УДК 681.3(045)

В.І.Месюра
Є.С.Щербіна

РОЗРОБКА АЛГОРИТМУ МАРШРУТИЗАЦІЇ ПЛАТЕЖІВ ДЛЯ ТЕХНОЛОГІЇ LIGHTNING NETWORK

Вінницький національний технічний університет

Анотація

Описано задачу маршрутизації платежів для технології lightning network, здійснено формулювання задачі у термінах теорії графів та запропоновано шляхи її вирішення. Запропоновано ряд ідей, що потенційно можуть вирішити поставлену задачу та масштабуватися на десятки мільйонів вершин та ребер.

Ключові слова: біткоін, блокчейн, маштабування, лайтнінг нетворк, маршрутизація, теорія графів

Abstract

The article describes the problem of routing payments for lightning network technology, reformulated the problem in terms of graph theory, and suggests ways to solve it. A number of ideas were suggested that could potentially solve a task and scale tens of millions of vertices and edges.

Keywords: bitcoin, blockchain, scaling, lightning network, routing, graph theory

Вступ

Біткоїн є одногранговою, децентралізованою платіжною системою яка використовує однойменну одиницю для обліку операцій. Для забезпечення функціонування і захисту системи використовуються криптографічні методи, але при цьому вся інформація про транзакції між адресами системи доступна у відкритому вигляді [1,2]. Біткоїн побудовано на технологій блокчейн [3].

Lightning Network є проектом, метою якого є усунення проблеми масштабованості біткоїну шляхом масштабування «поза мережею». Він призначений для забезпечення поновлення стану мікроканалу без використання будь-яких блокувань (в зазвичай не-змагальному випадку), що робить мікроплатежі виправданими (і без комісії). Lightning Network зажадає, щоб транзакція фінансування на блокчейне відкрила канал [4,5].

Швидкий розвиток технології Lightning Network робить надзвичайно актуальною проблему масштабування.

Постановка задачі дослідження

З метою розробки алгоритму маршрутизації платежів для технології Lightning Network подамо її графом, у якому кожна вершина подає lightning network daemon (програму-клієнта), а кожне ребро має ємність (виражену у біткоінах). Скористуємомось також поняттям ліквідності в одну зі сторін. Наприклад ємність каналу може дорівнювати 10 біткоїнам, при цьому ліквідність в сторону A→ B дорівнюватиме 6 біткоїнам а ліквідність в сторону B→A дорівнювати 4 біткоїнам.

Пошук маршруту платежу в Lightning Network зводиться при цьому до пошуку найкоротшого шляху в графі. Зауважимо, що оскільки граф може мати десятки мільйонів вершин та ребер то кожна вершина не може зберігати та оновлювати весь граф. Отже виникає задача пошуку найкоротшого шляху в умовах неповної інформації.

Результати досліджень

Проведені дослідження дозволили сформулювати доцільність таких основних ідей для вирішення задачі:

- збереження графу в межах певного радіусу, наприклад R = 3;
- об'єднання при здійсненні платежу A→B часткової інформації з обох вершин в єдиний граф для збільшення імовірності знаходження шляху;
- використання так званих маяків (beacon), тобто збереження кожною нодою (комп'ютером підключеним до мережі біткоїн з використанням протоколу p2p) не лише інформації у межах певного радіусу, але й деякої випадкової інформації щодо топології графу. Ця ідея дозволяє шукати маршрути довжиною більшою за 2 * R;
- використання централізованих рішень, а саме статичного або динамічного вибору певних вершини,

що будуть мати спеціальний статус та надавати допомогу іншим вершинам у пошуках необхідного шляху.

У ході подальшого дослідження планується провести моделювання вище вказаних ідей на різних топологіях графу та отримати кількісні та якісні показники.

Слідуючи загальноприйнятим підходам та постулатам мікросервісної архітектури задача моделювання розділяється на декілька модулів:

1) ядро - імплементація наведених ідей;
2) модуль генерації топології графу;
3) модуль отримання кількісних показників;
4) модуль візуалізації отриманих даних.

Даний підхід дозволяє надавати як API для інших програм так і отримувати дані у зручному для аналітиків графічному поданні. Окрім того модульний підхід дозволяє швидко локалізувати помилки при написанні програми та полегшує процес кооперації та об'єднання зусиль для команди програмістів.

Висновки

Запропоновано підхід до розв'язання проблеми маршрутизації платежів електронної валюти для технології Lightning Network, що дозволяє масштабуватися на десятки тисяч вершин і ребер відповідного графу.

Обґрунтовано доцільність розподілу задачу моделювання на чотири основні модулі: ядро, генерація топології графу, отримання кількісних показників (вірогідність успішного проходження платежу, середня довжина шляху), візуалізація отриманих даних.

Подальшою задачею досліджень є моделювання запропонованого підходу на різних топологіях графа та отримання кількісних та якісних показників (вірогідність успішного проходження платежу, середня довжина шляху та інших).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Биткойн [Електронний ресурс] / ВикипедиЯ. – Режим доступу: https://ru.wikipedia.org/wiki/Биткойн
2. Щербіна Є. С. Месюра В. І. Аналіз мов написання смарт контрактів існуючих крипто валют / Збірник праць XI Міжнародної науково-практичної конференції «Інтернет-Освіта-Наука - 2018» (ІОН-2018) – Вінниця : ВНТУ, 2018, с.184-185.
3. Khan Ian. What is Blockchain Technology? A Step-by-Step Guide For Beginners [Електронний ресурс] / Ian Khan. – – Режим доступу: https://blockgeeks.com/guides/what-is-blockchain-technology/
4. Lightning Network [Електронний ресурс]/Xcryptor - Режим доступу: https://ru.wikipedia.org/wiki/Биткойн
5. Poon J. The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments : DRAFT version 0.5.9.2 / Joseph Poon, Thaddeus Dryjarx [Електронний ресурс]. - 14.01.2016 – Режим доступу: https://lightning.network/lightning-network-paper.pdf.

Щербіна Евгеній Сергійович — провідний інженер «Бітфурі», м. Київ, email : sotonamitol@gmail.com

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

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

Shcherbyna Yevgen S. — Senior Engineer, "Bitfury", Kyiv, email : sotonamitol@gmail.com

Mesyura Volodymyr I. — - Cand. Sc. (Eng.), Assistant Professor, Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Mesyura Volodymyr I.*** - Cand. Sc., Assistant Professor, Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.