УДК 004.56
Коваль М. – ст. гр. СНнм-51
Тернопільський національний технічний університет імені Івана Пулюя

КОНСЕНСУСНІ АЛГОРИТМИ В БЛОКЧЕЙНІ. ОПИС POW ТА POS

Науковий керівник: старший викладач Шимчук Г.

Koval M.
Ternopil Ivan Puluj National Technical University

CONSENSUS ALGORITHMS IN THE BLOCKCHAIN. POW AND POS DESCIPTION

Supervisor: Senior Lecturer Shymchuk G.

Ключові слова: блокчейн, консенсус, алгоритм, PoW, PoS.
Key words: blockchain, consensus, algorithm, PoW, PoS.

Консенсусні алгоритми в блокчейні – це механізми, які дозволяють учасникам децентралізованої мережі досягти загальної згоди щодо поточного стану розподіленого реєстру. Завдяки цим алгоритмам, блокчейн-мережі можуть функціонувати без потреби в довірі між учасниками та без централізованого органу управління. Два основних типи консенсусних алгоритмів включають Proof-of-Work (PoW) та Proof-of-Stake (PoS) [1].

PoW заснований на вирішенні складних математичних задач, які вимагають значної обчислювальної потужності. Учасники мережі (майнери) конкурують за додавання нових блоків до блокчейна, вирішуючи ці задачі. Виграє той майнер, який першим знайде правильне рішення (доказ роботи), і його блок додається до ланцюжка. Завдяки витратам на обчислювальні ресурси та енергію, PoW утруднює атаки на мережу, оскільки зловмиснику потрібно витратити більше ресурсів, ніж можна заробити в результаті атаки [2]. Цей процес також утруднює здійснення атаки "51%", оскільки атакуючому потрібно контролювати більше половини обчислювальної потужності мережі, що є дуже витратно. Одним з недоліків PoW є високі витрати на енергію, оскільки майнери конкурують за додавання блоків, використовуючи великі обчислювальні потужності. Це підвищує вартість участі в мережі та може призводити до концентрації майнінгу в країнах з низькими енергетичними тарифами, що може підривати децентралізацію мережі. У PoW-моделі, майнери отримують винагороду в криптовалюті за додавання блоків, що стимулює їх підтримувати безпеку та коректність транзакцій [1].

В PoS алгоритмі, учасники валідують блоки на основі їх "ставки" у криптовалюті мережі. Чим більше криптовалюти має учасник, тим більше ймовірність, що йому буде дозволено валідувати блоки та отримувати відповідні винагороди. Відповідно, учасники мережі мають стимул підтримувати безпеку мережі та коректність транзакцій, оскільки це підвищує вартість їхнього портфеля криптовалюти. PoS також забезпечує захист мережі від атак, оскільки зловмисники повинні володіти значною кількістю криптовалюти, щоб здійснювати атаки [2]. Це зменшує можливість успішної атаки "51%", оскільки атакуючий ризикує значними власними активами. Оскільки PoS не вимагає значних обчислювальних ресурсів для вирішення математичних задач, цей алгоритм є екологічним та енергоефективним альтернативним рішенням порівняно з PoW. У PoS-моделі, учасники-валідатори отримують винагороду у вигляді транзакційних комісій та, в деяких випадках, додаткових криптовалютних винагород. Це стимулює валідаторів підтримувати безпеку та стабільність мережі,

оскільки їхній прибуток залежить від вартості криптовалюти та кількості успішно валідованих транзакцій [3]. В PoS-моделі, відсутність вимоги до обчислювальної потужності сприяє децентралізації мережі, оскільки більше учасників може стати валідаторами, не вкладаючи значних коштів у спеціалізоване обладнання.

Важливо зазначити, що крім PoW та PoS, існує також ряд інших консенсусних алгоритмів, які варто розглянути в залежності від потреб проекту. Наприклад, Leased Proof-of-Stake (LPoS) алгоритм дозволяє учасникам з меншими ставками "орендувати" свої активи більш великим учасникам для підвищення їх шансів на валідацію блоків та отримання винагороди. Це сприяє активності спільноти та децентралізації [2]. Також варто звернути увагу на консенсусні алгоритми з роду Federated Byzantine Agreement (FBA), які використовуються в Stellar та Ripple. FBA використовує кворуми для досягнення консенсусу між надійними вузлами мережі, що дозволяє досягти високої масштабованості та швидкості обробки транзакцій [3].

Зважаючи на широкий спектр можливих консенсусних алгоритмів та їх характеристик, розробники блокчейн-проектів повинні ретельно вивчити кожен з них, змоделювати можливі впливи на їх додатки та уважно розглянути фактори, такі як безпека, масштабованість, енергоефективність, децентралізація та стійкість до атак [1]. Окрім того, при виборі консенсусного алгоритму, варто також враховувати специфіку регуляторного середовища, в якому буде діяти проект, а також ставлення спільноти та інвесторів до різних видів алгоритмів.

Останнім часом багато проектів розглядають можливість переходу від PoW до PoS або інших енергоефективних консенсусних алгоритмів через зростаючу увагу до питань екології та сталого розвитку [2]. Найвідомішим прикладом такого переходу є Ethereum 2.0, що включає PoS консенсусний алгоритм замість PoW. Цей перехід спрямований на підвищення масштабованості, енергоефективності та безпеки мережі.

Важливо враховувати, що кожний консенсусний алгоритм має свої відмінності та особливості, що можуть впливати на децентралізацію, безпеку та стабільність блокчейн-мережі [1]. Тому при розробці нових проектів або оцінці існуючих блокчейнів важливо ретельно вивчити можливості та обмеження різних консенсусних алгоритмів, щоб визначити найбільш підходящий варіант для конкретного застосування.

Підсумовуючи, консенсусні алгоритми, такі як PoW та PoS, відіграють важливу роль в блокчейн-технології, дозволяючи учасникам децентралізованої мережі досягти згоди про стан розподіленого реєстру. Вони відрізняються за принципами роботи, безпекою та енергетичною ефективністю. PoW забезпечує високу безпеку за рахунок значних витрат на енергію, тоді як PoS пропонує енергоефективну альтернативу, що може стимулювати більшу децентралізацію мережі. Обидва алгоритми мають свої переваги та недоліки, тому вибір між ними залежить від потреб та пріоритетів конкретного блокчейн-проекту.

Література:

1. Buterin V. A next-generation smart contract and decentralized application platform. Ethereum. / V. Buterin / Mathematics, 2013, 36 p.
2. Kiayias A., Miller A., Zindros D. Non-interactive proofs of proof-of-work. / A. Kiayias, A. Miller, D. Zindros / IACR Cryptology ePrint Archive, 2017, 963 p.
3. Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2018). Ouroboros Genesis: Composable proof-of-stake blockchains with dynamic availability. Cryptology ePrint Archive, Report 2018/378.