

ПРОТОКОЛИ КОНСЕНСУСУ ТА ЇХ ЗАСТОСУВАННЯ У СИСТЕМАХ УПРАВЛІННЯ ВАНТАЖОПОТОКАМИ

Велегура Є.А.¹, Горячкін В.М.²

¹Український державний університет науки і технологій, Україна

²Український державний університет науки і технологій, ² к.т.н., доцент, Україна

Анотація. У тезах розглянуто сучасні протоколи консенсусу та їх використання в управлінні вантажопотоками на основі блокчейну. Проаналізовано технічні аспекти впровадження смарт-контрактів у логістичних процесах з акцентом на безпеку даних і транзакцій. Показано, що децентралізована мережа, в якій всі учасники повинні досягти згоди щодо змін у реєстрі, забезпечує високу цілісність інформації та захист від несанкціонованих втручань. Наведено приклади використання блокчейну в логістиці (відстеження вантажів, автоматизація документів) та обговорено переваги консенсусних алгоритмів у підвищенні прозорості, довіри між сторонами й стійкості систем вантажоперевезень. Зроблено висновок про перспективність застосування протоколів консенсусу для побудови захищених та ефективних систем управління ланцюгами постачання.

Ключові слова: блокчейн, консенсус-протокол, смарт-контракт, логістика, вантажопотоки, безпека, прозорість.

Вступ. Управління вантажопотоками є критично важливим аспектом логістики та ланцюгів постачання, що включає координацію перевезень, зберігання і передачу товарів від виробника до споживача. Традиційні централізовані системи управління логістикою часто стикаються з проблемами браку прозорості, довіри та безпеки даних. Вразливість таких систем полягає в існуванні єдиної точки відмови, що може призвести до збоїв або маніпуляцій даними з боку зловмисників. Наприклад, несинхронність інформації між різними учасниками (виробниками, перевізниками, складами) призводить до помилок та затримок, а централізована база даних може стати мішенню для кібератак. В останнє десятиліття технологія блокчейну пропонує рішення цих проблем шляхом розподіленого зберігання даних і використання протоколів консенсусу для їх узгодження між учасниками мережі. Блокчейн є незмінним розподіленим реєстром транзакцій, захищеним криптографічними методами, який усуває потребу в єдиному довіреному посереднику. Це особливо привабливо для логістики, де задіяно багато незалежних сторін.

Метою даної роботи є аналіз протоколів консенсусу, що застосовуються в блокчейн-системах управління вантажопотоками, та оцінка їх ролі у забезпеченні безпеки і надійності логістичних процесів. Основна увага приділяється технічним деталям реалізації смарт-контрактів у логістиці, питанням безпеки та практичним прикладам впровадження технології.

Протоколи консенсусу в блокчейн-логістиці. Протокол консенсусу визначає механізм, за яким вузли розподіленої мережі досягають згоди щодо актуального стану реєстру транзакцій. В публічних блокчейнах (наприклад, біткоїн, Ethereum) поширені енергоємні алгоритми консенсусу на зразок Proof-of-Work (PoW, доказ виконання роботи). PoW забезпечує високий рівень захисту від підробки записів, проте потребує значних обчислювальних ресурсів і часу для підтвердження блоків [2]. Це робить його малопридатним для швидкоплинних логістичних процесів, які вимагають високої пропускну здатності і низьких затримок. Натомість у корпоративних (приватних або консорціумних) блокчейн-системах управління ланцюгами постачання набули розвитку альтернативні протоколи консенсусу, що не потребують значних затрат енергії та часу. Прикладами є Proof-of-Stake (доказ частки володіння), Proof-of-Authority (доказ повноваження) та алгоритми на основі візантійської відмовостійкості (PBFT, RAFT тощо). Такі підходи дозволяють обмеженому колу відомих учасників (вузлів) швидко узгоджувати між собою блоки транзакцій, зберігаючи при цьому високий рівень довіри і незмінності даних. Застосування полегшених і масштабованих алгоритмів консенсусу підвищує продуктивність блокчейн-системи та зменшує витрати, що є критичним для глобальних логістичних мереж [2].

Безпека та довіра через децентралізацію. Розподілений характер блокчейну означає, що жоден окремий учасник не контролює всю систему – кожна транзакція повинна бути підтверджена більшістю або визначеною кворумом вузлів. Це забезпечує захист від несанкціонованих змін: для внесення підробленого запису зловмиснику потрібно скоординувати атаку на більшість вузлів мережі, що практично неможливо у добре спроектованій системі. Кожна зміна даних у реєстрі підтверджується консенсусом усіх

учасників, тому фальсифікація або видалення інформації стає надзвичайно складним. Таким чином, консенсусні протоколи підвищують цілісність даних і знижують ризики шахрайства, контрафакту чи несанкціонованого доступу. Крім того, використання криптографічних підписів і хеш-ланцюжків блоків означає, що будь-яка спроба змінити інформацію буде одразу виявлена іншими учасниками. Довіра між сторонами, що беруть участь у вантажоперевезеннях, забезпечується не централізованим посередником, а математично обґрунтованими механізмами перевірки та спільної верифікації транзакцій [1].

Смарт-контракти в логістичних процесах. Смарт-контракт – це програмний алгоритм, який автоматично виконує умови угоди при настанні визначених подій. У контексті логістики смарт-контракти застосовуються для автоматизації та контролю виконання типових процесів: оформлення транспортних документів, відстеження місцезнаходження та стану вантажу в режимі реального часу, управління запасами на складах, розрахунків між контрагентами тощо [1]. Наприклад, після відправлення партії товару смарт-контракт може сформувати електронну транспортну накладну і записати її у блокчейн-реєстр, де вона буде доступна всім учасникам перевезення (вантажовідправнику, перевізнику, отримувачу). Будь-які зміни в цьому документі можливі тільки за взаємною згодою (консенсусом) всіх сторін, що гарантує автентичність даних. Інший приклад – моніторинг умов перевезення: датчики IoT (температури, вологості, GPS тощо) можуть передавати дані до блокчейну; якщо параметри виходять за допустимі межі (скажімо, температура в рефрижераторі піднялася вище критичної), смарт-контракт автоматично сповістить перевізника та вантажоотримувача або ініціює інші наперед визначені дії. Таким чином, смарт-контракти підвищують оперативність реагування на події та виключають людський фактор у рутинних операціях, що зменшує кількість помилок і затримок.

Аспекти безпеки та довіри. Використання блокчейну у вантажній логістиці суттєво підвищує прозорість і підзвітність процесів. Усі транзакції (наприклад, передача товару, зміна статусу замовлення, підписання

документу) незмінно фіксуються в розподіленому реєстрі, що дає можливість аудиту кожного кроку постачання в майбутньому. Журнал транзакцій є спільним для всіх учасників, тому інформаційні розбіжності між сторонами усуваються – кожен має доступ до однаково достовірних даних про рух вантажів, що сприяє співпраці між учасниками ланцюга постачання.

З точки зору безпеки, консенсусний підхід і криптографічний захист роблять мережу стійкою до більшості кібератак: відомо, що однорангове зберігання даних без центрального вузла виключає єдину точку відмови і ускладнює несанкціонований доступ. Проте, слід враховувати і нові виклики безпеки. Смарт-контракти, будучи програмним кодом, можуть містити вразливості, що потребують ретельної перевірки перед впровадженням [4].

Помилки в коді смарт-контрактів вже ставали причиною інцидентів (як-от в Ethereum), тому для логістичних систем важливо застосовувати формальні методи верифікації контрактів та кращі практики програмування [5]. Крім того, в публічних ланцюгах можливі атаки типу 51%, коли один учасник концентрує більшість обчислювальних потужностей, але в корпоративних (приватних) системах це ризик мінімізовано шляхом контролю за колом вузлів.

Конфіденційність даних також є важливим питанням: у відкритому блокчейні вся інформація доступна всім вузлам, що неприпустимо для деяких комерційних даних. В таких випадках застосовуються гібридні рішення – приватні блокчейни або шифрування даних, коли чутлива інформація зберігається поза ланцюгом, а в блокчейні фіксуються лише хеші чи підтвердження.

Практичне впровадження. Блокчейн-технологія вже починає застосовуватися у сфері логістики. Відомий приклад – платформа TradeLens, створена компаніями IBM та Maersk для відстеження глобальних контейнерних перевезень. Ця система на базі блокчейну Hyperledger забезпечувала спільний доступ учасників галузі до даних про рух контейнерів і пов'язані документи. Вже протягом кількох місяців після запуску (2018 р.) до TradeLens приєдналися десятки портів, транспортних компаній та імпортерів для тестування рішення [6]. Хоча згодом проект було згорнуто, він продемонстрував потенціал

технології у зменшенні паперового документообігу та прискоренні операцій завдяки єдиному джерелу правди (англ. *single source of truth*).

Інші приклади включають використання блокчейну для відстеження походження продуктів у роздрібних мережах (для забезпечення якості та безпеки харчових продуктів), а також платформи на зразок VeChain, що застосовують консенсус Proof-of-Authority для моніторингу поставок у режимі реального часу. У наукових дослідженнях запропоновано чимало прототипів: зокрема, у дослідженні [3] описано блокчейн-протокол з консенсусним механізмом і розподілом ключів для захищеного обміну інформацією в фармацевтичному ланцюгу постачання, а в дослідженні [4] продемонстровано концепцію децентралізованого відстеження товарів із використанням смарт-контрактів на спільному реєстрі. Ці приклади підтверджують, що поєднання протоколів консенсусу та смарт-контрактів здатне вирішити низку практичних проблем логістики – від підробки документів до затримок у передачі інформації – та закласти основу для нових бізнес-моделей у вантажоперевезеннях.

Висновки. Впровадження блокчейн-технологій у системи управління вантажопотоками відкриває нові можливості для підвищення надійності та ефективності логістичних операцій. Протоколи консенсусу відіграють ключову роль у цих системах, забезпечуючи узгодженість даних між усіма учасниками мережі та створюючи довірене середовище без необхідності централізованого контролю. Смарт-контракти дозволяють автоматизувати виконання логістичних угод і процедур, зменшуючи вплив людського фактору та пришвидшуючи процеси. Децентралізована модель, підкріплена криптографією, гарантує високий рівень захисту інформації: дані про переміщення вантажів стають прозорими, але водночас захищеними від несанкціонованого втручання. З точки зору безпеки, блокчейн усуває багато вразливостей традиційних систем (таких як єдина точка відмови, можливість прихованої зміни записів), хоча і вимагає уваги до нових аспектів, зокрема безпеки смарт-контрактів та конфіденційності.

Таким чином, протоколи консенсусу та смарт-контракти мають значний потенціал у сфері логістики: їх застосування сприяє створенню стійких, прозорих та ефективних систем управління вантажопотоками. Подальші дослідження і пілотні проекти в цьому напрямі допоможуть вдосконалити масштабованість блокчейн-рішень, стандартизувати обмін даними між різними учасниками ланцюга постачання та вирішити поточні обмеження (наприклад, продуктивність та сумісність з існуючими системами). Безпекові аспекти залишаються пріоритетними: розвиток більш стійких алгоритмів консенсусу, аудит смарт-контрактів і комбінування блокчейну з іншими технологіями (IoT, хмарними сервісами) сприятиме ширшому впровадженню цих рішень у галузі вантажних перевезень. У підсумку, використання протоколів консенсусу в управлінні вантажопотоками є перспективним напрямом, що здатен революціонізувати глобальні ланцюги постачання, підвищуючи їх прозорість, безпеку та довіру між усіма сторонами.

ЛІТЕРАТУРА

1. Smart Contracts: Automation and Security in Freight Forwarding. Supply & Transport Logistics Blog, 15 жовтня 2024. URL: <https://supplyx.info/en/smart-contracts>.
2. Alqarni M.A., Alkathiri M.S., Chauhdary S.H., Saleem S. Use of Blockchain-Based Smart Contracts in Logistics and Supply Chains. Electronics, 12(6), 1340, 2023. URL: <https://www.mdpi.com/2079-9292/12/6/1340>.
3. Dwivedi S.K., Amin R., Vollala S. Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. Journal of Information Security and Applications, 54:102554, 2020. DOI: 10.1016/j.jisa.2020.102554.
4. Chang S.E., Chen Y.-C., Lu M.-F. Supply chain re-engineering using blockchain technology: a case of smart contract based tracking process. Technological Forecasting and Social Change, 144: 1–11, 2019. DOI: 10.1016/j.techfore.2019.03.015
5. Atzei N., Bartoletti M., Cimoli T. A survey of attacks on Ethereum smart contracts (SoK). Proc. Intl. Conf. Principles of Security and Trust (POST), LNCS 10204, pp. 164–186, 2017. DOI: 10.1007/978-3-662-54455-6_8.
6. Lopez E. Business Decision of the Year: Maersk and IBM team up to form TradeLens. Supply Chain Dive, 3 грудня 2018. URL: <https://www.supplychaindive.com/news/dive-award-2018-business-decision-ibm-maersk-blockchain/542162>.

CONSENSUS PROTOCOLS AND THEIR APPLICATION IN FREIGHT FLOW MANAGEMENT SYSTEMS

Velehura Yevhenii, Horiachkin Vadym

Abstract. *This paper presents a study of modern consensus protocols and their use in blockchain-based freight flow management. The technical aspects of implementing smart contracts in logistics processes are analyzed with a focus on data and transaction security. We show that a decentralized network, in which all participants must agree on updates to the ledger, ensures high data integrity and protection against unauthorized tampering. Examples of blockchain usage in logistics (cargo tracking, document automation) are provided, and the advantages of consensus algorithms in increasing transparency, trust among parties, and the resilience of freight systems are discussed. It is concluded that the application of consensus protocols is promising for building secure and efficient supply chain management systems.*

Keywords: *blockchain, consensus protocol, smart contract, logistics, freight flow, security, transparency.*

REFERENCES

1. Smart Contracts: Automation and Security in Freight Forwarding. Supply & Transport Logistics Blog, 15 October 2024. URL: <https://supplyx.info/en/smart-contracts>.
2. Alqarni, M.A., Alkathiri, M.S., Chauhdary, S.H., Saleem, S. Use of Blockchain-Based Smart Contracts in Logistics and Supply Chains. *Electronics* 12(6), 1340 (2023). URL: <https://www.mdpi.com/2079-9292/12/6/1340>
3. Dwivedi, S.K., Amin, R., Vollala, S. Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *J. Inf. Security and Applications* 54, 102554 (2020). DOI: 10.1016/j.jisa.2020.102554.
4. Chang, S.E., Chen, Y.-C., Lu, M.-F. Supply chain re-engineering using blockchain technology: a case of smart contract based tracking process. *Technol. Forecast. Soc. Change* 144, 1–11 (2019). DOI: 10.1016/j.techfore.2019.03.015.
5. Atzei, N., Bartoletti, M., Cimoli, T. A survey of attacks on Ethereum smart contracts (SoK). In *Proc. International Conference on Principles of Security and Trust (POST)*, LNCS 10204, 164–186 (2017). DOI: 10.1007/978-3-662-54455-6_8
6. Lopez, E. Business Decision of the Year: Maersk and IBM team up to form TradeLens. *Supply Chain Dive*, 3 Dec 2018. URL: <https://www.supplychaindive.com/news/dive-award-2018-business-decision-ibm-maersk-blockchain/542162/>.