**УДК: 004.043**

# СИСТЕМА ЕЛЕКТРОННОГО ГОЛОСУВАННЯ С ЗАХИСТОМ ВІД ФАЛЬСИФІКАЦІЙ

Черніков М. М.
к.т.н., доцент кафедри ІС Болтьонков В.О.
Одеськи Національній Політехнічний Університет, УКРАЇНА

**АННОТАЦІЯ.** У роботі розглянуто практичну реалізацію системи електронного голосування з використанням технологіх блокчейн для захисту від фальсифікацій. У якості блокчейну з підтримкой смарт-контрактів було використано систему Ethereum.

**Вступ**. Система електронного голосування значно спрощує процес отримання та обробки даних, але може мати недоліки, якими зможуть використатись для фальсифікації голосування, що є значною проблемою. Щоб цього уникнути, необхідно створити систему, яка значно понижує ризик фальсифікацій. Такою системою є голосування на основі технології блокчейну. Блокчейн, тобто ланцюжок блоків транзакцій — розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає. База захищена від підробки та переробки. Кожен блок містить часову мітку та посилання на попередній блок.

Блок транзакцій — спеціальна структура для запису групи транзакцій. Щоб транзакція вважалася достовірною («підтвердженою»), її формат і підписи повинні перевірити і потім групу транзакцій записати в спеціальну структуру — блок. Інформацію в блоках можна швидко перевірити. Кожен блок завжди містить інформацію про попередній блок. Усі блоки можна вибудувати в один ланцюжок, який містить інформацію про всі вчинені коли-небудь операції.

Якщо використовувати систему блокчейн як місце зберігання даних, можливо забезпечити захист від зміни даних після запису у систему. Також якщо використати якусь загальну систему та зробити голосування відкритим (але сховати справжні імена голосуючих за їх унікальними адресами), можливо надати доступ комісії для перевірки даних через стандартні методи блокчейну, код яких відкритий та перевірений. Для цієї задачі підходить блокчейн-система Ethereum.

Ethereum, Етеріум — платформа для створення практично будь-яких децентралізованих онлайн-сервісів на базі блокчейна, що працюють на базі розумних контрактів. Реалізована як єдина децентралізована віртуальна машина. Оскільки Ethereum сильно спрощує і здешевлює впровадження блокчейна, його впроваджують багато великих корпорацій для різних цілей. Для створення алгоритму голосування та зберігання даних необхідно створити смарт-контракт.

Смарт-контракт — комп'ютерний протокол, який спрощує, верифікує, або забезпечує дотримання переговорів, або виконання договору, перевіряє непотрібні пункти договору. Смарт- контракти, зазвичай, мають інтерфейс користувача і часто слідують логіці договірних положень. Прихильники розумних контрактів стверджують, що таким чином багато видів договірних положень може бути здійснено частково або повністю, самостійно або вдвох. Смарт-контракти спрямовані на забезпечення безпеки, яка перевершує традиційне договірне право, а також на зменшення операційних витрат. Смарт контракт додається до системи один єдиний раз та його код не може бути змінений після цього. Він зберігається на окремій адресі та усі транзакції, в яких виконуються методи смарт-контракту спрямовані до цієї адреси.

**Мета.** Метою роботи є побудова системи електронного голосування с захистом від фальсифікацій з використанням блокчейн-технологій.

**Основна частина роботи.** Для створення роботи використана система Ethereum та розроблен смарт-контракт на мові програмування Solidity, яку ця система підтримує. Для зручності голосування також був розроблений веб-додаток (серверна частина на мові програмування Java, та веб-інтерфейс з використанням розмітки HTML та стилів CSS), який інтегрується з системою блокчейн та слугує інтерфейсом для голосування та перевірки даних. Смарт-контракт є центром системи голосування та повинен брати на себе її захист. Перевірка даних у коді веб-додатка повинна бути тільки додатковою, а не основною.

Увесь процес голосування проходить через декілька підсистем (рис. 1).

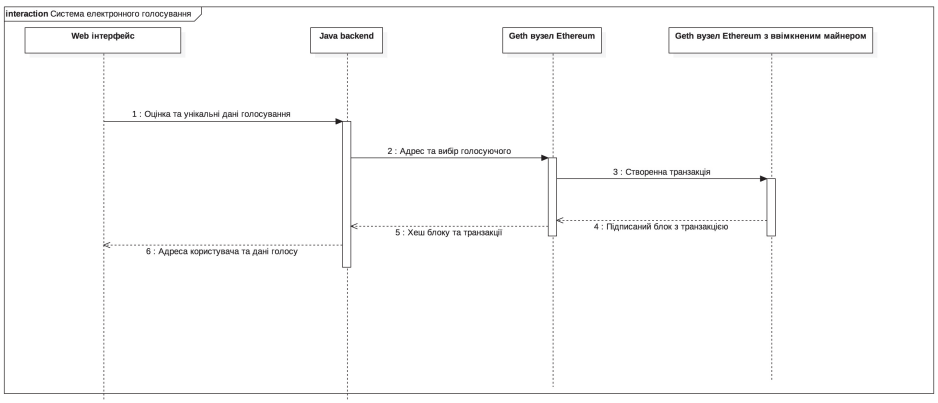


Рисунок 1 – Взаємодія систем при голосуванні

Спочатку дані надходять від користувача, який заповнив їх у веб інтерфейсі, до серверу (Java backend). Дані перевіряються на правильність та можливість користувача проголосувати. Якщо усі дані вірні, сервер відправляє їх на зберігання до блокчейну, використовуючи методи смарт- контракту. Сам вузол geth (так називається вузол блокчейну Ethereum) перевіряє дані та створює транзакцію виклика метода смарт-контракту. Для підписки транзакції та додавання до блоку необхідно передати її до майнеру (якщо блокчейн працює на PoW), або до авторизованого вузла, що має можливість підписувати блоки (PoA).

Методи смарт-контракту перевіряють та захищають від повторного голосування та не санкціанованого доступу до голосування. Під час запуску системи потрібно мати список з усіх голосуючих. Наприклад, якщо система використовуються для виборів і голосуючими є усі громадяни України, їх дані потрібно занести до серверу (Java backend), та сервер при розгортанні контракту створить усім голосуючим унікальні адреси та додасть їх до списку голосуючих контракту.

Для з'єднання серверу з вузлом geth слугує RPC інтерфейс Ethereum, який має назву web3 та строгий список методів. На сервері використовується бібліотека, яка є імплементацією web3 на мові програмування Java. Вона має назву web3j. Сервер та geth спілкуються через текстові повідомлення з використанням протоколу HTTP. Основними повідомленнями серверу, які відправляються до вузла, є створення контракту, створення користувачів з адресами, та виклики методів смарт- контракту (Наприклад, метод vote).

**Висновок.** Система електронного голосування значно спрощує процес отримання та обробки даних, але може мати недоліки, якими зможуть використатись для фальсифікації голосування, що є значною проблемою. У практичній частині був створений додаток, який інтегрується з блокчейн-системою Ethereum з використанням смарт-контракту, розробленим на мові програмування Solidity, для значного зниження можливості фальсифікації голосування.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ethereum Github Repository – Source code and documentation – [Електронний ресурс] / Режим доступу: https://github.com/ethereum

2. Ethereum Official Website – Democracy contract – [Електронний ресурс] / Режим доступу: https://www.ethereum.org/

3. Данильчук Р. К. Аналіз основних принципів технології blockchain / Р. К. Данильчук, О. С.Жураковська // Науковий огляд. – 2017. – № 10(42). – С. 1-11.

4. Prusty N. Building Blockchain Projects. Develop Real-time Practical DApps using Ethereum and JavaScript. — Birmingham — Mumbai: Packt Publ. , 2017. — 245 p.