УДК 654.07

А. В. Левкін

МЕТОДИ ВИРІШЕННЯ ПРОБЛЕМИ ПЕРЕБАЛАНСУВАННЯ В ПРОТОКОЛІ ДРУГОГО РІВНЯ LIGHTNING NETWORK

Вінницький національний технічний університет

Анотація

У Lightning Network є кілька методів, які відновлюють баланс, але жоден з них не є ідеальним. Представлені приклади дозволять поглянути на поточні інновації в цій області. Існує два основні методи обходу проблеми перебалансування: сплайсинг для внутрішньомережевих, і циклічні платежі для поверхневої мережі.

Ключові слова: Lightning Network, перебалансування, сплайсинг, циклічні платежі.

Abstract

The Lightning Network has a number of methods that maintain balance, but they are not ideal. The presented butts allow you to take a look at the current innovations in the whole region. There are two main methods to circumvent the problem of rebalancing: splicing for internal mesh, and cyclical payments for surface mesh.

Keywords: Lightning Network, rebalancing, splicing, cyclical payments.

Вступ

На сучасному етапі спостерігається великий інтерес до розробки платіжних систем які будуть забезпечувати велику пропускну здатність, та мінімальні комісійні збори. Велику роль відіграє концепція децентралізації, що дає змогу позбутися посередників і разом з ними, великі витрати на послуги. Lightning Network (англ. – мережа-блискавка) – технічне рішення, що реалізоване в якості протоколу другого рівня Blockchain. Розгорнутий поверх протоколу Bitcoin, LN використовує передові смарт-контракти для досягнення більш високої пропускної здатності транзакцій, зберігаючи при цьому peer-to-peer характер протоколу Bitcoin. Головною метою Lightning Network є масштабування і швидша робота мережі, зокрема, здійснення «блискавичних» мікроплатежів з більш низькими, ніж при звичайних транзакціях, комісіями. Якщо говорити просто, Lightning Network дозволяє користувачам проводити транзакції безпосередньо між собою, не записуючи інформацію в публічний Blockchain. Таким чином вирішуються відразу два завдання: більш швидкі і дешеві транзакції, а також скорочення обсягу даних Blockchain. Крім того, ця технологія сприяє більшій анонімності користувачів.

Результати дослідження

На початку грудня 2017 року, коли основна увага крипто-спільноти була прикута до стрімкого зростання цін на cryptocurrency, багато хто просто не помітили новину про те, що команди Blockstream, Lightning Labs і ASINQ домоглися сумісності своїх імплементацій протоколу, під назвою Lightning Network. В ході тестування роботи протоколу, була здійснена мікротранзакція на суму 0,015 mBTC між нодами Blockstream та C-Lightning і онлайн-кав'ярнею ASINQ Starblocks, що продає напій «блокачіно» [1]. Друга транзакція була створена для того, щоб розблокувати пост в блозі на контент-платформі Yalls. В процесі був задіяний гаманець ASINQ Eclair, за допомогою якого через C-Lightning в Yalls була відправлена невелика комісія. Будучи визнаним одним із найбільш ефективним рішенням щодо збільшення масштабування, яке в даний час вже використовується, мережа Lightning ефективно створює шар поверх протоколу Bitcoin, забезпечуючи швидкі та надійні транзакції, які можуть повністю розраховуватися з основним блокчейном Bitcoin. Ідея була запропонована Джозефом Пуном і Таддеус Дрієй в white paper, яка була опублікована ще в 2015 году [2]. Вони надали протокол, який знаходиться на вершині ланцюжка Bitcoin і в кінцевому підсумку ґрунтується на ній. Мережа складається з створених користувачами каналів, які відправляють платежі безпечним способом (відсутність довіри означає, що потреба в довірі або навіть знанні свого контрагента повністю відпадає). Платіжні канали необхідні для здійснення транзакцій між користувачами, які надають можливість фіксувати кінцевий стан в основну мережу Blockchain.

Для детального розгляду, спочатку потрібно зрозуміти, як влаштований протокол Lightning Network і та частина, яка відповідає за Trustless. Тепер потрібно поглибиться в «Теорію ігор», базовим завданням якої є «Теорема в'язня» [3]. За легендою є дві людини, які потрапили до в'язниці. Вони знаходяться в окремих камерах, і природно у них немає можливості поговорити і домовиться, про подальші їх дії. Вони для себе повинні вирішити, що вони роблять, зізнатися в скоєному або мовчати, і тим самим підставити свого содельніка. У цій ситуації є кілька можливих варіантів подій. Якщо вони разом будуть заперечувати свою провину, то обидва отримають по 1 року ув'язнення, вторимо варіантом буде, якщо один з ув'язнених визнається, а інший буде заперечувати провину, то тоді відбувається договір зі слідством, і людина, яка визнається отримає умовно-дострокове звільнення, а спільник, який не визнав свою провину отримає великий термін ув'язнення. Третім варіантом подій буде якщо вони обидва зізнаються і отримають по 8 років ув'язнення. Важливо не забувати, що у них немає можливості домовиться про план дій, кожен з них буде діяти індивідуально, і скоріше за все вони будуть здавати один одного і тоді обидва отримають по 8 років в'язниці. Але найкращим варіантом було б просто говорити неправду і згодом отримати по одному року ув'язнення.

	Зізнатися	Казати неправду
Зізнатися	-8; -8	0; -10
Казати неправду	-10; 0	-1; -1

Рис. 1 – Можливі варіанти подій

На рис. 1 показано можливі варіанти подій. Тепер мова зайде про таку цікаву особливість як «Ефективність по Парето». Якщо вирішується завдання по ефективності, то тоді вигідніше за все обом суб'єктам говорити неправду. Якщо вирішується завдання максимізації, тоді вигідніше за все кожному з них зізнатися і це буде так звана рівність по «Nash», це така ситуація, в якій жоден із суб'єктів не може максимізувати свій власний прибуток. Вони можуть разом зізнатися в скоєному, і обидва програють. Якщо зрівняємо це з ефективністю по Парето, то з точки зору теорії ігор вони вчинять правильно, але не максимально ефективно. Виходячи з таких ігор, є можливе рішення в протоколі LN, де у суб'єктів є можливість спілкуватися між собою, є можливість домовлятися про свої дії. У Lightning Network, якщо розглядати один платіжний канал з точки зору теорії ігор; два користувача повинні покласти певну кількість (припустимо BTC) в платіжний канал. Якщо все буде йти як було задумано, то обидва користувачі будуть залишатися при своєму, якщо один з них захоче порушити договір, то виникає ризик залишитися без своїх коштів. Це дозволяє бути впевненим що всі гратимуть за правилами, тому, що нікому не вигідно порушувати договір. У LN є кілька методів, які відновлюють баланс, але жоден з них не є ідеальним. Представлені приклади дозволять поглянути на поточні інновації в цій області. Існує два основні методи обходу проблеми перебалансування: «*сплайсинг*» для внутрішньомережевих, і «*циклічні платежі*» для зовнішньомережевих [4].

Найпростіший метод – це відкривати і закривати канали, повертати їх, і починати заново. Цей метод вимагає, як плати за з'єднання, так і часу для кожного каналу (а також часу підтвердження в основний ланцюжку Blockchain). Користувач повинен постійно відкривати і закривати канал, що є незручним рішенням, навіть незважаючи на те, що, це буде самим простим варіантом. Іншим варіантом буде рішення використання методу ланцюжка, яке називається «сплайсинг», що представляє собою кілька більш ефективних способів використання функціональності відкриття і закриття ланцюжка. Для прикладу, використовується ситуація, коли у Боба є 1 BTC в своєму каналі з Алісою, і Чарлі хоче відправити 1 BTC Алісі. У цьому прикладі, у Чарлі є 3 BTC в його каналі відправки з Бобом.

Чарлі 3 → 3 Боб 1 → 3 Аліса

↓

↓

Чарлі 2 → 4 Боб 0 → 4 Аліса

Виходячи з цієї ситуації, якщо Чарлі хоче відправить Алісі більше 1 BTC, то він цього не зможе зробити, тому, що у Боба не залишиться залишку коштів в його каналі з Алісою. *Сплайсинг*, дозволяє Бобу закрити свій канал з Чарлі і відкрити його в два етапи. Першим етап, має на увазі, що Бобу потрібно закрити свій канал з Чарлі і повернути його з 3 BTC, зберігаючи при цьому 1 BTC в ланцюжку, це еквівалентно 4 загальним BTC, які він мав раніше.

Чарлі 2 → 3 Боб 0 → 4 Аліса
1 BTC на каналі (Боба)

У другому етапі, Боб закриває свій канал з Алісою і додає 1 BTC, який знаходиться в каналі після «*сплайсингу*», що приводить до наступної ситуації:

Чарлі 2 → 3 Боб 1 → 4 Аліса

Користувач Боб, тепер може перенаправляти платіж з 1 BTC або менше між Чарлі і Алісою знову. Проте, Боб отримує два окремих платежі по каналі за проведення двох етапів «*сплайсингу*». Такий користувач в праві знімати невелику плату через те, що він є вузлом маршрутизації між Чарлі і Алісою.

Наведений приклад показує, що «*сплайсинг*» більш ефективний метод, ніж просте закриття і повторне відкриття каналів між сторонами, оскільки в цьому може брати участь лише один вузол (в цьому випадку таку роль відведено користувачеві Бобу). Незважаючи на підвищену ефективність, цей метод як і раніше несе витрати у вигляді комісії і вимагає часу підтвердження транзакції усередині мережі, що не дуже добре для окремих вузлів LN. Структури оплати з цього методу також призводять до подальших складнощів перебалансування.

Висновки

Lightning Network теоретично дає можливість масштабувати Bitcoin до безкінечного кількості транзакцій. Проблематичність полягає в тому, що є ліміт на відкриття каналів, так як блок формується раз в 10 хвилин, і якщо всі транзакції в блоці будуть для відкриття каналів, то в цьому випадку знадобиться багато часу, щоб забезпечити кожного користувача хоча б одним каналом. Для вирішення цієї проблеми, було імплементовано «підпис Шнорра», для зниження кількості даних необхідних для одного виходу. Також CoinJoin і його модифікації можуть допомогти з рішеннями проблем, які є у LN [5]. Все це дасть можливість використовувати блискавичну мережа не як мережу другого рівня над протоколом Bitcoin, а вже як мережу третього рівня над «Sidechain» або «Drivechain», які матимуть велику пропускну здатність і дадуть можливість каналам LN відкриватися в дочірні мережі, а не в основній мережі Bitcoin.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://forklog.com/stanet-li-lightning-network-otvetom-bitkoina-na-nizkie-komissii-altkoinov/
2. https://forklog.com/lightning-network-reshenie-problemy-masshtabirovaniya/
3. https://www.youtube.com/watch?v=BY6blBxH9bA&list=PLhZQuknA7yUBt82ow8rEfw_G8tNZjt3qB&index=25&t=533s
4. https://blockonomi.com/lightning-network-advances-hurdles/
5. https://forklog.com/lightning-network-reshenie-problemy-masshtabirovaniya/

Левкін Артем В'ячеславович — аспірант кафедри радіотехніки, Вінницький національний технічний університет, Вінниця, e-mail: **artem.levkin13@gmail.com**

Науковий керівник: ***Осадчук Олександр Володимирович*** — д-р техн. наук, професор, завідувач кафедри радіотехніки, Вінницький національний технічний університет, м.Вінниця, e-mail:osadchuk.av69@gmail.com

Levkin Artem Vyacheslavovich — graduate student of the Department of Radio Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: artem.levkin13@gmail.com

Supervisor: **Osadchuk Alexander Vladimirovich** — Dr. Tech. Sciences, Professor, Head of the Department of Radio Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: osadchuk.av69@gmail.com