DOI: 10.34185/1991-7848.itmm.2024.01.092

ДОСЛІДЖЕННЯ АЛГОРИТМІВ КОНСЕНСУСУ У МЕРЕЖАХ БЛОКЧЕЙНУ ПРИ ПРОЕКТУВАННІ ІНФОРМАЦІЙНИХ СИСТЕМ

Ситник Р.С.[1], Гнатушенко Вік.В.[1,2]

[1]*Український державний університет науки і технологій, вул. Лазаряна, 2, м. Дніпро, 49010, Україна*

[2]*Національний технічний університет «Дніпровська політехніка», пр. Дмитра Яворницького 19, м. Дніпро, 49005, Україна*

Анотація. *Ця робота містить огляд основних механізмів консенсусу в технології блокчейн. Розглядаються основні алгоритми консенсусу, такі як Proof of Work, Proof of Stake, Proof of Authority та інші, кожен з яких має свої унікальні особливості, переваги та обмеження. Автори аналізують ці механізми на основі таких критеріїв, як енергоефективність, безпека, масштабованість і децентралізація. Крім того, надаються рекомендації щодо вибору оптимального механізму консенсусу залежно від конкретних потреб і цілей проекту. Ця стаття є важливим ресурсом для дослідників, розробників і практиків, які цікавляться технологією блокчейн та її різними аспектами.*

Ключові слова: *блокчейн, децентралізовані системи, інформаційна система, механізм консенсусу, розподілений реєстр.*

Алгоритм консенсусу в блокчейні – це механізм, який використовується для визначення того, які транзакції будуть додані в блок і який учасник мережі матиме право додати цей блок до ланцюжка блоків. Він відіграє ключову роль у забезпеченні узгодженості даних і безпеки мережі блокчейн.

У блокчейні алгоритм консенсусу необхідний з таких причин [1]:

- Запобігання подвійним витратам (Double Spending): завдяки алгоритму консенсусу можна гарантувати, що одна й та сама криптовалюта не буде витрачена двічі, що є фундаментальним аспектом блокчейн-технології.
- Забезпечення безпеки: алгоритм консенсусу допомагає запобігти атакам на кшталт 51%, що можуть статися, якщо зловмисник отримає контроль над більшістю обчислювальної потужності або стейкінговою силою мережі.
- Гарантування надійності та узгодженості: за допомогою алгоритму консенсусу учасники мережі доходять згоди щодо стану системи та послідовності транзакцій, що забезпечує її надійну роботу.

Різні алгоритми консенсусу пропонують різні підходи до досягнення цих цілей. Кожен із цих алгоритмів має свої переваги та недоліки і може бути придатним залежно від конкретного контексту та задачі використання блокчейна, таких, як наприклад, фінанси, управління логістикою, управління ідентифікаціє6 та особистими даними, голосування тощо.

Опис найбільш популярних механізмів консенсусу:

Proof of Work (PoW) [2]:

Майнери вирішують криптографічні завдання, щоб створити блок, який потім потрібно додати до ланцюжка. Цей процес вимагає великої кількості енергії та обчислювальних потужностей. Система спеціально спроектована таким чином, щоб завдання ускладнювалося в міру зростання кількості блоків у ланцюзі. Коли майнер знаходить блок, він відправляє його в мережу для перевірки. Перевірка того, чи належить блок ланцюжку чи ні, є простим процесом. Переваги – безпека, розподіл монет. Недоліки – високе енергоспоживання, масштабованість, потенційні атаки 51%. Краще використовувати в мережах із високою стійкістю до атак і нечутливих до енергоспоживання. Приклади блокчейнів: Bitcoin, Litecoin, Monero, ZCash.

Proof of Stake (PoS) [3]:

Валідатори повинні блокувати деякі зі своїх монет як ставку. Після цього вони починають перевірку блоків. Коли вони виявляють блок, який може бути доданий у ланцюжок, вони підтверджують його, ставлячи на нього ставку. Якщо блок додається, то валідатори отримують винагороду, пропорційну ставці. Переваги – енергоефективність, знижене енергоспоживання, масштабованість, недоліки – можливість стейкера контролювати блокчейн залежно від його частки, проблеми з безпекою при довгій історії. Краще використовувати в мережах, де важлива енергоефективність і де немає проблем з нерівномірним розподілом монет. Приклади блокчейнів: VCash, BitBay, Qtum, Stratis.

Proof of Stake Time (PoST) [4]:

Доказ часу ставки використовує вік монети. Але замість того, щоб брати кількість монет для розрахунку віку, використовується період часу, протягом

якого монети утримувалися за конкретною адресою. До переваг можна віднести те, що облік часу володіння монетами може сприяти більш справедливому розподілу винагород, а до недоліків – складнощі в реалізації, потенційні проблеми з безпекою та управлінням часом. Приклади блокчейнів: Vericoin.

Delegated Proof of Stake (DPoS) [5]:

Значно доопрацьований алгоритм PoS. У DPoS токени не голосують за самі блоки, але голосують за обрання делегатів, які проведуть перевірку від свого імені. Делегати періодично переобираються, і система працює швидко. Якщо обрані вузли постійно пропускають блоки або публікують недійсні транзакції, ті, хто ставлять, голосують проти них і замінюють їх кращим варіантом. До переваг можна віднести більшу швидкість транзакцій, більш демократичне управління мережею. А до недоліків – меншу децентралізацію, можливість централізованих атак.

Краще використовувати в мережах, де важлива швидкість транзакцій і де існує довіра до делегатів. Приклади блокчейнів: Steemit, EOS, BitShares.

Proof of Elapsed Time (PoET) [6]:

Алгоритм поєднує переваги Proof of Work і Proof of of Stake. Майнінг починається традиційним способом – майнери змагаються у розв'язанні задачі та отриманні нагороди. Різниця в тому, що видобуті блоки не містять транзакцій, а містять тільки відомості про заголовок та адресу для винагороди за майнінг.

Щойно цей майже порожній блок буде видобуто, система перемикається на протокол PoS. Інформація заголовка використовується для вибору випадкової групи валідаторів для підпису блоку. Їх називають власниками монет (стейкхолдери), і чим більша частка валідатора, тим більше шансів, що їх буде обрано для підписання нового блоку. Щойно всі обрані валідатори підписують блок, він стає частиною блокчейна.

Якщо блок залишається непідписаним деякими з обраних валідаторів після закінчення заданого часу, то він відкидається як неповний і використовується наступний виграшний блок. Знову вибираються валідатори, і

це триває доти, доки виграшний блок не буде підписано всіма обраними валідаторами. валідаторами. Винагороду розподіляють між майнером, який переміг і валідаторами, які підписали блок. Приклади блокчейнів: мережа Ethereum Kovan.

Proof of Burn (PoB) [7]:

Майнер відправляє монети на випадкову адресу згенерованого хешу. Витратити кошти з цієї адреси практично неможливо, оскільки ймовірність підібрати до неї ключі прагне до нуля. За таке "спалювання" монет майнер отримує постійний шанс знайти PoB блок і отримати за нього нагороду. Шанси на майнінг збільшуються при збільшенні кількості "спалених" монет. До переваг можна віднести енергоефективність, розподіл монет, а до недоліків – втрата монет, що може викликати побоювання у власників за свої монети. Приклад блокчейну: Slimcoin.

Proof of Importance (PoI) [8]:

Значимість кожного користувача в мережі визначається як кількість коштів, наявних у нього на балансі, і кількість проведених транзакцій з/на його гаманець. В відміну від PoS, який враховує тільки баланс наявних коштів у користувача, PoI враховує як кількість коштів, так і активність користувача в блокчейн-мережі. Такий підхід залучає користувачів не просто тримати кошти у себе на рахунку, а й активно використовувати їх. До переваг можна віднести сприяння активній участі, більш справедливий розподіл винагород, а до недоліків – складнощі у визначенні "важливості", потенційні атаки. Приклад блокчейну: NEM.

Proof of Authority [9]:

Усі транзакції та блоки перевіряються за допомогою схвалених акаунтів (валідаторів). Проведення транзакцій і створення блоків відбувається в автоматичному режимі за допомогою обчислювальних потужностей валідатора. До переваг можна віднести – швидкі транзакції, контрольовані та надійні учасники, а недоліки – централізація, залежність від довіри до валідаторів. Приклад блокчейну: VeChain.

Під час вибору алгоритму консенсусу також необхідно враховувати поточні та майбутні потреби мережі, а також ресурси, доступні для реалізації та підтримки обраного алгоритму. Наприклад, якщо проєкт має обмежені обчислювальні ресурси, то вибір алгоритму, який вимагає мінімальної кількості обчислювальної потужності, може бути пріоритетним. Крім того, важливо враховувати ступінь децентралізації, оскільки різні алгоритми консенсусу мають різні рівні децентралізації, що може бути критичним фактором для деяких проєктів, особливо в контексті безпеки та опору централізованим атакам. Таким чином, під час вибору алгоритму консенсусу необхідно враховувати як технічні, так і організаційні аспекти, щоб забезпечити найкращу відповідність цілям і потребам проєкту.

Проведене дослідження використовується при проєктуванні інформаційних децентралізованих систем із застосуванням технології блокчейн та алгоритмів консенсусу, що дає можливість підвищити надійність системи, забезпечити її стійкість до навантаження та атак, зменшити ризики виникнення конфліктів даних та забезпечити швидкість та ефективність обробки транзакцій. При цьому важливо враховувати особливості кожного конкретного алгоритму консенсусу, їхню масштабованість, витрати на обчислення та енергопотребу, а також специфіку застосування в конкретних умовах. Розуміння цих аспектів дозволить ефективно використовувати алгоритми консенсусу для досягнення поставлених цілей та покращення функціонування інформаційних систем у різних галузях та сферах діяльності.

ЛІТЕРАТУРА / REFERENCE

1. Gramoli, V., 2020. From blockchain consensus back to Byzantine consensus. Future Generation Computer Systems, 107, pp.760-769.

2. Li, S.N., Yang, Z. and Tessone, C.J., 2020, August. Proof-of-work cryptocurrency mining: a statistical approach to fairness. In 2020 IEEE/CIC international conference on communications in China (ICCC workshops) (pp. 156-161). IEEE.

3. Saleh, F., 2021. Blockchain without waste: Proof-of-stake. The Review of financial studies, 34(3), pp.1156-1190.

4. Pike, D., Nosker, P., Boehm, D., Grisham, D., Woods, S. and Marston, J., 2015. PoST White Paper. [Електронний ресурс]. – Режим доступу: https://cdn.vericonomy.com/documents/VeriCoin-Proof-of-Stake-Time-Whitepaper.pdf.

5. Saad, S.M.S. and Radzi, R.Z.R.M., 2020. Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). International Journal of Innovative Computing, 10(2).
6. Bowman, M., Das, D., Mandal, A. and Montgomery, H., 2021. On elapsed time consensus protocols. In Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22 (pp. 559-583). Springer International Publishing.
7. Karantias, K., Kiayias, A. and Zindros, D., 2020. Proof-of-burn. In Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24 (pp. 523-540). Springer International Publishing.
8. Xiao, B., Jin, C., Li, Z., Zhu, B., Li, X. and Wang, D., 2021, December. Proof of importance: A consensus algorithm for importance based on dynamic authorization. In IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (pp. 510-513).
9. Manolache, M.A., Manolache, S. and Tapus, N., 2022. Decision making using the blockchain proof of authority consensus. Procedia Computer Science, 199, pp.580-588.

STUDY OF CONSENSUS ALGORITHMS IN BLOCKCHAIN NETWORKS IN THE DESIGN OF INFORMATION SYSTEMS

Roman Sytnyk, Viktoriia Hnatushenko

Abstract. *This paper provides an overview of the major consensus mechanisms in blockchain technology. The main consensus algorithms are discussed, such as Proof of Work, Proof of Stake, Proof of Authority and other, and each has its own unique features, advantages and limitations. The authors analyse these mechanisms based on criteria such as energy efficiency, security, scalability and decentralisation. In addition, there recommendations provided for selecting the optimal consensus mechanism depending on the specific needs and goals of the project. This article serves as an important resource for researchers, developers, and practitioners interested in blockchain technology and its various aspects.*

Keywords: *blockchain, decentralised systems, information system, consensus mechanism, digital ledger.*