КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.860
УДК 004.94:519.21

Шевченко Світлана Миколаївна
к.п.н., доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
к.ф.-м.н доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Складанний Павло Миколайович
к.т.н., доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Іщук Михайло Олександрович
студент 4 курсу спеціальності Інженерія програмного забезпечення
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0007-7931-5599
st7378695@stud.duikt.edu.ua

СТВОРЕННЯ БЛОКЧЕЙН-ПЛАТФОРМИ ДЛЯ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Анотація. Справжня демократія, міцна довіра людей до уряду та законна передача влади в країні можливі лише тоді, коли вибори проводяться чесно і правильно. Сучасні інформаційні технології сприяють інноваційним перебудовам у виборчих процесах, забезпечуючи оптимізацію процесу голосування, мінімізацію людських помилок, підвищення доступності для виборців. Разом з цим впровадження цифрових технологій породжує значні проблеми з інформаційною безпекою, зокрема, можлива зміна результатів голосування, маніпуляція, створюються загрози цілісності, доступності, конфіденційності та анонімності. Одним з ефективних рішень для забезпечення інформаційної безпеки в електронному голосуванні (e-voting) є блокчейн технології. Дане дослідження присвячене проблемі розробки вебсайту для електронного голосування з використанням блокчейн технології. На основі вивчення наукової літератури розкрито суть, принципи, переваги та недоліки даної технології. Представлено порівняльний аналіз найкращих практик впровадження технології блокчейн у процес е-голосування. Як приклад, описано процес розробки вебсайту для електронного голосування з використанням блокчейн технології: встановлені функціональні вимоги до даної системи, описано архітектуру програмного застосунку, змодельовано діаграму варіантів використання. Для розробки бекенду використовувалася TypeScript як основна мова програмування, Nest.js як фреймворк, PostgreSQL для керування даними, а також Web3.js для реалізації функціоналу бекенду. Фронтенд реалізовано з використанням мови програмування TypeScript, фреймворку React та Tailwind CSS для оформлення інтерфейсу. Розроблена платформа електронного голосування демонструє високу гнучкість і може бути імплементована для проведення різноманітних електоральних процедур. Її функціонал охоплює як вибори посадових осіб (наприклад, ректора університету), так і локальні голосування (наприклад, обрання старости академічної групи), а також референдуми з оцінки

діяльності структурних підрозділів. Виявлені в ході дослідження дані можуть збагатити навчальні матеріали для студентів галузі 12 Інформаційні технології.

Ключові слова: інформаційна безпека; цифрові технології; блокчейн; електронне голосування (e-voting); вебсайт.

ВСТУП

Постановка проблеми. Впровадження цифрових технологій у процес електронного голосування, попри підвищення зручності та ефективності, породжує значні проблеми з захистом інформації, що може підірвати довіру до виборів [1]. Ці проблеми стосуються цілісності, конфіденційності та доступності виборчого процесу, що є критично важливим для демократичного функціонування. Системи електронного голосування, як і будь-які інші цифрові платформи, уразливі до хакерських атак, зламів та впровадження шкідливого програмного забезпечення. Зловмисники можуть спробувати змінити результати голосування; видалити або додати голоси; відключити систему, застосовуючи DDoS-атаку; розкрити особисті дані виборців, що може призвести до неправомірного використання персональних даних.

Потенційні наслідки таких атак можуть бути катастрофічними, оскільки вони можуть призвести до спотворення результатів виборів і втрати легітимності всього демократичного процесу. На це вказують наведені статистичні дані: в Еквадорі голосування заочно на національних виборах було зірвано кібератаками з росії, Китаю, Індії, Бангладеш, Пакистану та Індії, що перешкодило багатьом зі 120 000 закордонних виборців отримати доступ до виборчої системи країни (2023 рік) [2]; злом виборчої комісії розкрив дані 40 мільйонів виборців Великої Британії (2022 рік) [3]. Автори [4] представили дослідження щодо аналізу безпеки частин електронної системи виборів 2015 року у Новому Південному Уельсі (Австрія) у реальному часі. Було виявлено уразливості, які можна використати для маніпулювання голосами, а включення аналітичного програмного забезпечення з незахищеного зовнішнього сервера призвела до повної компрометації конфіденційності та цілісності деяких голосів. У дослідженні [5] ставиться акцент на криптографічні недоліки, які були виявлені у системі електронного голосування SwissPost.

Такі інциденти з інформаційною безпекою підривають загальну довіру до виборчого процесу. Той факт, що 42% експертів виступили проти впровадження електронного голосування в Україні, приблизно відповідає верхній межі середнього рівня саме небезпеки впровадження електронного голосування [6]. Якщо громадськість не вірить, що голоси підраховуються чесно і без втручань, легітимність обраних представників може бути поставлена під сумнів [7]. У демократичному суспільстві довіра до виборів є наріжним каменем, і будь-яка загроза цій довірі є серйозним викликом.

Аналіз останніх досліджень і публікацій. Забезпечення інформаційної безпеки у виборчому електронному процесі є однією з основних проблем у сучасних дослідженнях з даної теми. Як свідчить аналіз наукових джерел [8] – [16], автори звертаються саме до застосування блокчейн технологій для максимального збереження рівня безпеки у е-голосуванні.

Так, у дослідженнях [8], [9] пропонуються системи, які працюють на Ethereum, де смарт-контракти відповідають за безпечне фіксування та точний підрахунок голосів.

Платформа онлайн-голосування з використанням хмарної гібридної технології блокчейн описана у роботі [10]. Дана система використовує автентифікацію на основі часових позначок з цифровим підписом для верифікації виборців та кандидатів під час

реєстрації та голосування. Смарт-контракти унеможливлюють стороннє втручання, а блокчейн захищає транзакції. Для гарантування точності та незмінності результатів застосовується практичний механізм консенсусу Візантійської відмовостійкості (PBFT).

Оглядові статті [11] – [16], що присвячені проблематиці імплементації технології блокчейн у системах електронного голосування, охоплюють широкий спектр фундаментальних та прикладних аспектів. Ці публікації ретельно аналізують різноманітні підходи, архітектурні рішення, виклики та потенційні переваги, що виникають при використанні децентралізованих реєстрів для проведення виборів. Вище представлене визначає важливість даного напрямку і визначає мету.

Мета статті. Метою статті є представлення розробки вебсайту для проведення електронного голосування з використанням блокчейн технології.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Технологія блокчейн: поняття, принципи, переваги та недоліки

Технологія блокчейн з’явилася наприкінці 20-го століття завдяки новаторській дослідницькій роботі американського фізика В. Скотта Сторнетти та американського криптографа і комп’ютерного вченого Стюарта Габера. Працюючи в дослідницькому центрі Bell Communications Research (Bellcore), вони ставили собі за мету розробити безпечний криптографічний архів, який міг би надійно зберігати записи, забезпечуючи при цьому їхню конфіденційність. Їх стаття 1991 року [17] визнана однією з найважливіших робіт у формуванні технології блокчейн. У 1995 році пропозиція від компанії Surety Technologies, яку заснували Сторнетта і Габер, стала першим комерційним впровадженням технології блокчейну і досі залишається найстарішим діючим блокчейном.

Термін блокчейн (англ. blockchain — ланцюжок блоків) визначається як спосіб шифрування, передачі та зберігання інформації в розподіленій мережі. Блокчейн — це розподілений цифровий реєстр, який функціонує як база даних, що зберігається одночасно на багатьох комп’ютерах (вузлах або нодах) у мережі. Кожен вузол має повну копію реєстру та оновлюється незалежно. Транзакція у контексті блокчейну — це запис про обмін даними або активами між двома чи більше учасниками мережі. Це може бути переказ криптовалюти, укладення смарт-контракту, реєстрація права власності на що-небудь або будь-яка інша дія, яка потребує запису в розподіленому реєстрі. Кожна транзакція містить інформацію про відправника, отримувача, суму (якщо це переказ), час і дату, а також інші дані, залежно від типу транзакції та конкретного блокчейну. Після створення транзакція підписується криптографічним ключем відправника, що гарантує її справжність і неможливість підробки. Транзакції збираються в блоки, які потім додаються до ланцюжка (блокчейну). Після підтвердження кількома вузлами мережі, транзакція стає незмінною частиною блокчейну, і її неможливо видалити або змінити.

Блокчейн-мережа працює в наступні етапи:

- нові транзакції транслюються всім вузлам мережі;
- вузли збирають ці транзакції та організовують їх у блок;
- кожен вузол бере участь у процесі пошуку підтвердження роботи свого блоку;
- як тільки вузол знаходить правильне значення, він ділиться своїм завершеним блоком з усіма іншими вузлами;
- вузли приймають блок тільки в тому випадку, якщо всі транзакції в ньому точні і не дублюються;

– підтвердженням прийняття блоку є ініціювання створення нового блоку, при цьому хеш прийнятого блоку слугує попереднім хешем у ланцюжку.

Блоки в ланцюжку розташовані в хронологічному порядку, пов'язані між собою та захищені криптографічними засобами. Кожен блок містить хеш-код попереднього блоку та корисне навантаження, яке може містити будь-яку інформацію, наприклад, дані про транзакції, операції, контракти, записи про фізичних осіб, компанії або нерухомість. Суть блокчейну полягає в постійно оновлюваному реєстрі: до нього можна лише додавати нові дані, але неможливо видалити чи змінити інформацію, що вже зберігається в попередніх блоках.

Ключова особливість блокчейну — його децентралізація, що означає відсутність єдиного центрального сховища даних. Для забезпечення достовірності та актуальності інформації всі вузли повинні координуватися. Це досягається завдяки алгоритму консенсусу: кожен вузол незалежно пропонує оновлення, а потім вузли голосують за них, щоб більшість підтвердила остаточну версію. Після досягнення консенсусу розподілений реєстр оновлюється, і кожен вузол записує останню узгоджену версію.

У роботі [18] розглядаються особливості, переваги та проблеми використання блокчейн технологій для створення розподілених безпечних корпоративних додатків.

Технологія блокчейну базується на кількох фундаментальних принципах, які забезпечують її унікальні переваги (табл. 1).

Таблиця 1

Основні принципи блокчейну

Принцип	Зміст
Розподіленість	Блокчейн функціонує як розподілений реєстр і залишається активним доти, доки існує хоча б один вузол у мережі.
Децентралізація	Жоден учасник мережі не має повного контролю над блокчейном. Всі вузли рівноправні, відсутня ієрархія чи головний вузол.
Безпека та незмінність	Блокчейн пропонує унікальне поєднання відкритості та безпеки завдяки передовим методам шифрування. Дані підтверджуються кількома вузлами мережі, що робить їх незмінними та непідробними.
Прозорість	Вся інформація про транзакції є відкритою для перевірки будь-ким, забезпечуючи абсолютну прозорість.
Відсутність посередників (бездовірність)	Блокчейн є «довіреною» системою: транзакції відбуваються безпосередньо між учасниками, автоматично перевіряються численними вузлами мережі. Це усуває потребу в посередниках, знижує транзакційні витрати та прискорює обробку.

Хоча технологія блокчейну пропонує значні переваги, вона також має певні недоліки та виклики, які стримують її широке впровадження (табл. 2).

Таблиця 2

Основні недоліки блокчейну

Недолік	Зміст
Масштабованість	Блокчейни мають обмежену пропускну здатність (кількість транзакцій за секунду). Наприклад, Bitcoin обробляє 3-7 транзакцій за секунду, а Ethereum — 13–15.
Безпека	Хоча сама архітектура блокчейну є безпечною, були зафіксовані випадки злому та порушення захисту, що свідчить про потенційні уразливості на рівні реалізації або взаємодії з користувачем.
Сумісність	Різні блокчейн-мережі часто несумісні між собою, що ускладнює обмін даними між ними.

Складність	Технологія блокчейну залишається складною для розуміння звичайним користувачем, що є перешкодою для її масового впровадження.
Регулювання	Наразі відсутня чітка та уніфікована нормативно-правова база для регулювання блокчейну. Ця невизначеність може стримувати організації від його використання.
Енергоспоживання	Процес майнінгу (створення нових блоків) є дуже енергоємним, що викликає занепокоєння щодо екологічності та ефективності використання ресурсів.

Блокчейн з погляду криптографії та захисту інформації

З точки зору криптографії та захисту інформації, блокчейн є надзвичайно потужною технологією [19]. Його безпека та надійність базуються на кількох ключових криптографічних примітивах, а саме:

1. Криптографічні хеш-функції. Кожен блок у блокчейні містить криптографічний хеш попереднього блоку. Це створює «ланцюжок» блоків, де будь-яка зміна в одному блоці призведе до зміни його хешу, що, в свою чергу, змінить хеш наступного блоку і так далі. Це робить будь-які спроби підробки або зміни даних легко помітними і практично неможливими, оскільки для цього потрібно було б перерахувати хеші всіх наступних блоків, що є обчислювально витратним.

2. Цифрові підписи. Транзакції в блокчейні захищені за допомогою цифрових підписів. Кожен учасник має пару ключів: публічний (відомий усім) та приватний (відомий лише власнику). При створенні транзакції вона підписується приватним ключем, а її справжність може бути перевірена будь-яким учасником мережі за допомогою публічного ключа. Це забезпечує автентифікацію відправника та незаперечність транзакції.

3. Розподілений консенсус. Механізми розподіленого консенсусу (наприклад, Proof-of-Work або Proof-of-Stake) хоча і не є суто криптографічним поняттям, відіграють ключову роль у захисті інформації. Вони гарантують, що інформація в реєстрі є узгодженою та достовірною для всіх учасників, навіть якщо деякі з них намагаються діяти зловмисно. Це досягається шляхом того, що більшість вузлів повинні підтвердити валідність нових блоків і транзакцій, роблячи надзвичайно складним внесення нелегітимних змін.

4. Незмінність. Завдяки комбінації цих механізмів, інформація, записана в блокчейні, стає незмінною. Після того, як транзакція додана до блоку і блок включений у ланцюжок, її практично неможливо видалити або змінити. Це забезпечує високий рівень довіри до даних, що зберігаються в блокчейні, оскільки вони є постійними та захищеними від несанкціонованих маніпуляцій.

Таким чином, з погляду захисту інформації, блокчейн пропонує децентралізовану, прозору та високобезпечну систему для зберігання та управління даними, що робить його привабливим для широкого спектру застосувань, де довіра та цілісність інформації є критично важливими.

Значення хешування у блокчейні

Хешування — це ключовий інструмент в інформаційній безпеці, що дозволяє за допомогою детермінованого алгоритму перетворювати дані будь-якого розміру на унікальний рядок фіксованої довжини (хеш). Хешування ефективно вирішує дві основні проблеми:

1. Обробка великих обсягів різнорідних даних. Спрощується робота з величезними масивами інформації (наприклад, при виявленні шкідливого програмного забезпечення або управлінні інцидентами інформаційної безпеки).
2. Виявлення дублікатів інформаційних об’єктів. Швидко відшукуються ідентичні об’єкти, що важливо для перевірки достовірності даних.

Завдяки хешуванню дані стискаються та швидко обробляються, що є критично важливим для забезпечення ефективної кібербезпеки [20], [21].

Хешування є ключовим елементом безпеки та цілісності блокчейну, що забезпечує його функціонування. Основними функціями хешування у блокчейні є наступні:

1. Зв'язування блоків. Кожен блок містить криптографічний хеш попереднього блоку, створюючи нерозривний «ланцюг». Будь-яка зміна в блоці змінює його хеш, порушуючи весь ланцюг і роблячи підробку очевидною, що забезпечує незмінність даних.
2. Цілісність даних. Хеші діють як «відбитки пальців» даних, миттєво сигналізуючи про будь-яку їх модифікацію, що дозволяє швидко перевіряти цілісність даних.
3. Механізм консенсусу (Proof-of-Work). У блокчейн-мережах таких, як Біткоїн, майнери змагаються за пошук хешу, що відповідає певним умовам. Це робить мережу безпечною та стійкою до атак, оскільки вимагає величезних обчислювальних ресурсів для внесення змін.
4. Ефективність та ідентифікація. Хеш-функції стискають великі обсяги даних у короткі унікальні ідентифікатори, що прискорює перевірку та спрощує ідентифікацію транзакцій і блоків.

Отже, саме хешування є основою децентралізації, безпеки, прозорості та незмінності блокчейну, формуючи довіру до даних у розподілених реєстрах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Надалі представимо практичну розробку (демоверсію) — вебсайт для електронного голосування з використанням блокчейн технології.

Функціональні вимоги до додатку

На основі аналізу існуючих систем електронного голосування, розроблена платформа має відповідати таким функціональним вимогам:

- аутентифікація користувачів — система повинна забезпечувати можливість безпечного входу користувачів;
- унікальність голосу — кожен користувач може проголосувати лише один раз в межах конкретного голосування, що запобігає подвійному голосуванню;
- незмінність результатів — результати голосування записуються в блокчейн, гарантуючи їхню незмінність та прозорість;
- доступ до результатів — після завершення голосування користувачі мають можливість переглядати його результати;
- онлайн-режим — система підтримує проведення голосувань в онлайн-режимі, забезпечуючи зручність та доступність.

Технології розробки

Основною мовою інтерфейсу обрано англійську, що відповідає статусу цієї мови як домінуючої у міжнародній мережевій комунікації.

Для реалізації серверної частини додатку для електронного голосування обрано Node.js. Для спрощення розробки та забезпечення модульності використано NestJS — фреймворк для Node.js, що підтримує TypeScript, впровадження залежностей (DI), валідацію та обробку помилок.

Вибрано PostgreSQL (об'єктно-реляційна СУБД) та Prisma ORM (з типобезпечним клієнтом) для зберігання та керування офчейн даними; Solidity — мова програмування для написання смарт-контрактів, що виконуються на віртуальній машині Ethereum (EVM); Web3.js — бібліотека для взаємодії з блокчейном Ethereum, забезпечує функціонал для роботи зі смарт-контрактами та транзакціями.

Безпека реалізована за допомогою JWT (JSON Web Tokens) для аутентифікації та авторизації, доповнена обмеженням частоти запитів (rate limiting), валідацією даних та захистом CORS. Інфраструктура серверної частини контейнеризована за допомогою Docker для забезпечення стабільних середовищ розробки та розгортання, а також спрощення масштабування та підтримки системи.

Для розробки клієнтської частини застосунку обрано TypeScript, Фронтенд-інтерфейс реалізовано за допомогою React — гнучкої JavaScript-бібліотеки з компонентною архітектурою, віртуальним DOM та високою масштабованістю, що забезпечує створення інтерактивних та підтримуваних інтерфейсів.

Для стилізації використано Tailwind CSS — утилітарний CSS-фреймворк, що дозволяє швидко створювати адаптивний дизайн та кастомізувати інтерфейси.

Інструментом збирання обрано Vite, який забезпечує швидку розробку та заміну модулів.

Клієнтська інфраструктура контейнеризована за допомогою Docker для спрощення розгортання та забезпечення стабільності середовища.

Архітектура додатку

Додаток реалізує трирівневу архітектуру (рис. 1).

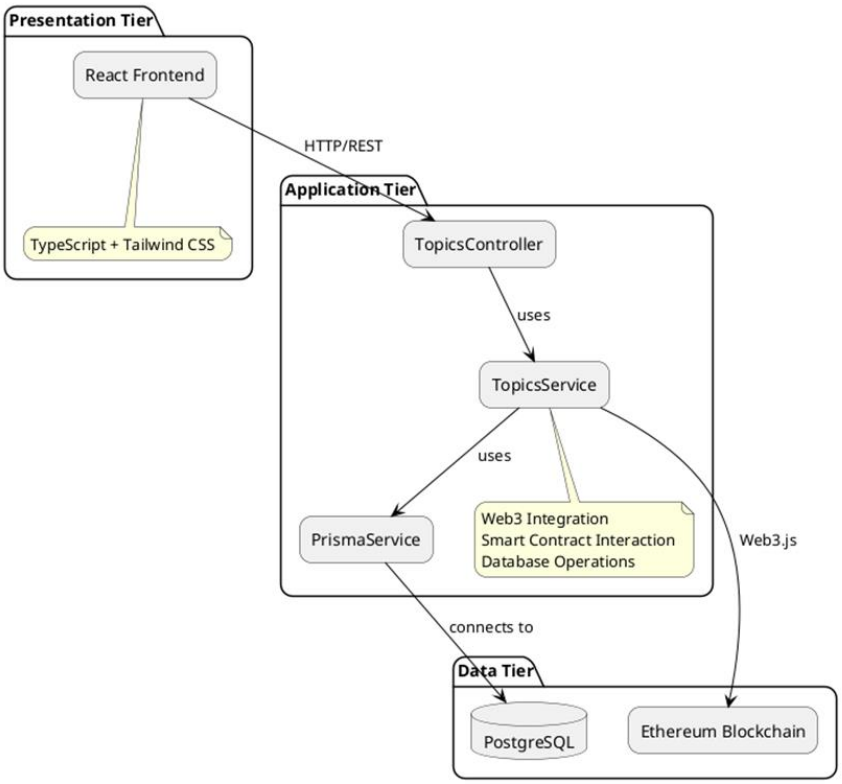

Рис. 1. Структура архітектури вебсайту

1. Рівень презентації (фронтенд): односторінковий додаток на React (TypeScript, Tailwind CSS). Він є інтерфейсом для виборців (панель голосування) та адміністраторів (адмін-панель), обробляє підключення гаманця, відображення тем, голосування та забезпечує взаємодію з бекендом через REST API та Web3-аутентифікацію.
2. Рівень бізнес-логіки (бекенд): реалізований на NestJS. Це ядро системи, що керує всіма операціями голосування (створення тем, валідація голосів) та взаємодією з блокчейном через BlockchainService (Web3.js для Ethereum, деплой смарт-контрактів, відправка голосів, отримання результатів).
3. Рівень даних: складається з PostgreSQL для офчейн даних (інформація про теми, користувачів); блокчейн Ethereum для незмінних транзакцій голосування та смарт-контрактів; Prisma ORM для типобезпечного доступу до PostgreSQL (CRUD-операції, модель Topic).

Такий розподіл забезпечує модульність, підтримуваність та масштабованість, а інтеграція блокчейну — безпеку та прозорість процесу голосування.

Діаграма прецедентів

На рис. 2 представлена діаграма прецедентів, яка показує різні варіанти використання додатку та відповідно користувачів системи.

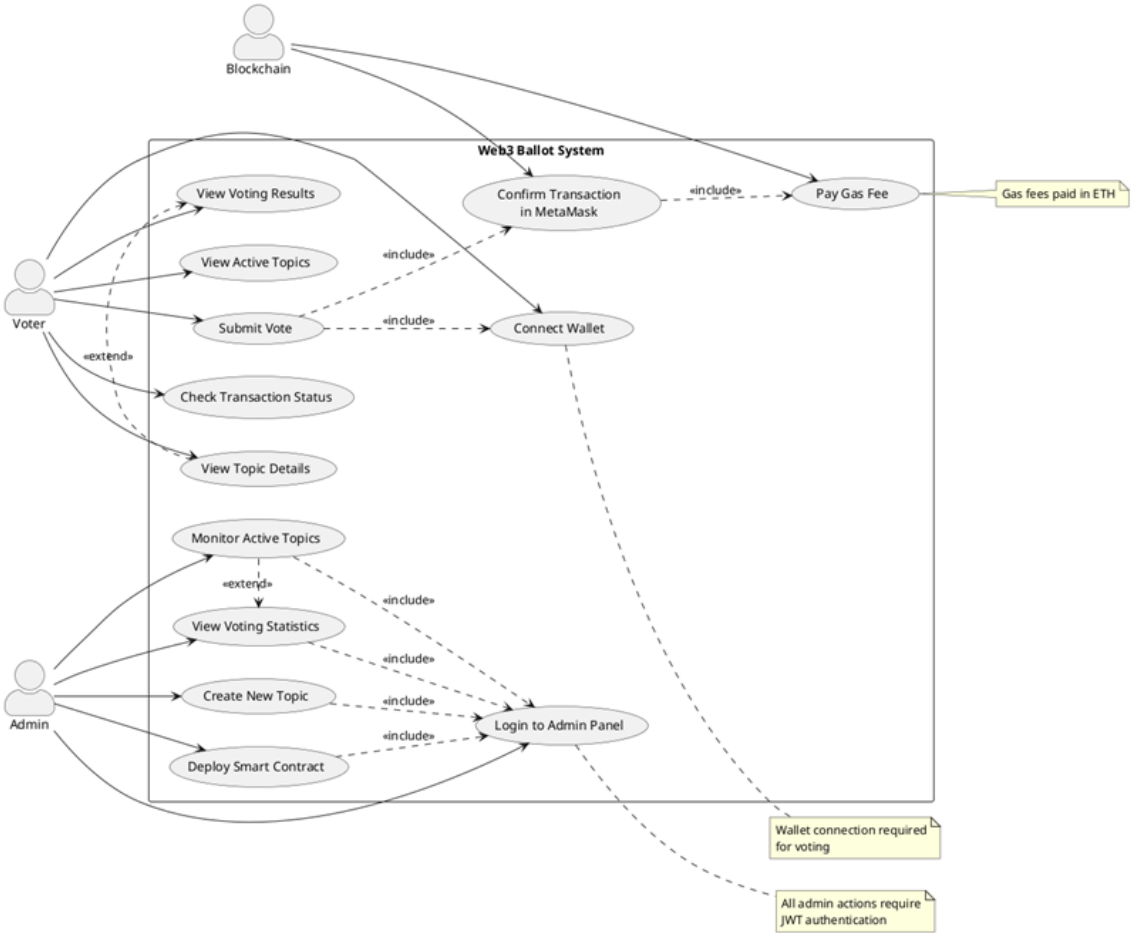

Рис. 2. Модель прецедентів

Для виборців автентифікація здійснюється через інтеграцію з гаманцем MetaMask. Неавторизовані користувачі мають доступ лише до головної сторінки входу (/), де вони можуть підключити свій Ethereum-гаманець для участі в голосуванні. Після автентифікації виборці отримують доступ до панелі голосування (/dashboard), де можуть переглядати активні теми голосування та брати в них участь, а також переглядати деталі тем (/topic/:contractAddress) для голосування.

Доступ до адміністративної панелі системи контролюється за допомогою API-ключів, що забезпечує окремий процес автентифікації для адміністраторів. Сама сторінка входу (/admin) є відкритою для всіх, проте доступ до функціоналу панелі адміністратора (/admin/dashboard) можливий лише після успішної перевірки прав адміністратора. Після входу адміністратори отримують можливість управляти темами для голосування, створювати нові опитування та налаштовувати права користувачів, що беруть участь у виборах.

Реалізація блокчейн частини

Смарт-контракт Ballot (рис. 3) призначений для безпечного електронного голосування без делегування голосів і організований навколо структур Voter (інформація про виборця) та Proposal (варіанти голосування).

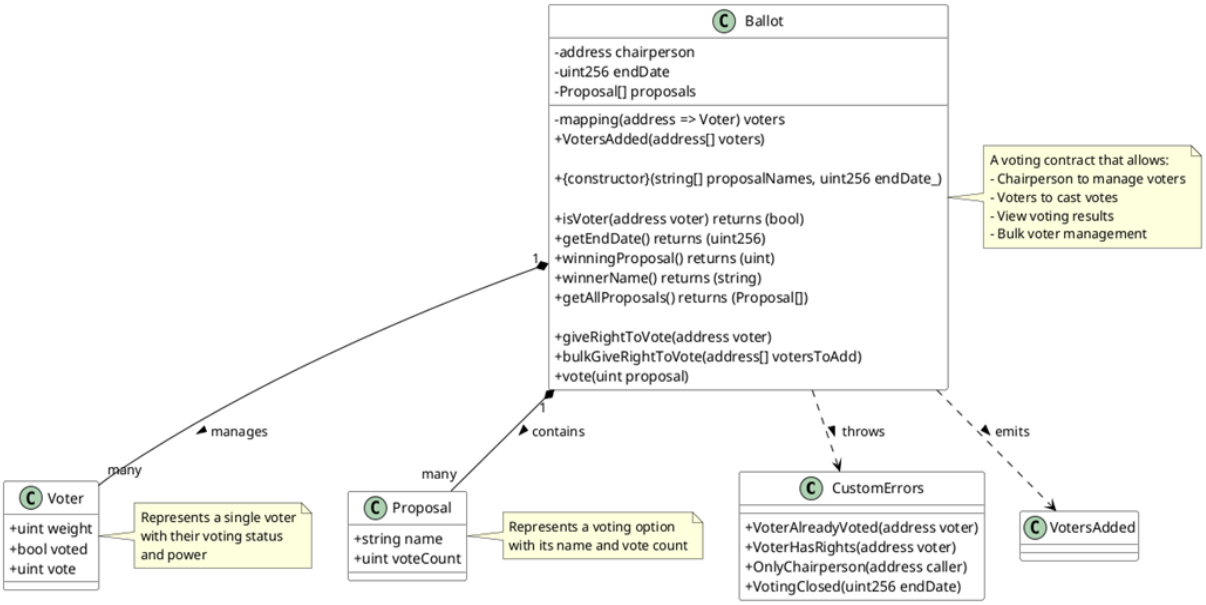

Рис.3. Функції та структури смарт-контракту

Voter зберігає вагу голосу, факт участі та обрану пропозицію, а Proposal — назву та підраховані голоси. Адміністратор (змінна chairperson) має ексклюзивний доступ до функцій управління, наприклад, надання прав голосу (giveRightToVote, bulkGiveRightToVote), з контролем доступу через користувацькі помилки (OnlyChairperson, VoterAlreadyVoted, VoterHasRights, VotingClosed).

Відображення voters пов’язує адреси з виборцями, а масив proposals зберігає всі пропозиції. Конструктор встановлює endDate та надає голові початкову вагу голосу.

Функція vote реалізує логіку голосування: перевіряє право виборця, терміни та реєструє голос, збільшуючи лічильник пропозиції з урахуванням ваги.

Допоміжні функції (winningProposal, winnerName, getAllProposals) надають доступ до результатів: визначають переможця та повертають інформацію про всі пропозиції з підрахованими голосами.

Результати функціонального та нефункціонального тестування підтвердили, що розроблений додаток відповідає ключовим вимогам електронних систем голосування, зокрема незмінність голосів після подання та перевірка достовірності їх запису, що є проблемою у процесі традиційного голосування.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Блокчейн технологія пропонує обґрунтовану та перспективну основу для створення більш надійних, прозорих та ефективних систем електронного голосування. Представлена демоверсія додатку для електронного голосування з використанням блокчейн технологій може бути використана для виборів посадових осіб (наприклад, ректора університету), або для локального голосування (наприклад, обрання старости академічної групи), а також у процесі референдумів з оцінки діяльності структурних підрозділів.

Виявлені в ході дослідження дані можуть збагатити навчальні матеріали для студентів галузі 12 Інформаційні технології. Вектор подальших досліджень спрямований на оптимізацію продуктивності та підвищенні зручності користувача.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Скороход О.П. (2024). Світовий досвід впровадження та використання цифрових технологій у виборчому процесі. *Політичне життя*., 124-130. https://doi.org/10.31558/2519-2949.2024.2.16
2. Cyberattacks impact Ecuador’s national election https://www.scworld.com/brief/cyberattacks-impact-ecuadors-national-election
3. Electoral Commission hack exposed data of 40 million UK voters https://techcrunch.com/2023/08/08/electoral-commission-hack-40-million-uk-voters/
4. J. Alex Halderman and Vanessa Teague. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In Proceedings of the 5th International Conference on E-Voting and Identity - Volume 9269 (VoteID 2015). Springer-Verlag, Berlin, Heidelberg, 35–53. https://doi.org/10.1007/978-3-319-22270-7_3
5. C. Culnane, A. Essex, S. J. Lewis, O. Pereira and V. Teague (2019) "Knights and Knaves Run Elections: Internet Voting and Undetectable Electoral Fraud," in *IEEE Security & Privacy*, vol. 17, no. 4, pp. 62-70, July-Aug. 2019, doi: 10.1109/MSEC.2019.2915398
6. Oleksandr Markovets and Mykola Buchyn. (2023) Threats and Perspectives of the Implementation of E-Voting in Ukraine SCIA-2023: 2nd International Workshop on Social Communication and Information Activity in Digital Humanities, November 9, 2023, Lviv, Ukraine CEUR-WS.org https://ceur-ws.org › Vol-3608 › paper 2
7. Alvarez, R. & Levin, Ines & Li, Yimeng. (2018). Fraud, convenience, and e-voting: how voting experience shapes opinions about voting technology. Journal of Information Technology & Politics. 15. 94-105. 10.1080/19331681.2018.1460288.
8. Abhishek Subhash Yadav, Ashish Uttamrao Thombare, Yash Vandesh Urade, and Abhijeet Anil Patil. (2020), “E-voting using blockchain technology. Interna tional Journal of Engineering Research & Technology (IJERT), https://doi.org/10.17577/IJERTV9IS070183
9. Xu, Ze and Cao, Sanxing. (2020), “Efficient Pri vacy-Preserving Electronic Voting Scheme Based on Blockchain”. 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), IEEE, pages 190-196, https://doi.org/10.1109/SmartIoT49966.2020.00036.
10. Beulah Jayakumari, S Lilly Sheeba, Maya Eapen, Jani Anbarasi, Vinayakumar Ravi, A. Suganya, Malathy Jawahar.(2024) E-voting system using cloud-based hybrid blockchain technology. Journal of Safety Science and Resilience, V. 5, Issue 1, 2024, p. 102-109. https://doi.org/10.1016/j.jnlssr.2024.01.002

11. Vivek, S. K., Yashank, R. S., Prashanth, Y., Ya shas, N. and Namratha M. (2020) "E-Voting Systems us ing Blockchain: An Exploratory Literature Survey", Sec ond International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2020, pp. 890-895, https://doi.org/10.1109/ICIRCA48 905.2020.918318 5
12. Jafar U, Aziz MJA, Shukur Z. (2021) Blockchain for Electronic Voting System-Review and Open Research Challenges. Sensors (Basel). 2021 Aug 31;21(17):5874. doi: 10.3390/s21175874. PMID: 34502764; PMCID: PMC8434614.
13. Kvitka, S., & Gusarevych, N. (2022). Application of Electoral Blockchain Technology in the Digital Voting System. Public Administration Aspects, 10(2), 23-30. https:// doi.org/10.15421/152209
14. Яланецький В. (2023) Електронні системи голосування на основі блокчейну. Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 2, pp. 67-72. https://doi.org/10.18372/2225-5036.29.17870
15. Mohammad Hajian Berenjestanaki, Hamid R. Barzegar, Nabil El Ioini, Claus Pahl. (2024) Blockchain-Based E-Voting Systems: A Technology Review. Electronics 2024, 13(1), 17; https://doi.org/10.3390/electronics13010017
16. Ohize, H.O., Onumanyi, A.J., Umar, B.U. et al. (2025). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Comput 28, 132 https://doi.org/10.1007/s10586-024-04709-8
17. Haber, S., Stornetta, W.S. (1991). How to time-stamp a digital document. *J. Cryptology* **3**, 99–111 https://doi.org/10.1007/BF00196791
18. Спасителева С.О., & Бурячок В.Л. (2018). Перспективи розвитку додатків блокчейн в Україні. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 1(1), 35–48. https://doi.org/10.28925/2663-4023.2018.1.3548
19. Sheping Zhai et al (2019) Research on the Application of Cryptography on the Blockchain. J. Phys.: Conf. Ser. 1168 032077 DOI 10.1088/1742-6596/1168/3/032077 https://iopscience.iop.org/article/10.1088/1742-6596/1168/3/032077/pdf
20. Жданова Ю.Д., Спасітєлєва С.О., Шевченко, С.М. & Кравчук К В. (2020). Прикладні та методичні аспекти застосування хеш-функцій в інформаційній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(8), 85–96. https://doi.org/10.28925/2663-4023.2020.8.8596
21. Wang, Maoning and Duan, Meijiao and Zhu, Jianming (2018). Research on the Security Criteria of Hash Functions in the Blockchain. BCC ‘18: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, Pp 47 – 55. https://doi.org/10.1145/3205230.3205238

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Svitlana Shevchenko
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Yuliia Zhdanova
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Pavlo Skladannyi
PhD, Associate Professor,
Head of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Mykhailo Ishchuk
4th year student of Software Engineering
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0007-7931-5599
st7378695@stud.duikt.edu.ua

CREATION OF A BLOCKCHAIN PLATFORM FOR ELECTRONIC VOTING

Abstract. True democracy, strong trust of people in the government and legal transfer of power in the country are possible only when elections are held honestly and correctly. Modern information technologies contribute to innovative restructuring of electoral processes, ensuring optimization of the voting process, minimizing human errors, increasing accessibility for voters. At the same time, the introduction of digital technologies creates significant problems with information security, in particular, possible changes in voting results, manipulation, threats to integrity, availability, confidentiality and anonymity. One of the effective solutions for ensuring information security in electronic voting (e-voting) is blockchain technology. This study is devoted to the problem of developing a website for electronic voting using blockchain technology. Based on the study of scientific literature, the essence, principles, advantages and disadvantages of this technology are revealed. A comparative analysis of the best practices for implementing blockchain technology in the e-voting process is presented. As an example, the process of developing a website for electronic voting using blockchain technology is described: functional requirements for this system are established, the architecture of the software application is described, and a use case diagram is modeled. TypeScript was used as the main programming language for the backend development, Nest.js as a framework, PostgreSQL for data management, and Web3.js for implementing the backend functionality. The frontend was implemented using the TypeScript programming language, the React framework, and Tailwind CSS for interface design. The developed electronic voting platform demonstrates high flexibility and can be implemented for various electoral procedures. Its functionality covers both elections of officials (for example, the rector of the university) and local votes (for example, the election of the head of an academic group), as well as referendums to evaluate the activities of structural units. The data identified during the study can enrich educational materials for students of the 12th Information Technology branch.

Keywords: information security; digital technologies; blockchain; electronic voting (e-voting); website.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Skorokhod, O. (2024). Global experience of implementation and use of digital technologies in the election process. *Political life*, 124–130. https://doi.org/10.31558/2519-2949.2024.2.16
2. *Cyberattacks impact Ecuador's national election*. (n.d.). https://www.scworld.com/brief/cyberattacks-impact-ecuadors-national-election
3. *Electoral Commission hack exposed data of 40 million UK voters*. (n.d.). https://techcrunch.com/2023/08/08/electoral-commission-hack-40-million-uk-voters/
4. Halderman, J. A., & Teague, V. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. *In Proceedings of the 5th International Conference on E-Voting and Identity, 9269*, 35–53. https://doi.org/10.1007/978-3-319-22270-7_3
5. Culnane, C., Essex, A., Lewis, S. J., Pereira, O. & Teague, V. (2019). Knights and Knaves Run Elections: Internet Voting and Undetectable Electoral Fraud. *In IEEE Security & Privacy, 17(4),* 62–70. https://doi.org/10.1109/MSEC.2019.2915398
6. Markovets, O., & Buchyn, M. (2023). Threats and Perspectives of the Implementation of E-Voting in Ukraine. *SCIA-2023: 2nd International Workshop on Social Communication and Information Activity in Digital Humanities, 3608.*
7. Alvarez, R., Levin, I., & Li, Y. (2018). Fraud, convenience, and e-voting: how voting experience shapes opinions about voting technology. *Journal of Information Technology & Politics, 15,* 94–105. https://doi.org/10.1080/19331681.2018.1460288
8. Yadav, A. S., Thombare, A. U., Urade, Y. V., & Patil, A. A. (2020). E-voting using blockchain technology. *International Journal of Engineering Research & Technology (IJERT)*. https://doi.org/10.17577/IJERTV9IS070183
9. Xu, Z., & Cao, S. (2020). Efficient privacy-preserving electronic voting scheme based on blockchain. In *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)* (pp. 190–196). IEEE. https://doi.org/10.1109/SmartIoT49966.2020.00036
10. Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. (2024). E-voting system using cloud-based hybrid blockchain technology. *Journal of Safety Science and Resilience, 5*(1), 102–109. https://doi.org/10.1016/j.jnlssr.2024.01.002
11. Vivek, S. K., Yashank, R. S., Prashanth, Y., Yashas, N., & Namratha, M. (2020). E-voting systems using blockchain: An exploratory literature survey. In *Second International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 890–895). IEEE. https://doi.org/10.1109/ICIRCA48905.2020.9183185
12. Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. *Sensors (Basel), 21*(17), 5874. https://doi.org/10.3390/s21175874
13. Kvitka, S., & Gusarevych, N. (2022). Application of electoral blockchain technology in the digital voting system. *Public Administration Aspects, 10*(2), 23–30. https://doi.org/10.15421/152209
14. Yalanetskyi, V. (2023). Blockchain-based electronic voting systems. *Ukrainian Scientific Journal of Information Security, 29*(2), 67–72. https://doi.org/10.18372/2225-5036.29.17870
15. Berenjestanaki, M. H., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-based e-voting systems: A technology review. *Electronics, 13*(1), 17. https://doi.org/10.3390/electronics13010017
16. Ohize, H. O., Onumanyi, A. J., Umar, B. U., et al. (2025). Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing, 28,* 132. https://doi.org/10.1007/s10586-024-04709-8
17. Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*, 99–111. https://doi.org/10.1007/BF00196791
18. Spasiteleva, S. O., & Buriachok, V. L. (2018). Perspectives for development of blockchain applications in Ukraine. *Cybersecurity: Education, Science, Technique, 1*(1), 35–48. https://doi.org/10.28925/2663-4023.2018.1.3548
19. Zhai, S., et al. (2019). Research on the application of cryptography on the blockchain. *Journal of Physics: Conference Series, 1168*, 032077. https://doi.org/10.1088/1742-6596/1168/3/032077

20. Zhdanova, Y., Spasiteleva, S., Shevchenko, S., & Kravchuk, K. (2020). Applied and methodical aspects of using hash functions for information security. *Cybersecurity: Education, Science, Technique, 4*(8), 85–96. https://doi.org/10.28925/2663-4023.2020.8.8596
21. Wang, M., Duan, M., & Zhu, J. (2018). Research on the security criteria of hash functions in the blockchain. In *BCC '18: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts* (pp. 47–55). https://doi.org/10.1145/3205230.3205238