УДК 004.75

# СИСТЕМА ГОЛОСУВАННЯ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN

**Шпінталь М.Я.[1)] , Джулій М.В.[2)], Коцій І.С.[3)]**
*Західноукраїнський національний університет*
*к.т.н., доцент; [2)] аспірант; [3)] магістрант*

## І. Постановка проблеми

Стрімкий розвиток технологій має сприяти спрощенню та прозорості важливих державних процесів. На даний момент в Україні запроваджено, та успішно функціонує декілька систем на основі технології Blockchain, але головна проблема нашої держави досі актуальна.

Стаття присвячена аналізу та розробці системи електронного голосування на основі технології блокчейн. В даній статті розглянуті основні недоліки існуючого процесу голосування, та розглянуто можливості впровадження принципово нового підходу до проведення голосування. Завдяки якому вирішуються проблеми фальсифікації, анонімності та прозорості.

## ІІ. Мета роботи

Метою роботи розгляд проблем існуючої системи виборів та розгляд можливості переносу процесу голосування в цифровий простір. Розгляд технології Blockchain як найбільш підходить для вирішення основних проблем існуючого процесу голосування.

## ІІІ. Аналіз проблем існуючого процесу голосування

Основні недоліки існуючого процесу голосування можна розділити на такі секції:

- Технічні: можливість не контрольованого вкидання бюлетені, фальсифікація, використання зникаючого чорнила на ділянках для підробки результатів, підробка протоколів, порушення таємниці голосування, навмисні помилки в підрахунках, низька швидкість підрахунку результатів.
- Соціальні: підкуп; адміністративний тиск на виборця, явка виборців.
- Економічні**:** висока вартість для державного бюджету.

Звичайно, ці проблеми стараються вирішити тим чи іншим способом проведення голосування, але все зводиться до змішаної виборчої системи. Де намагаються зменшити негативні впливи на виборчий процес [3].

На даний момент частину з описаних проблем вирішують електронні системи голосування які застосовуються в таких країнах як Індія, Бразилія, Естонія, Нідерланди, США [1], хоча такі системи мають деякі мінуси, зокрема:

- Проблеми з безпекою - електронні системи можуть бути зламані.
- Проблеми з верифікацією результатів виборів - на відміну від паперових бюлетенів, які можна перерахувати.
- Можливість некоректної роботи системи через помилки в програмному забезпеченні.

В основі технології блокчейн лежить транзакційна модель: у кожного користувача є гаманець, з унікальними публічним і приватним ключами, якими він підтверджує будь-які зміни даних. Вся інформація про транзакції зберігається в послідовно записаних блоках, таким чином, хеш даних попереднього блоку входить в дані наступного так забезпечується незмінність даних, зміна будь-якого блоку автоматично зробить не валідними всі наступні блоки. Блокчейн зберігає всю інформацію про всі транзакції одночасно на всіх вузлах, яка не може бути змінена або видалена [2].

Застосування блокчейна дає додаткові переваги:

Надійність результатів. Результати голосування, організованого з застосуванням блокчейн технологій, неможливо підробити. Завжди можна перевірити, скільки голосів було випущено на початку голосування, як вони розподілялися по гаманцях і в який час проводилися транзакції.

Прозорість процесу. Блокчейн дає можливість контролю за ходом голосування, так як будь-яка зацікавлена особа може розгорнути вузол з повною копією всіх даних і самостійно проаналізувати їх на рівні блокчейна.

Анонімність. Кожен учасник голосування має можливість створити пару з публічного і приватного ключа на локальній машині і ніхто, крім нього не буде знати про те, що конкретний гаманець належить саме йому.

Голосування на основі технології blockchain може мати наступний вигляд:

1. Виборець має з'явитися до органу ведення Реєстру виборців з паспортом та ідентифікаційним кодом. Після перевірки особи виборця йому буде наданий одноразовий ключ, який необхідний для того, щоб виборець міг додати свій відкритий ключ у базу даних.
2. Виборець, використовуючи свій персональний пристрій, генерує електронний цифровий підпис. Авторизовавшись на сайт, за допомогою одноразового ключа, виборець публікує свій відкритий ключ. Відкритий ключ публікується у списку виборців навпроти відповідного виборця. Генерація ключів є обов'язковою процедурою для усіх виборців для забезпечення коректної роботи системи.
3. Виборець має завантажити та встановити програмне забезпечення для електронного голосування на свій персональний пристрій. Хеш-сума програмного забезпечення має бути опублікована на сайті, для того щоб виборець мав змогу переконатися, що було завантажено та встановлено офіційне програмне забезпечення і в нього не були внесені будь-які зміни.
4. Після закінчення завантаження програмного забезпечення баз даних система електронного голосування автоматично відправить запит на отримання випадкових вхідних даних для вирішення асиметричної задачі.
5. Асиметрична задача вирішується на пристрої виборця або в мережі blockchain. Знаходження рішення задачі є ресурсномістким процесом. Отримане рішення задачі, підписане приватним ключем, передається до мережі. Рішення задачі є доказом виконаної роботи (PoW) та є аналогом підпису виборця у виборчому списку при традиційному голосуванні. Вирішення ресурсномісткої задачі необхідно для захисту системи електронного голосування від можливого масового фіктивного голосування, оскільки дане завдання вимагатиме наявності великої обчислювальної потужності у зловмисників.
6. Виборець підписує свій бюлетень приватним ключем та відправляє запит на додавання підписаного бюлетеня у базу даних.
7. Після перевірки того, що цей бюлетень ще не був доданий до бази даних та підписаний особистим ключем виборця, він додається у мережу блокчейн, а виборцю надається можливість додати свій голос у базу даних.
8. Після того, як виборець проголосував, для підтвердження голосування йому потрібно залишити свій підпис. Підпис та час голосування буде використаний для генерації хеш-суми. Генерація хеш-суми відбуватиметься на персональному пристрої виборця. Ця хеш-сума буде додана до голосу виборця, який буде записаний у базу даних.
9. Голос виборця записується у базу даних, після чого можливість виборця додати голос до бази даних анулюється.
10. Додавання нових голосів після завершення виборів має бути неможливим, для забезпечення достовірності результатів.

Варіантів реалізації може бути багато, так як технології не стоять на місці, наприклад можна використати смарт-контракти. Але децентралізовані системи не позбавлені недоліків. Основна проблема децентралізованої системи це "Атака 51%". Означає що в децентралізованій системі хтось володіє 51% ресурсів, фактично володіє всією системою. Також до проблем можна віднести вартість введення та підтримки подібної системи. Якщо хтось має більше 51% обчислювальної потужності, то він може вирішувати задачі (PoW) швидше ніж інші, це означає, що він має повноваження вирішувати, який блок допустимий. Але всі недоліки можливо вирішити і дана система може запропонувати надійну на прозору систему голосувань [4].

## Висновок

У даній роботі було проаналізовано існуючу виборчу систему та можливість її заміни на електронну систему голосувань. Розглянуто можливий алгоритм роботи системи та її недоліки.

## Список використаних джерел


ectronic voting [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Electronic_voting.

2. Blockchain [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Blockchain.
3. Порівняльний аналіз основних виборчих систем: проблема вибору оптимальної моделі виборчої системи для України у плані дотримання демократичних принципів виборів. // Українська національна ідея: реалії та перспективи розвитку. – 2009. – №21. – С. 58–62.

Challenges. // International Journal of Network Security. – 2017. – С. 653–659.