باسمه تعالی

پیشنهاد پروژه اول درس Distributed optimization and learning

تاریخ تحویل 21 آبان 1401

نام و نام خانوادگی : حمید رضا کاشانی **شماره دانشجویی**: 810100441 **ایمیل**: hr.kashani110@gmail.com

1. عنوان موضوع پیشنهادی :

High throughput cryptocurrency routing in payment channel networks

بیشترین توان عملیاتی با بار ورودی در مسیر بابی رمزارز های شبکه کانال پرداخت (شبکه خارج از زنجبره بلاک چین)

2. مرجع (مراجع) اصلی – برگرفته از کنفرانس ها و یا نشریات معتبر بین المللی- که مبنای انتخاب کاربرد قرار گرفته است :

[1] Sivaraman, Vibhaalakshmi, et al. "High throughput cryptocurrency routing in payment channel networks." *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*. 2020.

[2] Sivaraman, Vibhaalakshmi, et al. "Routing cryptocurrency with the spider network." *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*. 2018.

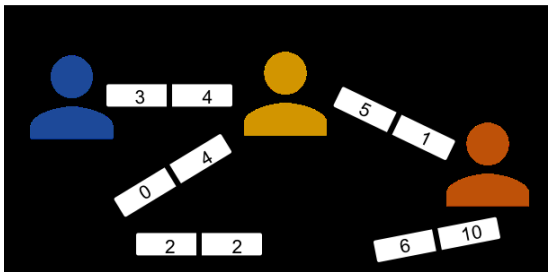
3. توضیح مختصر در مورد کاربرد انتخابی :

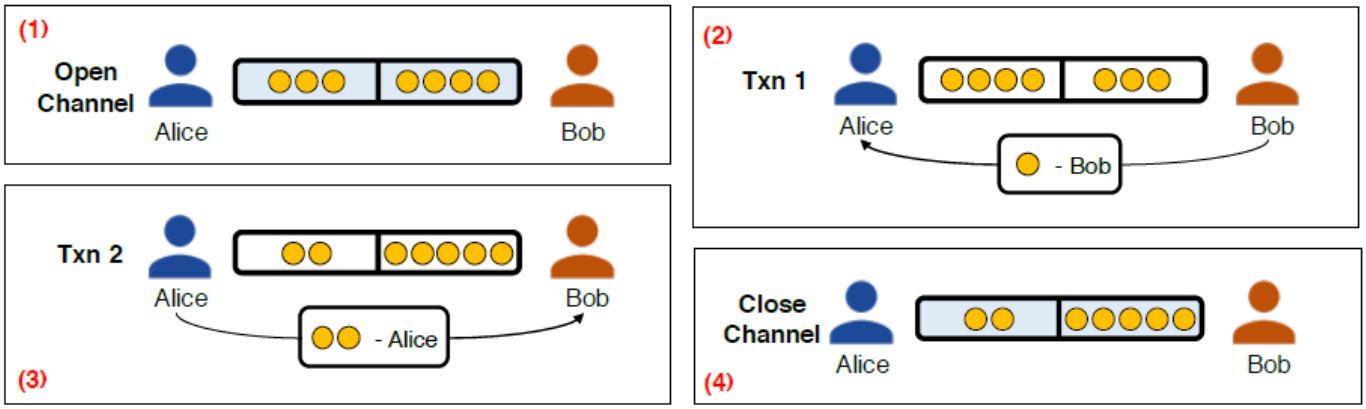
شبکه های کانال پرداخت یا PCN ها شبکه ای از نود هایی هستند که دو به دو با یکدیگر کانال پرداخت ایجاد می کنن و بدون تکرانش در زنجیره بلاک قابلیت پرداخت را در شرایطی داخل نود های شبکه می دهد. این شبکه به علت مشکل مقیاس پذیری در برخی رمز ارز ها مانند بیتکون ایجاد شده است زیرا هر بلاک درزمانی با میانگین ثابت و حجم محدود رمز ارز ایجاد می شود و با زیاد شدن تقاضا بلاکچین نمی تاند اسکیل پیدا کنند و باید مشترکین برای پرداخت در صف قرار بگیرن .

این شبکه به این صورت کار می کند که هر نود با چند نود دیگر در شبکه کانال ایجاد کرده است و در این شبکه هر دو نودی که بخواهند با هم تراکنش داشته باشند باید ارز های خود را با انتقال ار بین کانال های موجود به نود مورد نظر برسند و هر نود میانی هزینه انتقال ارز از خود را که قبلا اعلام کرده است از ارز های انتقالی بر می دارد و به نود بعدی می دهد .

نحوه ی ایجاد کانال اینگونه است که هر دو نود مقداری ارز را در حسابی چند امضا در زنچیره بلاک چین قرار می دهد برای مثال هر نود ده ارز را در حساب کانال قرار می دهد و یک کانال با ظرفیت 20 را تشکیل می دهد که هر نود می تواند ده ارز را هنگام تراز بودن کانال از خود انتقال دهد و به طور مثال با عبور دو ارز از یک طرف تعادل کانال به هم ریخته و به 8 و 12 تبدیل می

شود و در صورتی که یک طرف کانال 0 شود دیگر نمیتوان از آن طرف کانال ارز انتقال داد مگر این که کانال جدید بین دو نود در بلاکچین ایجاد شود و کانال قبلی بسته شود که این عمل برای دو نود هزینه ایجاد می کند .





منابع عکس از مقاله [1]

پس مسیریابی ها در شبکه باید به گونه ای باشد که تعادل کانال ها حفظ شود که ابن به این معنی است که مقدار ارز عبوری از کانال از دو نود برابر شود . همینطور این را هم باید در نظر گرفت که هر کانال محدودیتی دارد در انتقال ارز از خود که متناسب با ظرفیت آن است.

4. توضیح مختصر پیرامون نحوه ی مدل سازی کاربرد انتخابی خود به گونه ای که بتوان روش های decomposition را روی آن پیاده سازی کرد:

مدل به صورت شبکه ریز است که روی تقاضای بین هردونود گسسته شده است.

نوتیشن مدل:

$G(V, E)$	Graph of the PCN with a set of V routers and E payment channels
$\mathcal{P}_{ij}$	Set of paths that sender i uses to receiver j
$\mathcal{P}$	$\bigcup_{i,j \in V} \mathcal{P}_{ij}$
x_p	Average rate of transaction-units on path p between sender i and receiver j
x_{uv}	$\sum_{p \in \mathcal{P}:(u,v) \in p} x_p$
d_{ij}	Demand from sender i to receiver j
c_{uv}	Total amount of tokens escrowed into payment channel (denotes channel size)(u, v)
Δ	Average time (s) over which tokens sent across a payment channel are unusable

Table 4.1: Notation for routing problem

و مدل مسئله مسبر یابی به همراه قید های آن: U تابع رضایت مندی است که برای حل مسئله باید محدب باشد

$$\begin{aligned}
\text{maximize} \quad & \sum_{i,j \in V} U\Big(\sum_{p \in \mathcal{P}_{ij}} x_p\Big) \\
\text{s.t.} \quad & \sum_{p \in \mathcal{P}_{ij}} x_p \le d_{ij} \quad \forall i,j \in V \\
& x_{uv} + x_{vu} \le \frac{c_{uv}}{\Delta} \quad \forall (u,v) \in E \\
& x_{uv} = x_{vu} \quad \forall (u,v) \in E \\
& x_p \ge 0 \quad \forall p \in \mathcal{P}.
\end{aligned}$$

5. **معرفی روش های بهینه سازی اضافه بر Dual، Primal، ADMM که قصد پیاده سازی آن را دارید:**

هنوز در نظر گرفته نشده است.

6. **در صورتی که هر یک از روش های Dual، Primal، ADMM و centralized بر روی کاربرد انتخابی شما قابل پیاده سازی نیست، در مورد علت آن توضیح دهید.**

مسئله پیچیدگی هایی دارد که باید از استاد و ta های درس برای رفع آن کمک گرفته شود.