DOI https://doi.org/10.36059/978-966-397-479-8-124

ОБГРУНТУВАННЯ НАДІЙНОСТІ МЕХАНІЗМУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ПІДМІНИ ТА ВИДАЛЕННЯ В БЛОКЧЕЙН-МЕРЕЖАХ

Горелікова Т. О.
аспірантка
Запорізький національний університет
м. Запоріжжя, Україна

Блокчейн-технології, зокрема їх використання в системах, що забезпечують зберігання і передачу данних, набули значного поширення завдяки своїй прозорості та стійкості до атак. Для забезпечення надійності та ефективності в блокчейн-системах важливим аспектом є процес валідації нових блоків, коли перевірка правильності транзакцій та додавання нових блоків до мережі здійснюється через певний алгоритм консенсусу та процес валідації вже існуючої мережі під час кожної транзакції. Блокчейн-мережа з випадковим вибором вузлів для перевірки блоків поєднує в собі інноваційний механізм децентралізації, криптографічну надійність та високу ефективність. Основною ідеєю є використання алгоритмів еліптичних кривих для генерації випадкових чисел, які визначають вузли, що перевірятимуть блоки. Такий підхід розподіляє навантаження в мережі, знижуючи обчислювальні витрати й підвищуючи масштабованість системи.

Головний процес механізму починається із створення нового блоку майнером. Для його перевірки обирається обмежена кількість випадково визначених вузлів. Випадковість вибору може гарантувати, що перевірка буде неупередженою, а використання хеш-функцій підвищує криптографічну стійкість. Завдяки цьому блокчейн стає менш вразливим до атак, спрямованих на компрометацію певних вузлів.

Особливу роль у цьому підході відіграють вузли повного типу, які у традиційних блокчейнах перевіряють увесь ланцюг блоків. У новій моделі випадкові вузли перевіряють лише випадково обрані ділянки ланцюга(блоки), що значно знижує їхнє навантаження. Для забезпечення цілісності використовуються структури Merkle-дерева, які дозволяють швидко і точно визначати змінені блоки.

Цей підхід створює баланс між продуктивністю та безпекою, адже навіть часткова перевірка гарантує, що всі ділянки блокчейну будуть охоплені. Завдяки криптографічним методам зловмисникам майже

неможливо передбачити, які вузли або блоки будуть перевірятися, що суттєво підвищує захист системи [1–4].

Для проведення дослідження було стоворено кілька тестових блокчейн-систем, що використовують механізм випадкового вибору вузлів для валідації. Аналіз проводився за допомогою різних інструментів моніторингу та моделей симуляцій. Ось ключові технології та інструменти, що використовувались під час дослідження:

1. Тестові блокчейн-системи: Для тестування були створені кілька тестових копій блокчейн-мереж, які використовують консенсус Proof of Work (PoW) і впроваджено в них розроблений метод з різною конфігурацією. Ці системи включали публічні блокчейн мережі з відкритим кодом середнього рівня (300–700 вузлів).

2. Моніторинг безпеки: Для оцінки рівня безпеки використовувались інструменти, такі як Chainalysis та BlockCypher, які дозволяють здійснювати глибокий аналіз транзакцій у блокчейні та виявляти аномалії, такі як спроби атаки або маніпуляції з даними. За допомогою цих інструментів було здійснено аналіз транзакцій у різних блокчейн-мережах, щоб оцінити рівень захищеності під час застосування механізму випадкового вибору вузлів для валідації.

3. Моделювання за допомогою Python: Для проведення симуляцій та аналізу ефективності впровадженого механізму використовувались бібліотеки NumPy та SciPy в мові програмування Python. За допомогою цих інструментів було змодельовано різні варіанти атак на блокчейн-мережу та оцінено їхній вплив на стабільність і безпеку системи. Наприклад, було протестовано сценарії атаки 51%, коли зловмисники намагаються отримати контроль над більшістю вузлів мережі.

4. Симуляція атак та валідації: Моделювання включало створення різних сценаріїв атак, наприклад, атак типу Sybil, коли атакуючі створюють фальшиві вузли для контролю над мережею, і double-spending, коли транзакції намагаються бути витрачені двічі. Блоки та транзакції випадково розподілялися між вузлами для оцінки того, наскільки механізм випадкового вибору вузлів здатний протистояти таким атакам. Використовувався метод Monte Carlo для визначення ймовірностей успішних атак при різних умовах.

Результати тестів

1. Безпека: Протидія атакам

Одним з основних елементів дослідження була оцінка рівня безпеки блокчейн-систем з механізмом випадкового вибору вузлів. Це тестування включало аналіз ефективності захисту системи від атак за допомогою таких інструментів, як Chainalysis. Протестовані системи показали значне зниження успіху атак у порівнянні з системами, де для валідації блоків використовувались постійно закріплені вузли.

– За даними Chainalysis, серед усіх атак, що відбулися протягом тестування, лише 20% успішно досягли мети в системах з впровадженим методом, порівняно з 40% у традиційних системах.

– У системах з випадковим вибором кількість фальшивих вузлів, які змогли здійснити контроль над мережею, була на 30% меншою в порівнянні з традиційними системами.

2. Швидкодія системи

Тестування швидкодії показало, що метод підвищує швидкість роботи за рахунок зменшення обсягу перевірених даних на кожному вузлі. Замість повної перевірки ланцюжка блоків, кожен вузол типу повного типу перевіряє лише 10% – 30% випадково обраних блоків. Це дозволяє знизити навантаження на систему, зменшити час перевірки та покращити масштабованість. Для оцінки цього параметра використовувався інструмент BlockCypher, який дозволяє виміряти час між підтвердженням транзакцій та додаванням блоку до мережі.

Використання структури Merkle-дерева дозволяє перевіряти цілісність ланцюжка без повного аналізу даних. Корінь дерева містить єдиний хеш, який підтверджує цілісність всього ланцюжка. Якщо кореневий хеш збігається, перевірка завершується миттєво. У разі невідповідності лише кілька гілок потребують аналізу, що займає небагато часу.

3. Економія енергоресурсів

Енергетичні витрати є важливим аспектом для блокчейн-систем, оскільки перевірка транзакцій та додавання нових блоків потребують значної кількості обчислювальних потужностей. За результатами тестів, проведених за допомогою NumPy для моделювання навантаження, системи з випадковим вибором вузлів демонструють значно менше енергоспоживання.

Враховуючи симуляції, було визначено, що за рахунок оптимального розподілу навантаження енергоспоживання зменшується на 20% порівняно з системами з фіксованими вузлами.

4. Масштабованість

У тестах з великою кількістю вузлів час на валідацію блоків залишався стабільним і не перевищував межі, характерні для систем з фіксованими вузлами. Це свідчить про високу адаптивність системи до змін в її розмірі.

Прогнозування

Прогнозування результатів на основі отриманих даних свідчить, що в довгостроковій перспективі блокчейн-системи з випадковим вибором вузлів мають потенціал знизити рівень атак та значно покращити ефективність. Прогноз за допомогою методів регресії показав, що ймовірність успішних атак зменшиться на 25–30% за 2–3 роки використання технології.

Проведене дослідження показало, що механізм випадкового вибору вузлів і блоків для валідації блоків і усієї мережі у блокчейн-системах є потужним інструментом для підвищення безпеки, зниження енергетичних витрат та покращення масштабованості. Цей підхід може дозволити знизити ризики атак, покращити швидкодію системи та зробити її більш адаптивною до змін. Подальший розвиток такого механізму може значно покращити ефективність блокчейн-технологій у майбутньому.

Література:

1. Horelikova T. O., Choporov S. V. Analysis of Information Security Methods Against Substitution and Deletion Based on Blockchain Technology. *Computer Science and Applied Mathematics*. 2024. P. 54–66.

2. Jafari A., Aghajani M., Mohammadian A. Random Checkpointing Mechanisms in Blockchain Networks: Enhancing Data Integrity and Security. *Journal of Information Security and Applications*. 2022. No 63. P. 103–116.

3. Zhu Q., Liao L., Luo X. Blockchain Data Protection Through Randomized Validation Points: Theory and Applications. *IEEE Transactions on Information Forensics and Security*. 2022. Vol. 17. P. 421–435.

4. Hong X., Xu W. Ensuring Blockchain Security: Data Immutability and the Role of Random Checkpoints. *Information Systems*. 2023. No 106. P. 102–113.