

УДК 004.3

Неласа Г.В.¹, Самойлик С.С.¹, Неласий О.В.²

¹ доц. НУ «Запорізька політехніка»

² асп. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ СУЧАСНИХ НАПРЯМКІВ РОЗРОБКИ ПРОТОКОЛІВ КОНСЕНСУСУ В ТЕХНОЛОГІЇ БЛОКЧЕЙН

У контексті технології блокчейн термін "консенсус" позначає процедуру розподіленого обчислення деякого спільного значення для всіх учасників, що поєднує елементи голосування та узгодження. Правила консенсусу дозволяють забезпечити обробку інформації в блокчейні, запобігти появі форків (розгалужень ланцюга блоків) а також перевіряти чесність учасників.

Протокол консенсусу містить правила для створення наступного блоку, процедури вирішення конфліктів, а також правила, які заохочують учасників мережі підтримувати функціонування блокчейну та дотримуватися протоколу. Проблема побудови протоколів узгодження у розподілених мережах була відома задовго до виникнення поняття "блокчейн" і формулювалася як проблема "візантійських генералів" в інтерактивних алгоритмах. На сьогоднішній день, відомі такі основні підходи як Proof-of-Work (PoW), Proof-of-Stake (PoS) та Byzantine Fault Tolerance (BFT), в рамках яких вже розроблено багато протоколів, які розрізняються як алгоритмами, що використовуються, так і наявністю відповідних властивостей.

Основні властивості сучасних протоколів консенсусу:

- safety – здатність облікової системи зберігати основні принципи функціонування та інтереси чесних учасників за будь-яких зловмисних впливів;

- finality – властивість, яка вказує на можливість скасування прийнятого рішення або підтверджених даних;

- liveness – властивість, яка гарантує, що якщо всі чесні учасники хочуть додати запис до загальної бази даних, то в результаті вона буде туди додана;

- persistence – здатність облікової системи зберігати незмінність кінцевого стану своєї бази даних навіть після відмови валідаторів;

- permissioned – вказує на обмеження, тобто необхідність отримати дозвіл на участь у певному процесі;

- permissionless означає вільний доступ до участі в деякому процесі;

- resiliency – стійкість до атак.

Історично найпершим успішним в практичній реалізації став протокол консенсусу *підтвердження роботи PoW (Proof-of-Work)*[1]. Необхідність повільного виконання певного, досить складного, завдання дало можливість отримати затримку в часі при формуванні кожного блоку, достатню для виконання синхронізації мережі. Використання односпрямованих хеш-функцій вносить необхідну асиметрію в процес узгодження стану мережі: надає можливість швидко і легко перевірити результат, для отримання якого використовуються важкі обчислення. При цьому ймовірність створення наступного блоку певним майнером пропорційна його обчислювальним потужностям (хешрейту). Однак протокол Proof-of-Work є повільним у роботі, а також вимагає значного споживання електроенергії та обчислювальних потужностей для розрахунків. Головним недоліком PoW-консенсусу, є те, що важкі розрахунки, які проводяться в процесі майнінгу, не мають жодного корисного застосування і слугують лише для забезпечення надійності мережі. Також існує потенційна загроза атаки 50%, коли користувач або група користувачів контролюють більшість видобувних потужностей мережі, що дозволяє їм маніпулювати подіями в мережі.

Від цих недоліків позбавлений протокол *доказу участі PoS (Proof-of-Stake)*, який наразі використовується Ethereum 2.0 (Beacon Chain) та деякими іншими блокчейн-мережами. Тут валідатори обираються для створення нових блоків на основі їх ставки (stake) (частки криптовалюти, яку вони тримають і «блокують» як заставу). Чим більша частка валідатора у загальній сумі, тим більше його шанси на генерацію наступного блоку і отримання нагороди. Менше споживання енергії в порівнянні з PoW та краща масштабованість і швидший час підтвердження транзакцій роблять PoS гідною альтернативою для PoW. Безпека в PoS залежить від припущення, що валідатори мають сильний економічний стимул бути чесними. У протоколі *делегованого доказу участі DPoS (Delegate-Proof-of-Stake)* основний принцип полягає у поділі голосуючих і валідуючих учасників. Власники монет з вагою голоса, пропорційно своїм балансам, обирають вузли-валідатори.

Головна перевага протоколів, основаних на *BFT* підході – гарантоване кінцеве число кроків, тобто раундів роботи протоколу, за яке всі вузли приходять до єдиного рішення. Перший такий протокол, застосований практично *Practical BFT* був запропонований у 1999 році [2]. Клієнт звертається до сервера, якого обирає лідером. Лідер передає ці повідомлення іншим серверам. Після цього сервера повідомляють один одному про те, що надійшли певні повідомлення і їх необхідно внести до спільної бази даних. Кожен із валідаторів має підтвердити, що він отримав підтвердження від інших учасників. Коли валідатор отримав підтвердження від $\frac{2}{3}$ інших учасників про включення повідомлення до своєї копії бази даних, воно вноситься в локальну копію даного валідатора.

Протокол *Hashgraph* [3] працює швидко та добре масштабується. Кожен із валідаторів збирає свої транзакції, вибирає довільним чином іншого учасника та надсилає йому дані про свої транзакції, а також інформацію, яку повідомили йому інші вузли, коли підключалися до нього, тобто валідатор «слухає», приймає всі повідомлення, які надходять до нього, а після цього довільним чином обирає іншого учасника та надсилає йому всі транзакції разом зі своїми. Він вимагає більшого обсягу трафіку, ніж Algorand, але в той же час є дуже ефективним. Hashgraph забезпечує властивості Safety і Liveness, тобто додавання нових транзакцій та узгодження єдиного рішення. Він працює навіть в умовах повністю асинхронної мережі, коли повідомлення можуть бути затримані на великий проміжок часу або взагалі викинуті. Крім того, в мережі відсутній лідер, що дозволяє зловмисникові виводити з ладу ті вузли, які йому виявляються цікавими, може змушувати їх працювати за своїми намірами. Однак, поки зберігається $\frac{2}{3}$ чесних користувачів, протокол забезпечує високий рівень безпеки.

Протокол Algorand [4] використовує той самий BFT-підхід, але він орієнтований на те, що серед усіх учасників випадково обирається певний

підкомітет, який виконує підтвердження транзакцій. Причому це підтвердження відбувається у кілька етапів, на кожному з яких вибирається свій підкомітет. Протокол гарантує з високою ймовірністю, близькою до одиниці, що підкомітет є чесним, якщо більше $\frac{2}{3}$ учасників мережі є чесними, тобто кожен із підкомітетів також матиме $\frac{2}{3}$ чесних учасника. Тут немає лідера, тому немає точки для атаки типу «відмова в обслуговуванні» (DoS-атаки). Цей протокол забезпечує високу пропускну спроможність облікової системи, швидке підтвердження транзакцій та захист від атаки «adaptive corruption».

Подальшого дослідження потребують такі протоколи: Ouroboros, BFT-Smart, Honeybadger BFT, SBFT, GPBFT, Red Belly, Tendermint, HotStuff, PaLa, Fast-HotStuff, Streamlet, Polygraph, DAG, Avalanche. Важливо зазначити, що розглянуті протоколи консенсу мають свої переваги та обмеження, а вибір протоколу залежить від конкретного випадку використання, цілей мережі та компромісів між такими факторами, як безпека, масштабованість, децентралізація та енергоефективність. Різні блокчейн-проекти можуть вибирати різні консенсусні протоколи на основі своїх конкретних вимог і пріоритетів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
2. Miguel Castro and Barbara Liskov, Practical Byzantine Fault Tolerance//3rd Symposium on Operating Systems Design and Implementation (OSDI 99) New Orleans, LA, 1999.
3. Baird, L. The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance, 2016, <http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf>
4. Build the future on Algorand [Електронний ресурс] - режим доступу: <https://developer.algorand.org>