

УДК 004.42

DOI 10.30837/bi.2025.2(103).08

І. В. Кириченко¹, Г. Ю. Терещенко², К. О. Гоцуляк³, В. О. Каленик⁴¹ХНУРЕ, м. Харків, Україна, iryna.kyrychenko@nure.ua, ORCID iD: 0000-0002-7686-6439²ХНУРЕ, м. Харків, Україна, hlib.tereshchenko@nure.ua, ORCID iD: 0000-0001-8731-2135³ХНУРЕ, м. Харків, Україна, kateryna.horishnia@nure.ua, ORCID iD: 0009-0001-9032-4249⁴ХНУРЕ, м. Харків, Україна, vira.kalenyk@nure.ua

ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРОЗОРОСТІ ВИБОРЧИХ ПРОЦЕСІВ В ОРГАНІЗАЦІЯХ

У роботі розглянуто підхід до створення децентралізованої системи електронного голосування на основі блокчейна Ethereum. Модель поєднує смарт-контракти, механізм commit–reveal та токени прав голосу у форматі SBT, що забезпечує прозорість, захист від маніпуляцій і неможливість передачі голосу. Офчейн-сервер використовується лише для журналювання подій та аналітики, не впливаючи на підрахунок. Експериментальні дослідження у мережі Sepolia підтвердили коректність роботи системи та її придатність для застосування в організаційних виборах. Результати демонструють перспективність блокчейн-підходу для підвищення довіри та безпеки цифрових виборчих процесів.

БЛОКЧЕЙН, ЕЛЕКТРОННЕ ГОЛОСУВАННЯ, СМАРТ-КОНТРАКТИ, COMMIT–REVEAL, ПРОЗОРИСТІ ВИБОРІВ, ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ, SOULBOUND-ТОКЕНИ, ETHEREUM

I. V. Kyrychenko, G. Yu. Tereshchenko, K. O. Gotsulyak, V. O. Kalenyk. Blockchain-Based Approach to Ensuring Transparency in Organizational Voting Processes. This paper presents a decentralized electronic voting system built on the Ethereum blockchain. The proposed model integrates smart contracts, a commit–reveal mechanism, and soulbound voting rights tokens to ensure transparency, resistance to manipulation, and prevention of vote transfer. An off-chain server is used only for logging and analytics, without affecting vote counting. Experimental evaluation in the Sepolia test network confirmed the system's correctness and suitability for organizational voting scenarios. The results highlight the potential of blockchain-based solutions to enhance trust, security, and transparency in modern digital voting processes.

BLOCKCHAIN, ELECTRONIC VOTING, SMART CONTRACTS, COMMIT–REVEAL, ELECTION TRANSPARENCY, DECENTRALIZED SYSTEMS, SOULBOUND TOKENS, ETHEREUM

Вступ

Електронні виборчі системи дедалі частіше впроваджуються у великих компаніях, університетах, громадських організаціях та комітетах як інструмент оперативного й зручного прийняття колективних рішень. Перехід до цифрових форм голосування обумовлений потребою у швидкості, доступності та автоматизації виборчих процесів, а також прагненням зменшити витрати на організацію традиційних паперових виборів. Проте незважаючи на очевидні переваги, більшість сучасних веб-систем голосування залишаються вразливими до низки загроз, що суттєво знижують рівень довіри до їхніх результатів [1].

Проблеми централізованих платформ полягають у можливості маніпуляцій з боку адміністратора, зміні або видаленні бюлетенів, некоректному підрахунку голосів, а також у ризику компрометації сервера, на якому зберігаються всі дані. Централізована модель створює єдину точку відмови, а доступ адміністратора до внутрішніх даних відкриває можливості для втручання, фальсифікацій чи прихованих модифікацій результатів [2, 3]. Навіть за умови використання сучасних криптографічних методів, таких як шифрування чи електронні підписи, довіра учасників до системи значною мірою залишається пов'язаною з довірою до того, хто контролює серверну інфраструктуру [4].

Блокчейн-технології дають змогу усунути або значно зменшити ці ризики, забезпечуючи незмінність даних, публічний журнал подій, можливість незалежного аудиту та прозору перевірку результатів голосування. Децентралізовані мережі усувають необхідність у довіреному посереднику, а всі операції зберігаються у вигляді послідовних, захищених від змін блоків. Особливо важливою є можливість застосування смарт-контрактів, які реалізують підрахунок голосів детермінованим способом, без участі довіреного сервера, що повністю усуває людський фактор при визначенні підсумків виборів [5].

Окремої уваги заслуговує той факт, що блокчейн дозволяє перевірити правильність результатів будь-якому сторонньому спостерігачеві. Користувачі можуть переглядати всі події голосування у публічному реєстрі, а валідність даних гарантується криптографією та принципами консенсусу [6]. Такий підхід підвищує довіру до виборчого процесу та робить можливими чесні, прозорі вибори в організаціях будь-якого масштабу.

Метою роботи є створення прототипу децентралізованої системи електронного голосування, яка гарантує прозорість, перевірюваність і безпеку виборчого процесу, а також формалізація вимог, моделі та архітектури майбутнього рішення.

У межах дослідження передбачається аналіз сучасних підходів до електронного голосування, визначення

недоліків централізованих систем, розробка архітектурної моделі з використанням блокчейна, створення смарт-контрактів для реалізації виборчих процедур та проведення експериментальних досліджень роботи прототипу.

1. Огляд існуючих рішень

Дослідження у сфері електронного голосування протягом останніх років привели до появи різноманітних систем, однак більшість із них залишаються обмеженими у питаннях прозорості та захисту від маніпуляцій [5]. Традиційні веб-платформи, що застосовуються у компаніях, університетах та громадських організаціях, базуються на централізованій архітектурі, де всі дані зберігаються та обробляються на одному сервері. У такій моделі адміністратор має широкі технічні можливості впливати на перебіг голосування, а відсутність зовнішнього аудиту не дозволяє учасникам перевірити достовірність підрахунку голосів. Незважаючи на використання криптографічних механізмів захисту, централізація залишає системи вразливими до підміни, видалення або маніпулювання результатами.

Спробою вирішити ці проблеми стали криптографічні платформи без використання блокчейна. Найвідомішим прикладом є система Helios, яка реалізує гомоморфне шифрування та дозволяє відкрито перевіряти правильність підрахунку [7]. Однак навіть такі рішення не усувають залежність від сервера, на якому здійснюється прийом, зберігання та первинна обробка бюлетенів, що зберігає ризик внутрішньої компрометації. Комерційні мобільні платформи, такі як Voatz, пропонують удосконалені механізми автентифікації, проте їхні алгоритми не є відкритими, а використання приватних блокчейнів позбавляє виборчий процес необхідної прозорості [8].

Поява публічних блокчейнів, зокрема Ethereum, дала можливість створювати децентралізовані системи голосування, у яких підрахунок і зберігання даних не контролюються жодною окремою стороною. Найпоширенішим підходом у таких рішеннях є механізм `commit-reveal`, що дозволяє приховувати вибір до завершення голосування та забезпечує його перевірюваність після розкриття [9]. Завдяки незмінності блокчейна результати виборів стають доступними для незалежної перевірки, а смарт-контракти усувають людський фактор у підрахунку голосів. Проте навіть блокчейн-платформи залишають деякі виклики, пов'язані з вартістю транзакцій, необхідністю взаємодії через криптогаманці та відсутністю універсальних стандартів управління правами голосу.

Таким чином, попри значну кількість існуючих рішень, більшість систем не забезпечують одночасно прозорість, перевірюваність, відсутність довіреної сторони та зручність використання. Це підтверджує необхідність створення нової моделі електронного

голосування, яка поєднуватиме переваги публічного блокчейна, відкритої архітектури та доступності для широкого кола користувачів.

2. Постановка задачі

У сучасних умовах організації різного масштабу потребують інструментів, які дозволяють проводити вибори швидко, безпечно та прозоро, незалежно від місця знаходження учасників. Однак традиційні підходи до електронного голосування не здатні повною мірою забезпечити довіру до результатів, оскільки спираються на централізовану інфраструктуру, де адміністратор відіграє ключову роль у зберіганні та обробці даних [10]. Це створює низку потенційних ризиків, серед яких підміна бюлетенів, приховані зміни результатів, видалення даних або втручання у логіку підрахунку. Щоб усунути ці загрози, необхідно розробити систему, яка б не покладалася на довірені сторони та водночас забезпечувала технічну можливість для незалежної перевірки всіх етапів виборчого процесу.

Поставлена в роботі задача полягає у створенні моделі та прототипу децентралізованої системи голосування, яка ґрунтується на використанні блокчейн-технологій як механізму забезпечення незмінності даних та прозорого аудиту. Для її реалізації необхідно визначити вимоги до системи, що охоплюють як функціональні властивості, так і загальні принципи взаємодії між учасниками процесу. Система має підтримувати реєстрацію виборчих кампаній, визначення часових меж голосування, авторизацію виборців, подання голосів у заздалегідь прихованому вигляді та їх подальше розкриття після завершення голосування. Важливим аспектом є побудова механізму підтвердження права на участь у голосуванні, що виключає можливість дублювання голосів або участі неавторизованих користувачів.

Для досягнення поставленої мети необхідно формалізувати моделі даних, які описують виборчі кампанії, учасників, бюлетені та результати голосування, а також визначити архітектуру системи, що поєднуватиме можливості блокчейна та допоміжних офчейн-компонентів. Особливе місце займає визначення протоколу взаємодії між виборцем і смарт-контрактом, який повинен гарантувати приватність вибору у період голосування та можливість його верифікації після завершення процедури. Найбільш придатним для цього є механізм `commit-reveal`, який дозволяє не розкривати вибір до завершення голосування та водночас унеможливує його зміну заднім числом [11].

Крім того, необхідно сформулювати вимоги до підрахунку голосів, який має виконуватися автоматично і детерміновано у смарт-контракті, що гарантує відсутність впливу людського фактора. Система повинна забезпечувати відкритість журналу подій, доступність результатів і можливість перевірки правильності під-

рахунку будь-яким зацікавленим учасником. Разом із тим важливо передбачити використання офчейн-компонентів для логування подій, аналітики та підвищення зручності користування, не порушуючи принцип децентралізованого підрахунку.

3. Модель та архітектура системи

Розроблення децентралізованої системи електронного голосування вимагає формування цілісної архітектурної моделі, яка поєднує можливості публічного блокчейна, офчейн-компонентів та клієнтських застосунків. Архітектура має забезпечувати прозорість виборчого процесу, незалежність підрахунку голосів від довірених сторін, захист від фальсифікацій, а також можливість зовнішнього аудиту. В основі системи лежить використання блокчейна Ethereum як платформи для зберігання критично важливих даних та виконання смарт-контрактів, що реалізують логіку голосування [9, 12]. Для структурування моделі виборчого процесу було використано UML-діаграми, які дозволяють формально описати ролі учасників, їхню взаємодію та внутрішню структуру компонентів системи [13, 14].

Центральним елементом архітектури є смарт-контракт ElectionManager, який відповідає за створення виборчих кампаній, визначення часових меж етапів голосування, приймання зашифрованих голосів, виконання процедури розкриття та підрахунок результатів. Контракт зберігає всі події у блокчейні, забезпечуючи їх незмінність та доступність для перевірки. Важливою особливістю є реалізація протоколу commit–reveal, який дозволяє приховати вибір виборця на етапі голосування та гарантує коректність розкриття після завершення процедури. Кожен голос подається у вигляді хешу, сформованого з урахуванням випадкової криптографічної солі, що виключає можливість підбору значення або передчасного розкриття голосу [15].

Ще одним компонентом ончейн-рівня є контракт VotingRightToken, реалізований за стандартом ERC-1155 у форматі soulbound-токенів [16]. Він забезпечує механізм підтвердження прав голосу, який неможливо передати або скопіювати. Така модель дозволяє гарантувати, що кожен виборець має лише один голос, а також унеможливорює участь у виборах неавторизованих користувачів. Управління правами голосу відбувається у смарт-контракті, а сам факт володіння токеном зберігається у блокчейні, що створює додатковий рівень прозорості.

Архітектура системи доповнюється офчейн-компонентами, які виконують допоміжні, але важливі функції. Серверна частина розроблена на Node.js і відповідає за журналювання подій, зберігання метаданих виборів, взаємодію з базою даних і виконання службових операцій, що не впливають на процес підрахунку голосів. Офчейн-рівень отримує події зі смарт-контракту через бібліотеку ethers.js, зберігає

їх у базі SQL Server та надає можливість аналітики, аудиту та адміністративного моніторингу. Зберігання журнальних записів окремо від блокчейна не порушує принципів прозорості, оскільки критично важливі дані все одно залишаються у децентралізованому реєстрі, а офчейн-логіка використовується виключно для підвищення зручності користування та зменшення вартості операцій.

Клієнтський застосунок реалізований на Angular і забезпечує взаємодію користувачів із системою. Його архітектура передбачає роботу у двох режимах: адміністративному та виборчому. Адміністратор може створювати вибори, визначати часові межі етапів, керувати правами голосу та переглядати стан виборчої кампанії через офчейн-сервер. Виборець, у свою чергу, може підключити гаманець MetaMask, отримати токен права голосу, подати commit голосу, розкрити його після завершення голосування та переглянути підсумки [17, 18]. Усі операції, пов'язані з голосуванням, виконуються безпосередньо у блокчейні, що виключає втручання адміністратора у процес приймання голосів.

Для структурування моделі виборчої системи було створено три основні UML-діаграми, які формально описують ролі, компоненти та динаміку роботи системи.

Діаграма прецедентів (рис. 1) відображає зовнішню поведінку системи та визначає функції, доступні кожній ролі. Адміністратор створює вибори, керує етапами та правами голосу; виборець подає commit, виконує reveal та переглядає результати; аудитор перевіряє публічні події у блокчейні.

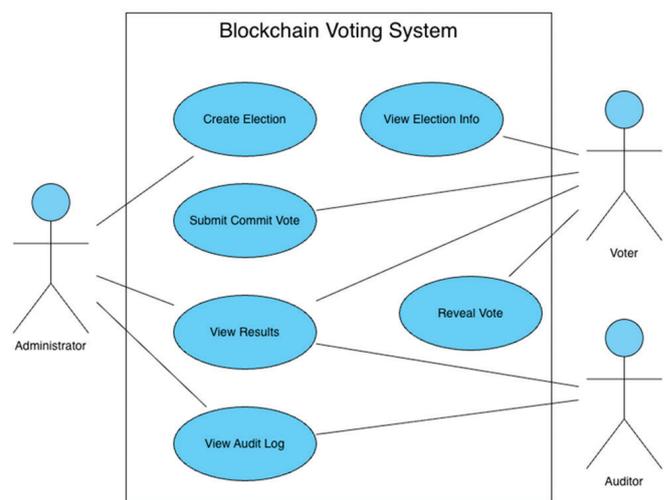


Рис. 1. Use Case Diagram

Діаграма класів (рис. 2) деталізує внутрішню архітектуру, включаючи контракти ElectionManager і VotingRightToken, моделі виборців, кандидатів та виборчих кампаній, а також офчейн-сервіси й клієнтські модулі. Вона відображає структурні зв'язки між блокчейном, сервером і фронтендом та показує, як зберігаються й обробляються ключові дані.

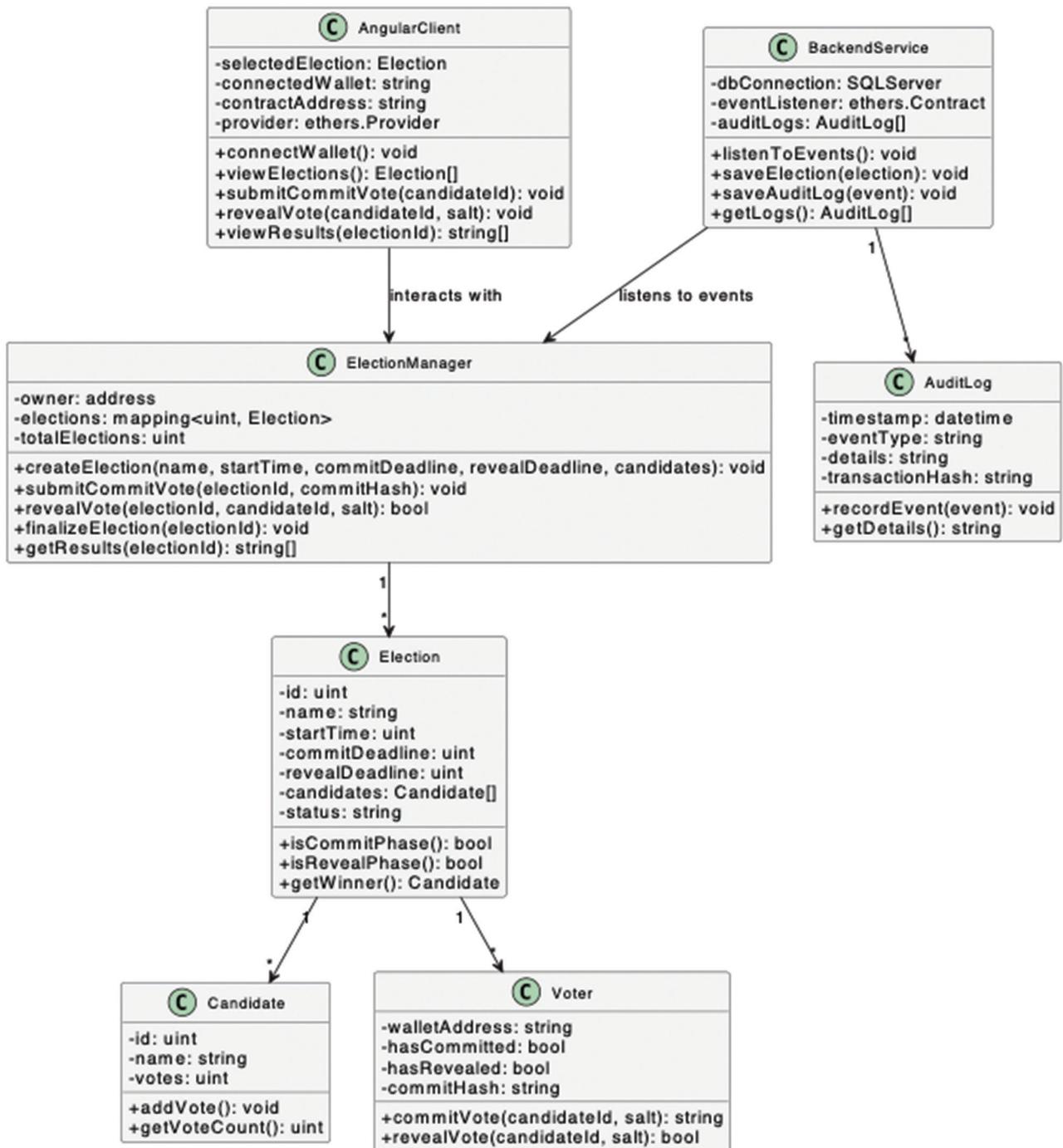


Рис. 2. Class Diagram

Діаграма послідовності (рис. 3) ілюструє покрокову взаємодію під час голосування: надсилання commit, підпис транзакцій через MetaMask, обробка подій смарт-контрактом, логування офчейн-сервісом та подальше розкриття голосів.

Узагальнена архітектура системи демонструє поєднання децентралізованої логіки підрахунку голосів із допоміжними механізмами зберігання метаданих та аналітики, що дозволяє досягти високого рівня безпеки, прозорості та практичної зручності використання. Такий підхід забезпечує надійну модель голосування, яка придатна для застосування у широкому спектрі організаційних сценаріїв.

4. Програмна реалізація і експериментальні дослідження

Реалізація прототипу системи електронного голосування ґрунтується на поєднанні блокчейн-технологій та сучасних веб-фреймворків, що дозволило створити повноцінний функціональний комплекс, придатний для тестування у реальних організаційних умовах. Основний обсяг логіки, відповідальної за безпеку, прозорість та підрахунок голосів, був реалізований у вигляді смарт-контрактів на платформі Ethereum. Для розробки смарт-контрактів використано мову Solidity та фреймворк Hardhat, який забезпечує можливість локального тестування, автоматизованої компіляції,

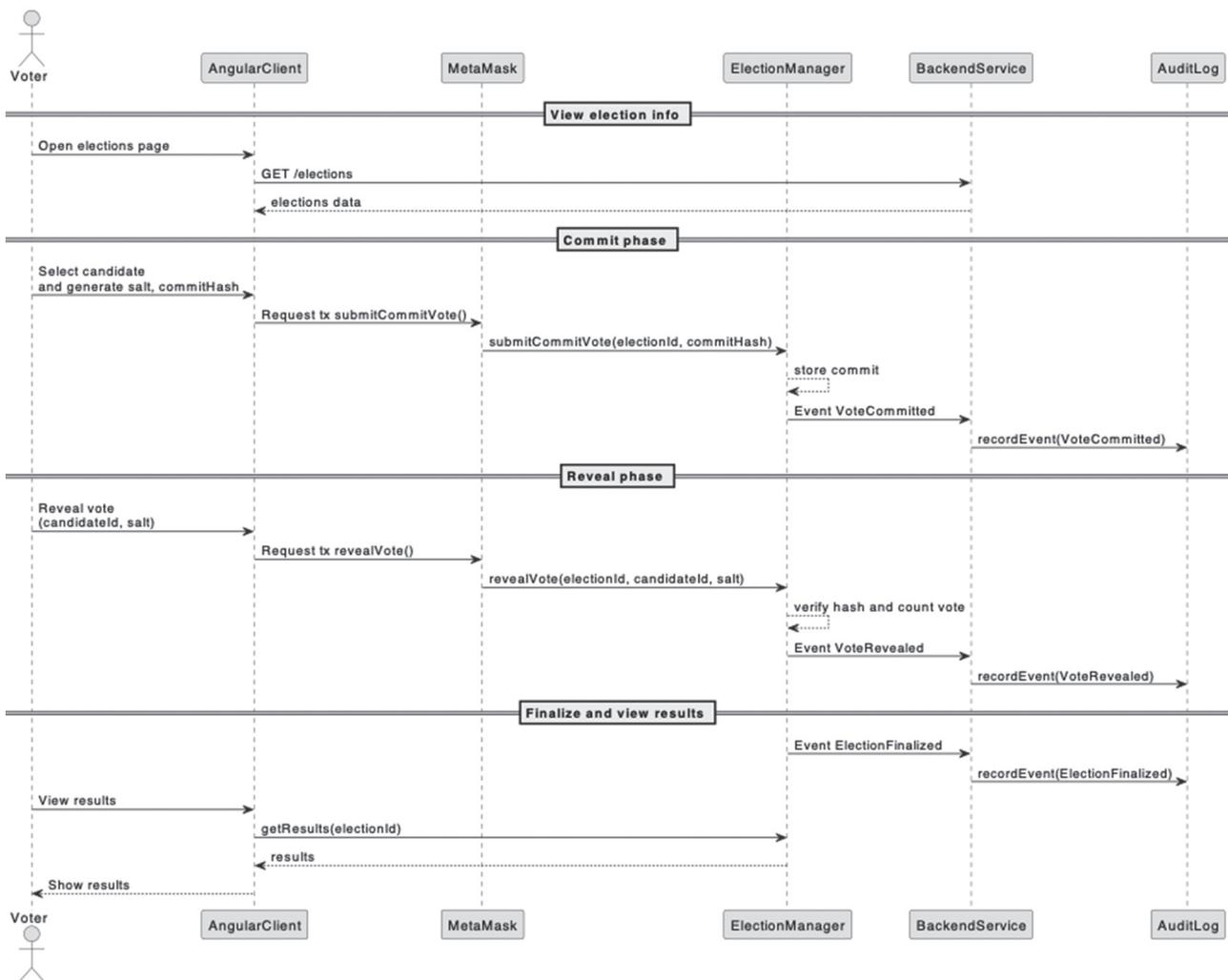


Рис. 3. Sequence Diagram

розгортання та емуляції взаємодії з мережею. Контракти розгорнулися у тестовій мережі Sepolia, що дозволило відтворити сценарії реальної роботи без витрат у публічній мережі.

Смарт-контракт ElectionManager реалізує механізм створення виборів, збереження параметрів виборчої кампанії та виконання протоколу commit–reveal. На етапі commit виборець надсилає хеш свого голосу разом із криптографічною сіллю, а після завершення голосування виконує розкриття значення, що дозволяє смарт-контракту перевірити коректність хешу та зберегти голос. Такий підхід виключає можливість зміни голосу заднім числом та забезпечує чесність процедури. Додатково було реалізовано контракт VotingRightToken, який відповідає за видачу токенів прав голосу у форматі SBT. Це унеможливує передачу або дублювання голосів, оскільки кожен токен прив’язаний до конкретної адреси і не може бути переміщений.

Офлайн-інфраструктура системи була реалізована на Node.js із використанням Express. Цей компонент не впливає на підрахунок голосів, але відіграє важливу роль у зручності роботи та виведенні даних для адміністратора. Сервер взаємодіє зі смарт-контрактами

через бібліотеку ethers.js, отримує та зберігає журнальні події, включаючи коміти, розкриття голосів та фіналізацію виборів. Метадані, а також технічні журнальні записи, зберігаються у базі даних SQL Server, що забезпечує можливість додаткової аналітики, фільтрації подій та виявлення потенційних аномалій у поведінці користувачів.

Клієнтський застосунок був створений на основі Angular і забезпечує інтуїтивний інтерфейс для обох ролей – адміністратора та виборця. Підключення MetaMask відбувається безпосередньо в браузері, що дозволяє користувачам підписувати транзакції та взаємодіяти з блокчейном без посередників. Виборець може переглядати доступні виборчі кампанії, надіслати commit-хеш голосу, виконувати розкриття після завершення голосування та переглядати результати у режимі реального часу. Адміністратор отримує доступ до інструментів створення виборів, керування часовими етапами та моніторингу стану виборчих процесів.

Для оцінки ефективності системи було проведено низку експериментів у тестовій мережі Sepolia. Було виміряно вартість транзакцій різних типів, затримку виконання операцій та поведінку системи за умов

збільшеного навантаження. Вартість *commit*-транзакції в середньому становила від 0.0004 до 0.0007 доларів США, що робить модель придатною для практичного використання в організаціях, де кількість виборців є обмеженою. Підрахунок голосів і фіналізація виборів виконувалися смарт-контрактом практично миттєво, а час відгуку клієнтського застосунку переважно залежав лише від швидкодії мережі *Ethereum*.

Під час експериментів також було протестовано механізм обробки спроб повторного голосування, відтворення недійсних розкриттів та некоректних комітів. Смарт-контракт успішно блокував повторні спроби надсилання голосів від однієї адреси та відхиляв розкриття, яке не відповідало раніше поданому хешу. Це підтверджує здатність системи забезпечувати захист від маніпуляцій без втручання адміністратора. Офчейн-журналування дало змогу додатково проаналізувати активність учасників та підтвердило відповідність усіх смарт-контрактних подій даним у базі.

Отримані результати свідчать про практичну можливість використання розробленої архітектури в умовах реальних організаційних процесів. Система продемонструвала стійкість до маніпуляцій, передбачувану поведінку під навантаженням та технічну здатність до масштабування. Проведені дослідження підтверджують, що поєднання блокчейна з офчейн-компонентами забезпечує необхідний баланс між безпекою, прозорістю та зручністю використання.

5. Обговорення, новизна та практичне значення роботи

Розроблений прототип децентралізованої системи електронного голосування демонструє можливість практичного застосування блокчейн-технологій у виборчих процесах організацій різного типу. На відміну від традиційних централізованих платформ, які покладаються на серверну інфраструктуру та довіру до адміністратора, запропонована система забезпечує прозорість та перевірюваність усіх ключових етапів голосування. Запис подій у блокчейні, використання відкритої логіки смарт-контрактів та автоматизований підрахунок голосів виключають можливість прихованих втручань, а також усувають загрозу фальсифікацій та маніпуляцій результатами. Це дозволяє досягти нового рівня довіри між учасниками виборчого процесу, оскільки контроль над даними більше не концентрується у руках однієї сторони.

Новизна запропонованого підходу полягає у поєднанні кількох концептуальних рішень, які рідко зустрічаються у комплексі в існуючих системах. Одним із таких рішень є використання токенів прав голосу у форматі *soulbound*-токенів, що забезпечують незмінність і непередаваність виборчого права. Цей підхід дозволяє будувати прозору модель авторизації виборців, у якій неможливо дублювати або продавати голоси, що

є однією з головних проблем класичних систем. Іншим важливим елементом новизни є інтеграція офчейн-журналування та аналітики, яка поєднується з ончейн-захистом. Така архітектура дозволяє зберігати критичні події у блокчейні, а другорядні дані – у швидкій та гнучкій офчейн-системі, що робить підхід одночасно безпечним і зручним для адміністраторів [19].

Особливого значення набуває реалізація механізму *commit-reveal*, який забезпечує конфіденційність вибору та гарантує коректність його розкриття. Завдяки цьому механізму система виключає можливість раннього доступу до інформації про голоси, а також унеможлиблює їх модифікацію після завершення голосування. Ця властивість є критично важливою у будь-яких виборах, де довіра виборців до процесу базується на переконанні, що голоси не будуть підмінені чи видалені. У поєднанні з децентралізованою архітектурою *commit-reveal* формує технічну основу для побудови повністю прозорих виборчих процесів.

Практичне значення системи проявляється у можливості її адаптації до різних сценаріїв організаційного управління. Система може використовуватися для виборів студентського самоврядування, прийняття рішень у корпоративних структурах, формування дорадчих комітетів, проведення внутрішніх опитувань тощо. Завдяки відкритій логіці підрахунку та відсутності централізованого контролера система може слугувати інструментом для проведення голосувань у середовищах, де відсутній високий рівень довіри між учасниками або де існує ризик політичної чи адміністративної упередженості.

Важливо підкреслити, що запропонований прототип не є кінцевим рішенням, а радше демонструє практичну життєздатність архітектурної концепції. Подальший розвиток системи може включати впровадження більш ефективних криптографічних методів, оптимізацію вартості транзакцій, підтримку більш масштабованих мереж та розробку зручніших інтерфейсів для нетехнічних користувачів. З огляду на глобальний тренд до цифровізації демократичних процесів, дослідження у цьому напрямі має значний потенціал та здатне забезпечити основу для створення надійних, децентралізованих виборчих платформ нового покоління [20].

Таким чином, обговорення результатів дозволяє зробити висновок, що поєднання смарт-контрактів, токенів прав голосу та механізму *commit-reveal* формує інноваційний підхід до організації виборчих процесів у середовищі з підвищеними вимогами до безпеки та прозорості. Система демонструє здатність вирішувати ключові проблеми традиційних платформ та відкриває можливості для масштабного впровадження блокчейн-голосування у практичну діяльність організацій.

Висновки

У роботі було розглянуто проблему забезпечення прозорості, безпеки та довіри у процесі електронного голосування, що є особливо актуальним у сучасних організаціях, де виборчі процедури дедалі частіше переходять у цифрову форму. Аналіз існуючих рішень показав, що традиційні централізовані системи не здатні повною мірою усунути ризики маніпуляцій, тоді як наявні криптографічні або комерційні платформи не забезпечують достатнього рівня відкритості та незалежного аудиту. У цьому контексті блокчейн-технології постають ефективним інструментом для побудови децентралізованих виборчих систем, де ключові дані залишаються незмінними, а процес підрахунку голосів є відкритим та перевірюваним.

У межах роботи було розроблено модель та прототип децентралізованої системи голосування, що поєднує механізм commit–reveal, смарт-контракти для управління виборчим процесом та токени прав голосу у форматі SBT. Запропонована архітектура забезпечує прозору взаємодію між учасниками, виключає вплив адміністратора на критичні етапи голосування та надає можливість незалежного аудиту всіх подій. Реалізація системи включає ончейн-компоненти на базі Ethereum та офчейн-інфраструктуру, призначену для аналітики й підвищення зручності використання. Проведені експериментальні дослідження підтвердили технічну життєздатність моделі, її стійкість до маніпуляцій і здатність працювати у реальних організаційних сценаріях.

Отримані результати демонструють перспективність використання блокчейна для організації виборів у середовищах, де важливою є відсутність довіреної сторони та забезпечення високого рівня прозорості. Прототип показав, що децентралізовані механізми можуть не лише замінити традиційні підходи, але й значно підвищити рівень довіри до результатів. Подальший розвиток системи може включати оптимізацію вартості транзакцій, впровадження розширених криптографічних протоколів захисту вибору, розширення можливостей масштабування та адаптацію інтерфейсу для широкого кола користувачів. Отже, запропоноване рішення створює основу для побудови ефективних та безпечних виборчих платформ нового покоління.

Список літератури:

- [1] Huang J. The application of blockchain technology in voting systems: A review / J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, K. Choo // *ACM Computing Surveys*. – 2021. – Vol. 54, №3. – P. 1–28.
- [2] Hajian Berenjestanaki M. Blockchain-based e-voting systems: a technology review / M. Hajian Berenjestanaki, H. Barzegar, N. El Ioini, C. Pahl // *Electronics*. – 2023. – Vol. 13, №1. – P. 1–21.
- [3] Jafar U. A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems / U. Jafar, M. Ab Aziz, Z. Shukur, H. Hussain // *Sensors*. – 2022. – Vol. 22, №19. – P. 7585.
- [4] Chouhan V., Arora A. Blockchain-based secure and transparent election and vote-counting mechanism using secret sharing scheme / V. Chouhan, A. Arora // *Journal of Ambient Intelligence and Humanized Computing*. – 2023. – Vol. 14. – P. 14009–14027.
- [5] Akinbohun S., Apeh S., Olaye E., Ogebeide O. Literature review of blockchain-based voting system: framework and concept // *Journal of Civil and Environmental Systems Engineering*. – 2023. – Vol. 20, №1. – P. 72–83.
- [6] Al-Maaitah S., Qatawneh M., Quzmar A. E-voting system based on blockchain technology: A survey // *Proc. of International Conference on Information Technology (ICIT)*. – IEEE, 2021. – P. 200–205.
- [7] Helios Voting. – URL: <https://vote.heliosvoting.org/>
- [8] Voatz. – URL: <https://voatz.com/>
- [9] Ethereum Foundation. Solidity Documentation. – URL: <https://docs.soliditylang.org/>
- [10] Sharp M., Roberts L., Xiao H. Blockchain-Based E-Voting Mechanisms: A Survey and Comparative Analysis // *Journal of Information Security and Applications*. – 2024.
- [11] Rahman M. Implementation of blockchain-based e-voting system / M. Rahman et al. // *Multimedia Tools and Applications*. – 2023. – Vol. 83, №1. – P. 1–32.
- [12] ethers.js Documentation. – URL: <https://docs.ethers.io/>
- [13] Visual Paradigm. UML Modeling Tool. – URL: <https://www.visual-paradigm.com/>
- [14] PlantUML Documentation. UML Diagram Generator. – URL: <https://plantuml.com/>
- [15] Denis González C., Frias Mena D., Massó Muñoz A., Rojas O., Sosa-Gómez G. Electronic voting system using an enterprise blockchain // *Applied Sciences*. – 2022. – Vol. 12, №2. – P. 531.
- [16] Dai W., Liu C. Soulbound tokens and decentralized identity // *IEEE Access*. – 2023. – Vol. 11. – P. 1221–1233.
- [17] MetaMask Documentation. – URL: <https://docs.metamask.io/>
- [18] OpenZeppelin Smart Contracts. – URL: <https://docs.openzeppelin.com/contracts>
- [19] Zhang X., Lee Y. Secure smart-contract-based voting using Ethereum blockchain // *IEEE Access*. – 2021. – Vol. 9. – P. 34335–34347.
- [20] Kim S., Park J. Privacy-preserving blockchain voting: State-of-the-art review // *Computers & Security*. – 2022. – Vol. 118. – P. 102731.

Надійшла до редколегії 29.09.2025