УДК 004.9
А. А. Титжинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПОРІВНЯЛЬНИЙ АНАЛІЗ КОНСЕНСУСНИХ АЛГОРИТМІВ У КОНТЕКСТІ ЇХНЬОЇ СТІЙКОСТІ ДО АТАК

UDC 004.9
A. A. Tytzhynskyi

COMPARATIVE ANALYSIS OF CONSENSUS ALGORITHMS IN THE CONTEXT OF THEIR RESISTANCE TO ATTACKS

Консенсусні алгоритми є ключовими елементами технології блокчейн, забезпечуючи узгодженість і безпеку розподіленого реєстру. Різні алгоритми мають унікальні підходи до вирішення завдань забезпечення стійкості до атак, таких як атаки 51%, сибіл-атаки та інші види порушень. Дослідження спрямоване на порівняльний аналіз таких алгоритмів, як Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) та Practical Byzantine Fault Tolerance (PBFT) [1].

Proof of Work забезпечує безпеку через складність обчислювальних задач, що ускладнює реалізацію атак. Проте висока енергозатратність та можливість централізації через пул майнінгу є серйозними недоліками. Proof of Stake покладається на підтвердження транзакцій учасниками з найбільшими ставками. Це дозволяє зменшити енергозатрати, але підвищує ризики концентрації влади у великій кількості активів [2]. У контексті DPoS пропонується модель делегованої участі, що зменшує кількість валідаторів, роблячи мережу швидшою, але створює ризики, пов’язані з довірою до делегатів. PBFT спрямований на мінімізацію впливу зловмисників у мережах, які мають до однієї третини недобросовісних вузлів. Це робить його ефективним для приватних мереж, але малопридатним для масштабованих публічних мереж [3].

Дослідження показало, що стійкість до атак значною мірою залежить від механізмів вибору валідаторів, моделі винагороди та архітектури мережі. Наприклад, PoW ефективно протистоїть сибіл-атакам, але вразливий до атак 51% через можливість централізації майнінгу. PoS має нижчу ймовірність таких атак, але ризикує через економічну нерівність. DPoS забезпечує високу швидкість транзакцій, але залежність від обраних делегатів може стати слабким місцем. PBFT демонструє високий рівень стійкості в умовах обмеженої кількості учасників, проте його ефективність падає з ростом масштабів мережі [4]. Таким чином, вибір консенсусного алгоритму має базуватися на специфіці використання блокчейн-мережі, її розмірі, рівні довіри між учасниками та потенційних ризиках. Для публічних децентралізованих мереж найбільш підходять PoW і PoS, тоді як приватні мережі можуть використовувати PBFT для досягнення високої швидкості та безпеки [5].

Подальші дослідження мають зосереджуватися на розробці гібридних моделей, які поєднують переваги різних підходів, мінімізуючи їхні недоліки. Це дозволить забезпечити більшу стійкість блокчейн-систем до атак та підвищити їхню ефективність у різних умовах використання.

Література

1. Zhebka S. V., Vlasenko V. O., Aronov A. O., Kolodiuk A. V., 2024. Solution to the dilemma of choosing a consensus algorithm in distributed systems. TIT: Telecommunications and Information Technology. No. 3, pp. 25-34. tit.dut.edu.ua.
2. Hilevskyi O. M., 2023. Comparative analysis of existing cryptocurrencies with the PoS consensus algorithm from the perspective of effective implementation reserves in terms of speed. Diploma work. Kyiv Polytechnic Institute. ela.kpi.ua.
3. Albrecht J., Andreina S., Armknecht F., Karame G., Marson G., Willingmann J., 2024. Larger-scale Nakamoto-style Blockchains Don't Necessarily Offer Better Security. ArXiv. URL: https://arxiv.org/abs/2404.09895.
5. «Analysis of consensus mechanisms in decentralized systems», 2023. A review of various consensus algorithms, including Proof of Work, Proof of Stake, Delegated Proof of Stake, and Practical Byzantine Fault Tolerance. PeerDH. peerdh.com.
6. «Performance benchmarks of consensus algorithms for decentralized oracles», 2023. Evaluation of key performance metrics of consensus algorithms such as throughput, latency, scalability, and fault tolerance, with comparisons of PoW, PoS, DPoS, and PBFT. PeerDH. peerdh.com.