НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ В ЕНЕРГЕТИЦІ – 2025»

Збірник матеріалів конференції
26 березня 2025 р.

Київ – 2025

УДК 620.9 + 349 + 004 + 003.26

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол № 3 від 27.03.2025)

Організаційний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Програмний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Відповідальний за випуск:
В.О. Артемчук

Usage of blockchain technologies in energetics – 2025: collection of materials of the scientific and practical conference, Kyiv, March 26, 2025, PIMEE of NAS of Ukraine. - 2025. - 84 p.

Використання блокчейн технологій в енергетиці – 2025 : збірник матеріалів науково-практичної конференції, м. Київ, 26 березня 2025 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2025. – 84 с.

В.О. Побережник, В.С. Балацька

КОНЦЕПЦІЯ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПІДТВЕРДЖЕННЯ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ДАНИХ

Блокчейн сьогодні знайшов своє застосування у багатьох сферах [1]. Основними характеристиками технології, які забезпечують її успіх є:

- Незмінність: жодна інформація, збережена у блокчейні, не може бути змінена.
- Децентралізованість: на відміну від традиційних систем, роботу мережі підтримується кожним вузлом мережі.
- Криптографія: публічні адреси користувачів генеруються за допомогою криптографічних методів, які не дозволяють визначити приватний ключ, а кожен блок даних в блокчейні криптографічно пов'язаний із наступним – геш попереднього блоку зберігається у наступному, що дозволяє зберігати блоки пов'язані між собою і виявляти будь-які зміни.

Ці характеристики дозволяють розглядати блокчейн як своєрідну базу даних, яка може забезпечувати цілісність та автентичність даних, пов'язуючи дані та їхнього творця публічним ключем, за замовчуванням. Тому, застосування технології блокчейн можна розглядати як основу для створення системи, яка можна виконувати завдання підтвердження цілісності даних, що є важливим для роботи різних ресурсів, зокрема для державних реєстрів, оскільки вони потребують інформацію, яка є достовірною, цілісною та автентичною, щоб унеможливити будь-які махінації із нею.

Однак, попри очевидні переваги технології, вона має свої недоліки [2]. Однак, одним із основних недоліків є проблема масштабованості мережі, оскільки розмір блокчейну негативно впливає на швидкодію мережі, збільшуючи час на обробку транзакцій в мережі. Окрім цього збільшуватиметься і сама вартість обслуговування мережі з ростом розміру даних, які циркулюють в мережі, яскравим прикладом цього процесу є блокчейн Bitcoin як для підтримки своєї роботи щорічно споживає 87 ТВт.год [3], що зумовлене використанням алгоритму PoW [4].

Якщо нівелювання недоліку споживання великої кількості енергії можна обійти вибором іншого алгоритму консенсусу, наприклад, PoS [5], то сама обробка інформації потребує вибору іншого підходу до обробки самої інформації. Вирішенням цієї проблеми є застосування підходу, який виносить обробку інформації за межі мережі блокчейн, але зберігає в мережі лише необхідні дані для підтвердження даних. Такий підхід відомий як Layer 2[6].

Спираючись на ідеї Layer 2 можна розробити концепцію застосування технології блокчейн для забезпечення цілісності та автентичності інформації.

Основний принцип роботи такої системи заснований на ідеї збереження відбитку даних у мережі блокчейн. Такий підхід дозволить зберігати дані

поза мережею блокчейн, що знизить навантаження на саму систему, а самі відбитки даних – у мережі блокчейн, що дозволить гарантувати достовірність відбитків, що дозволить користувачам системи підтвердити цілісність та достовірність даних. Відбиток даних можна отримати шляхом генерування геш значення даних, наприклад через застосування алгоритмів сімейства SHA-2, які одночасно визнанні безпечними і дозволяють гешувати об'єми інформації розміром до 2^{64} байтів. Також для забезпечення автентичності інформації, можна застосувати алгоритм HMAC, який одночасно дозволяє підтверджувати цілісність та автентичність інформації. Такий підхід дозволить зберігати саму інформацію у потенційно небезпечному середовищі, перевагою якого є те, що воно може значно ефективніше зберігати саму інформацію, однак не має тих переваг, які надає блокчейн, а в блокчейні зберігати лише відбитки даних, оскільки він дозволяє забезпечувати збереження незмінною, однак не може продемонструвати таку саму простоту у збереженні даних та масштабуванні, як традиційні системи. Тобто такий підхід дозволяє використати блокчейн одночасно із традиційними системами збереження даних, що дозволить одночасно задіяти їхні сильні сторони та нівелювати слабкі. Втім, варто зазначити, що при розробці такої системи слід зважати на ряд викликів, які можуть постати, зокрема те, що такий спосіб є ефективним, коли інформацію створює та підписує сторона із високим рівнем довіри, оскільки такий метод не дозволяє підтвердити правдивість інформації, оскільки він орієнтований на те, щоб підтвердити цілісність та автентичність, а не доброчесність користувачів системи.

1. 40 blockchain applications | real-world use cases in 2025 - webisoft blog. (б. д.). Webisoft. https://webisoft.com/articles/blockchain-applications/

2. GeeksforGeeks. (2022, 2 лютого). Advantages and disadvantages of blockchain - geeksforgeeks. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-blockchain/

3. How much energy does bitcoin consume? | crypto.com. (б. д.). Crypto.com | Securely Buy, Sell & Trade Bitcoin, Ethereum and 400+ Altcoins. https://crypto.com/bitcoin/bitcoin-energy-consumption

4. Academy, B. (2018, 6 грудня). What is proof of work (pow)? | binance academy. Binance Academy. https://academy.binance.com/uk-UA/articles/proof-of-work-explained

5. Academy, B. (б. д.). Proof of stake (pos) | binance academy. Binance Academy. https://academy.binance.com/uk-UA/glossary/proof-of-stake

6. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). SoK: Layer-two blockchain protocols. У Financial cryptography and data security (с. 201–226). Springer International Publishing. https://doi.org/10.1007/978-3-030-51280-4_12