УДК 681.12

Ю. Ю. Нікітін

ПРОГРАМНІ ЗАСОБИ СИСТЕМИ ОНЛАЙН ГОЛОСУВАННЯ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Вінницький національний технічний університет

Анотація

В даній роботі розглядається алгоритм та метод розробки програмного засобу для створення надійної та безпечної системи голосування за допомогою технології блокчейн.

Ключові слова: метод, алгоритм, програмний засіб, блокчейн, голосування.

Abstract

This paper describes an algorithm and a method for developing a software tool for creating a reliable and secure voting system using blockchain technology.

Keywords: method, algorithm, software, blockchain, voting.

Багато країн використовують машини для голосування, які є досить застарілими, тому вони стають дорогими для підтримки, а також мають ряд недоліків. Система голосування, побудована з використанням технології блокчейн, може вирішити деякі з цих питань, виключивши шанси отримати більше голосів, ніж зареєстрованих виборців, припинити шахрайство виборців, представити аудиторські звіти, які можуть бути перевірені масами, за допомогою яких буде підвищуватися прозорість голосування.

Блокчейн - це структура даних, в якій дані організовуються як блоки, а блоки об'єднуються разом, щоб сформувати ланцюг транзакцій. Створення кожного блоку засноване на останньому блоці найактуальнішого ланцюга, і вони обробляються вузлами в мережі за допомогою Peer-to-Peer (P2P) з'єднання. Кожне створення вимагає дотримання механізмів консенсусу, таких як доказ роботи (PoW), який використовується в біткоіні та доказові стану (PoS), що використовується в PPCoin [1]. Алгоритм роботи системи представлено на рис. 1.

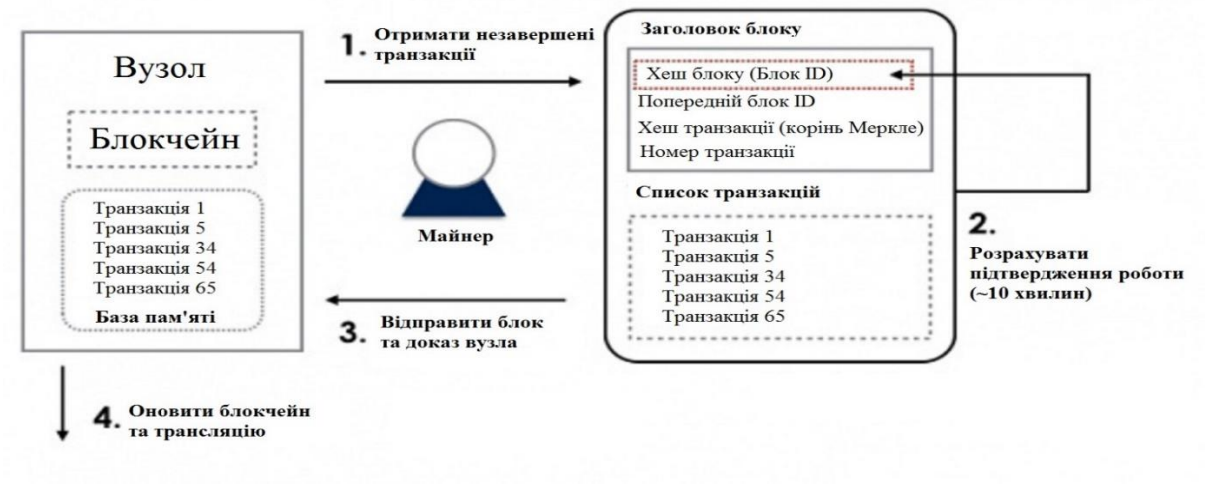

Рис. 1. Алгоритм роботи системи за допомогою технології блокчейн.

Якщо протягом одного короткого періоду створюється більше одного блоку, вся мережа P2P приймає тільки найдовший ланцюжок, що може призвести до створення конкуренції. Ця конкуренція гарантує, що мережа завжди підтримує унікальний ланцюжок. Відповідно до механізмів консенсусу, спотворені дані вузлів, такі як відхилення від початкового ланцюга, будуть виявлені та відхилені від інших вузлів [2]. На рис. 2 представлено схему створення транзакцій в системі блокчейн.

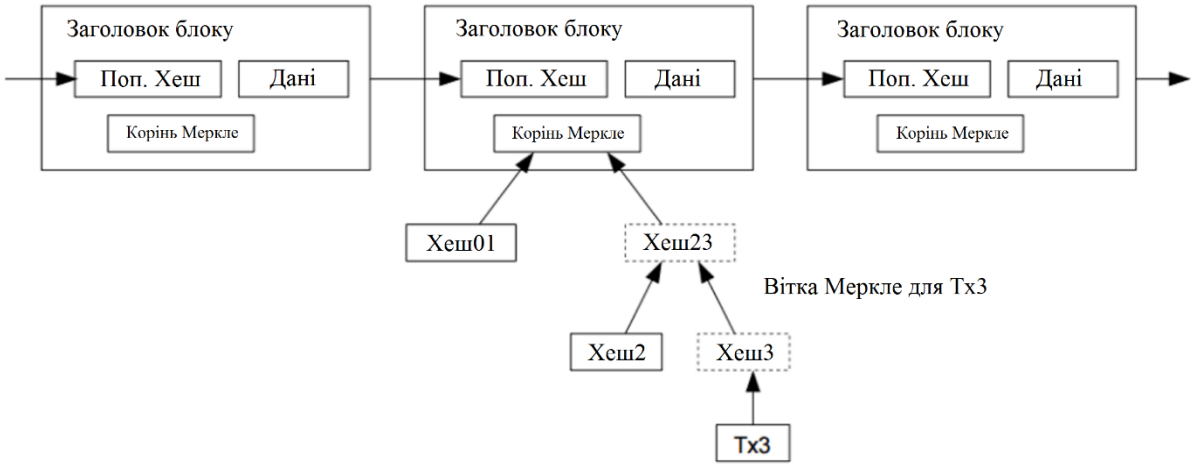

Рис. 2. Схема створення транзакцій в системі блокчейн.

Архітектура програмного засобу має два окремих блокчейни, один для інформації про виборців, а інший - для голосування. Ці блокчейни утримаються повністю окремо, щоб обмежити будь-яку загрозу для об'єднання голосів для окремих партій окремим виборцям, зберігаючи при цьому можливість відстежувати, хто голосував, і скільки голосів дійсно присутні.

Блокчейн, що містить інформацію про те, хто зареєструвався для голосування, також дозволяє системі забезпечити кожного виборця унікальними голосами. Після реєстрації кожен користувач отримує право на голосування після перевірки даних. Щоб забезпечити, що зареєстровані виборці унікальні, існує 3-хфакторний метод автентифікації.

Використовуючи технологію блокчейн, запропоновано алгоритм і програмний засіб для онлайн голосування. Розглянутий метод дозволяє підвищити прозорість та надійність системи голосування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. King S., Nadal S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. Self-published paper, August 19 (2012) – 68p.

2. Andrychowicz M., Dziembowski S., Malinowski D., Mazurek L.: Secure multiparty computations on bitcoin. In: 2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014, IEEE Computer Society (2014) – 443p.

Нікітін Юрій Юрійович — студент групи 1КІ-16м, факультет інформаційних технологій та комп'ютерної інженерії, група 1КІ-16м, Вінницький національний технічний університет, м. Вінниця.

Науковий керівник – ***Черняк Олександр Іванович*** – к.т.н., доцент, Вінницький національний технічний університет, м. Вінниця.

Nikitin Yurii Y. — Department of Building Heating and Gas Supply, Vinnytsia National Technical University, Vinnytsia.

Supervisor - ***Chernyak Alexander I.*** — Cand. Sc. (Eng), Assistant Professor, Vinnytsia National Technical University, Vinnytsia.