Аналіз функціональності платіжного протоколу Lightning Network

Анастасія Сапожкова[1], Олександр Сєвєрінов[1], Андрій Власов[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14,
E-mail: anastasiia.sapozhkova@nure.ua,
E-mail: oleksandr.sievierinov@nure.ua

2. Науковий центр Повітряних Сил, Харківський національний університет Повітряних Сил, УКРАЇНА, м. Харків, вул. Клочківська, 228,
E-mail: vav_and@i.ua

***Коротка анотація** – Lightning is a decentralized network using smart contract functionality in the blockchain to enable instant payments across a network of participants. The Lightning Network is dependent upon the underlying technology of the blockchain. By using real blockchain transactions and using its native smart-contract scripting language, it is possible to create a secure network of participants which are able to transact at high volume and high speed.*

Ключові слова – Lightning Network; платіжна мережа; смарт-контракт; блокчейн.

I. Вступ

Lightning Network - це технологія, що дозволяє трансформувати будь-яку криптовалюту в швидкий і надійний платіжний засіб з мінімальними комісіями. Її розробили двоє програмістів: Джозеф Пун і Тедж Дрійа в 2016 році, активна фаза тестування і запуску почалася тільки в кінці 2017 року. Lightning Network планується використовувати для проведення мікроплатежів у біткоїні (і інших криптовалютах) і розвантаження його основної мережі. Завдяки використанню цієї технології кількість транзакцій в секунду може збільшитися в сотні тисяч разів, а комісія за переказ зведеться до мінімальних значень або зовсім буде дорівнювати нулю.

Типова транзакція в мережі біткоін виглядає так: відправник хоче перевести певну суму в BTC одержувачу і щоб все пройшло гладко, він повинен заплатити чималу комісію, яка йде іншому учаснику мережі в якості нагороди за включення транзакції в блок. Транзакція стає в чергу - відправник і одержувач чекають, поки вона запишеться в блок, і тільки тоді отримують кінцевий результат. Все це є побічними ефектами малого розміру блоку (всього 1 Мб для біткоін-мережі) і величезної кількості транзакцій в черзі [1].

Lightning Network вирішує цю проблему за допомогою так званих «каналів оплати». Технологія дозволяє налаштувати окремі мережі між двома учасниками основної мережі, внутрішні транзакції яких не будуть записуватися в блокчейн, а тільки зберігатися в рамках мережі каналу. Це означає, що користувачі можуть здійснювати скільки завгодно транзакцій між собою, не завантажуючи основну мережу.

При роботі за такою схемою в блокчейн записується тільки факт відкриття і закриття каналу с вказаним початковим і кінцевим балансом сторін, а всі транзакції, що пройшли по каналу, не займають місце у блокчейні. Така мережа може працювати не тільки з двома учасниками - вона запросто масштабується до будь-якого розміру, поєднуючи відправників і одержувачів ланцюжком в один канал, вибираючи оптимальний маршрут. Важливий момент: мережа пересилає по каналам не кошти, а тільки інформацію про володіння ними, тобто, згадану вище розписку, адже для відкриття каналу потрібне внесення сторонами певного депозиту.

II. Вирішення проблеми та результати

Network - це peer-to-peer платіжна мережа для проведення мікротранзакцій, що підтримує такі криптовалюта, як Bitcoin, Ethereum, Litecoin. Завданням цієї мережі є прискорення кріптовалютних платежів без делегування володіння грошима третій стороні, а також об'єднання різних криптовалюта в єдину мережу з прикордонними точками у вигляді децентралізованих бірж.

Двома елементами будь-peer-to-peer мережі є вузол і з'єднання:

– під вузлом в Lightning Network може розумітися мобільний додаток / десктоп програма / серверне ПЗ, яке підтримує протокол спілкування Lightning Network. Одним з таких прикладів є реалізація на мові Go;

– під з'єднанням в Lighting Network розуміється платіжні канал - відношення між учасниками, яке реєструється в блокчейн і регулюється смарт-контрактом.

Кожен вузол має можливість приймати і відправляти платежі, а також виступати в ролі провідника платежів, отримуючи за це комісію. Надіслати платіж від одного учасника мережі до іншого можна тільки в разі наявності шляху, що складається з платіжних каналів, що з'єднує одержувача і відправника. За допомогою можливості взяття комісії за проведення платежу, в мережі стимулюється створення вузлів, які з'єднують між собою безліч інших користувачів. В якості таких вузлів в майбутньому можуть виступати біржі і онлайн гаманці, а також інші організації, які будуть будувати свої послуги на основі даної технології.

Відмінність Lightning Network від таких мереж як Visa і MasterCard полягає в тому, що приєднатися до неї може будь-хто. Досягається це властивість "відкритості" за допомогою використання смарт-контрактів. Також варто врахувати, що в Lightning Network вбудовані алгоритми, подібні мережі Tor, тому одержувач і відправник платежу не відомі вузлів-провідникам. Як саме досягаються ці властивості, описано в технічних частинах даного циклу статей.

Lightning Network може бути застосована до будь-якого блокчейну, який підтримує деякі основні можливості, такі як мультипідписні транзакції, мітки часу та основні смарт контракти.

Якщо LN розташована на вершині мережі біткойн, мережа біткойнів може значно збільшити ємність, конфіденційність, деталізацію та швидкість, не жертвуючи принципами довірчої операції без посередників.

Конфіденційність. Платежі мережі Lightning Network є набагато приватнішими, ніж платежі на блокчейні біткойн, оскільки вони не є загальнодоступними. Хоча учасники маршруту можуть бачити платежі, поширювані по їх каналах, вони не знають відправника або одержувача.

Перемінність. LN робить набагато складніше застосовувати спостереження та чорні списки на біткойні, що підвищує взаємозв'язок валюти.

Швидкість. Транзакції Bitcoin з використанням мережі Lightning Network вирішуються за мілісекунди, а не за хвилини, оскільки HTLC видаляються без здійснення транзакцій до блоку.

Гранулярність. LN може дозволити платежі, принаймні настільки малі, як обмеження "пилу" біткойн, можливо, навіть менше. Деякі пропозиції дозволяють збільшувати субстатоші.

Потужність. LN збільшує місткість біткойн-системи на кілька порядків. Немає практичної верхньої межі кількості платежів в секунду, яку можна прокладати через LN, оскільки це залежить тільки від потужності та швидкості кожного вузла.

Безтурботна операція. LN використовує транзакції bitcoin між вузлами, які працюють як рівні, не довіряючи один одному. Таким чином, мережа Lightning зберігає принципи роботи системи біткойн, значно розширюючи її робочі параметри.

Як згадувалося раніше, протокол мережі Lightning Network - це не єдиний спосіб запровадження маршрутизованих платіжних каналів. Інші пропоновані системи включають Tumblebit і Teechan. Однак у цей час LN вже була розгорнута на тест-мережі. Кілька різних команд розробили конкуруючі реалії LN і працюють над єдиним стандартом сумісності (так званий BOLT). Цілком імовірно, що LN буде першою мережею каналів розрахункових каналів, яка буде розгорнута у виробництві.

У 2015 році проект Bitcoin зіткнувся з проблемою, яка полягала в масштабуванні. Мережа не могла обробляти більшу кількість транзакцій щосекунди, ніж встановлений ліміт в 3-7 операцій. Цей ліміт закладений в саму концепцію створення платформи, а саме збільшення показників пропускної здатності системи за допомогою збільшення блоків призвело б до зниження ефективності принципів децентралізованого управління криптовалютою, оскільки єдина точка відмови відсутня.

Розробники застосували для вирішення даної проблеми кілька різних схем, що в результаті призвело до створення форку Bitcoin Cash і поділу блокчейна, при цьому сам Bitcoin почав використовувати масштабування через Lightning Network.

Таким чином, за допомогою опису функціональності продукту Lightning Network, йому можна дати наступне визначення: проект являє собою розробку, орієнтовану на підвищення пропускних показників біткоін-мережі при досягненні частоти операцій, яку можна порівняти з показниками мережі Visa.

Висновок

Останні кілька років технологія блокчейн все більше застосовується сучасним суспільством. Блокчейн – розподілений електронний реєстр, в якій реєструється кожна транзакція, яка відбувається в системі. Блокчейн має змогу вирішувати проблеми такі як: безпека, висока доступність та швидкість виконання транзакцій[2].

Як було вже зазначено, досить часто користувачами даної технології є цифрові валюти, не виняток і найвідоміша з них – біткоін. Ринок цифрових валют досить швидко розвивається, так максимальна капіталізація ринку криптовалют складала 190 млрд. доларів. Проте це не єдине ефективне застосування цієї технології, так, ринок стартапів на базі використання технології blockchain, за оцінками експертів, залучить у 2018 році інвестицій на суму 3 млрд. доларів, що цілком впевнено робить технологію альтернативою традиційним венчурним інвестиціям.

Варто звернути увагу, що використання технології блокчейн викликає зацікавлення і в Україні. Так стало відомо, що Україна уклала угоду з міжнародною технологічною компанією Bitfury Group про переведення всіх електронних державних даних на блокчейн.

Таким чином стає зрозуміло, що технологія Blockchain є певною мірою революційною та може бути використана в різних сферах людської діяльності. Зокрема, мова йде про такі реалізації як: криптовалюти, різного роду реєстри, корпоративного, або ж державного значення. Але у криптовалют, зокрема у біткойна, є великий недостаток – пропускна здатність. Через це виникає велика кількість технологій, що намагаються виправити цю проблему. Найвиразнішою та найперспективнішою з таких є технологія Lightning Network.

Література

[1] Andreas M. Antonopoulos Mastering Bitcoin: Unlocking Digital Cryptocurrencies / Andreas M. Antonopoulos – K. : NGITS, 2014. – С. 150 – 290.

[2] Don Tapscott, Alex Tapscott Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott, Alex Tapscott Blockchain – K. : Information Systems, 2016 – С. 100 – 150.