УДК 004.75

РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИМУЛЯТОРУ ДЛЯ ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ PROOF-OF-WORK

Соловйова Діана Вячеславівна
доктор технічних наук, професор, директор ІКС Антощук Світлана Григорівна
Національний університет «Одеська Політехника», УКРАЇНА

АНОТАЦІЯ. У даній роботі представлено методику вдосконалення технології блокчейну *Proof-of-work*. Запропоновано використовувати симулятор, що імітує поведінку реальних вузлів мережі блокчейну, сумісно з додатковою конфігурацією, що налаштовується, з метою перевірки гіпотез, що покликані мінімізувати час, що витрачається на транзакцію.

Вступ. Технологія блокчейну, що являє собою багатофункціональну та багаторівневу інформаційну технологію, яка призначена для надійного зберігання, обліку та передачі інформації, є надзвичайно затребуваною та актуальною у сьогоденні. Технологія блокчейну охоплює всі сфери життя суспільства та має безліч сфер застосування, відкриває нові можливості з маніпулювання даними, забезпечуючи їхню конфіденційність, цілісність та безпеку, що є дуже цінним [1]. Аналізуючи технологію блокчейну, можна виділити один базовий механізм, що забезпечує її функціонування, – механізм консенсусу. З усіх відомих алгоритмів консенсусу найнадійнішим та найбезпечнішим є *Proof-of-Work* (*PoW*). Але, не дивлячись на усі переваги цього механізму консенсусу, він має великий недолік, що робить користування цим механізмом значно менш комфортним, – це задовгий час, що витрачається на підтвердження транзакції.

Мета роботи. Отже, для усунення проблеми з механізмом *Proof-of-Work*, що роздивляється у цій роботі, необхідно вирішити задачу – зменшення кількості часу, що витрачається на транзакцію. Це пропонується реалізувати шляхом розбиття системи на підмережі: коли консенсус приймається не всією спільнотою, а «групами» окремо. Саме таким чином досягається мінімізація часу транзакції у алгоритмі *Proof-of-State (PoS*). Однак для динамічного механізму консенсусу *PoW* готового рішення, що б успішно застосовувалося у блокчейн-технологіях, нема [2]. Всі існуючі алгоритми розбиття блокчейн-мережі на підгрупи використовуються лише для статичних алгоритмів, проте *PoW* є динамічним та має певні особливості: у мережі PoW нема області видимості, користувач не бачить перелік вузлів та ін. Ці особливості значно ускладнюють реалізацію кластеризації для механізму консенсусу *PoW* [3]. Жоден з існуючих алгоритмів не реалізовує розподілення мережі *PoW* на підмережі з метою мінімізації швидкості часу. Цей процес є дуже складним, бо дуже важко виявити необхідні параметри для моделювання такої мережі.

Основна частина. Задачею даного дослідження є перевірка сформульованих гіпотез, що мають на меті саме збільшення швидкості транзакції. Для перевірки запроновано змоделювати модельну мережу блокчейну з метою проведення експериментів та тестування гіпотез, що потенційно можуть вирішити проблему з *PoW*. Проаналізовано метрики, що характеризують продуктивність роботи мережі блокчейну. Наведено конкретні існуючі числові значення. Мета роботи полягає в покращенні таких метрик як транзакції за секунду, зменшення затримки транзакції, збільшення пропускної здібності, проте обов’язково не погіршити показники енергоефективності та час блокування.

Для здійснення необхідних експериментів та моделювання мережі блокчейн пропонується використати симулятор мережі, що побудована на механізмі консенсусу *PoW*, але з додаванням додаткових конфігурацій, що налаштовуються з метою проведення тестування гіпотез. Симулятор мережі блокчейну складається з двох частин: *P2P* мережа (децентралізована однорангова мережа) та протокол *PoW*. Він дозволяє будувати мережеві топології у блокчейні (рис. 1) та проводити з ними різні маніпуляції, при цьому фіксуючи результати [4]. Програмне забезпечення симулятора реалізовано як веб-додаток на JavaScript, що складається з чотирьох

основних класів: *Network, Miner/node, NetworkBuffer* і *Block/Header*. Клас мережі інкапсулює всі інші екземпляри класу та відповідає за підтримку параметрів мережевого рівня *P2P* [5]. Клас підтримує параметри рівня консенсусу *PoW*, а також *NetworkBuffer*, який діє як маршрутизатор, що з'єднує вузли. Блокчейн-реєстри зберігаються в Майнері та реалізовані як масив/зв'язаний список заголовків блоків. Вузли побудовані з функціями для видобутку, широкомовної передачі інформації, надсилання/отримання заголовків блоків і підтримки структури зв'язування блоків у блокчейні [6].

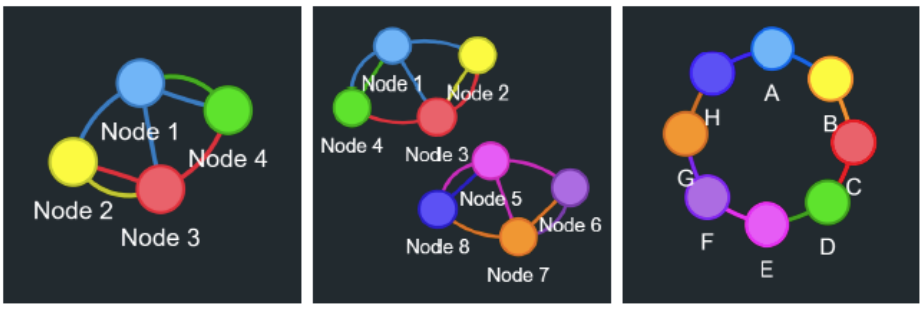

Рисунок 1 – Створення моделей мережевий топологій у симуляторі

Симулятор мережі блокчейну пропонує широкий спектр можливостей і особливостей для проведення досліджень у сфері мереж і майнінгу криптовалюти. Ми використовуємо симулятор для аналізу конкретних сценаріїв, щоб виділити функції та можливості. Пропонується розробити додаткову конфігурацію, що налаштовується, з метою перевірки наступних гіпотез. Щоб встановити необхідні конфігурації для моделювання системи та розширення можливостей симулятора мережі блокчейн, проаналізуємо задачу мінімізації часу транзакції у мережі з механізмом консенсусу PoW. Маємо задачу розбиття системи на підсистеми, задачу моделювання псевдомережі. Під час моделювання системи треба урахувати область видимості: можливість зважування, таблиця відстаней. Рахуємо діаметр групи (діаметр кластера *d*), максимальна відстань у групі <= *d*. Урахувати також важливо кількість зв'язків вузлів та наявність у мережі повнозв'язних вузлів та вузлів з декількама зв'язками. Для кожного з подібних елементів – це окремий випадок. Та під час даного моделювання важливим є обрання критерію, що має характерізувати підгрупи. Ряд вузлів об'єднуються у групу – так звані «кристали» (центри кристалізації) – поки цей критерій виконується. Масив критеріїв представлено вузлами.

У ході дослідження та моделювання має бути реалізовано ідею «динамічного розбиття на групи». Система розбивається на підсистеми – групи. Це розбиття відбувається дінамично. Розбиття реалізуємо наступним чином. Спочатку у певній групі розрахуємо «потужність» групи. Та після визначення потужності виконаємо низку дій та отримаємо ознаки груп для майбутньої їхньої кластерізації. Визначаємо центр кристалізації за потужністю групи, звідси вузлам стає «вигідно» та «невигідно» підд'єднатися до певних груп (через різну потужність груп). Тому з'являється поняття «переходу» вузла до іншої групи (окрашування груп та вузлів відповідними різними кольорами). Звідси постає задача створення правил переходу з одної групи в іншу для вузлів. Правила переходу з одної групи до іншою встановимо власні та будемо тестувати їхню ефективність у створеній моделі динамічної системи. Наприклад, встановимо правило: перехід до іншої групи є можливим не раніше 10 публікацій блоків для певного вузла; або перехід до іншої групи не можливий раніше 5 фіналізацій для вузла тощо.

З цього випливає список конкретних параметрів-конфігурацій, що ми будемо змінювати в симуляторі мережі та спостерігати за поведінкою мережі блокчейн. По-перше, необхідно мати можливість самостійно задавати кількість вузлів, груп, потужність вузлів та відстані між ними. Це має бути гнучка модель, щоб змінювати відстані, потужність під час тестування гіпотез та проведення експериментів для мінімізації часу транзакцій. В рамках даного дослідження створено модель мережі 10x10 на 100 вузлів з метою проведення експериментів для перевірки гіпотез. Наступним кроком є обрання та тестування алгоритмів кластерізації мережі. Їхнє

вивчення, розрахування діаметру кластерів, що знаходяться в мережі та реалізація моделі переходу вузлів з одної групи до іншої, правил переходів, перекрашування вузлів.

Висновки. Отже, у ході даного дослідження розроблено симулятор мережі блокчейн та протестовано його застосування для удосконалення технології блокчейну *Proof-of Work* з метою зменшення часу, що витрачається на транзакцію, тестування відповідних гіпотез. Використано симулятор, побудована мережа на механізмі консенсусу *PoW*, з додаванням додаткових конфігурацій, що налаштовуються. Таким чином, дане дослідження розширює усі попередні можливості моделювання мережі блокчейн. У ході подальшого дослідження буде проведено моделювання поведінки біткойнів шляхом моделювання мережевої топології, де буде проімітовано поведінку реальних вузлів та реалізовано ідею «динамічного розбиття на групи» шляхом встановлення необхідних конфігурацій з метою дослідження, яким чином макети впливають на розподілений консенсус системи в цілому, і відповідно буде вимірено результати з метою отримання необхідних висновків щодо тестування гіпотез.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. International Journal of Mechanical and Production Engineering Research and Development. URL: https://www.scopus.com/sourceid/21100814505 (дата звернення: 29.03.2023).
2. Leading SCIE and SCOPUS Indexed Journals in Blockchain Technology. URL: https://slogix.in/blockchain-technology/leading-journals/ (дата звернення: 17.04.2023).
3. What Is Proof of Work (PoW) in Blockchain? URL: https://www.investopedia.com/terms/p/proof-work.asp (дата звернення: 18.04.2023).
4. J. Kim, M. Nakashima, W. Fan, S. Wuthier, X. Zhou, I. Kim, and S.- Y. Chang, “Anomaly detection based on traffic monitoring for secure blockchain networking,” in International Conference on Blockchain, 2021 (дата звернення: 25.04.2023).
5. Blockchain – Proof of Work (PoW). URL: https://www.geeksforgeeks.org/blockchain-proof-of-work-pow/amp/ (дата звернення: 28.04.2023).
6. E. W. Zegura, K. L. Calvert, and S. Bhattacharjee, “How to model an internetwork,” in Proceedings of IEEE INFOCOM’96. Conference on Computer Communications, vol. 2. IEEE, 1996, pp. 594–602 (дата звернення: 28.04.2023).

DEVELOPMENT AND RESEARCH OF A SIMULATOR TO IMPROVE PROOF-OF-WORK BLOCKCHAIN TECHNOLOGY

Diana Soloviova

doctor of technical sciences, professor, director of ICS, Svetlana Antoshchuk

Odessa Polytechnic National University, UKRAINE

ANNOTATION. This paper presents the method of improving Proof-of-work blockchain technology. It is proposed to use a simulator modelling the behavior of real blockchain network nodes, compatible with additional configurable configuration, in order to test hypotheses designed to minimize the time spent on a transaction.