برای B پول بفرستد و B همان پول را به C ارسال کند و تراکنش A به C با یک واسطه انجام خواهد شد. بنابراین نود های موجود در شبکه میتوانند در دو نقش کاربر(فرستنده یا گیرنده) یا سرویس دهنده(واسطه) ایفای نقش کنند. نود های واسطه در ازای انتقال تراکنش های کاربران کارمزد دریافت میکنند پس تمایل دارند که تا حد امکان تراکنش های بیشتری را مسیریابی کنند؛ اما از طرفی اگر واسطه ها حریصانه تمام تراکنش های کاربران را مسیریابی کنند، کانال هایشان خالی از پول میشود. مثلا در مثال بالا فرض کنید A قصد دارد تعداد تراکنش زیادی برای C بفرستد، اگر B تمام این تراکنش ها را مسیریابی کند، هیچ پولی در کانال B-C برای او باقی نخواهد بود و در عوض Bمقدار زیادی پول در کانال A-B مقدار زیادی پول خواهد داشت. در چنین شرایطی میگوییم کانال B نامتعادل شده است. نامتعادل شدن کانال امر مطلوبی نیست زیرا مانع انتقال تراکنش های بعدی در جهت خالی شده از پول میشود. پس نود های واسطه شبکه کانال های پرداخت در هر لحظه با یک تصمیم گیری آنلاین روبرو هستند؛ اینکه کدام یک از تراکنش های کاربران را انتقال دهند. بنابراین در مجموع میبینیم که نود های شبکه کانال های پرداخت چه هنگام ایجاد کانال و چه بعدا د زمان ارسال تراکنش های برون بلاکچینی باید مدام تصمیمات آنلاینی در خصوص مدیریت کانال خود بگیرند.

نود های شبکه کانال های پرداخت نیاز به الگوریتمی برای مدیریت کانال خود دارند. این الگوریتم باید آنی باشد به این معنی که الگوریتم برای اتخاذ تصمیمات زمان زیادی ندارد. طراحی یک الگوریتم بهینه آنلاین که درباره مدیریت سپرده های نود ها تصمیم گیری میکند نه تنها در این حوزه مورد نیاز است بلکه میتواند در حوزه های دیگر همچون شبکه های مخابراتی برای حل مسأله admission control هم سود بخش باشد. در این پایان نامه الگوریتم آنلاینی برای مدیریت یک تک کانال پرداخت طراحی میکنیم. الگوریتم ما یک الگوریتم آنلاین است به این معنی که هیچ فرض خاصی روی توزیع تراکنش های آینده ندارند و تنها با اطلاعات گذشته و لحظه حال تصمیمی اتخاذ میکند. در این پایان کران بالای هزینه الگوریتممان را برای بدترین دنباله تراکنش [۶] ممکن اثات میکنیم؛ و در نهایت با پیاده سازی نشان میدهیم که الگوریتم ما در عمل بسیار بهتر از تضمین تئوری اثبات شده عمل میکند و همچنین دو heuristic با الهام از الگوریتم اصلی طراحی میکنیم که در عمل هزینه را تا نصف هزینه الگوریتم اصلی کاهش میدهد.

کلیدواژه‌ها: بلاکچین، شبکه کانال های پرداخت، الگوریتم آنلاین، admission control

---

[۶] worst-case analysis

فصل ۱

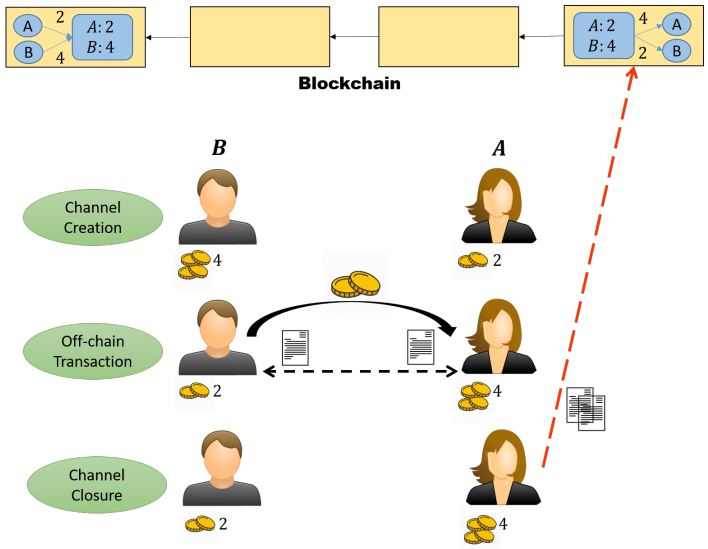
مقدمه

بلاکچین هایی همچون بیتکوین به دلیل ماهیت توزیع شده والگوریتم اجماع پیچیده و وقت گیری که دارند با مشکل عدم مقیاس پذیری روبرو هستند. عدم مقیاس پذیری به این معنی است که سیستم نمیتواند تعداد بسیار زیاد تراکنش را پردازش کند. به طور مثال بلاکچین بیتکوین تنها میتواند ۷ تراکنش در ثانیه را پردازش کند در حالیکه رقبای متمرکز بلاکچین همچون visa بیش از هزاران تراکنش را در هر ثانیه پردازش میکنند. به علاوه، حتی وقتی تراکنش ها وارد بلاکچین میشوند تایید شدن آن ها معمولا حداقل چند دقیقه به طول می انجامد، به طور مثال در بلاکچین بیتکوین نزدیک یک ساعت طول میکشد تا یک تراکنش تأیید نهایی شود. یکی از مورد استقبال ترین راه حل هایی که برای حل مشکل مقیاس ناپذیری و کندی بلاکچین ارائه شده است استفاده از شبکه کانال های پرداخت[۱] است. شبکه کانال های پرداخت اولین بار با پیاده سازی Lightning Network روی بلاکچین بیتکوین معرفی شد. [۱] بعد ها شبکه کانال های پرداخت Raiden هم با الهام از Lightning Network بر بلاکچین اتریوم[۲] توسعه داده شد. [۲] کاربران میتوانند با ارسال یک تراکنش ایجاد کانال [۳] روی بلاکچین، یک کانال پرداخت ایجاد کنند. با این تراکنش در واقع طرفین کانال پرداخت، مقداری پول را در این کانال پرداخت به سپرده میگذارند. پس از ایجاد کانال، طرفین میتوانند بدون مراجعه به بلاکچین و با رد و بدل کردن تعدادی امضای دیجیتال برای هم تراکنش محلی فوری[۴] با کارمزد بسیار اندک و بفرستند. مبادله امضاهای دیجیتال برای حفظ امنیت مالی طرفین الزامی است.

---

[۱] payment channel network
[۲] Ethereum
[۳] channel creation
[۴] instant

شکل ۱-۱ نحوه کار یک کانال پرداخت را نشان میدهد. ابتدا کاربر A ۲ واحد پول و کاربر B ۴ واحد پول سپرده میکند و یک کانال پرداخت میسازند. تراکنش ایجاد کانال روی بلاکچین قرار میگیرد. پس از ایجاد کانال امکان ارسال تراکنش برون بلاکچینی فراهم میشود. B میخواهد برای A دو واحد پول واریز کند پس A و B امضاهای دیجیتال رد و بدل میکنند و دو واحد پول به صورت برون بلاکچینی به موجودی A اضافه میشود. پس از مدتی A تصمیم میگیرد کانال را ببندد؛ از امضاهای رد و بدل شده پیشین استفاده میکند تا یک تراکنش بستن کانال ایجاد کند. پس از اجرای این تراکنش هر کدام از A و B سه واحد پول میگیرند. توجه کنید که در مرحله دوم A و B میتوانند به تعداد نامحدود تراکنش برون بلاکچینی ایجاد کنند. پس با دو تراکنش درون بلاکینی، امکان ایجاد تعداد نامحدود ترامنش برون بلاکچینی ارزان و سریع فراهم شد. اما باید توجه کرد که مجموع موجودی A و B که به آن ظرفیت کانال [۵] می گویند همواره عدد ثابت ۶ است و قابل افزایش یا کاهش نیست.



شکل ۱-۱: نحوه شکل گیری، استفاده و بستن یک کانال پرداخت

از اتصال کاربران مختلف با کانال های پرداخت یک شبکه از کانال های پرداخت ایجاد میشود که میتواند افرادی که کانال پرداخت مستقیم به هم ندارند را هم با یک یا تعدادی واسطه به هم متصل کند. مثلا ۳ کاربر A-B-C را در نظر بگیرید که A-B و B-C کانال پرداخت دارند. در این صورت A و C اگرچه کانال پرداخت مشترک ندارند اما میتوانند از B به عنوان واسطه استفاده کنند و برای هم تراکنش برون بلاکچینی ارسال کنند؛ بدین صورت که A مقدار پول مورد نظر را برای B می فرستد و B همان مقدار پول را برای C میفرستد. این دو تراکنش ها atomic هستند که به این معنی است که یا هر دو آنها انجام

[۵] capacity

میشوند و یا هر دو برگشت میخورند. معمولا فرد واسطه یعنی B مقداری کارمزد از A میگیرد اما این کارمزد در برابر کارمزد های تراکنش های درون بلاکچینی بسیار ناچیز است و صرفا نقش ایجاد انگیزه برای واسطه ها را دارد. البته گاهی نود های واسطه ممکن است برخی تراکنش ها را به دلایلی رد کنند. مثلا ممکن است اندازه تراکنش بیشتر از موجودی آن نود واسطه در کانال باشد یا اینکه موجودی نود واسطه را در حد غیر قابل قبولی کاهش دهد و یا اینکه میزان کارمزد آن مطلوب نود واسطه نباشد.

یکی از مشکلات بسیار مهم شبکه کانال های پرداخت این است که بعد از ایجاد کانال هیچ راهی برای افزودن سپرده به کانال وجود ندارد. مثلا در مثال بالا در کانال A-B فرض کنید با شروع از سپرده اولیه ۴ – ۲ ،A ۲ تراکنش هر کدام به ارزش ۱ بیتکوین برای B میفرستد؛ پس از انجام این دو تراکنش موجودی آنها در کانال به ترتیب ۶ – ۰ خواهد بود. پس از این تا زمانی که B تراکنشی برای A نفرستد، A نمیتواند تراکنشی بفرستد زیرا موجودی اش صفر است. به کانال پرداختی که در آن موجودی یک نفر صفر(یا بسیار کم است) کانال نامتعادل [۶] میگوییم. کانال های نامتعادل برای کاربران به خصوص برای نود های واسطه اصلا مطلوب نیستند زیرا امکان ایجاد تراکنش از یک سمت کانال را به کل از بین میبرند. در این پایان نامه گاهی نود های واسطه را سرویس دهنده [۷] می نامیم. نود های سرویس دهنده نود هایی هستند که با هدف درآمد سازی به شبکه کانال های پرداخت ملحق میشوند و با ذخیره کردن مقدار چشم گیری سپرده، تعداد زیادی کانال با کاربران زیادی ایجاد میکنند تا تراکنش های آنها را مسیریابی کنند و در ازای آن کارمزد بگیرند. داشتن کانال های نامتعادل توانایی سرویس دهنده ها را در انتقال تراکنش ها از یک جهت کاهش میدهد و برای کسب و کار آنها مشکل ایجاد میکند. Lightning network دو راه حل را برای حل مشکل کانال های نامتعادل پیشنهاد میدهد:

۱. شارژ کردن درون بلاکچینی: در این روش طرفین کانال نامتعادل آن کانال را میبندند و کانال جدیدی با سپرده بیشتر باز میکنند. این عمل باعث ایجاد دو تراکنش درون بلاکچینی میشود. یک تراکنش برای بستن کانال قدیمی و یک تراکنش برای ایجاد کانال جدید.

۲. متعادل کردن برون بلاکچینی: این روش بدون مراجعه به بلاکچین و صرفا با تعدادی تراکنش برون بلاکچینی توزیع سپرده ها را در کانال نامتعادل تغییر میدهد و به نسبت روش قبل ارزان تر است. در بخش ؟؟ به طور مفصل این روش را توضیح میدهیم.

از آنجاییکه هر دو روش بالا هزینه بر هستند و محدودیت هایی را اعمال میکنند، تصمیم گیری بر

[۶] depleted channel
[۷] service provider

سر اینکه چه زمانی کدام یک از آنها انجام گیرد تصمیم سختی است. همچنین توجه کنید که به عنوان یک کاربر یا یک نود واسطه، معمولا نود اطلاعات دقیقی از تراکنش های آینده ندارد و در نتیجه نود ها باید سیاست تصمیم گیری ای را اتخاذ کنند که بر اساس تاریخچه و بدون فرضی روی تراکنش های آینده، تصمیم گیری میکند.

هدف این پایان نامه این است که سیاست آنلاینی طراحی کند یک تک کانال پرداخت را در کلی ترین حالت ممکن در نظر میگیرد و به سوالات زیر که برای بیشینه کردن سود و کمینه کردن هزینه طرفین کانال مطرح میشود پاسخ میدهد:

۱. چه زمانی ایجاد یک کانال پرداخت نسبت به ارسال درون بلاکچینی تراکنش به مقرون به صرفه است؟

۲. اگر تصمیم به ایجاد کانال پرداخت شد، طرفین چه مقدار سپرده باید در آن قرار دهند؟

۳. اگر طرفین میخواهند نقش واسطه را ایفا کنند چه تراکنش هایی را باید بپذیرند و چه تراکنش هایی را نپذیرند؟

۴. اگر کانال پرداخت نامتعادل شد، طرفین باید کدام یک از راه های مقابله با کانال نامتعادل را اتخاذ کنند و سپرده کانال را چقدر باید تغییر دهند؟

۱-۱ اهمیت موضوع

هدف از طراحی شبکه کانال های پرداخت ایجاد بستری ارزان و سریع برای انجام تراکنش های کوچک و روزانه [۸] است. بهره بری کاربران از شبکه کانال های پرداخت تا حد زیادی به نحوه مدیریت کانال توسط آنها و سرویس دهنده ها بستگی دارد. مدیریت نادرست کانال ها توسط کاربران میتواند منجر به نامتعادل شدن کانال های آن ها شود و معمولا هزینه اصلاح یک کانال نامتعادل بسیار زیاد است. همچنین مدیریت نادرست کانال ها توسط سرویس دهنده هاهم به ضرر خود سرویس دهنده ها و هم به ضرر کاربران است. اگر سرویس دهنده ها نتوانند کانال های خود را درست مدیریت کنند، سود آنها کاهش می یابد و انگیزه ای برای ارائه خدمات نخواهند داشت که با توجه به اهمیت حیاتی سرویس دهنده

[۸] micro payment

ها برای شبکه، این امر بسیار مضر است. با بررسی آخرین داده های موجود از Lightning Network [۳] میتوان دید که در سال ۲۰۲۱ حدود ۶۳۰۰ در شبکه وجود دارد که بیش از ۵۰ درصد آن ها تنها از ۱۰ سرویس دهنده خدمات میگیرند. یعنی اگر ۱۰ سرویس دهنده اصلی Lightning Network عملکرد مناسبی نداشته باشند، نیمی از شبکه مختل خواهد شد! در واقع بدون وجودسرویس دهنده ها، امکان ارسال تراکنش های با واسطه از بین میرود و همه کاربران مجبورند کانال های دو به دو با هم ایجاد کنند.

در نتیجه ارائه الگوریتمی که این مسئله مدیریت کانال را در یک مدل واقع بینانه، با کمترین فروض محدود کننده و به صورت بهینه حل کند، بسیار ارزشمند است.

۱-۲ دست آورد های تحقیق

در این پایان نامه برای حل مسأله مدیریت آنلاین کانال های پرداخت، ابتدا از حل تئوری یک نسخه بسیار ساده شده و غیرواقع گرایانه مسأله شروع میکنیم و سپس در دو گام مدل را پیچیده تر واقع گرایانه تر میکنیم طوری که مسأله نهایی تا حد خوبی بیشتر پیچیدگی های کانال های پرداخت در دنیای واقعی را در بر دارد. این دو زیر مسأله به شرح زیر هستند:

۱. **زیر مسأله ۱ (کانال یکطرفه همیشه پذیرنده[۹])** کانال پرداختی ساده و غیرواقع نگرانه ای با دو کاربر A و B را در نظر بگیرید که در آن همیشه فقط A برای B پول میفرستد، یعنی کانال یکطرفه است. همچنین فرض کنید که باید تمام تراکنش ها حتما انجام شود و کاربران امکان رد کردن تراکنش ها را ندارند(اگر A یک کاربر عادی باشد رد تراکنش به این معنی است که A تراکنشش را خارج از کانال پرداخت و از طرق دیگر انجام میدهد و اگر A یک سرویس دهنده باشد رد کردن تراکنش به این معنی است که A تصمیم میگیرد از کارمزد این تراکنش صرف نظر کند و این تراکنش را مسیریابی نکند). همچنین برای ساده سازی فرض کنید که اگر پول A در کانال پرداخت تمام شد، باید کانال را ببندد و کانال جدید باز کند یا به عبارت دیگر تنها راه متعادل کردن کانال، شارژ کردن درون بلاکچینی است و متعادل کردن برون بلاکچینی برای ساده سازی مجاز نیست. این مدل، اولین و ساده ترین مدلی است که بررسی میکنیم و برای آن الگوریتمی

[۹] Unidirectional stream without rejection

مسئله	نسبت رقابتی	کران پایین
Unidirectional stream without rejection	2	2
Unidirectional stream with rejection	$2+\frac{\sqrt{5}-1}{2}$	$2+\frac{\sqrt{5}-1}{2}$
Bidirectional stream	$7+2\log C$	$\theta(\sqrt{\log C})$

جدول ۱-۱: خلاصه نتایج تئوری این پایان نامه. ستون اول نام (زیر)مسأله، ستون دوم نسبت رقابتی و ستون

آنلاین با نسبت رقابتی [۱۰] برابر ۲ ارائه میدهیم و اثبات میکنیم که این بهترین نسبت رقابتی ای ست که یک الگوریتم آنلاین میتواند به آن دست یابد.

۲. **زیر مسأله ۲ (کانال یکطرفه مجاز به رد تراکنش [۱۱])** در این زیر مسأله همانند مدل قبلی جهت تراکنش ها همیشه یکطرفه است اما این بار دارندگان کانال میتوانند تصمیم بگیرند کدام تراکنش ها را انتقال دهند و کدام ها را رد کنند. مشابه مدل قبل متعادل کردن برون بلاکچینی مجاز نیست. برای این مدل الگوریتم آنلاین با نسبت رقابتی $۲+\frac{\sqrt{۵}-۱}{۲}$ ارائه میدهیم و اثبات میکنیم که این الگوریتم بهینه است.

۳. **مسأله اصلی (کانال دوطرفه [۱۲])** در کلی ترین حالت مسأله تراکنش ها در هر دو جهت وجود دارند و صاحبان کانال نه تنها میتوانند تراکنش ها را به دلخواه بپذیرند یا رد کنند بلکه میتوانند از هر دو روش شارژ کردن درون بلاکچینی و متعادل کردن برون بلاکچینی برای متعادل کردن کانال خود استفاده کنند. برای این مدل الگوریتم آنلاین با نسبت رقابتی $۷+۲\log C$ طراحی میکنیم. (C یک عدد ثابت است که بستگی به ویژگی های گراف شبکه کانال های پرداخت دارد و مثلا در Lightning Network حدودا برابر ۴ است). همچنین به عنوان کران پایین نشان میدهیم که هیچ الگوریتم آنلاینی با نسبت رقابتی $o(\sqrt{\log C})$ وجود ندارد.

الگوریتم ها و اثبات های تئوری زیرمسأله ۱ و ۲ به عنوان بلوک های سازنده برای حل مسأله اصلی مورد استفاده قرار میگیرد.

---

[۱۰] competitive ratio معیاری است که هزینه یک الگوریتم آنلاین را با هزینه الگوریتم بهینه آفلاین که از پیش به تمام تراکنش های آینده دسترسی دارد، مقایسه میکند. در قسمت ؟؟ به طور مفصل این معیار و نحوه محاسبه آن را توضیح میدهیم.

[۱۱] Unidirectional stream with rejection

[۱۲] Bidirectional stream

۱-۳ ساختار پایان‌نامه

این پایان‌نامه شامل پنج فصل است. فصل دوم دربرگیرنده‌ی تعاریف اولیه‌ی مرتبط با پایان‌نامه است. در فصل سوم مسئله‌ی دورهای ناهمگن و کارهای مرتبطی که در این زمینه انجام شده به تفصیل بیان می‌گردد. در فصل چهارم نتایج جدیدی که در این پایان‌نامه به دست آمده ارائه می‌گردد. در این فصل، مسئله‌ی درخت‌های ناهمگن در چهار شکل مختلف مورد بررسی قرار می‌گیرد. سپس نگاهی کوتاه به مسئله‌ی مسیرهای ناهمگن خواهیم داشت. در انتها با تغییر تابع هدف، به حل مسئله‌ی کمینه کردن حداکثر اندازه‌ی درخت‌ها می‌پردازیم. فصل پنجم به نتیجه‌گیری و پیش‌نهادهایی برای کارهای آتی خواهد پرداخت.

فصل ۲

مفاهیم اولیه

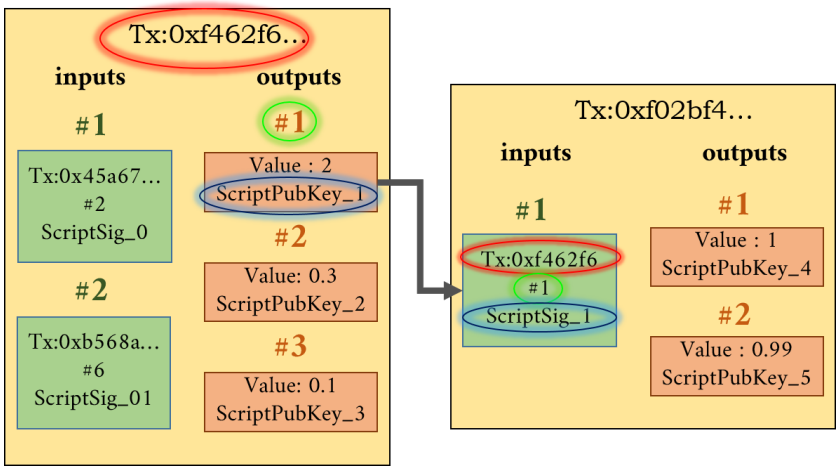
در این فصل مفاهیم اولیه لازم برای فهم مسأله و نتایج پایان نامه را مطرح میکنیم. ابتدا نحوه پردازش تراکنش ها در بلاکچین بیتکوین را توضیح میدهیم و سپس توضیح میدهیم که تراکنش های یک کانال پرداخت چه تفاوتی با تراکنش های عادی درون بلاکچینی دارند و چگونه میتوان تراکنش برون بلاکچینی امن داشت. در این بخش هنگام توضیح جزئیات پروتکل ها بلاکچین بیتکوین و شبکه کانال های پرداخت آن یعنی Lightning network را به عنوان معیار در نظر میگیریم زیرا اولا امروزه Lightning network با داشتن بیش از ۱۷۰۰۰ نود، پرکاربر ترین شبکه کانال های پرداخت موجود است [۴] و ثانیا مفاهیم پایه ای تراکنش های درون بلاکچینی و برون بلاکچینی کمابیش برای تمام بلاکچین ها یکسان است و تنها تفاوت در پروتکل های پیاده سازی شده است، پس تفاوت چندانی ندارد که کدام بلاکچین را به عنوان معیار قرار دهیم.

۲-۱ تراکنش ها در بیتکوین

بیتکوین یک بلاکچین UTXO-based است، در این سیستم هر تراکنش یک یا تعدادی ورودی و یک یا تعدادی خروجی دارد. در هر تراکنش مجموع بیتکوین ورودی ها برابر است با مجموع بیتکوین خروجی ها و کارمزد تراکنش. شکل ۲-۱ را ببینید. هر تراکنش یک هش [۱] یکتا دارد که شناسه تراکنش محسوب میشود. هر کدام از ورودی های یک تراکنش یکی از خروجی های یک تراکنش قدیمی تر را خرج میکند.

[۱] hash

هر خروجی دو داده در بر دارد : ۱)مقدار پول موجود در آن ۲) یک کد قفل کننده (ScriptPubKey) که کلید عمومی [۲] و سایر مشخصات کسی که میتواند خروجی را خرج کند مشخص میکند. مثلا در شکل ۲-۱ به خروجی شماره ۱ تراکنش سمت چپ دقت کنید. این خروجی دو بیتکوین دارد و کد قفل کننده ScriptPubKey_1، کلید عمومی کسی که میتواند این پول را خرج کند مشخص میکند. این خروجی توسط ورودی شماره ۱ تراکنش سمت راست خرج میشود. هر ورودی سه داده را در بر دارد ۱) هش تراکنشی که میخواهد یکی از خروجی های آن را خرج کند (در این مثال هش تراکنش سمت چپ که با قرمز رنگ مشخص شده است) ۲) شماره خروجی مورد نظر(در این مثال، عدد ۱ که با سبز رنگ مشخص شده است) ۳) یک کد باز کننده قفل که شامل امضای صاحب پول و سایر اثبات های مورد نیاز خروجی است (در این مثال، ScriptSig_1 که با رنگ سرمه ای مشخص شده است) . همچنین دقت کنید که در تراکنش سمت راست ورودی ۲ بیتکوین دارد و مجموع خروجی ها ۱/۹۹ بیتکوین است؛ ۰/۰۱ بیتکوین هم به عنوان کارمزد شبکه در نظر گرفته شده است.



شکل ۲-۱: ساختار یک تراکنش در بیتکوین

توجه کنید که کد قفل کننده و باز کننده قفل باید سازگار باشند مثلا دو عبارت زیر سازگار هستند:

ScriptPubKey: locked with <PubKey_A>
ScriptSig: Signature of A

کد قفل کننده میتواند شروط بیشتر و پیچیده تری هم برای خرج کننده خروجی ایجاب کند. مثلا به کد قفل کننده و بازکننده زیر توجه کنید که به امضای هر دو کاربر A و B نیازدارد. این خروجی مانند یک حساب دو کاربره عمل میکند زیرا برای خرج کردن پول آن تایید هر دو کاربر A و B لازم است.

[۲] public key

ScriptPubKey: locked with <PubKey_A> and <PubKey_B>
ScriptSig: Signature of A and signature of B

قفل زمانی تراکنش های بیتکوین میتوانند شامل جزئیات دیگری مانند قفل زمانی[۳] هم باشند. قفل زمانی به این معنی است که یک تراکنش را پیش از زمان مقرر نمیتوان به بلاکچین ارسال کرد. به طور مثال اگر شما تراکنشی با قفل زمانی December 31 بسازید و آن را پیش از این تاریخ به بلاکچین ارسال کنید، ماینر ها این تراکنش را ثبت نمیکنند و تا روز December 31 صبر کرده و بعد آن را ثبت میکنند.

خروجی های خرج نشده [۴] به خروجی هایی که تاکنون خرج نشده اند Unspent Transaction Output (UTXO) میگویند. ماینر[۵] ها در شبکه بیتکوین دو وظیفه اصلی دارند:

۱. اطمینان حاصل کنند که هیچ خروجی ای بیش از یکبار خرج نمیشود .

۲. بررسی کنند که هر کد باز کننده به درستی کد قفل کننده متناظر را باز میکند.

۲-۲ تراکنش های کانال پرداخت

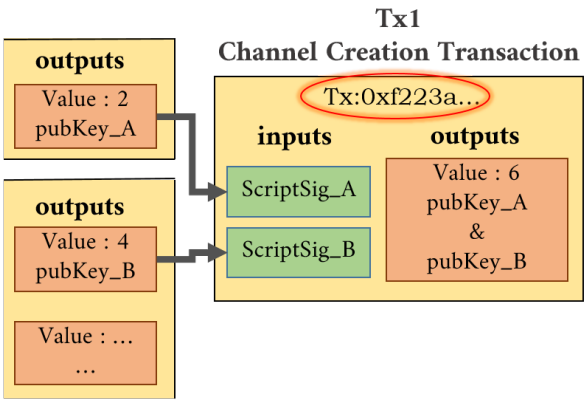
در این بخش نوع ساخت و استفاده از کانال پرداخت های بر مبنای زمان[۶] ها را توضیح میدهیم. کانال پرداخت های رایج در Lightning Network معمولا از نوع punishment based payment channel هستند که جزئیات پیچیده تری نسبت به کانال های بر مبنای زمان دارند. با این وجود چون اصول اولیه و کلیات هر دو این پروتکل ها مشابه هم است، فهم اصول کانال های بر مبنای زمان کافی است. برای خواندن درباره تفاوت این دو پروتکل ایجاد کانال میتوانید به منبع [؟] مراجعه کنید.

۲-۲-۱ ایجاد کانال

همانطور که پیش از این گفته شد، دو کاربر برای ایجاد کانال پرداخت باید یک تراکنش درون بلاکچینی "ایجاد کانال" بسازند. شکل ۲-۲ تراکنش Tx1 را نشان میدهد که نمونه ای از یک تراکنش ایجاد کانال

[۳] time lock
[۴] UTXO
[۵] miner
[۶] time based payment channels

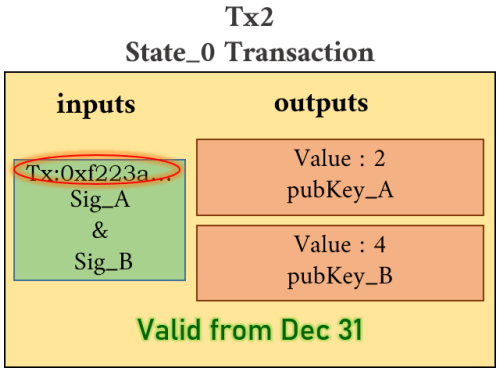
است. A یکی از UTXO هایش به ارزش ۲ بیتکوین و B یکی از UTXO هایش به ارزش ۴ بیتکوین را در کانال سپرده میکنند. خروجی Tx1 یک UTXO دو کاربره با موجودی ۶ است.



شکل ۲-۲: مثالی از یک تراکنش ایجاد کانال پرداخت. این تراکنش درون بلاکچینی است یعنی روی بلاکچین بیتکوین فرستاده میشود.

۲-۲-۲ استفاده از کانال

همزمان یا اندکی پیش از امضای تراکنش درون بلاکچینی Tx1، A و B مشترکا یک تراکنش برون بلاکچینی (Tx2) هم ساخته و هر دو آن امضا میکنند اما آن را روی بلاکچین نمیفرستند، این تراکنش تنها در حافظه محلی A و B ذخیره میشود.

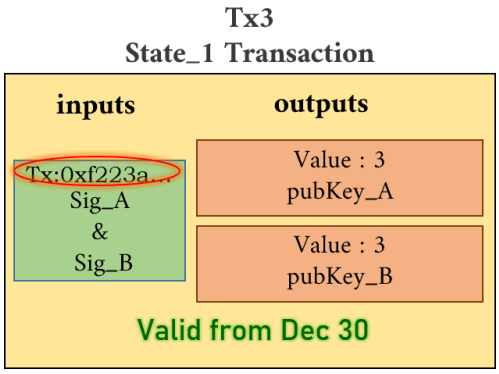


شکل ۲-۳: تراکنش حالت صفر کانال پرداخت. این تراکنش برون بلاکچینی است یعنی توسط A و B مشترکا ساخته و امضا شده و ذخیره می شود ولی تا زمان بسته شدن کانال روی بلاکچین قرار نمیگیرد.

Tx2 تک خروجی تراکنش Tx1 را خرج میکند و ، پول موجود در کانال را به همان نسبت اولیه ۴ – ۲ بین A و B تقسیم میکند. تراکنش Tx2 تنها پس از زمان مقرر قفل زمانی(در این مثال December 31)

بر بلاکچین ثبت میشود. Tx2 در واقع توزیع پول در کانال را در لحظه ایجاد آن یا لحظه صفر نشان میدهد به همین دلیل به آن تراکنش لحظه صفر میگوییم. در صورتی که هیچ تراکنشی بین A و B انجام نگیرد و پس از مدتی یکی از A یا B تصمیم بگیرد کانال را ببندد، آن فرد میتواند تراکنش Tx2 را روی بلاکچین قرار دهد. چون Tx2 پیش از این توسط هر دو A و B امضا شده است پس تراکنش معتبری است و بعد از تاریخ قفل زمانی آن A و B هر کدام میتوانند سهم خود را از کانال پرداخت بگیرند و کانال بسته میشود. اما در عمل A و B کانال پرداخت ساخته اند تا از آن استفاده کنند نه اینکه آن را بلافاصله ببندند پس تراکنش Tx2 عملا هیچگاه استفاده نمیشود. این تراکنش تنها و تنها ساخته میشود تا به هر دو طرف تضمین دهد که اگر طرف دیگر پاسخگو نبود، پول آن ها در کانال قفل نمیماند و هر کدام میتوانند سهم خود را از کانال دریافت کنند.

اکنون با یک مثال توضیح میدهیم که در عمل چگونه از کانال پرداخت ایجاد شده در شکل ۲-۲ استفاده میشود. فرض کنید B میخواهد برای A ۱ بیتکوین در کانال پول بریزد. B تراکنش برون بلاکچینی Tx3 نمایش داده شده در شکل ۲-۴ را میسازد و امضا میکند و برای A میفرستد. A هم Tx3 را امضا کرده و ذخیره میکند. Tx3 توزیع پول موجود در کانال را به ۳ – ۳ تغییر میدهد. هرگاه هر کدام از A یا B بخواهند این کانال را ببندند کافی است Tx3 را روی بلاکچین بفرستد و در تاریخ December 30 سهم خود از کانال را پس بگیرند.

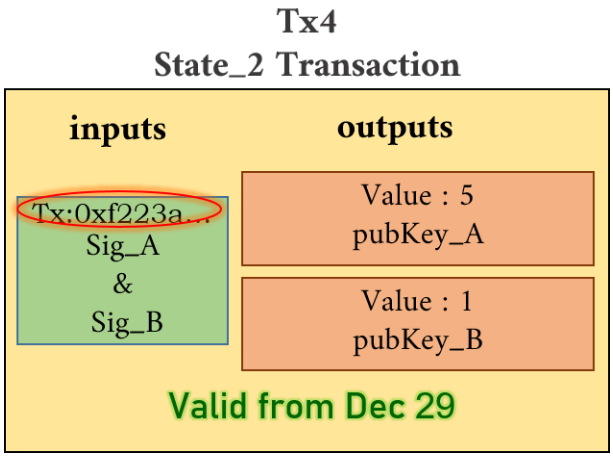


شکل ۲-۴

اما یک مشکل وجود دارد؛ چگونه تضمین دهیم که هیچ کدام از طرفین تراکنش قدیمی تر Tx2 را روی بلاکچین قرار نمیدهند تا کانال را با یک توزیع پول قدیمی ببندند؟ دقت کنید که هر دو Tx2 و Tx3 تک خروجی تراکنش Tx1 را خرج میکنند بنابراین فقط یکی از آن ها قابل اجرا روی بلاکچین است. محدودیت زمانی اعمال شده روی خروجی تراکنش های Tx2 و Tx3 تضمین کننده این است که تراکنشی که دیرتر تولید شده است، Tx3، زودتر اجرا خواهد شد؛ با یک مثال این موضوع را توضیح

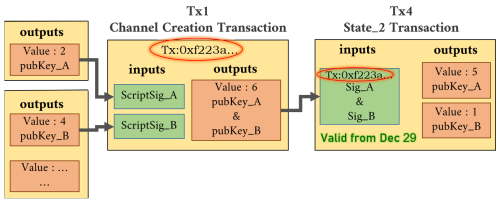
میدهیم. فرض کنید A میخواهد سر B کلاه بگذارد و بدون هیچ اطلاع قبلی تراکنش Tx2 را روی بلاکچین قرار میدهد؛ B با دیدن این عمل، تراکنش Tx3 را به بلاکچین میفرستد. قفل زمانی Tx3 روز December 30 باز میشود پس این تراکنش یک روز زودتر از Tx2 قابل اجرا است. تراکنش Tx3 در روز December 30 انجام میشود و بعد از آن، تراکنش Tx2 دیگر قابل اجرا نخواهد بود زیرا ورودی آن قبلا توسط Tx3 مصرف شده است.

منطق مشابهی در تمام مدت استفاده از کانال استفاده میشود مثلا اگر روز بعد B بخواهد به A ۲ بیتکوین بدهد، باید تراکنش Tx4 را تولید کند و امضا کرده و برای او بفرستد.



شکل ۲-۵

در نهایت وقتی طرفین تصمیم بگیرند کانال پرداخت را ببندند، آخرین تراکنش را روی بلاکچین میفرستند یعنی در نهایت فقط یکی از تراکنش های Tx2 Tx3 Tx4 اجرا میشود. همانطور که در بالا توضیح دادیم، قفل زمانی کاهنده تراکنش ها تضمین میکند که همیشه جدید ترین تراکنش اجرا شود.



شکل ۲-۶: بستن کانال پرداخت

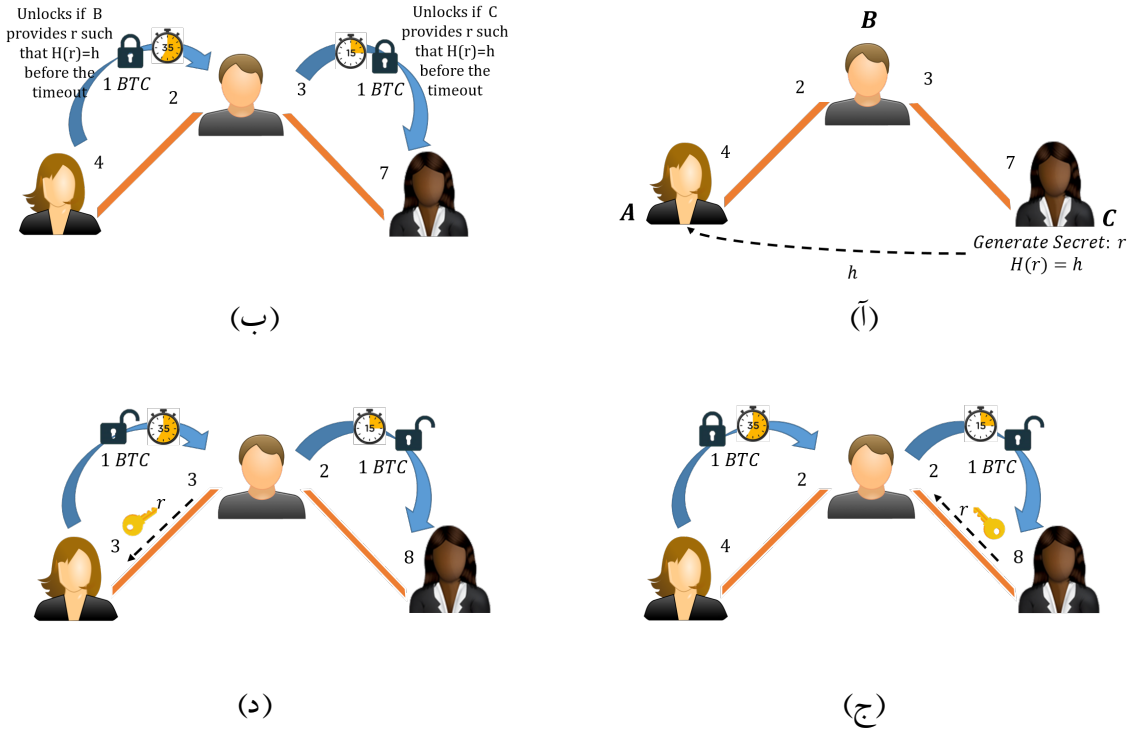
شکل ۲-۶ نشان میدهد که چطور تراکنش Tx4 با خرج کردن تک خروجی Tx1، کانال پرداخت را میبندد.

۲-۳ تراکنش های با واسطه

همانطور که در قسمت قبل توضیح دادیم، با ایجاد یک کانال پرداخت دو کاربر A و B میتوانند تنها با دو تراکنش درون بلاکچینی تعداد دلخواهی تراکنش برون بلاکچینی برای هم بفرستند اما همچنان محدودیت این روش این است که کاربران دو به دو باید کانال پرداخت ایجاد کنند. برای حل این مشکل توسعه دهندگان Network Lightning پروتکلی طراحی کرده اند که این امکان را به کاربران میدهد که با یک یا چندین واسطه تراکنش برای هم بفرستند [۱]. تراکنش با واسطه را با یک مثال توضیح میدهیم. به شکل ۲-۷ توجه کنید، کاربر A و B با هم و کاربر B و C با هم کانال دارند و کاربر A میخواهد با استفاده از B به عنوان واسطه برای C ۱ بیتکوین بفرستد. در شکل ۲-۷آ که مرحله اول را نشان میدهد میتوانید موجودی هر فرد در کانال ها پیش از انجام تراکنش را ببینید. در این مرحله C یک مقدار تصادفی و محرمانه r را انتخاب کرده و آن را از یک تابع چکیده ساز[۷]، که در اینجا با $H(.)$ نمایش داده شده است عبور میدهد تا h حاصل شود و بعد h را برای A ارسال میکند. در اینجا لازم است توضیح مختصری درباره توابع چکیده ساز بدهیم. این توابع یک ورودی از طول دلخواه را گرفته و به خروجی به طول معین تبدیل میکنند. در حالیکه محاسبه این توابع از نظر محاسباتی ساده است اما محاسبه وارون آن ها دشوار است بنابراین با داشتن h محاسبه r ممکن نیست.

در مرحله دو که در شکل ۲-۷ب نمایش داده شده، A یک تراکنش ۱ بیتکوینی برای B میفرستد اما شرط اینکه این تراکنش اجرا شود این است که B بتواند پیش از زمان معین timeout r را طوری پیدا کند که $H(r) = h$ سپس B تراکنش مشابهی را منتها با timeout کوتاه تر تولید کرده و برای C میفرستد. تنها کسی که r را میداند C است پس پیش از به پایان رسیدن C timeout، r را برای B فرستاده (شکل ۲-۷ج) و قفل تراکنش باز میشود و ۱ بیتکوین به صورت برون بلاکچینی از B به C واریز میشود. سپس چون timeout تراکنش A-B بیشتر از timeout تراکنش B-C است B زمان کافی خواهد داشت که r را برای A بفرستد و ۱ بیتکوین خود را از او بگیرد (شکل ۲-۷د) و به این ترتیب B همان پولی را که در کانال با C از دست میدهد در کانال با A بدست می آورد. اگر زمان timeout هر کدام از تراکنش ها بگذرد آن تراکنش کلا برگشت میخورد پس اگر C آفلاین شود و نتواند r را تا پیش از timeout نفرستد، تراکنش B-C برگشت میخورد و بالطبع چون B هم به هیچ وجه نمیتواند r را پیدا کند، تراکنش A-B هم برگشت میخورد به همین دلیل میگوییم این تراکنش ها atomic هستند یعنی یا هر دو با هم انجام میشوند یا هر دو برگشت میخورند.

[۷] Hash function



(ب) (آ)

(د) (ج)

شکل ۲-۷: مراحل انجام یک تراکنش با واسطه در شبکه کانال های پرداخت

۲-۴ الگوریتم های آنلاین

[۸] در این قسمت به طور مختصر توضیح میدهیم که منظور از الگوریتم آنلاین چیست و چرا ضرورت دارد که برای حل مساله تصمیم گیری مدیریتی شبکه کانال های پرداخت از الگوریتم آنلاین استفاده کنیم. الگوریتم های آنلاین الگوریتم هایی هستند که فرض خاصی روی توزیع ورودی های مساله ندارند و برای موقعیت هایی قابل استفاده هستند که محیط به قدری سریع تغییر میکند که اصولا فرض روی توزیع متغیر ها فرض قابل قبولی نیست و یا اینکه محیط به اصطلاح متخاصم [۹] است یعنی محیط دنباله ورودی را انتخاب میکند و میتواند ورودی هایی را انتخاب کند که الگوریتم شما در بدترین حالت ممکن خودش عمل کند. پس در این روش تحلیل الگوریتم را طوری طراحی میکنیم که در صورت بدترین ورودی ممکن هم بتوان تضمین کرد الگوریتم خیلی بد عمل نمیکند. مساله و الگوریتم آنلاین را با مثال معروف کرایه اسکی [۱۰] توضیح میدهیم. فرض کنید شما میخواهید اسکی بازی کنید و تجهیزات ندارید و هزینه

[۸] online algorithms
[۹] adversarial
[۱۰] Ski-Rental

اجاره کردن اسکی برای مدت زمان t ماه t تومان است. از طرفی اگر تجهیزات اسکی را بخرید باید ۱ تومان بپردازید اما دیگر نیاز به پرداخت کرایه ندارید. حالا شما در سر این دو راهی هستید که بعد از چه مدت زمانی (z) تجهیزات را بخرید. مسلما اگر شما بدانید که تا چه مدت قصد دارید اسکی بازی کنید تصمیم گیری راحت است زیرا اگر بدانید که قصد دارید بیش از یکماه اسکی بازی کنید به صرفه تر است که تجهیزات را همان ابتدا بخرید و در غیر این صورت تجهیزات را کرایه کنید. اما مشکل این است که شما از قبل نمیدانید که چقدر میخواهید اسکی بازی کنید و این زمان (u) به صورت متخاصمانه توسط محیط تعیین میشود. هزینه الگوریتمی که در زمان z تجهیزات را میخرد به صورت زیر تعیین میشود:

$$Cost_z(u) = \begin{cases} u & u \leqslant z \\ z+1 & u > z \end{cases} \tag{۱-۲}$$

الگوریتم بهینه OPT الگوریتمی است که مقدار u را میداند. الگوریتم بهینه در این مثال برای $u > 1$ تجهیزات را میخرد و در غیر این صورت تجهیزات را اجاره میکند.

$$Cost_{\mathrm{OPT}}(u) = \begin{cases} u & u \leqslant 1 \\ 1 & u > 1 \end{cases} \tag{۲-۲}$$

تعریف ۲-۱ *الگوریتم آنلاین* ALG *را* `r-competitive` *گوییم اگر به ازای هر ورودی* I *همواره داشته باشیم:*

$$Cost_{\mathrm{ALG}}(I) \leqslant r \cdot Cost_{\mathrm{OPT}}(I)$$

برای مثال کرایه اسکی، الگوریتم آنلاینی را در نظر بگیرید که تا پایان ماه اول تجهیزات را کرایه میکند و در پایان ماه اول تجهیزات را میخرد. اگر $u \leqslant 1$ باشد هزینه این الگوریتم برابر هزینه OPT است اما اگر $u > 1$ باشد، هزینه این الگوریتم ۲ است در حالیکه هزینه الگوریتم بهینه ۱ است پس ضریب رقابتی این الگوریتم آنلاین ۲ است یعنی برای بدترین ورودی ممکن هم هزینه این الگوریتم ۲ برابر هزینه بهینه است.

اکنون تمام مقدمات مورد نیاز را مطرح کرده ایم و میتوانیم مستقیما وارد مدل بندی ریاضی مسئله مان شویم.

Bibliography

[1] J. Poon and T. Dryja. The bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf, 2015.

[2] Raiden network. https://raiden.network/, 2017.

[3] C. Decker. Lightning network research; topology, datasets. https://github.com/lnresearch/topology. Accessed: 2022-04-01.

[4] Lightning network search and analysis engine.