УДК 004.8

Щербіна Є.С.
Месюра В.І.

МОДЕЛІ ПОДАННЯ МЕРЕЖІ ЛАЙТНІНГ У БІТКОЇН БЛОКЧЕЙНІ

Вінницький національний технічний університет

Анотація
У даній роботі було проаналізовано технологію мережі лайтнінг та її основні компоненти. Розглянуто появу нового класу задач пов'язаних з маршрутизацією платежів. Було запропоновано моделі представлення мережі лайтнінг, що можуть бути використані при вирішенні задач маршрутизації.
Ключові слова: криптовалюта, біткоїн, блокчейн, лайтнінг, теорія графів.

Abstract
In this paper, the lightning network technology and its main components were analyzed. The emergence of a new class of tasks related to the routing of payments is considered. Lightning network representation models have been proposed that can be used to solve routing problems.
Keywords: cryptocurrency, bitcoin, blockchain, lightning, graph theory.

Вступ

Лайтнінг нетворк (lightning network) - це технологія, що намагається фундаментально вирішити проблему масштабування біткоїн блокчейну.

Основна ідея полягає у тому, що якщо двом учасникам мережі необхідно здійснити транзакцію (наприклад переказ 1-го біткоїну), не потрібно публікувати її на блокчейні, чекати глобального консенсусу щодо цієї транзакції, тощо. Достатньо домовитися між собою, а в блокчейн звертатися лише в разі непорозумінь або не кооперативної поведінки однієї зі сторін. Не дивлячись на здавалось би просту ідею технічний устрій мережі лайтнінг (lightning network) є досить складним. Він спирається на велику кількість елементів, серед яких варто відмітити:

- непідтверджені транзакції
- механізм захисту від подвійної витрати (double spend) [1]
- мультипідпис [2]
- тимчасові блокування
- хеши і секрети.

Основна частина

До появи лайтнінг нетворк (lightning network) - існував схожий, проте менш потужний алгоритм, що мав назву payment channels (платіжні канали).

Цей механізм дозволяє проводити миттєві платежі між двома учасниками, у яких був відкритий прямий канал між собою. Лайтнінг нетворк - є суттєвим кроком вперед, оскільки дозволяє провести платіж між двома учасниками Алісою та Керол, за умови, що Аліса має канал з Бобом а, Боб з Керол. Зверніть увагу, що відсутність прямого каналу Аліси з Керол не є обов'язковою. В більш загальному випадку платіж може бути проведений через будь-яку кількість посередників. Це призвело до виникнення нового класу задач, а саме побудови моделей для представлення мережі lightning, пошуку оптимальних шляхів для проведення платежу, ребалансування мережі, тощо [3].

У даній статті ми зупинимося на моделях подання мережі лайтнінг.

Графова модель Lightning Network

В термінах теорії графів користувач мережі може бути представлений вершиною графу. При цьому відкритий канал між двома людьми зручно подати орієнтованим ребром графу. З кожним ребром у графі асоціюємо одне число, яке подаватиме кількість замкнених біткоїнів. Протокол Лайтнінг (Lightning)

Network надає можливість провести платіж між двома вершинами A та B, якщо існує відповідний маршрут у графі [4].

Зауважимо, що розмір платежу не має перевищувати кількість замкнених біткоїнів на будь-якому ребрі графа.

Для зручності будемо позначати асоційоване з ребром число літерою K, а мінімальне значення K на певному шляху MIN_K.

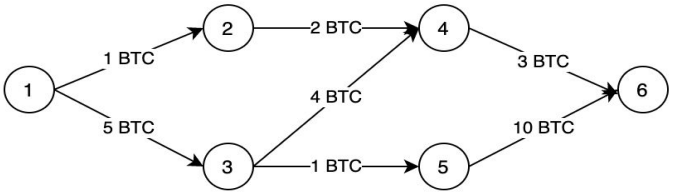

Рис.1 - Графова модель

Наприклад на рис.1, максимальний розмір платежу, що може бути проведений між вершинами 1 та 6 дорівнює 3 BTC. Оптимальний маршрут 1 -> 3 -> 4 -> 6, згідно з нашими позначеннями K1 = 5 BTC, K2 = 4 BTC, K3 = 3BTC -> MIN_K = 3 BTC.

Мережева модель Lightning Network

З іншої сторони при графовому поданні платіжної мережі Лайтнінг (Lightning) Network, кожне ребро має як пропускну здатність так і вартість. Вершина уособлює собою людину, а ребро - платіжний канал в рамках якого здійснюється платіж, пропускна здатність вимірюється кількістю біткоїнів замкнених у каналі, а вартість є комісією (fee) [5].

Платіж у графовій моделі Лайтнінг (Lightning) Network подається шляхом у мережі. Якщо ми хочемо провести платіж розміром 1 BTC усі ребра на шляху повинні мати пропускну здатність більшу або рівну за один BTC, до того ж під час проходження платежу на кожному ребрі сплачується комісія.

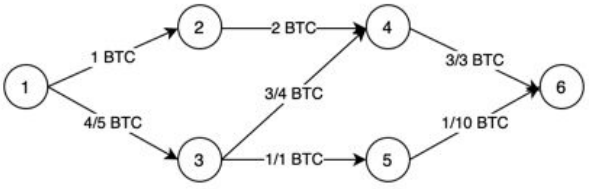

Рис.2 - Мережева модель

Наприклад, на рис.2, максимальний розмір платежу, що може бути проведений між вершинами 1 та 6 дорівнює 4 BTC. Вздовж маршруту 1 -> 3 -> 5 -> 6 буде проходити 1 BTC, вздовж маршруту 1 -> 3 -> 4 - > 6 буде проходити 3 BTC. Таким чином маємо наступну насиченість ребер:

- 1 -> 3 = 4 із 5
- 3 -> 5 = 1 із 1
- 5 -> 6 = 1 із 10
- 3 -> 4 = 3 із 4
- 4 -> 6 = 3 із 3

Висновки

У даній роботі було розглянуто новий клас задач, який постає перед розробниками лайтнінг нетворк. Було запропоновано моделі представлення мережі лайтнінг, що можуть бути використані для вирішення задач маршрутизації або зведенню цих задач до загальновідомих та проаналізованих задач теорії графів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Електронний журнал Wikipedia. “Double-spending”, 2020. [Електронний ресурс]. Режим доступу: https://en.wikipedia.org/wiki/Double-spending

2. Електронний журнал BitcoinWiki. “Multisignature”, 2020. [Електронний ресурс]. Режим доступу: https://en.bitcoin.it/wiki/Multisignature
3. Joseph Poon, Thaddeus Dryja. “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”, 2016. [Електронний ресурс]. Режим доступу: http://lightning.network/lightning-network-paper.pdf
4. Електронний журнал MAXimal. “Пошук у ширину”, 2008. [Електронний ресурс]. Режим доступу: https://e-maxx.ru/algo/bfs.
5. Електронний журнал MAXimal. “Потік мінімальної вартості”, 2008. [Електронний ресурс]. Режим доступу: https://e-maxx.ru/algo/min_cost_flow

Щербіна Євгеній Сергійович — *аспірант кафедри КН, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sototonamitol@gmail.com*

Месюра Володимир Іванович*— канд. техн. наук, доцент, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.*

Evgeniy S. Scherbina *— postgraduate of the Computer Sciences Chair, Vinnytsia National Technical University, Vinnytsia, e-mail: sototonamitol@gmail.com*

Volodymyr I. Mesyura *— Ph.D., Assistant Professor, Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.*