УДК 004.415, 004.056

Т.О. ГОРЕЛІКОВА
Запорізький національний університет
О.В. ЧОПОРОВА
Київський національний економічний університет імені Вадима Гетьмана

РАНДОМІЗОВАНЕ ПІДТВЕРДЖЕННЯ БЛОКІВ У БЛОКЧЕЙН-СИСТЕМАХ

У статті запропоновано метод «Рандомізоване підтвердження блоків», призначений для підвищення безпеки, децентралізації та ефективності блокчейн-мереж різного масштабу. Метод базується на випадковому виборі вузлів для перевірки транзакцій та впровадженні контрольних точок для забезпечення узгодженості даних, відновлення після збоїв та корекції помилок. Випадковість у виборі перевіряючих вузлів унеможливлює централізоване маніпулювання мережею, знижує ризик зговору та зловмисного впливу великих учасників, робить проведення атак значно складнішим і менш прогнозованим. Контрольні точки дають змогу системі регулярно перевіряти стан блокчейну, автоматично коригувати неточності й забезпечують адаптивне відновлення після технічних збоїв або цілеспрямованих атак, зокрема 51%-атаки, подвійного блокування та спроб цензури транзакцій. Для надійного збереження критичних даних контрольні точки дублюються на кількох супервузлах, які вибираються випадковим чином із механізмом перевірки хешів на основі криптографічно захищених випадкових чисел, що унеможливлює підробку або зміну інформації. Упровадження випадкового вибору вузлів також дає змогу зменшити обчислювальне навантаження на учасників, підвищує продуктивність і масштабованість системи, швидше підтверджувати блоки та обробляти більшу кількість транзакцій. Метод демонструє ефективне поєднання принципів децентралізації, криптографічного захисту та адаптивного контролю даних. Він має на меті усунути деякі недоліки класичних систем, такі як централізація валідаторів, висока уразливість до втручання в систему, підробки і фальсифікації даних та неможливість ретроспективної перевірки даних, і відкриває нові можливості для створення безпечних, масштабованих та надійних блокчейн-мереж із високою стійкістю до зловмисних дій та технічних збоїв. Випадковий вибір учасників має на меті ускладнити маніпуляції з блокчейном, оскільки не можна передбачити, хто буде перевіряти блоки. Це має зробити мережу стійкішою до атак, таких як атаки «51%», коли зловмисники можуть контролювати більшість потужностей мережі.

Ключові слова: *блокчейн, випадковий вибір, контрольні точки, вузли, валідація.*

T.O. HORELICOVA
Zaporizhzhia National University
O.V. CHOPOROVA
Kyiv National Economic University named after Vadym Hetman

RANDOMIZED BLOCK CONFIRMATION IN BLOCKCHAIN SYSTEMS

The article proposes a method called «Randomized Block Verification» designed to improve the security, decentralization, and efficiency of blockchain networks of various scales. The method is based on randomly selecting nodes to verify transactions and implementing checkpoints to ensure data consistency, failure recovery, and error correction. Randomness in the selection of verifying nodes makes centralized manipulation of the network impossible, reduces the risk of collusion and malicious influence by large participants, and makes attacks much more difficult and less predictable. Checkpoints allow the system to regularly check the state of the blockchain, automatically correct inaccuracies, and provide adaptive recovery from technical failures or targeted attacks, including 51% attacks, double blocking, and attempts to censor transactions. To reliably store critical data, checkpoints are duplicated on several super-nodes, which are randomly selected with a hash verification mechanism based on cryptographically protected random numbers, which makes it impossible to forge or change information. The implementation of random node selection also reduces the computational burden on participants, increases the performance and scalability of the system, allows for faster confirmation of blocks and processing of a larger number of transactions. The method demonstrates an effective combination of the principles of decentralization, cryptographic protection and adaptive data control. It aims to eliminate some of the shortcomings of classical systems, such as the centralization of validators, high vulnerability to system interference, data forgery and falsification, and the inability to retrospectively verify data, and opens up new opportunities for creating secure, scalable and reliable blockchain networks with high resistance to malicious actions and technical failures. The random selection of participants is intended to make it more difficult to manipulate the blockchain, as it is not possible to predict who will validate blocks. This should make the network more resistant to attacks such as «51%» attacks, where attackers can control most of the network's capacity.

Key words: *blockchain, random selection, checkpoints, nodes, validation.*

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

Постановка проблеми

Розвиток блокчейн-технологій завжди супроводжувався пошуком компромісу між безпекою, децентралізацією (розподіл контролю та управління мережею між багатьма учасниками (вузлами), а не концентрацію його в руках єдиного центрального органу чи посередника) та ефективністю. Стандартні методи підтвердження блоків, такі як Proof-of-Work (PoW) та Proof-of-Stake (PoS), мають свої обмеження. PoW забезпечує децентралізацію, але потребує великих обчислювальних ресурсів, що робить його енергозатратним, повільним, уразливим до атак. PoS, своєю чергою, хоча й пришвидшує роботу блокчейну, проте не вирішує питання безпеки, адже більший контроль над блокчейн-системою отримують ті, хто має більше ресурсів у цій системі(порушення принципів децентралізації) [1; 2].

Атаки на блокчейн-системи є серйозними загрозами для їхньої безпеки та стійкості, оскільки вони підривають довіру, децентралізацію та консенсус (механізм або набір правил, за допомогою яких вузли розподіленої мережі (комп'ютери) доходять загальної згоди щодо правильності та порядку транзакцій), які є основою цієї технології. Однією з найвідоміших проблем є атака «51%», за якої зловмисник, котрий володіє більше ніж половиною обчислювальних потужностей мережі (частіше зустрічається в системах PoW), може переписувати блоки та історію транзакцій. Прикладом є атака на Ethereum Classic, яка спричинила крадіжку коштів у розмірі мільйона доларів і завдала шкоди репутації мережі, та випадок із Bitcoin Gold, де атака «51%» дала змогу зловмисникам украсти кошти на суму понад 18 млн доларів [3].

Не менш небезпечна і сибіл-атака, яка передбачає створення безлічі підроблених вузлів для отримання непропорційного впливу на мережу. Подібні атаки особливо критичні для блокчейнів, де консенсус залежить від голосування чи репутації вузлів (PoS та інші на цій основі). Наприклад, у системах Delegated PoS зловмисник може маніпулювати виборами валідаторів, створюючи загрозу централізації та консенсусу. Результатом таких атак стає утрата контролю над системою та уразливість мережі перед зміною інформації, що зберігається, і підробкою нової.

Атаки на консенсус також демонструють значний ризик. Вони включають маніпуляції процесом додавання блоків або впливу на валідаторів. У деяких системах зловмисники можуть вступати в змову для контролю мережі, як це було у блокчейні EOS. Ці дії підривають прозорість та рівноправність учасників, що, своєю чергою, ставить під сумнів децентралізованість мережі [4].

Окрім цього зараз існують більш тонкі атаки, такі як eclipse-атака, за якої вузол блокчейна ізолюється й отримує неправдиву інформацію про блоки та транзакції. Це дає зловмисникам змогу маніпулювати роботою вузла та порушувати консенсус, адже у класичній блокчейн-системі кожен вузол бере участь у погодженні кожної транзакції. Якщо eclipse-атака ізолює певну кількість вузлів, система буде дискредитована.

Зрештою, усі ці загрози демонструють важливість розроблення стійких механізмів захисту блокчейнів. Спеціалісти із захисту інформації вже деякий час працюють над цією проблемою, і були запропоновані деякі рішення. Системи, де вузли перевіряють лише випадково вибрані блоки або розподіляють обчислювальні завдання за випадковим принципом, можуть значно підвищити стійкість мережі до даних атак.

Аналіз останніх досліджень і публікацій

Концепція, коли для перевірки нових блоків випадково чи за заданим принципом вибираються вузли, уже використовується в деяких сучасних блокчейн-проєктах, хоча реалізується у різних варіаціях. Наприклад, у блокчейнах, які працюють на алгоритмах консенсусу PoS або його різновидах, вузли-валідатори вибираються по рівнях з урахуванням їх матеріального внеску в мережу. У таких системах, як Ethereum 2.0, Tezos або Cardano, для створення та перевірки блоків використовується принцип вибору, який базується на кількості монет, внесених у систему власником вузла.

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

Ethereum перейшов на алгоритм PoS з оновленням The Merge, що завершилось 15 вересня 2022 р., суттєво знизивши енергоспоживання (~на 99%). Для роботи валідатором необхідно придбати 32 ETH. Вибір валідатора для пропозиції блоку відбувається пропорційно обсягу вкладених коштів [5]. Це може створити ситуацію, коли кілька груп валідаторів можуть координувати дії чи стати об'єктом тиску з боку засновників мережі. Додатковим слабким місцем є уразливість до атаки довгострокової реорганізації ланцюга, якщо старі валідатори розпродують ключі зловмиснику.

Проєкт Cardano використовує серію доказово безпечних PoS-протоколів Ouroboros, розроблених академічною групою під керівництвом Аггелос Киайас (Университет Единбургу) [6; 7]. Cardano з протоколом Ouroboros позиціонується як найбільш формалізоване та математично обґрунтоване рішення PoS. Проте теоретична бездоганність приховує низку практичних слабкостей. По-перше, протокол складний у реалізації та потребує ідеальної роботи механізму криптографічної випадковості для вибору учасників мережі, який не реалізований практично. Будь-які уразливості у генерації випадкових чисел потенційно можуть використовуватися для передбачення чи заміни вибраних учасників. По-друге, Cardano страждає від того самого ризику централізації вузлів, що й Ethereum: незважаючи на велику кількість наборів вузлів, частка стейка розподілена нерівномірно. Окрім того, в умовах низької активності учасників децентралізація мережі виявляється скоріше декларативною, ніж фактичною. У реальній атаці достатньо контролювати кілька великих наборів вузлів, щоб вплинути на порядок блоків.

Tezos – блокчейн із консенсусом Liquid PoS, розроблений Артуром і Кетлін Брейтман. Валідатори вибираються за допомогою псевдовипадкового генератора (PRNG) на основі значення заплачених монет, збереженого в блокчейні, тобто результати детерміновані, але непередбачувані завчасно [8]. Tezos використовує механізм Liquid Proof-of-Stake (LPoS), який дає змогу користувачам делегувати свої права у мережі іншим учасникам мережі без утрати власності на токени (монети), що заборонено в інших механізмах. Це означає, що власник токенів передає іншому учаснику право виконувати дії вузла від його імені у процесі управління мережею, але при цьому сам залишається власником токенів і може їх використовувати або забрати назад у будь-який момент. Такий підхід значно спрощує участь у мережевому управлінні, оскільки не всі користувачі мають технічну можливість або бажання безпосередньо брати участь у роботі мережі.

Водночас виникає структурна проблема: делегування фактично концентрує вузли у невеликій групі операторів, що знижує рівень децентралізації та підвищує ризик координації між ними для власної вигоди.

Хоча мережа передбачає штрафи за порушення правил, наприклад за одночасне створення двох блоків (атака «подвійного блокування»), оператори з великою кількістю делегованих токенів можуть проводити цензуру транзакцій або маніпулювати валідацією. Таким чином, система залишається уразливою до концентрації впливу через делегування та соціальний тиск на основних учасників.

Інший підхід застосовується в алгоритмі Pure PoS, який реалізований у блокчейні Algorand. У цій моделі вузли, що беруть участь у валідації транзакцій та створенні нових блоків, вибираються випадковим чином, але ймовірність вибору вузла прямо пропорційна обсягу його стейку (кількості токенів).

Pure PoS був запропонований Сільвіо Мікалі (MIT) і впроваджений у Algorand, який стартував у 2019 р. Головна особливість алгоритму – секретний самовибір учасників консенсусу. Кожен вузол локально запускає Verifiable Random Function (VRF), яка визначає, чи буде вузол автором нового блоку або братиме участь у верифікації. Ймовірність вибору пропорційна стейку вузла.

Після цього вузол створює доказ вибору (proof), який може перевірити будь-який інший учасник мережі. При цьому особистість вибраного вузла стає відомою лише під час поширення

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

повідомлення про блок, що захищає мережу від атак типу DDoS. Завдяки цьому забезпечується ще більш рівномірний розподіл навантаження на мережу, а також зменшуються витрати часу на досягнення консенсусу [9]. Однак ключова вада тут – залежність від активності учасників. Насправді, лише небагато користувачів підтримують вузли, лише купують місце у мережі за токени та делегують участь валідації спеціалізованим структурам. Це руйнує ідею повної децентралізації та призводить до концентрації управління мережею колом людей. Ще однією уразливістю є так звана проблема «дилюції безпеки»: за надто низької кількості активних учасників імовірність атак усередині невеликих груп зростає.

Системи з шардінгом, такі як Zilliqa, також використовують механізм випадкового вибору вузлів для перевірки окремих сегментів ланцюжка. У шардінгових системах блокчейн розділений на шарди – невеликі незалежні частини, кожна з яких перевіряється окремою групою вузлів. Це дає змогу суттєво підвищити масштабованість мережі, адже кожен вузол відповідає лише за частину даних, а не за весь блокчейн. Теоретично така архітектура дає масштабованість та енергоефективність, але її складність – це водночас і головний мінус. Система шардингу уразлива до атак на малі шарди: якщо зловмисник контролює більше третини вузлів у конкретному шарді, він може порушити його роботу, підмінити дані чи додати невалідовані дані. Це особливо небезпечно в періоди, коли загальна кількість учасників невелика і деякі шарди виявляються занадто малими.

Нижче наведено табл. 1, що дає змогу наочно порівняти особливості Ethereum 2.0, Tezos, Cardano, Algorand і Zilliqa та оцінити ризики й переваги кожної системи.

Табл. 1 демонструє порівняння п’яти популярних блокчейн-мереж за ключовими параметрами їхніх механізмів консенсусу. Вона включає:

− Тип консенсусу – алгоритм, який забезпечує підтвердження транзакцій і створення блоків у мережі.

− Сильні сторони – основні переваги та технічні переваги кожного механізму консенсусу, що підвищують безпеку та ефективність мережі.

− Основні недоліки – обмеження та складнощі, пов’язані з участю користувачів, енергоспоживанням або централізацією.

− Уразливості до атак – потенційні загрози, на які мережа може бути схильна через концентрацію впливу, технічні особливості алгоритму або людський фактор.

Хоча всі ці підходи частково відображають ідею випадкового вибору вузлів для перевірки блоків і ланцюгів, ідея, коли вузли повного типу (Full Node) перевіряють лише випадково вибрані частини ланцюжка, не є загальноприйнятою практикою. Така концепція може мати великий потенціал, оскільки дає змогу суттєво знизити навантаження на вузли без утрати безпеки [3].

Таблиця 1

Порівняльна характеристика блокчейн-мереж за механізмом консенсусу

Мережа	**Консенсус**	**Сильні сторони**	**Основні недоліки**	**Уразливості до атак**
Ethereum 2.0	PoS	Математична безпека, механізми розподілу, фіналізація блоків	Високий бар'єр входу (32 ETH), концентрація у стейкінг-пулах, складність для звичайних користувачів	Long-range атака при продажі ключів, централізація пулів може імітувати 51%-атаку
Tezos	PoS	Доступність для делегування, низький поріг участі	Централізація у операторів, залежність учасників від довіри до валідатора	Маніпуляції під час валідації, продаж делегації вузла, цензура транзакцій

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

Продовження таблиці 1

Мережа	Консенсус	Сильні сторони	Основні недоліки	Уразливості до атак
Cardano	Ouroboros PoS	Формально доведена безпека, низьке енергоспоживання	Складність протоколу, залежність від випадковості, нерівномірний розподіл стейку	Захоплення кількох великих наборів вузлів може вплинути на мережу, атаки за слабкої генерації випадковості
Algorand	Pure PoS	Анонімний вибір валідаторів, швидка фіналізація, висока теоретична децентралізація	Низька активність користувачів, залежність від активності мережі	За низької активності можлива «розбавленість безпеки», зниження стійкості до довгострокових атак
Zilliqa	Гібрид (шардинг)	Масштабованість, висока пропускна здатність, стійкість до класичної 51%-атаки	Складність реалізації, енергоспоживання, ризик слабких шард	Захоплення >1/3 вузлів у шарді, атаки на малі шарди за низької диверсифікації

Саме тому був розроблений і запропонований метод «Рандомізоване підтвердження блоків», який використовує випадковий вибір вузлів для перевірки транзакцій та контрольні точки для забезпечення узгодженості даних одночасно.

Мета дослідження

Мета методу: забезпечити безпечну, децентралізовану та ефективну перевірку транзакцій у блокчейн-мережі, зменшити ризики централізації та маніпуляцій, а також підвищити стійкість системи до різноманітних атак і збоїв.

Завдання, які вирішує метод:

Децентралізація перевірки транзакцій: випадковий вибір вузлів для підтвердження блоків унеможливлює концентрацію голосів і централізовані маніпуляції.

Захист від атак: метод підвищує стійкість мережі до атак типу «51%», подвійного блокування, цензури транзакцій та картелізації великих учасників.

Забезпечення узгодженості даних: контрольні точки гарантують перевірку цілісності блокчейну та корекцію помилок у разі їх накопичення.

Відновлення після збоїв: система може адаптивно відновлювати стан блокчейну з останньої контрольної точки, мінімізуючи втрати даних і порушення цілісності транзакцій.

Підвищення ефективності та масштабованості: обмежена група випадково вибраних перевіряючих зменшує обчислювальне навантаження на вузли, прискорює процес підтвердження блоків та підвищує продуктивність мережі.

Надійне збереження критичних даних: супервузли зберігають контрольні точки з резервуванням та механізмами перевірки хешів, що унеможливлює підробку або втрату інформації.

Цей підхід базується на фундаментальній ідеї про те, що якщо учасники процесу підтвердження вибираються випадковим чином, то жоден окремий вузол або група не зможуть заздалегідь передбачити, хто саме буде здійснювати перевірку. Це унеможливлює централізоване маніпулювання мережею та робить атаки значно складнішими. Також випадковість у виборі контрольних точок дає змогу запобігати можливому накопиченню помилкових даних у блокчейні, оскільки система автоматично перевіряє та коригує інформацію.

Уведення контрольних точок дає змогу мережі самостійно відновлюватися після збоїв або атак. Це важливо, адже класичні блокчейни працюють у режимі безперервного додавання нових блоків без можливості ретроспективної перевірки. Якщо у традиційних системах будь-яка помилка або злом може викликати значні проблеми, то новий метод дає змогу блокчейну адаптивно відновлюватися, підтримуючи стабільність і цілісність транзакцій.

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

У цьому методі використовується випадковий вибір учасників, які будуть перевіряти транзакції та блоки. Це означає, що не всі учасники мережі перевіряють усі транзакції, а лише вибрана випадкова, кожний раз різна група. Для того щоб вибір цієї групи був справедливим, використовуються криптографічно захищені випадкові числа (генеровані за допомогою квантового генератор випадкових чисел). Такий підхід дає змогу значно зменшити обсяг обчислень для кожного учасника, зберігаючи при цьому високу ступінь безпеки, оскільки система стає менш уразливою до атак.

Наприклад, замість того щоб кожен учасник перевіряв увесь ланцюг блоків, система випадковим чином вибирає певну кількість учасників, які займаються перевіркою транзакцій. Це дає змогу розвантажити мережу та прискорити процес підтвердження блоків, а також ускладнити можливість маніпуляцій або атак із боку великих гравців.

У даному разі контрольні точки у цьому методі є визначеними моментами часу, коли перевірка даних відбувається більш ретельно. Вибір цих точок також здійснюється на основі випадковості, щоб уникнути маніпулювання системою. Кожна контрольна точка має певну кількість перевірок та кваліфікованих учасників, що дає можливість зробити мережу більш стійкою до змін і зловмисних атак.

Контрольні точки – це заздалегідь визначені моменти або етапи у ланцюзі блоків, коли система «перевіряє» стан блокчейн-мережі, перевіряючи правильність і консистентність даних.

Вони використовуються для двох основних завдань. Перше – це перевірка цілісності даних. Кожен вузол, працюючи з блоками, перевіряє, чи збігаються дані в контрольних точках із установленими стандартами. Якщо є відхилення від них, система автоматично запускає механізми корекції, попереджаючи учасників про потенційні порушення. Друге – відновлення у разі збою. Контрольні точки діють як «пам'ять» системи. У разі збоїв чи атак на мережу (наприклад, за спроби маніпуляції блоками чи спотворення даних), можна здійснити відновлення з останньої контрольної точки, що зменшує ймовірність утрати критично важливої інформації.

Контрольні точки зберігаються к супервузлах (Super Nodes). Це спеціальні вузли, які виконують додаткову функцію збереження важливих даних мережі, зокрема контрольних точок.

Для збереження контрольних точок мережа вибирає групу супервузлів випадковим чином. Це зменшує ймовірність атак та маніпуляцій. Вибір базується на алгоритмі випадковості.

Кожна контрольна точка копіюється на кілька (пропорційна кількість мережі) супервузлів, що підвищує надійність. Наприклад, якщо контрольна точка створена в блоці 1 000, вона буде розміщена мінімум на 10 супервузлах, і для її відновлення потрібно підтвердження хоча б семи з них. Цю кількість можна варіювати.

Хеш контрольної точки записується в блокчейн, що унеможливлює її зміну або підробку. Якщо дані на певному супервузлі будуть змінені, система зможе перевірити достовірність, порівнявши хеші.

Коли вузол потребує перевірки або відновлення, він надсилає запит до супер-вузлів. Щоб підтвердити правильність контрольної точки, мінімум 80% супервузлів повинні надати однакову версію даних.

Деякі звичайні вузли можуть кешувати контрольні точки для швидшого доступу, зменшуючи навантаження на супервузли.

Якщо супервузол виходить із мережі, мережа автоматично вибирає новий супервузол і копіює на нього контрольні точки. Якщо вузол утрачає дані, він отримує їх від інших супервузлів, використовуючи механізм перевірки хешів [1; 2].

Виклад основного матеріалу дослідження

Для забезпечення випадковості вибору учасників для валідації блоків використовуються криптографічно захищені випадкові числа. Це можуть бути числа, згенеровані на основі

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

еліптичних кривих (наприклад, рівняння $y^2 = x^3 + a*x + b$, де a і b – параметри кривої, а x і y – координати точок на кривій). Це дає змогу отримати передбачувані випадкові значення, які є важливими для чесного та захищеного процесу вибору учасників.

Замість того щоб кожен вузол перевіряв усі блоки, як у традиційних блокчейн-системах, використовується метод випадкового розподілу навантаження. Після того як майнер створює новий блок і вирішує криптографічну задачу (PoW), блок передається у мережу. Для перевірки цього блоку випадковим чином вибирається підмножина вузлів (у межах визначеного діапазону), що дає змогу рівномірно розподілити навантаження і знизити обчислювальні витрати.

Для валідації блоків використовується випадковий вибір контрольних точок – блоків, які підлягають перевірці. Це дає змогу зменшити кількість блоків, які перевіряються, оскільки перевіряються лише випадково вибрані блоки, а не весь ланцюг.

Для оптимізації перевірки блоків і забезпечення їх цілісності використовується структура Меркле-дерева. Кожен блок перетворюється на унікальний хеш, який об'єднується з хешами сусідніх блоків, утворюючи новий хеш для батьківського вузла. Процес триває до кореня дерева, який містить загальний хеш усього ланцюга. Це дає змогу перевіряти лише частину даних, що значно знижує навантаження на мережу.

За допомогою математичної операції модуля ($r \times |N|$) визначається, які саме вузли будуть брати участь у перевірці блоку. Це дає змогу рівномірно розподілити навантаження між усіма учасниками мережі та мінімізувати ресурси, необхідні для валідації. Вузли перевіряють лише випадково вибрані частини блокчейну, а не весь ланцюг.

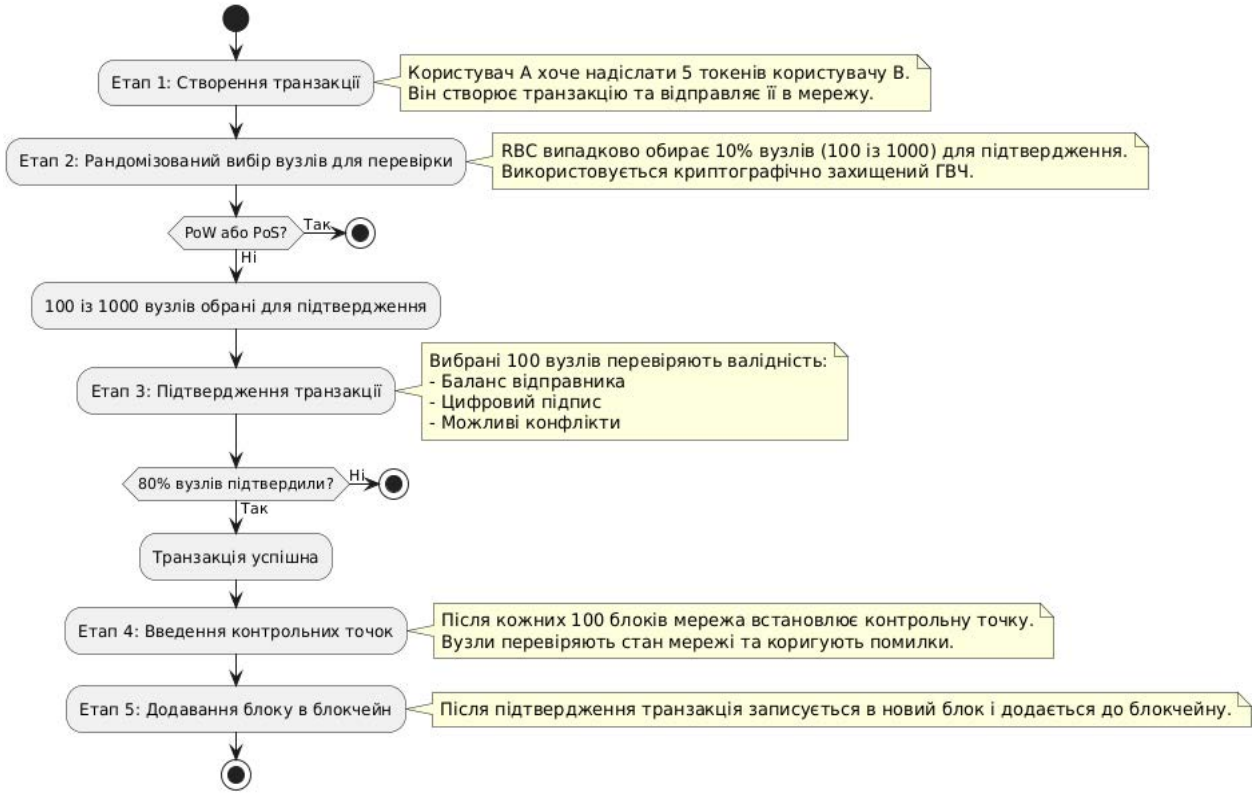

Рис. 1. Блок-схема прикладу роботи мережі з методом RBC

Джерело: розроблено авторами

Якщо хеш кореня Меркле-дерева не збігається, мережа ініціює поглиблену перевірку даних, починаючи з гілок дерева. Це дає змогу швидко виявити маніпуляції та атакувати несанкціоновані зміни, що забезпечує високу безпеку системи.

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

Система, заснована на випадковому виборі учасників і контрольних точок, робить блокчейн більш стійким до атак та маніпуляцій, оскільки процес перевірки блоків повністю непередбачуваний. Це забезпечує більшу безпеку і децентралізацію мережі.

Блок-схема описує процес підтвердження транзакцій у RBC. Спочатку користувач A створює транзакцію та відправляє її у мережу. Далі випадково вибирається 10% вузлів для перевірки, використовуючи криптографічно захищений генератор випадкових чисел. Вибрані вузли перевіряють баланс відправника, цифровий підпис і можливі конфлікти. Якщо 80% із них підтверджують транзакцію, вона вважається успішною. Після кожних 100 блоків мережа створює контрольну точку для перевірки та виправлення можливих помилок. Завершальний етап – додавання підтвердженої транзакції до нового блоку в блокчейні.

Переваги методу:

– Ефективність. Використання випадкового вибору учасників і контрольних точок дає змогу значно зменшити обчислювальні витрати на перевірку блоків. Мережа може обробляти більшу кількість блоків і транзакцій за менший час, що підвищує загальну ефективність та масштабованість системи.

– Справедливість і рівність. Випадковий вибір учасників для валідації дає кожному вузлу мережі рівні шанси бути вибраним для перевірки блоків, що дає змогу уникнути ситуацій із централізацією контролю і зловживаннями.

– Безпека. Використання криптографічних методів для генерації випадкових чисел і побудови Меркле-дерев забезпечує високу стійкість до атак і маніпуляцій із боку зловмисників. Мережа має високу ступінь захисту від фальсифікацій і несанкціонованих змін.

– Децентралізація. Завдяки випадковому вибору вузлів для перевірки блоків мережа стає більш децентралізованою. Це означає, що жоден вузол не має можливості взяти на себе повний контроль над валідацією блоків, що значно знижує ризик централізованих атак або маніпуляцій із боку великих учасників.

– Покращення масштабованості. Замість того щоб кожен учасник перевіряв кожен блок, що сильно навантажує систему, випадковий вибір учасників дає змогу зменшити кількість перевірок і тим самим підвищити пропускну здатність системи. Це дає блокчейну змогу масштабуватися і обробляти більше транзакцій без значних затрат на обчислення.

– Зниження витрат на обчислення. Метод випадкового вибору дає змогу знизити обчислювальні витрати, оскільки не потрібно перевіряти кожен блок або кожну транзакцію. Це робить процес валідації більш економічним і дає змогу знизити витрати на енергію.

– Забезпечення високої безпеки та довіри. Випадковий вибір і контрольні точки дають змогу забезпечити високий рівень безпеки, оскільки зловмисникам важко маніпулювати системою, коли вони не можуть передбачити, які блоки будуть перевірятися, а також який вузол буде вибраний для перевірки.

Об'єднаний метод випадкового вибору учасників і контрольних точок є ефективним та реальним підходом до покращення роботи блокчейн-систем. Завдяки цьому методу можна значно підвищити масштабованість, безпеку та децентралізацію, зменшуючи витрати на обчислення та забезпечуючи рівні шанси для всіх учасників у процесі валідації. Це відкриває нові можливості для розвитку блокчейн-технологій.

Висновки

Цей метод є реальним та ефективним завдяки поєднанню криптографії, випадковості й математичних моделей, які разом створюють нову ефективну систему для перевірки транзакцій. Випадковий вибір учасників дає змогу значно знизити обчислювальні витрати, покращити продуктивність системи та зробити її більш стійкою до маніпуляцій. Криптографічні механізми, які використовуються для забезпечення випадковості, гарантують, що процес вибору учасників залишається прозорим і безпечним.

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

Метод «Рандомізоване підтвердження блоків» реалізує низку принципових покращень порівняно з класичними механізмами консенсусу, такими як PoS або Liquid PoS:

– Учасники, які підтверджують транзакції та блоки, вибираються випадково за допомогою криптографічно захищених генераторів випадкових чисел.

– Жоден вузол або група не може передбачити, хто буде перевіряти транзакції, що унеможливлює централізоване маніпулювання мережею та знижує ризик картелізації великих учасників.

– Зменшує ймовірність атак, пов'язаних із концентрацією голосів, цільовими маніпуляціями або цензурою транзакцій.

– Контрольні точки визначаються у певні моменти часу та використовуються для ретельної перевірки стану блокчейну.

– Кожна контрольна точка перевіряється кваліфікованою групою вузлів, що гарантує коректність і цілісність даних.

– У разі збоїв або атак мережа може відновити стан блокчейну з останньої контрольної точки, що знижує ризик утрати критично важливої інформації і робить систему більш стійкою до довгострокових атак.

– Контрольні точки дублюються на кількох випадково вибраних супервузлах, що зменшує можливість маніпуляцій і підвищує надійність збереження даних.

– Хеш контрольної точки записується в блокчейн, що унеможливлює її зміну або підробку.

– Для підтвердження правильності контрольної точки необхідна консенсусна згода більшості супервузлів (наприклад, ≥80%), що ускладнює атаки на окремі вузли та маніпуляції даними.

– Не всі вузли перевіряють увесь ланцюг блоків, а лише вибрана випадковим чином група, що зменшує обчислювальні витрати без зниження безпеки.

– Мережа стає більш масштабованою та швидшою, а процес підтвердження блоків – оперативнішим.

– Випадковість вибору вузлів та контрольних точок ускладнює проведення атак типу «51%», подвійного блокування та цензури транзакцій.

– Контрольні точки дають змогу швидко відновити консистентний стан мережі після будь-яких спроб маніпуляцій або збою вузлів.

Цей метод поєднує кілька технологій, таких як криптографія для забезпечення випадковості, нові математичні моделі для оптимізації процесів перевірки і захисту від атак, а також випадковий вибір учасників, що допомагає зберігати баланс у децентралізованій мережі. Це дає змогу значно покращити масштабованість і безпеку блокчейн-систем без утрати її децентралізованої природи.

Оскільки перевірка транзакцій відбувається лише для вибраної групи учасників, усі інші вузли можуть зосередитися на своїх завданнях, не витрачаючи надмірних ресурсів на обробку всіх транзакцій. Це дає змогу мережі працювати швидше та ефективніше.

Випадковий вибір учасників ускладнює маніпуляції з блокчейном, оскільки не можна передбачити, хто буде перевіряти блоки. Це робить мережу стійкішою до атак, таких як атаки «51%», коли зловмисники можуть контролювати більшість потужностей мережі.

Завдяки випадковому вибору учасників для валідації цей метод не дає змоги великим компаніям або майнінговим пулам отримати занадто великий контроль над мережею. Кожен учасник має рівні шанси бути вибраним для перевірки блоків, що допомагає зберігати принципи рівності та справедливості в мережі.

Завдяки цьому методу блокчейн-системи можуть бути більш масштабованими, безпечними і ефективними, що відкриває нові можливості для їх використання в різноманітних сферах.

https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 ISSN 2618-0332 (print), 2618-0340 (online)

Список використаної літератури

1. Horelikova T.O. Enhanced data protection in blockchain: mitigating tampering and deletion through randomized checkpoints. *Infocommunication and Computer Technologies.* 2024. T. 2. P. 40–47. https://doi.org/10.36994/2788-5518-2024-02-08-05
2. Горелікова Т.О. Механізм захисту інформації від підміни та видалення у блокчейн-мережах. *Екзистенційні виклики освіти, науки, безпеки та здоров'я в сучасних умовах: дослідження молодих учених*, м. Одеса, 12 грудня 2024 р. Одеса, 2024. С. 89. https://doi.org/10.32782/2663-5682/2024/41/19
3. Saad M., Spaulding J., Njilla L., Kamhoua C., Shetty S., Nyang D. Aziz Mohaisen, Exploring the Attack Surface of Blockchain: A Systematic Overview. *IEEE Communications Surveys & Tutorials***.** 2020. https://doi.org/10.1109/COMST.2020.2975999
4. Guru A., Mohanta B.K., Mohapatra H., Al-Turjman F., Altrjman,C., Yadav A. A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Journals Applied Sciences.* 2023. T. 13, № 4. P. 2604. https://doi.org/10.3390/app13042604
5. Neu J., Kiayias A., Danezis G. Incentive Analysis of Ethereum's Proof-of-Stake Protocol. *IEEE Symposium on Security and Privacy.* 2023. https://doi.org/10.1109/SP46215.2023.00108
6. Kiayias A., Russell A. Ouroboros-BFT: A Simple Byzantine Fault Tolerant Consensus Protocol [Cryptology ePrint Archive. 2018]. URL: https://eprint.iacr.org/2018/1049.pdf
7. David B., Gaži P., Kiayias A., Russell A. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. *Edinburgh Research Explorer.* 2017. P. 573. https://doi.org/10.1007/978-3-319-78375-8_3
8. Neuder M., Moroz D. Rithvik Rao R., Parks D. Defending Against Malicious Reorgs in Tezos Proof-of-Stake. *AFT '20:* Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, New York, October 21–23. NY, United States. 2020. P. 46–58. https://doi.org/10.48550/arXiv.2009.0541
9. Gilad Y., Hemo R., Micali S., Vlachos G., Zeldovich N. Algorand : Scaling Byzantine Agreements for Cryptocurrencies. 2017. URL: https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf (дата звернення: 11.10.2025).

References

1. Horelikova, T.O. (2024). Enhanced data protection in blockchain: mitigating tampering and deletion through randomized checkpoints. *Infocommunication and Computer Technologies,* 2, 40–47. https://doi.org/10.36994/2788-5518-2024-02-08-05 [in English].
2. Horelikova, T.O. (2024). Mekhanizm zakhystu informatsii vid pidminy ta vydalennia u blokcheinmerezhakh [Mechanism for protecting information from substitution and deletion in blockchain networks], Ekzystentsiini vyklyky osvity, nauky, bezpeky ta zdorovia v suchasnykh umovakh: doslidzhennia molodykh uchenykh, materialy Vseukrainskoi naukovo-praktychnoi konferentsii [Existential challenges of education, science, security and health in modern conditions: Research by young scientists, Proceedings of the All-Ukrainian Scientific and Practical Conference], Odesa, December 12, 2024. https://doi.org/10.32782/2663-5682/2024/41/19 [in Ukrainian].
3. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Aziz Mohaisen, A. (2020). Exploring the Attack Surface of Blockchain: A Systematic Overview. *IEEE Communications Surveys & Tutorials.* https://doi.org/10.1109/COMST.2020.2975999 [in English].
4. Guru, A., Mohanta, B.K., Mohapatra, H., Al-Turjman, F., Altrjman, C., & Yadav, A. (2023). A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Journals Applied Sciences,* 13 (4), 2604. https://doi.org/10.3390/app13042604 [in English].
5. Neu, J., Kiayias, A., & Danezis, G. (2023). Incentive Analysis of Ethereum's Proof-of-Stake Protocol. *IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/SP46215.2023.00108 [in English].

6. Kiayias, A., & Russell, A. (2018). Ouroboros-BFT: A Simple Byzantine Fault Tolerant Consensus Protocol [Cryptology ePrint Archive]. Retrieved from https://eprint.iacr.org/2018/1049.pdf [in English].
7. David, B., Gaži, P., Kiayias, A., & Russell, A. (2017). Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. *Edinburgh Research Explorer.* https://doi.org/10.1007/978-3-319-78375-8_3 [in English].
8. Neuder, M., Moroz, D. Rithvik Rao, R., & Parks, D. (2020). Defending Against Malicious Reorgs in Tezos Proof-of-Stake. *AFT '20:* Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, New York, October 21–23. NY, United States. https://doi.org/10.48550/arXiv.2009.0541 [in English].
9. Gilad, Y., Hemo, R., Micali, S., Vlachos G., & Zeldovich, N. (2017). Algorand: Scaling Byzantine Agreements for Cryptocurrencies. [arXiv]. Retrieved from https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf [in English].

Горелікова Тетяна Олексіївна – здобувач вищої освіти на третьому (освітньо-науковому) рівні вищої освіти за спеціальністю «Комп'ютерні науки» Запорізького національного університету. E-mail: uyxkdyc@gmail.com, ORCID: 0009-0001-9098-4618.

Чопорова Оксана Володимирівна – доктор філософії, доцент кафедри комп'ютерних наук Київського національного економічного університету імені Вадима Гетьмана. E-mail: o.choporova@gmail.com, ORCID: 0000-0003-3167-7869.

Horelikova Tetiana Oleksiivna – Postgraduate Student in Computer Science of the Zaporizhzhia National University. E-mail: uyxkdyc@gmail.com, ORCID: 0009-0001-9098-4618.

Choporova Oksana Volodymyrivna – PhD in Computer Science, Associate Professor at the Department of Computer Science of the Kyiv National Economic University named after Vadym Hetman. E-mail: o.choporova@gmail.com, ORCID: 0000-0003-3167-7869.

Дата надходження статті: 31.10.2025
Дата прийняття статті: 02.12.2025
Опубліковано: 30.12.2025