УДК 004.75
Врублевич І. – ст. гр. СНнм-61
Тернопільський національний технічний університет імені Івана Пулюя

РОБОТА МЕТОДІВ ТРАНЗАКЦІЙ В БЛОКЧЕЙН-СИСТЕМІ НА ОСНОВІ КОНСЕНСУСУ PROOF OF REPUTATION

Науковий керівник: доцент, к. т. н. Марценко С.В.

Vrublevych I.
Ternopil Ivan Puluj National Technical University

WORKING OF TRANSACTION METHODS IN A BLOCKCHAIN SYSTEM BASED ON PROF OF REPUTATION CONSENSUS

Supervisor: associate professor, Ph.D. in Technical Sciences Serhii Martsenko

Ключові слова: блокчейн, мемпул, транзакція, JSON
Keywords: blockchain, mempool, transaction, JSON

Основні елементи архітектури блокчейн-системи, що використовує модель Proof of Reputation включають блокчейн, вузли мережі, механізм репутації, система управління транзакціями і сам алгоритм консенсусу. Блокчейн виступає в ролі розподіленого реєстру, який включає блоки з транзакціями, пов'язані між собою криптографічним хешем [1]. Кожен вузол у мережі повинен брати активну участь у процесах валідації транзакцій та блоків. На рис. 1 зображено процес транзакції в блокчейн-системі, починаючи від етапу відправки транзакції до її фінального додавання в блокчейн. Для розробки використана мова Pytnon із бібліотеками.

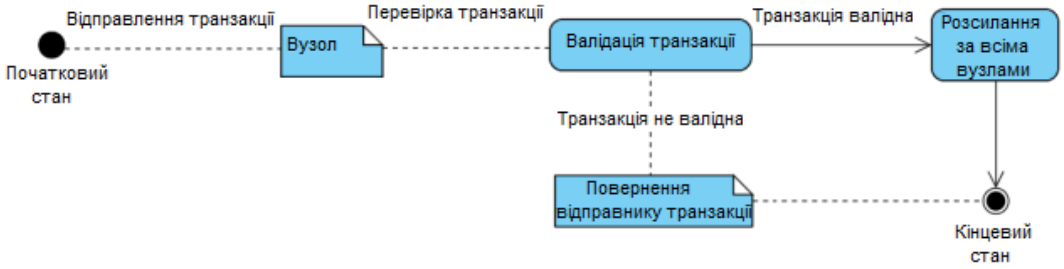

Рисунок 1 – Процес транзакції

Для надсилання користувачем нових транзакцій був реалізований декоратор @app.route який має як вхідний аргумент маршрут /transactions/new та http метод POST. Метод new_transaction обробляє створення нових транзакцій через web -інтерфейс. Цей асинхронний метод приймає POST -запити та використовується для додавання транзакцій до мемпулу блокчейн-системи. Коли користувач надсилає запит на цей маршрут, метод спочатку отримує дані транзакції з тіла запиту за допомогою request.get_json(). Дані транзакції організовані в JSON форматі, де ключі відповідають різним атрибутам транзакції, таким як відправник, одержувач і сума переказу. Метод перевіряє, що всі необхідні поля присутні у даних транзакції, що забезпечує їхню повноту та коректність. Якщо у цих даних відсутнє хоча б одне обов'язкове поле, метод повертає відповідь з кодом стану HTTP 400, вказуючи на помилку у наданих даних. Це

запобігає додаванню неповних чи некоректних транзакцій до списку непідтверджених транзакцій. Після перевірки та підтвердження повноти даних транзакція збагачується інформацією про поточний сайт, який обробляє запит. Далі транзакція асинхронно додається до списку непідтверджених транзакцій блокчейну з за допомогою функції create_task, яка дозволяє обробляти додавання транзакції у фоновому режимі. Це покращує продуктивність системи. Метод завершується відправкою підтвердження про успішний прийом транзакції в форматі JSON, з повідомленням про статус та код стану НГГР 201, що означає успішне створення ресурсу. Це підтвердження є сигналом для користувача про те, що його транзакція була коректно прийнята та додана до списку непідтверджених транзакцій для подальшої обробки.

Метод add_to_mempool асинхронно керує процесом додавання транзакцій до мемпулу блокчейн-системи. Спочатку метод виконує перевірку вхідної транзакції, використовуючи метод validate_transaction. Ця функція перевіряє відповідність транзакції певним критеріям (наявність усіх необхідних даних та їх коректність). Перевірка гарантує, що тільки допустимі та повні транзакції будуть оброблені та додані до списку непідтверджених транзакцій. Після перевірки метод витягує ключ, надає унікальний ідентифікатор транзакції зі словника даних транзакції. Ключ є для того, щоб переконатися, що транзакція не була додана до списку непідтверджених.

Якщо ж транзакції ще не має у списку непідтверджених, вона додається туди, зберігаючись за своїм унікальним ключем. Після успішного додавання транзакції до списку непідтверджених, метод ініціює асинхронне розсилання цієї транзакції іншим вузлам у мережі за допомогою методу broadcast_transaction. Ця операція поширює інформацію про нову транзакцію через мережу, дозволяючи іншим вузлам отримати і додати цю транзакцію до своїх локальних списків непідтверджених транзакцій. Метод add_to_mempool забезпечує централізоване управління транзакціями в очікуванні їх обробки та включення до блоків.

Метод receive_transaction призначений для прийому транзакцій від інших вузлів через веб-інтерфейс. Цей метод асинхронно обробляє вхідні запити POST, що містять транзакції, і додає їх до списку непідтверджених транзакцій. Коли вузол блокчейн-мережі відправляє транзакцію іншому вузлу, він використовує HTTP POST-запит з даними транзакції у форматі JSON. При отриманні такого запиту метод receive_transaction спочатку отримує дані транзакції з тіла запиту через виклик request.get_json(). Перш ніж транзакція буде додана в список непідтверджених, важливо переконатися, що запит дійсно надходить від одного з вузлів мережі, а не від неавторизованого джерела. Потрібно перевірити №-адреси відправника запиту на відповідність списку відомих вузлів блокчейну. Цей крок критично важливий для безпеки та надійності системи. Після перевірки та підтвердження того, що транзакція надійшла від довіреного вузла, метод викликає функцію add_to_mempool, щоб додати транзакцію до списку непідтверджених. Функція add_to_mempool перевіряє валідність транзакції, і якщо вона проходить всі перевірки, транзакція додається до списку непідтверджених для подальшої обробки. Завершує роботу методу надсилання відповіді у форматі JSON, який підтверджує успішне додавання транзакції до списку непідтверджених.