Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ імені К. Д. УШИНСЬКОГО»

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ДРУГА ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

25 квітня 2025 р.

Одеса – 2025

Інформатика, інформаційні системи та технології: тези доповідей двадцять другої всеукраїнської конференції студентів і молодих науковців. Одеса, 25 квітня 2025 р. - Одеса, 2025. – 315 с.

Друкується за рішенням Вченої Ради
Університету Ушинського
(протокол № 16 від 29.05.2025 р.)

Організатори конференції продовжують традицію обміну досвідом у сфері освіти та використання інформаційних технологій. У конференції приймають участь студенти, аспіранти та молоді науковці вищих навчальних закладів України.

Тематика конференції охоплює наступне коло питань: сучасні інформаційні технології; інтелектуальні системи; методика викладання інформатики; інформаційні технології в освіті; психолого-педагогічне забезпечення інформатизації навчальної діяльності; дистанційна освіта і глобальні телекомунікаційні мережі; математичне моделювання й інформаційні технології; інформатизація системи керування освітою; інформаційні технології в менеджменті.

Наукові керівники:

завідувачка кафедри прикладної математики та інформатики
фізико-математичного факультету Університету Ушинського, д. т. н., проф. Т. Л. Мазурок,
завідувач кафедри математичного забезпечення комп'ютерних систем факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. т. н., проф. Є. В. Малахов

Оргкомітет:

Голова:

Ректор Університету Ушинського,
д. і. наук, доц. А. В. Красножон

Заступники голови:

Проректор з наукової роботи Університету Ушинського, д. політ. н., проф. Г.В. Музиченко
Декан факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. ф-м. н., проф. Ю. А. Ніцук

Члени оргкомітету:

д. т. н., проф.	Є. В. Малахов	д. т. н., проф.	Т. Л. Мазурок
д. т. н., проф.	Ю. О. Гунченко	к. п. н., доц.	А. О. Яновський
ст. викладач	І. М. Лісіцина	викладач	О. Я. Рубанська
ст. викладач	Н. Ф. Трубіна	к. ф.-м. н.	О. П. Бойко
ст. викладач	В. А. Корабльов	PhD, associated prof. (Poland)	A. Rychlik

БЛОКЧЕЙН-ТЕХНОЛОГІЇ: АЛГОРИТМИ КОНСЕНСУСУ

Дворчук Д. С., Шпінарева І. М.
Одеський національний університет імені І. І. Мечникова

Ключові слова: блокчейн, алгоритми консенсусу, PoW, PoS, BFT, PoEWAL.

Поява технології блокчейна докорінно змінило розуміння розподілених систем та механізмів довіри у цифрових середовищах. Спочатку задумана як базова технологія для криптовалютних систем, таких як Bitcoin і Ethereum, блокчейн перетворилася на універсальну платформу в таких областях, як IT та телекомунікації, роздрібна торгівля, фінансові послуги , виробництво, системи публічного голосування та забезпечує безпеку, прозорість та ефективне управління даними у різних галузях.

Мета даної роботи – виявити проблеми та недоліки блокчейн-технології, а також запропонувати нові напрямки її розвитку.

Блокчейн-технологія має ряд переваг, зокрема, можна виділити ключові характеристики, які вплинули на її розвиток: децентралізація; незмінність інформації; прозорість; анонімність. Проте, незважаючи на численні переваги блокчейнів однією з основних проблем є швидкість обробки транзакцій. Для поліпшення пропускної спроможності блокчейна застосовуються як рішення, що коригують архітектуру самої мережі (L1), і технології другого рівня (L2), які є свого роду надбудовами до L1 блокчейну.

Блокчейн першого рівня – це базовий блокчейн, який самостійно обробляє та фіналізує транзакції у власній мережі без участі іншої мережі. Рішення поліпшення швидкості обробки транзакцій першому рівні мережі блокчейн полягають у змінах основний мережі блокчейна. Такими рішеннями є зміна алгоритму консенсусу, що забезпечує згоду між учасниками мережі щодо стану розподіленого реєстру. Розглянемо алгоритми консенсусу.

Proof-of-Work (PoW) – алгоритм підтвердження транзакції, що ґрунтується на вирішенні математичних завдань з використанням обчислювальних потужностей комп'ютерів-майнерів. PoW вважається найбільш витратним алгоритмом консенсусу, оскільки він вимагає потужних комп'ютерів для обчислення хешей розв'язання криптографічних завдань.

Proof-of-Stake (PoS) не вимагає великої кількості обчислювальних потужностей і може значно скоротити час транзакцій на 40% швидше, ніж PoW, споживаючи при цьому значно менше енергії, тому вважається більш ефективним рішенням [1]. Однак, користувач з великою кількістю токенів обов'язково буде домінувати в мережі і це порушення децентралізації.

Delegated Proof of Stake (DPoS) – делегований доказ володіння часткою є альтернативою консенсусам PoW і PoS. Вище перераховані протоколи консенсусу,

використовуються у відкритих блокчейн системах, які працюють у суспільному середовищі та націлені на децентралізацію.

Протоколи консенсусу BFT, дозволяють досягти високої продуктивності та масштабованості блокчейну за рахунок вибору невеликої кількості учасників для перевірки та підтвердження транзакцій.

Byzantine Fault Tolerance (PBFT) – протоколи консенсусу, в яких анонімність не є важливим аспектом, тобто вузли знають якусь інформацію про один одного (спочатку вузли автентифіковані). Завдяки цьому можна оптимізувати алгоритми консенсусу та досягти набагато більшої пропускної спроможності.

Delegated Byzantine Fault Tolerance (DBFT) – це делегований алгоритм консенсусу візантійської стійкості до відмови з великим масштабуванням мережі.

Federated Byzantine Agreement (FBA) – федеративна візантійська угода і не вимагає дозволу чи заздалегідь відомого набору учасників, на відміну від PBFT та інших варіацій BFT.

У 2020 році було опубліковано новий алгоритм консенсусу PoEWAL, який є легким ймовірним алгоритмом консенсусу і дозволяє кожному вузлу в блокчейні брати участь у стратегії консенсусу.

Алгоритм консенсусу WBFT опублікований у 2022 році і використовує динамічний механізм зважування для вузлів консенсусу. WBFT покращує пропускну здатність системи та затримку консенсусу.

Автори Y.Wu, P. Song та ін.[2] представили гібридний алгоритм консенсусу блокчейна, що поєднує переваги алгоритмів PoS та PBFT у двоетапній стратегії. Пропонований алгоритм зменшує кількість вузлів консенсусу до постійного значення за допомогою перевіреного псевдовипадкового сортування та виконує засвідчення транзакції між вузлами.

Ітак, існуючі алгоритми консенсусу страждають від низької пропускної здатності, високої затримки, нестабільної продуктивності та від проблеми стійкості і вразливість до цільових атак. Поєднання оптимізованих алгоритмів консенсусу та машинного навчання відкриває нові горизонти для блокчейн-систем.

Література

1. Kushwaha, S.S.; Joshi, S.; Singh, D.; Kaur, M.; Lee, H.-N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. IEEE Access 2022, 10, 6605–6621. DOI:10.1109/ACCESS.2021.3140091
2. Y.Wu, P. Song, F. Wang Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain, Mathematical Problems in Engineering 2020 (11):1-13 DOI:10.1155/2020/7270624

Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ імені К. Д. УШИНСЬКОГО»

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ДРУГА ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Збірник робіт

Збірник робіт надрукований в авторській редакції
без внесення суттєвих змін оргкомітетом

Підписано до друку 25.04.2025
Здано у виробництво 25.04.2025
Формат 60x84/16. Папір офсетний. Друк офсетний.
Тираж 50 примірників

Надруковано з готового оригінал-макета