Алгоритми консенсусу у BlockChain корпоративних системах

https://doi.org/10.31713/MCIT.2024.064

Юрій Тулашвілі
Луцький національний технічний університет
Луцьк, Україна
y.tulashvili@lutsk-ntu.com.ua

Юрій Лук'янчук
Луцький національний технічний університет
Луцьк, Україна
iuriilukianchuk87@gmail.com

Abstract **– The concept of the new generation of the Internet is based on decentralization and today is widely implemented in cryptocurrency tokens and information systems based on blockchain technology. The purpose of the article is to investigate the impact of algorithms for confirming the authenticity of information on the effectiveness of the functioning of corporate information systems using blockchain technology through the analysis of existing concepts of consensus. The scheme of the corporate information system of document circulation proposed by the authors of the article in previous works using blockchain technology is based on ensuring the decentralization of the system and the integrity of data regarding the preservation and revision of the institution's documents. To automate the consensus process using a smart contract, the system uses a dynamic consensus.**

Keywords **– blockchain technology; consensus process; corporate information system of document circulation**

I. Вступ

Блокчейн сьогодні являє собою нову прогресивну технологію Web 3.0, яка дає користувачам більше контролю над своїми даними та забезпечує більш відкрите та прозоре середовище обміну інформацією. У Web 3.0 немає єдиного центру управління, у цілому мережа контролюється самими учасниками. Концепція нового покоління інтернету заснована на децентралізації та сьогодні широко реалізується у криптовалютних токенах та інформаційних системах на технології блокчейн.

Основна ідея блокчейн заснована на тому, щоб забезпечити гарантії цілісності даних без опори на керуючий мережею центр шляхом децентралізованого зберігання інформації. Вся інформація та дані зберігаються в учасників мережі, які є розподіленими вузлами, а не в централізованому центрі керування. Яскравими прикладами нового децентралізованого підходу є криптовалютні системи та корпоративні інформаційні системи, що побудовані на технології блокчейн, які працюють на основі децентралізованого реєстру транзакцій, що забезпечує надійність, прозорість і безпеку обміну даними та активами між учасниками.

Оскільки блокчейн є мережевою технологією, то для успішного функціонування поставлених завдань у корпоративній системі мають приймати всі учасники. Технологія грунтується на забезпеченні гарантії того, що дані залишаються однаковими на всіх вузлах. Це створює довіру між сторонами, що ведуть бізнес, навіть коли вони не знають один одного. Вся ідея блокчейну полягає в тому, щоб забезпечити гарантії цілісності даних без опори на центральний авторитет та забезпечити достовірність інформації, що зберігається у блоках. У процесі підтримання цілісності інформації за технологією блокчейн значну роль відіграє операція консенсусу, яка застосовується для прозорого підтвердження достовірності інформації. Метою статті є дослідити вплив на ефективність функціонування корпоративних інформаційних систем, що використовують технологію блокчейн, алгоритмів підтвердження достовірності інформації через аналіз існуючих концепцій консенсусу.

II. Стан дослідження проблеми

Технологія блокчейн характеризується декількома особливостями, які роблять її унікальною: децентралізацією (жоден суб'єкт не має повного контролю над блокчейном), консенсусом (щоб додати транзакцію до блокчейну, інші вузли повинні надати згоду), криптографією (блокчейн використовує криптографічні пристрої для захисту транзакцій у блокчейні від злому) і незмінністю (як тільки транзакцію було додано до блокчейну, її неможливо змінити чи видалити – можна додавати лише нові транзакції).

Достовірність інформації є основною перевагою функціонування інформаційних систем на основі блокчейн і, у свою чергу, грунтується на принципах консенсусу та незмінності. Дотримання цих принципів гарантує, що всі дані в мережі є однаковими та недоступними до змін без погодження. Технологія блокчейн використовує алгоритми консенсусу (правила узгодження) для досягнення єдності серед всіх учасників-вузлів щодо стану кожної транзакції та реєстру транзакцій, який і є безпосередньо сам блокчейн. Це гарантує, що всі дані в мережі є однаковими та недоступними до змін без погодження. Найбільш поширеними правилами консенсусу, що застосовуються у технології блокчейн є алгоритми економічного стимулювання: Proof of Work (PoW - «доказ роботи»); Proof of Stake (PoS - «підтвердження частки») та їх модифікації [1, 2], а також алгоритми математичних обчислень

гарантій безпеки на основі Byzantine Fault Tolerance (BFT - «Візантійська стійкість до відмов») [3, 4].

Проведений дослідниками [1-3, 5, 6] аналіз алгоритмів економічного стимулювання висвітлює, що на сучасному етапі більшість систем, які базуються на технології блокчейн, використовують широку гаму алгоритмів консенсусу. Алгоритм консенсусу доказ роботи proof-of-work (PoW) поширився завдяки біткойну та є найвідомішим способом підтвердження транзакцій. Основна ідея полягає в тому, що вузли мережі блокчейн (майнери), які підтверджують транзакції, повинні виконувати досить складну обчислювальну роботу (обчислення алгоритму), результат якої був би легко і швидко перевірений іншими вузлами мережі. Перший вузол-майнер, який виконає всі необхідні обчислення, винагороджується мережею блокчейн. Всі вузли ведуть боротьбу між собою, збільшуючи пропускну здатність обчислювальних ресурсів, щоб першим отримати винагороду. Процес майнінгу, у якому майнери - дуже потужні комп'ютери, під'єднані до мережі - змагаються за вирішення складних математичних задач. У нагороду за свої зусилля вони отримують новостворені монети. Головними недоліками цього алгоритму є: атаки на існуючі блокчейни коли майнери можуть намагатися здійснювати корисливий майнінг (зловмисник може спробувати подвоїти витрати, використовуючи ту саму монету для здійснення більше транзакцій, щоб збільшити свою відносну частку майнінгу в блокчейні); - витрати на електроенергію, а саме, велика кількість вузлів виконують обчислення, але в реальності тільки один, перший, виконує успішну роботу і отримує винагороду.

Для подолання проблем PoW був розроблений новий механізм консенсусу, а саме доказ частки володіння (PoS), який дозволяє досягти консенсусу шляхом доведення права власності на частку [2]. За цим алгоритмом творцем наступного блоку в блокчейні вибирається вузол, який має більший баланс - кількість ресурсів, наприклад, монет у криптовалюті. Вузол не отримує винагороду за створення самого блоку. За проведення транзакції виплачується винагорода. Основаним недоліком цього алгоритму є нерівномірність виплачених винагород майнерам, що створює прецедент збагачення одних і тих же вузлів криптовалютного блокчейну.

Спробою виправити цей недолік є алгоритм Delegated Proof-of-Stake (DPoS), один з різновидів алгоритму консенсусу Proof-Of-Stake, у якому користувачі все ще роблять ставки своїх криптовалютних монет. Однак замість того, щоб самостійно брати на себе відповідальність за перевірку блоку, користувачі (або зацікавлені сторони) роблять ставки своїх монет, щоб делегувати роботу, голосуючи за вузол, який перевірить блок від їх імені. Таким чином такий механізм консенсусу отримав назву «делеговане підтвердження частки».

Також знаходять застосування проаналізовані в працях [2, 6, 8, 9] алгоритми консенсусу, що базується на комбінації Proof of Work і Proof of Stake: підтвердження активності Proof of Activity (PoA); підтвердження ємності Proof-of-Capacity (PoC); доказ горіння Proof-of-Burn (PoB); орендований доказ Leased Proof-of-Stake (LPoS); доказ важливості Proof-of-Importance (PoI); сімейство консенсусних протоколів підтвердження частки Ouroboros. При тому, що усі алгоритми консенсусу мають як свої переваги, так й недоліки їх застосовують різні криптовалютні системи на основі технології блокчейн (Bitcoin, Ethereum, Stellar, Chia, Slimcoin, Decred, Dash, Qtum, NEO).

Проведений дослідниками [10-16] аналіз висвітлює, що у блокчейн мережах з обмеженою кількістю учасників, як це є у корпоративних системах, немає сенсу використовувати непродуктивні та повністю розподілені типи консенсусів, на кшталт Proof of Work і Proof of Stake. Це дає завжди збільшення вартості проведення та зберігання транзакцій: одна справа зберігати транзакцію на десятках корпоративних вузлах, а зовсім інша - на сотнях тисяч у всьому світі, як укриптовалютних системах. Тому для таких систем найбільшої ефективності для забезпечення достовірності інформації набувають алгоритми консенсусу на основі математичних обчислень гарантій безпеки, які розглянемо з погляду застосування для корпоративних систем.

III. Основний виклад

Алгоритми математичних обчислень гарантій безпеки застосовують консенсус на основі BFT. Такий підхід заснований на тому, що з n вузлів мережі блокчейн може виникати кількість учасників системи t, які можуть відхилятись від специфікації протоколу, тобто коли деякі вузли мережі не відповідають або дають неправильну інформацію.

Алгоритм BFT побудований на розв'язанні задачі "Візантійських генералів". Її рішення лежить в основі стійкості P2P мереж, коли вузли обмінюються між собою файлами і зберігають один і той же набір даних. За BFT можливість приходити до консенсусу під час голосування гарантує цілісність реєстру, його послідовність і живучість, якщо є згода понад двох третин всіх вузлів, тобто припускається кількість візантійських спотворень

$$t < n/3. \quad (1)$$

Тоді, усі "чесні" вузли можуть отримати миттєву впевненість у тому, що транзакція в кінцевому підсумку буде виконана.

Алгоритм BFT знайшов свій розвиток у таких протоколах консенсусу:

- Practical Byzantine Fault Tolerance (PBFT) - це оригінальний класичний консенсусний протокол, який використовує 2 раунди голосування. Алгоритм реалізує такі кроки [10]:

  - вузол надсилає запит на виклик операції служби узгодження;

  - служба узгодження передає запит до повних вузлів, що мають резервні копії блокчейну та примають участь у консенсусі;

  - повні вузли опрацьовують запит і надсилають відповідь вузлу, що ініціював запит;

- вузол чекає *n/3+1* відповіді від *n* повних вузлів з однаковим результатом, це є результат операції узгодження.

PBFT був розроблений для ефективної роботи в асинхронних мережах і оптимізований для зниження накладних витрат [11].

- Istambul BFT (IBFT), простий і елегантний візантійський відмовостійкий консенсусний алгоритм, який використовується для реалізації реплікації кінцевого автомата в блокчейні Quorum [12]. IBFT перейняв з алгоритму PBFT трифазний консенсус, що складається з етапів *PRE-PREPARE*, *PREPARE* та *COMMIT* [13]. Система допускає не більше *t* несправні процеси з *n*, а саме реалізує умову n = 3t+1. Алгоритм є детермінованим, заснованим на лідері (рис.1).

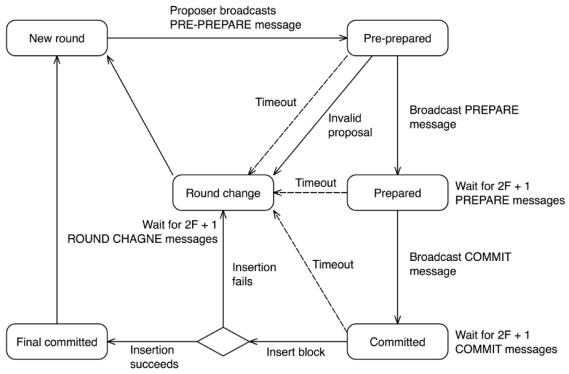

Рис.1. Процес взаємодії валідаторів у IBFT [13]

Перед кожним раундом вузли, що виконують роль валідаторів, обирають одного з них на роль лідера. Вибраний лідер пропонує нову пропозицію з транзакціями для включення в ланцюжок блокчейну та передає її валідаторам спільно з повідомленням *PRE-PREPARE*. Після отримання *PRE-PREPARE* повідомлення валідатори змінюють свій стан на *PRE-PREPARED*. Після здійснення цієї дії всі вузли повинні переконатися, що всі валідатори працюють в одній послідовності та в тому самому раунді. Після отримання валідатором *2t+1* повідомлень *PREPARE* він набуває нового стану *PREPARED* і потім передає повідомлення *COMMIT*. На цьому кроці валідатор повідомляє своїм партнерам про те, що він приймає запропонований блок і збирається додати його в ланцюжок. Дочекавшись *2t+1* повідомлень *COMMIT*, валідатори переходять у стан *COMMITTED* і додають новий блок у ланцюжок.

- Delegated Byzantine Fault Tolerant (DBFT) розроблено на основі механізму PBFT командою NEO. Він поєднує характеристики протоколів PBFT і DPoS. Кожен користувач у ланцюжку блоків NEO може вибирати делегатів. Як показано на рис. 2, у моделі системи DBFT є три сторони, включаючи кандидатів, радників і звичайні вузли [14]. Кандидати обираються з усіх вузлів у системі блокчейн на початку процесу консенсусу. Оскільки вони можуть представляти інтереси більшості вузлів, вони сформують альтернативний пул вузлів, які виконують PBFT. Радники: у кожному циклі виконання члени ради вибираються з кандидатів за допомогою алгоритму випадкового вибору (RS). Вони відповідають за реалізацію алгоритму PBFT для досягнення консенсусу. Основні та резервні копії в PBFT обираються з членів ради. Звичайні вузли: усі вузли, крім кандидатів і радників.

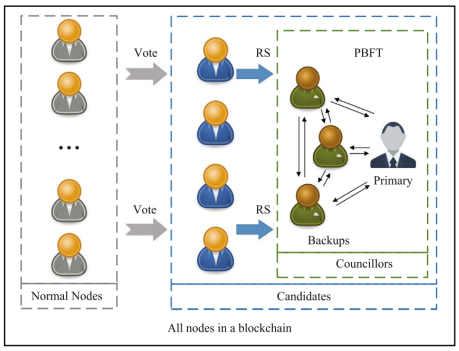

Рис.2. Процес взаємодії валідаторів у IBFT [14]

- Verifiable Byzantine Fault Tolerance (VBFT) - новий алгоритм консенсусу, який поєднує в собі класичний PoS, випадкову функцію (VRF), що перевіряється, і візантійську відмовостійкість (BFT) [16]. VBFT розроблено для забезпечення високої пропускної здатності, низької затримки та візантійської відмовостійкості при збереженні безпеки та децентралізації. Даний механізм розроблений спеціально для потреб платформи ONTology. VBFT може підтримувати масштабованість консенсусних груп, за допомогою VRF гарантує випадковість та справедливість генерації консенсусної сукупності, а також забезпечує швидке досягнення кінцевого стану. На відміну від DBFT, у цьому алгоритмі усунуто проблему ризику централізації. Послідовність VBFT [16]:

- вибір консенсусного вузла: для участі в процесі консенсусу вибирається фіксована кількість вузлів консенсусу, також відомих як учасники консенсусу або валідатори. Вибір консенсусних вузлів може базуватися на таких факторах, як частка, репутація або інші критерії, визначені мережею.

- пропозиція та перевірка: процес консенсусу починається, коли призначений вузол консенсусу пропонує новий блок транзакцій. Інші вузли консенсусу в мережі отримують запропонований блок і незалежно перевіряють його достовірність за допомогою криптографічних методів.

- верифікована випадкова функція (VRF): VBFT містить перевірену випадкову функцію (VRF) для вибору підмножини консенсусних вузлів для участі в процесі перевірки блоку. VRF забезпечує випадковість і справедливість у виборі консенсусних вузлів, запобігаючи маніпуляціям або упередженням у процесі консенсусу.

- голосування та погодження: після перевірки запропонованого блоку вузли консенсусу

віддають свої голоси, щоб схвалити або відхилити блок. Попередньо встановлений поріг позитивних голосів потрібен, щоб блок вважався підтвердженим і доданим до блокчейну.

IV. Висновки

Існуючі корпоративні інформаційні системи не можуть продовжувати працювати відповідно до традиційних вимог транзакцій. Їх доведеться модифікувати до сучасних вимог з інтегруванням технології блокчейну. Корпоративні інформаційні системи включатимуть блокчейни, що міститимуть вичерпні дані щодо існуючих сховищ даних, забезпечать асинхронну взаємодію усіх учасників системи у вигляді розподілених вузлів блокчейну.

Запропонована авторами статті у попередніх роботах схема корпоративної інформаційної системи документообігу [17] з використанням технології блокчейн грунтується на забезпеченні децентралізації системи та цілісності даних щодо збереження та перегляду документів установи. Для автоматизації процесу консенсусу за допомогою смарт-контракту система застосовує алгоритм динамічної згоди, який грунтується на протоколі консенсусу BFT. Вузол, що здійснює транзакцію повинен за певними правилами, які визначені у таблиці правил, провести її за погодження між іншими вузлами, після чого створюється та додається новий блок до блокчейну. В залежності від того, яка транзакція відбулась - запит даних чи завантаження документу до хмарного сховища, буде сформований блок до блокчейну запитів чи блок до блокчейну даних. Вузли взаємодіють між собою та сховищем даних, що дає можливість підтримувати цілісність мережі та отримувати інформацію щодо оновлення документів в корпоративній інформаційній системі шляхом синхронізації блокчейну. Операція включення до блокчейну нового блоку потребує його узгодження іншими вузлами за правилами консенсусу.

У подальшому впровадження та дослідження корпоративної інформаційної системи документообігу передбачає порівняльне дослідження ефективності алгоритмів динамічної згоди, протоколів BFT для розробки ефективніших і результативних методів захисту механізмів блокчейну.

У подальшому дослідження та впровадження корпоративної інформаційної системи документообігу передбачає порівняльне дослідження ефективності алгоритмів криптографічного захисту транзакцій у блокчейні від злому.

Література

[1] Don Tapscott, Alex Tapscott. Blockchain Revolution. How the technology behind Bitcoin is changing money, business, and the world. Penguin Random House LLC, New York, 2016. P. 324. URL: https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf.

[2] Cong Nguyen, Hoang Dinh Thai, Diep N. Nguyen, Dusit Niyato and others. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. June 2019 IEEE Access. 7. URL: https://doi.org/10.1109/ACCESS.2019.2925010..

[3] Miguel Correia. From Byzantine Consensus to Blockchain Consensus. 2019. URL: https://www.dpss.inesc-id.pt/~mpc/pubs/Chapter-From-Byzantine-Consensus-to-Blockchain-Consensus.pdf.

[4] Kiayias Aggelos, Russell Alexander. Ouroboros-BFT: A Simple Byzantine Fault Tolerant Consensus Protocol. Cryptology ePrint Archive (Report 2018/1049). Retrieved November 23, 2020. URL: https://eprint.iacr.org/2018/1049.

[5] Kirill Grigorchuk. Overview of 9 blockchain consensus algorithms. DigitalForest Blog. 2019. URL: https://digiforest.io/en/blog/blockchain-consensus-algorithms.

[6] Arthur Gervais, Ghassan Karame, Karl Wüst, Vasileios Glykantzis. On the Security and Performance of Proof of Work Blockchains. 2016. URL: https://www.researchgate.net/publication/309451429_On_the_Security_and_Performance_of_Proof_of_Work_Blockchains.

[7] Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi, Laila Fetjah. An Overview of Blockchain ConsensusAlgorithms: Comparison, Challengesand Future Directions. Advances in Intelligent Systems and Computing. October 2020. Springer. URL: https://doi.org/10.1007/978-981-15-6048-4_31.

[8] Кучковський В. В. Алгоритми консенсуса блокчейн систем. Вісник Хмельницького національного університету. Серія: Технічні науки. № 3 (297), 2021. С. 30–33.

[9] Kiayias Aggelos, Russell Alexander, David Bernardo, Oliynykov Roman. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In Katz, J.; Shacham, H. (eds.). Advances in Cryptology – Crypto 2017. Cham: Springer. pp. 357–388. URL: https://doi.org/10.1007/978-3-319-63688-7_12.

[10] CASTRO, M. AND LISKOV, B. 1999b. Practical Byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI), USENIX, New Orleans, USA, February 1999. URL: https://pmg.csail.mit.edu/papers/osdi99.pdf.

[11] What Is Zilliqa (ZIL)? Binance Academy. URL: https://academy.binance.com/uk/articles/what-is-zilliqa-zil.

[12] Henrique Moniz. The Istanbul BFT Consensus Algorithm. URL: https://doi.org/10.48550/arXiv.2002.03613.

[13] Istanbul Byzantine Fault Tolerance. URL: https://github.com/ethereum/EIPs/issues/650.

[14] Yu Zhan, Baocang Wang, Rongxing Lu, Yong Yu. DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains. Information Sciences. Volume 559, June 2021, Pages 8-21. URL: https://www.cs.unb.ca/~rlu1/paper/ZhanWLY21.pdf.

[15] Pierre Tholoniat, Vincent Gramoli. Formal Verification of Blockchain Byzantine Fault Tolerance. URL: https://www.researchgate.net/publication/342079183_Formal_Verification_of_Blockchain_Byzantine_Fault_Tolerance.

[16] Garima Singh.Verifiable Byzantine Fault Tolerance (VBFT) consensus. URL: https://www.linkedin.com/pulse/verifiable-byzantine-fault-tolerance-vbft-consensus-garima-singh-t9bhf.

[17] Тулашвілі Ю.Й., Лук'янчук Ю.А. Перспективи розвитку технології blockchain у корпоративних інформаційних системах. Комп'ютерне моделювання та програмне забезпечення інформаційних систем і технологій : зб. наук. праць IV Міжнародної науково–практичної конф. КМПЗ_2024. Чернівці, 30 травня – 01 червня 2024. Львів: ЛНУ імені Івана Франка, 2024. С.293-297.