УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.125

ПРОТОКОЛ ДОСЯГНЕННЯ КОНСЕНСУСУ OUROBOROS ДЛЯ БЛОКЧЕЙН МЕРЕЖ

Набойщиков Б.Ю.
Науковий керівник – PhD, доцент Родінко М. Ю.
Харківський національний університет ім. В.Н. Каразіна, каф. МСіТ, м. Харків, Україна
naboishchykov2020ks13@student.karazin.ua

This work is dedicated to providing a general description of the Ouroboros protocol as the first developed Proof-of-Stake consensus protocol built on a secure blockchain, along with its formal rationale, as well as the concept of Verifiable Random Function, which is commonly used in the protocol.

Блокчейн протоколи на основі Proof of Work (PoW), такі як Bitcoin, розраховують на велику кількість ресурсів для генерації блоків в ланцюжках записів. І хоч на практиці це може й не бути проблемою для деяких компаній або користувачів – альтернативний протокол взаємодії з блокчейном все ж таки мав бути розроблений для потреб клієнтів з вимогами до ресурсів. Протокол на основі Proof of Stake (PoS) – «Ouroboros» запропонував свою концепцію роботи яка вирішувала проблеми протоколів PoW, гарантуючи такі ж стандарти безпеки.

До недавнього часу блокчейн протоколи PoW мали лідируючу позиції на ринку – але різкий перехід таких платформ як Ethereum на PoS – призвело до підвищеної зацікавленості в таких методах. Також, можливість блокчейну створювати децентралізовану, прозору та незмінну систему запису, що може ефективно взаємодіяти з різноманітними пристроями в мережі IoT розширює можливості використання PoS[1].

Proof-of-Stake (PoS) — широко поширений альтернативний механізм, який працює за принципом «підтвердження частки». Замість того, щоб покладатися на енергоємне обладнання для перевірки транзакцій, PoS використовує мережеві пристрої або вузли для перевірки та запису транзакцій, а також отримує винагороду у вигляді криптовалюти. Замість хешування даних процес перевірки в PoS в основному визначається випадковістю обчислень, при цьому вага участі вузла залежить від суми фінансової застави або частки, яку він вніс у мережу через ставку[2].

Алгоритми PoS використовують різні методи для вибору вузлів, які слугуватимуть валідаторами. Імовірність того, що вузол стане валідатором,

зростає з кількістю токенів, які він поставив, а також є більша ймовірність відбору для вузлів, які зберігають свої токени протягом більш тривалого періоду часу, не витрачаючи їх.

Хоча процес вибору валідатора в PoS надає перевагу учасникам з більшою часткою, цей протокол включає випадкові механізми для запобігання централізації, забезпечуючи справедливий і неупереджений відбір[3].

Ouroboros — це перший доведено безпечний протокол Proof-of-Stake і перший протокол блокчейну, заснований на рецензованих дослідженнях. Ouroboros поєднує унікальну технологію та математично перевірені механізми для забезпечення безпеки, стабільності та масштабованості блокчейнів, які його використовують.

Ouroboros використовує криптографію, комбінаторику та математичну теорію ігор для забезпечення цілісності, довговічності та продуктивності протоколу. Він забезпечує такий же рівень безпеки, як консенсус Proof-of-Work. Застосовуючи випадковий вибір лідера та вимагаючи, щоб принаймні 51% від загальної частки належало чесним учасникам, протокол гарантує безпеку. Крім того, він проходить постійний розвиток і ретельний аналіз безпеки. Управління мережею розподіляється між пулами розміщення, якими керують оператори вузлів із необхідною інфраструктурою для постійного та надійного з'єднання. Лідер слота обирає пул ставок для кожного слота, і пул отримує винагороду за додавання нового блоку до ланцюжка[4]. Стабільний консенсус в Ouroboros досягається завдяки використанню верифікованої випадкової функції(VRF).

У 1999 році група інформатиків і математиків, у тому числі Сільвіо Мікалі, Майкл Рабін і Саліл Вадхан, представили концепцію випадкової функції, що піддається перевірці (Verifiable Random Function, VFR) в опублікованій статті. З тих пір було зроблено прогрес для вдосконалення технології. У 2015 році Денніс Гофхайнц і Тібор Ягер використали криптографію еліптичної кривої для створення високозахищеного VRF. Пізніше, у 2019 році, Нір Бітанскі продемонстрував, що VRF можна побудувати за допомогою різних загальних примітивів, розширюючи можливості за межі алгебраїчних конструкцій. VRF, по суті, є генераторами випадкових чисел (RNG), які проходять криптографічну перевірку. Після його використання спеціалізований алгоритм забезпечує підтвердження VRF. Щоб кваліфікуватись як VRF, функція f має відповідати певним умовам.

Представлення f є компактним і неявним, що ускладнює ефективне обчислення. З іншого боку, існує компактне та явне представлення f, яке дозволяє «власнику» ефективно обчислювати його.

Таким чином, дану пару можна розглядати як відкритий ключ PKf та його відповідний секретний ключ SKf.

Більшість ГВЧ не генерують криптографічно перевірювані випадкові числа, що робить їх сприйнятливими до маніпуляцій, таким чином обмежуючи їх використання. Забезпечуючи безпеку випадкових чисел, VRF відкриває багато важливих застосувань, наприклад:

– Інтернет-безпека – VRF використовується для захисту повідомлень системи доменних імен (DNS);

– технологія нульового знання – VRF використовується для розробки протоколів захисту від нульового розголошення;

– неінтерактивна система лотерей – VRF забезпечує чесні та ефективні результати лотереї;

– блокчейн і смарт-контракти – VRF став важливою частиною децентралізованих протоколів і смарт-контрактів [5].

Таким чином, протокол консенсусу Ouroboros на основі Proof of Stake дозволяє досягти високого рівня безпеки за допомогою концепції VFR, при цьому, забезпечуючи значну швидкість обробки транзакцій та заощаджуючи енергоресурси системи.

Список використаних джерел

1. Просолов В. В. Використання блокчейн технології з машинним навчанням для безпечних IoT / В. В. Просолов, Г. З. Халімов // Проблеми інформатизації : тези доповідей одинадцятої міжнар. наук.-техн. конф., 16–17 листопада 2023 р. – Баку-Харків-Бельсько-Бяла, 2023. – Т. 2, секція 3,6. – С. 46. (дата звернення: 04.03.2024).

2. Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus / Mikolaj Karpinski, Lyudmila Kovalchuk, Roman Kochan, Roman Oliynykov, Mariia Rodinko, Lukasz Wieclaw. Sensors. 2021. Vol. 21, no. 19. P. 6408. URL: https://doi.org/10.3390/s21196408. (дата звернення: 04.03.2024).

3. Blockchain Consensus Algorithms: A Survey. Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, Alan Colman. 2020. 39 c. URL: https://www.researchgate.net/publication/338738073_Blockchain_Consensus_Algorithms_A_Survey. (дата звернення: 04.03.2024).

4. Roman Oliynykov, Aggelos Kiayias, Alexander Russell, Bernardo David. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. 2017. 67 c. URL: https://iohk.io/en/research/library/papers/ouroboros-a-provably-secure-proof-of-stake-blockchain-protocol/. (дата звернення: 02.03.2024).

5. Micali S., Rabin M., Vadhan S. Verifiable random functions. 40th annual symposium on foundations of computer science (17-19 січня 1999р.). New York, USA (date of access: 04.03.2024).