Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет інформатики
Кафедра мультимедійних систем

Кваліфікаційна робота

освітній ступінь – бакалавр

на тему: **«Розробка вебдодатку для функціонування DAO (Decentralized Autonomous Organisation) для блокчейну CEDRA»**

Виконала: студентка 4-го року навчання,

Спеціальності
F5 «Інженерія Програмного Забезпечення»

Стрілецька Катерина Олександрівна

Керівник Гороховський К.С.
старший викладач
«__» _____ 2026 р.

Київ – 2026

Національний університет «Києво-Могилянська академія»
Факультет інформатики
Кафедра інформатики
Освітній ступінь бакалавр
Спеціальність F5 «Інженерія Програмного Забезпечення»
Освітня програма бакалавр

ЗАТВЕРДЖУЮ
Завідувач кафедри інформатики
Гороховський К.С.
«__» _____ 2026 р

ЗАВДАННЯ
ДЛЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТЦІ
Стрілецькій Катерині Олександрівні

1. Тема роботи: **«Розробка вебдодатку для функціонування DAO (Decentralized Autonomous Organisation) для блокчейну CEDRA»**, керівник роботи Гороховський Кирило Семенович, старший викладач

2. План роботи

Анотація

Вступ

Розділ 1. Дослідження та аналіз предметної області

Розділ 2. Аналіз технічного завдання та проєктування застосунку

Розділ 3. Розробка застосунку

Висновки

Список використаної літератури

ГРАФІК ПІДГОТОВКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

№ з/п	**ПЕРЕЛІК РОБІТ**	Термін виконання	Дата ознайомлення наукового керівника	Підпис наукового керівника	Примітки
1.	Вибір теми, затвердження її на засіданні кафедри та закріплення наукового керівника Узгодження календарного графіка підготовки кваліфікаційної роботи. Ознайомлення студента з критеріями оцінювання кваліфікаційної роботи (п. 8.5)	вересень – жовтень			
2.	Вивчення джерел літератури, матеріалів архівів, періодичних видань, збір та узагальнення фактів, даних	жовтень			
3.	Складання плану каліф. роботи та узгодження з науковим керівником	листопад			
4.	Написання практичної частини роботи	жовтень – лютий			
5.	Написання розділів роботи	листопад – лютий			
6.	Проміжний контроль виконання роботи	січень			
7.	Написання кваліфікаційної роботи в цілому, ознайомлення з її першим варіантом наукового керівника	грудень – лютий			
8.	**Розділ 1** (постановка проблеми, теоретичні основи, огляд літературних джерел)	грудень – січень			
9.	**Розділ 2** (аналітично-дослідницька частина)	лютий			
10.	**Розділ 3** (опис та підсумок результатів роботи)	березень-квітень			
11.	Повне завершення написання кваліфікаційної роботи, оформлення її згідно з вимогами й подання на відгук науковому керівнику	березень			
12.	Подання кваліфікаційної роботи для перевірки письмових робіт студентів НаУКМА на відповідність вимогам академічної доброчесності	березень			
13.	Публічний захист кваліфікаційної роботи перед екзаменаційною комісією	згідно з розкладом роботи ЕК			

Графік узгоджено 11 листопада 2025 р.

Науковий керівник Гороховський Кирило Семенович

Виконавець кваліфікаційної роботи Стрілецька Катерина Олександрівна

Зміст

Анотація

У даній кваліфікаційній роботі розглянуто створення вебдодатку для функціонування децентралізованих автономних організацій (DAO) на блокчейні Cedra. На основі порівняльного аналізу провідних DAO протоколів, таких як Uniswap Governance, Aave, MakerDAO та Squads, було визначено основні архітектурні патерни та механізми управління, а також було виявлено ключові недоліки та обмеження існуючих рішень. Завдяки глибокому аналізу сучасних підходів до зберігання даних було обґрунтовано необхідність гібридного підходу. Такий детальний аналіз став основою для проєктування власної системи.

Особливу увагу приділено реалізації смарт-контракту мовою Move з інноваційним механізмом подвійного кворуму для балансування token-weighted voting та протидії концентрації влади. Розроблено механізм спільного управління активами - multisig, повноцінний життєвий цикл пропозиції, реалізований з використанням архітектурного патерну сигнальних пропозицій (signaling proposals) як альтернативу автоматичному виконанню, що підвищує безпеку прийняття рішень. Для повноцінної роботи вебдодатку було розроблено окремий індексатор для збору, обробки та кешування блокчейн-подій у базі даних, що забезпечило швидку роботу клієнтського інтерфейсу.

Результати дослідження мають теоретичне значення для розвитку теорії децентралізованих систем управління та практичне застосування у створенні DAO-інфраструктури для блокчейну Cedra.

Ключові слова: Move, Cedra, DAO, мультипідпис (multisig), токен управління (governance token), децентралізоване управління, token-weighted voting, смарт-контракт, гібридна архітектура, Move Virtual Machine (MVM).

Вступ

Актуальність теми

Сучасний етап розвитку інформаційних технологій характеризується зростанням популярності Web3, що поступово витісняє централізований підхід Web2. Такий перехід базується на використанні технології блокчейн як головного рушія децентралізації. На зміну корпоративним та централізованим органам управління у Web3 було знайдено рішення. А саме автономні організації, DAO - децентралізовані автономні організації представляють собою нову форму економічних організацій для управління та прийняття рішень, а також управління фінансовими операціями, що використовує технологію блокчейн та смарт-контракти, забезпечуючи прозорість та мінімізуючи ризики махінацій та зловживанням влади. У такій моделі користувачі не просто споживачі, а активні учасники процесу, на відміну від сучасних традиційних форм організацій, де все контролюється централізовано та ієрархічно, DAO функціонує без центрального органу влади. Децентралізовані організації дотримуються заздалегідь визначених правил закодованих у смарт-контрактах. Саме ці правила визначають як саме члени подають пропозиції, голосують, делегують свої голоси та управляють спільними ресурсами. На сьогодні організації працюють задля реалізації різноманітних цілей, наприклад для змін в протоколах, колекціонуванні чи інвестуванні або грантової підтримки.

Мета дослідження

Метою даної кваліфікаційної роботи є дослідження та удосконалення сучасних підходів до побудови DAO, результатом чого є розробка Web3 застосунку

для повного функціонування децентралізованих автономних організацій на блокчейні Cedra.

Об’єкт дослідження

Об'єктом дослідження є процеси децентралізованого управління та прийняття колективних рішень у блокчейн-організаціях.

Предмет дослідження

Предметом дослідження є методи, механізми та архітектурні рішення для реалізації децентралізованих автономних організацій на блокчейні Cedra.

Методи дослідження

Основними методами дослідження є збір та обробка , порівняльний аналіз, проєктування, розробка та тестування програмного забезпечення.

Постановка задачі

1. Дослідити принципи та особливості роботи DAO та виявити ключові механізми управління.
2. Провести порівняльний аналіз сучасних DAO-протоколів для визначити оптимальні архітектурні патерни та технічні рішення.

3. Спроєктувати архітектуру застосунку.
4. Спроєктувати та розробити смарт-контракт для механізмів функціональності DAO мовою Move.
5. Розробити серверну частину з індексатором блокчейн-подій для синхронізації стану смарт-контрактів з реляційною базою даних.
6. Реалізувати клієнтський інтерфейс з інтеграцією криптогаманців для взаємодії користувачів з блокчейном.
7. Провести тестування розроблених механізмів та перевірити відповідність функціональним вимогам.

Структура роботи

Кваліфікаційна робота складається зі вступу, трьох розділів, загального висновку та списку використаних джерел.

У вступі обґрунтовано актуальність теми, визначено основну мета роботи, предмет та методи дослідження, а також встановлено головні завдання.

У першому розділі проведено аналіз предметної області та аналіз сучасних підходів до управління на основі дослідження протоколів DAO: Uniswap Governons, Aave DAO, MarkerDAO, а також розглянуто принципи спільного управління активами на прикладі Squads. Також обґрунтовано вибір блокчейн-платформи та мови програмування Move. Проаналізовано архітектурні підходи до зберігання даних та обґрунтовано вибір гібридного підходу. Крім цього, формуються кінцеві принципи та механізми управління, що будуть імплементовані у вебзастосунок.

У другому розділі проаналізовано технічне завдання та описано загальну архітектуру системи, а також її технічні особливості.

У третьому розділі детально описана розробка застосунку та наведені результати виконаної роботи, обґрунтовано обмеження поточної реалізації та окреслено перспективи подальшого масштабування проєкту.

Розділ 1. Дослідження та аналіз предметної області

1.1 Загальні відомості та принципи функціонування DAO

Вперше поняття DAO почали використовувати 1990-х роках, проте тоді це стосувалось більше систем, що працюють на усунення глобалізації. Більш сучасну концепцію запропонував Даніель Ларімера, саме він популяризував термін “DAC” (Decentralized Autonomous Corporations/Companies) як концептуальну основу для опису компаній, що базуються на блокчейні, в яких акціонери є і працівниками і отримувачами прибутку одночасно. Децентралізовані автономні корпорації або компанії узагальнено є підкласом DAO, проте між ними існує різниця в комерційній складові. В той час як у DAC існує чітка концепція акцій, що дають їхнім власникам постійні надходження, DAO не є комерційною структурою, хоча учасники організації можуть заробляти капітал через участь в екосистемі, а не шляхом інвестування. Більш детальний опис самого терміну DAO розглянув Віталік Бутерін в 2013 році у своєму досліджені “DAOs, DACs, DAs and More: An Incomplete Terminology Guide”. В дослідженні він розмежував поняття децентралізованих організацій, де основне визначення DAO наступне: “Це сутність, яка функціонує в інтернеті та існує автономно, але водночас значною мірою залежить від найму працівників для виконання певних завдань, які сам автомат виконати не може. DAO має внутрішній капітал, тобто DAO містить певну внутрішню власність, яка є цінною в певному сенсі, і має можливість використовувати цю власність як механізм винагороди за певні дії.”. Тобто на відміну від децентралізованих організацій (DO), де рішення приймають люди, DAO працює автономно, виконуючи рішення за створеним протоколом - “автоматизація в центрі, а люди на периферії”.

Такі децентралізовані автономні організації є прикладом структури нового покоління, які є автономними, прозорими та відкритими, базуючись на технології блокчейн, завдяки чому створюється демократична структура на зміну ієрархічній. DAO характеризуються наступними пунктами:

- онлайн-спільнота з розподіленням учасників;
- використання блокчейн технологій;
- наявність однієї мети у спільноті (це може бути покращення внутрішньої роботи компанії, створення чи управління нового продукти, а також залучення інвестицій чи коректне розподілення ресурсів);
- спільне управління;
- одна скарбниця.

Під час дослідження принципів функціонування DAO, варто виділити три основні критерії, що є найважливішими в її функціонуванні. Перш за все це спільнота організації, учасники DAO мають власні унікальні токени управління, що є цифровим активом, що надає право на участі в голосуванні, запровадженні нових змін, мати доступ до спільноти DAO, тобто безпосередньо мати вплив на подальший її розвиток. Говорячи про процес отримання токенів управління, то не можна виділити одне правило загальне для всіх організацій, кожна організація в праві вирішувати самостійно яким чином буде надавати свої токени користувачам. Згідно з дослідженням Christian Ziegler & Isabell Welpe “A Taxonomy of Decentralized Autonomous Organizations” за 2022 рік, існують чотири види доступу до спільноти:

1. Відкритий (Користувачу не потрібно володіти активами чи мати приналежність до організації, для того, щоб приєднатися).
2. Володіння токенами (Користувач, повинен мати заздалегідь визначену кількість токенів для того, щоб приєднатися).

3. Стейкінг (Token Staked) (Користувач повинен заставити або заблокувати частину токенів на певний період для того, щоб отримати доступ до спільноти).
4. Запрошення (Такий спосіб приєднання є дуже обмеженим і надається лише тоді, коли претендент на участь у DAO є частиною гаманця з мультипідписом DAO, часто власники підписів DAO визначаються під час заснування і рідко коли змінюються).

Для того, щоб учасники спільноти не тільки отримували власну вигоду, а й працювали на покращення спільноти в DAO можуть бути запроваджені різні типи нагород, а саме репутаційні токени (REP, зазвичай використовуються для голосування в DAO, не можна їх передавати), токени управління (схожі на попередній тип проте їх можна передавати), а також інші види токенів, це можуть бути стейблкоїни або сторонні активи. Проте для коректного управління голосування ДАО, слід використовувати токени управління (governance token) - одиничний токен типу ERC20, ERC721. До того ж, важливість голосу визначає кількість токенів конкретного члена спільноти, чим більше кількістю токенів користувач володіє тим більш значущий є його голос. Проте в такому випадку важливо не загубити основну ідею децентралізованих систем і не дати повний контроль так званим “китам”. Переходячи до останньої характеристики - скарбниця (treasury) варто зазначити, що кожне DAO має своє фінансування, адже DAO має отримувати дохід від інвестицій, від надання певних послуг чи через продаж власних токенів.

Зважаючи на популярність та успіх таких систем, DAO все ж таки стикаються з викликами.

1. **Безпекові ризики:** DAO управляється смарт-контрактами, які вразливі до помилок та можуть бути ціллю зловмисників для отримання доступу до коштів чи маніпуляції голосами. Саме тому організації мають впроваджувати

суворі аудити, а також використовувати кращі парадигми та підходи з кібербезпеки.

2. **Ризики централізації та управління:** Не зважаючи на те, що DAO створено для забезпечення повної децентралізації та унеможливити узурпування владою, все ж таки і надалі існує проблема, коли концентрація влади переходить вузькому колу осіб. Для боротьби з такими ризиками впроваджують нові системи голосування або системи на основі репутації.
3. **Юридичні виклики:** Через те що DAO це досить нова технологія, вона змушена стикатися з бюрократичними складовими. Так часто юридичний статус DAO може сильно відрізнятися в різних країнах, або ж взагалі бути відсутнім. Лише декілька юрисдикцій (Кайманові острови, Вайомінг, Швейцарія, ОАЕ) пропонують спеціалізовані правові форми для DAO, кожна з яких має обмеження, наприклад високі витрати на створення, податкові зобов'язання від 0% до 9%, розкривати кінцевих бенефіціарних власників (осіб, які контролюють DAO або володіють 20–25% чи більше прав управління) та інше. Це ускладнює розвиток та масштабованість.

Отже, підсумовуючи весь процес керування та життєдіяльності DAO починається з створення належної системи управління. Де головним органом влади є спільнота DAO, яка може створювати пропозиції, голосувати, приймати рішення, витрачати токени зі спільної скарбниці, використовуючи мультипідпис гаманця

1.2 Огляд та порівняльний аналіз існуючих аналогів розробки

1.2.1. Uniswap Governance

UniswapDAO це великий та успішний протокол DAO побудований на блокчейні Ethereum. Учасники організації володіють відповідними токенами UNI,

стандарту ERC20, функціональність якого має більш глибоку силу ніж торгівельний актив. Завдяки UNI члени організації можуть:

- голосувати за створенні пропозиції,
- висувати власні пропозиції, щодо розвитку та змін в протоколі, що визначають майбутнє платформи,
- делегувати свою вагу голосу іншим,
- брати участь у спільному розподілі коштів з скарбниці DAO.

Архітектура управління Uniswap чітко розділена на 3 фази та використовує гібридний механізм: on-chain з off-chain.

- **Request for Comment (RFC, бажано 7 днів)**

  На першій фазі користувач розміщує ідею на форумі і презентує її аудиторії. Мета RFC знайомити спільноту з ідеями, виявити суперечності та надати можливість автору формалізувати пропозицію. Цей етап відбувається поза блокчейном і не передбачає створення чи виконання транзакцій.

- **Temperature Check (5 днів)**

  Наступний off-chain етап, відбувається у вигляді голосування на платформі Snapshot, де учасники підтверджуються криптографічним підписом. Мета цієї фази підтвердити актуальність та важливість пропозиції, без надлишкових витрат на газ. На успішне проходження даної фази вказує досягнення необхідного кворуму у 10 мільйонів UNI.

- **Пропозиція управління**

  Остання фаза відбувається на блокчейні. Голосування за пропозицію реалізується через смарт-контракт, у разі успішного завершення, код смарт-контакту автоматично виконується через механізм Timelock з затримкою 48 годин. Користувач, який створює пропозицію повинен мати, щонайменше 1 мільйон токенів.

Процес голосування реалізований завдяки механізму делегування. Для того, щоб проголосувати учасники DAO мають делегувати свої голоси іншим учасникам

або ж самому собі. Цей механізм реалізований як функція delegate() в смарт контракті. Метою делегування є збільшити активність серед користувачів, надавши можливість пасивним учасникам передати власну вагу голосу без передачі права власності.

Переваги:

- Використання гібридного формату. Обговорення, що відбувається на форумі не записується на блокчейн, що економить газ. Проте вже останній етап голосування є on-chain, для забезпечення прозорості та чесності. Використання такого підходу є надійним і ефективним рішенням.
- Організація відкрита для нових учасників.
- Інтеграція механізму Timelock для запобіганню маніпуляцій та захисту від атак.
- Можливість делегування голосів. Завдяки цьому користувачі, які не компетентні можуть передати свою вагу голосу іншим особам, при тому в будь-який момент вони можуть припинити делегування.

Недоліки та обмеження:

- Високий газ на Ethereum mainnet.
- Високі пороги токенів під час створення пропозиції чи голосування за неї створює фінансовий бар’єр для користувачів з меншою кількістю активів, відповідно й ризик щодо виникнення контролю більшими власниками.

Отже, аналіз Uniswap Governance довів, що платформа є еталонним прикладом розроблення механізму управління. Незважаючи на недоліки, використання гібридного підходу та трифазного етапу голосування, а також імплементація механізму делегування доводять ефективність та безпеку на практиці.

1.2.2. Aave DAO

Aave DAO ще один приклад популярної децентралізованої організації, спільнота, якої є власниками токенів AAVE. Токен управління AAVE є стандартом ERC-20 і надає власнику брати активну участь у життєдіяльності організації. Особливістю цієї організації є те що кожен токен управління має два повноваження:

- Повноваження для голосування. Дає змогу користувачу брати участь в голосуваннях,
- Повноваження для пропозиції. Дає змогу користувачеві створювати пропозиції.

Такий підхід більш гнучкий, адже завдяки ньому користувачі можуть розподіляти повноваження різним адресам незалежно одне від одного. Ще однією ключовою перевагою є використання Safety module (модуля безпеки), він призначений для захисту Aave від втрат активів, реалізований шляхом замороження токенів в малоймовірному випадку дефіциту коштів. Щоправда наразі його поступово замінює новий механізм Umbrella, який ефективніший, адже використовує автоматизований механізм стейкінгу.

Процес управління AaveDAO структурно подібний до Uniswap, адже теж використовує декілька етапів і гібридний підхід. Проте на відміну від Uniswap AaveDAO підтримує cross-chain виконання.

Переваги:

- Використання гібридного підходу економить газ та підвищує ефективність процесу управління.
- Використання cross-chain. Це означає, що протокол розгорнутий на кількох блокчейнах, проте центральним залишається один - Ethereum. Це допомагає масштабувати структуру та економить витрати.
- Використання Safety Module застерігає організацію від дефіциту коштів.
- Роздільне делегування підвищує гнучкість управління порівняно з традиційними моделями управління.

Недоліки та обмеження:

- Потенційним ризик може бути перехід до централізація, через збільшення токен холдерів, які контролюють велику частину токенів.
- Використання cross-chain управління ускладнює аудити та підвищує потенційні ризики атак.

Отже, Aave є сучасними та розвиненим DAO з активною спільнотою, який використовує нові технічні підходи. Для розробки DAO на Cedra актуальним є впровадження механізму роздільності повноваження для токенів. Ця особливість може покращити функціональність Cedra DAO та додати гнучкості. Проте імплементація роздільного голосування може значно перевантажити логіку смарт-контракту, що в свою чергу вимагає кращих перевірок безпеки та аудитів. Також важливим для імплементації в проєкт є використання cross-chain, проте такий підхід краще розглядати на етапі маштабованості проєкту, а не MVP.

1.2.3. MakerDAO

Наступним прикладом є одне з найуспішніших та найстаріших протокольних DAO - MakerDAO, що також працює на базі Ethereum. Децентралізована структура має власний токен MKR, який дозволяє брати активну участь у покращенні протоколу makerDAO. Економіка голосування влаштована таким чином, що на результат голосування впливає саме кількість токенів, а не кількість користувачів, які проголосували (token-weighted voting). Використання такого підходу може погано вплинути на перебіг голосування, що може призвести до узурпування владою. Процес управління MakerDAO досить подібний до цього ж процесу в попередніх організації, а також поєднує в собі гібридний підхід голосування. Проте має особливість, а саме механізм Emergency Shutdown. Він розроблений для того, щоб захистити системи в кризових ситуаціях, таких як хакерські атаки чи порушення безпеки. Крім MKR, Marker протокол має також стейблкоїн - Dai, саме він забезпечує стабільність організації. І саме завдяки механізму Emergency

Shutdown та наявність стейблкоїнів Dai робить організацію стабільно та більш захищеною.

Переваги:

- Робоча та працююча модель управління стейблкоїнами, дозволяє фінансувати рішення скарбниці без конвертації в зовнішні активи.
- Для кризових ситуацій розроблений спеціальний механізм.
- Складна система прийняття рішень, яка поділена на декілька блоків. Проте саме це дозволяє ДАО ефективно працювати.

Обмеження та недоліки:

- Використання безперервного голосування погіршує процес аудиту та аналіз активності.
- Складний процес входження для нових учасників та ризик помилок у смарт-контракті через високу складність системи.
- Існує ризик централізації через відсутність обмежень для кількості.

Підсумовуючи, MakerDAO має чудові особливості розробки в сфері управління стейблкоїном, механізмі безпеки для кризових ситуацій. Досвід цього DAO доводить важливість використання потужних механізмів безпеки. Імплементація механізму Emergency Shutdown є вдалим підходом для проєктованої системи, проте виходить за межі поточного обсягу роботи.

1.2.4 Squads

Squads вперше був оприлюднений у 2021 як додаток для управління розгорнутий в системі блокчейну Solana. Проте згодом Squads було перекваліфіковано через потребу у безпеці та децентралізованому управлінні активами. Тому наразу Squads - це стандартний протокол multisig, який використовують сотні DAO, венчурні фонди та DeFi-проєкти, такі як Helium, Jito та Pyth.

В основі Squads лежить відкритий, незмінний, стандарт гаманця для смарт-контрактів - Squads Protocol. Унікальність цієї платформи в тому, що вона надає функціональність для команд призначати детальні ролі кожному члену multisig: Proposer, Approver, Executor. А також платформа дозволяє заздалегідь визначати ліміти витрат без потреби багаторазових затверджень невеликих транзакцій. В останньому оновлені протокол був розширений з урахуванням можливості створювати фінтех-додатки та покращення безпечного управління on-chain активами. Наразі Squads Protocol v4 має такі особливості: time locks (блокування часу), spending limits (ліміти витрат), ролі, суб-акаунти, множинні платежі та підтримка таблиць пошуку адрес.

Так як Squads першочерго побудований для Solana, то він має такі переваги над іншими традиційним гаманцями як: нижча комісія, краща швидкість, безперебійна інтеграція з dApps та зручність у використанні. Варто зазначити, що протокол формально верифікований, що забезпечує вищий рівень гарантії, ніж традиційні аудити. До того ж правила протоколу виконуються безпосередньо валідаторами мережі Solana, а не централізованим управлінням.

Проте Squads тримає фокус переважно на управліні спільними активами та їх безпеці, тоді як функціональність управління, а саме голосування, створення пропозицій реалізовано через сторонні сервіси, а не нативно.

1.2.5 Загальні висновки порівняльного аналізу

Проведений аналіз чотирьох платформ дозволяє сформувати основні архітектурні рішення та патерни, які варто імплементувати в розробленому мною проєкті для блокчейну CEDRA.

1. **Багатофазовий процес прийняття рішень**. Трифазна система голосування з використанням Snapshot у Uniswap або аналогічна система у Aave доводять свою ефективність, запобігаючи поспішним рішенням. Проте головною перевагою цього підходу є фільтрація пропозицій для економії комісії. Для

проєктованої системи буде реалізовано мінімум дві фази: активне голосування та стан очікування (pending), з налаштовуваним voting_period на рівні смарт-контракту.

2. **Token-weighted voting.** Незважаючи на ризик концентрації влади, обрана модель голосування є базовою та реалізована у всіх розглянутих протоколах DAO. Цей підхід обраний через прозорість, технічну зрілість та збільшення зацікавленості спільноти, за якої учасник несе пропорційну відповідальність за прийняті рішення відповідно до частки в протоколі. Для усунення ризику концентрації влади передбачено реалізацію механізмів кворуму у смарт-контракті, подібно до Uniswap Governance.
3. **Multisig для управління скарбницею DAO**. Імплементація механізму multisig обумовлена досвідом Squads та MakerDAO. Завдяки розподіленому управлінні активами довіреними членами DAO, зменшується ризик до маніпуляцій та витоку активів. Саме тому передбачена реалізація multisig за схемою M-of-N для захисту активів організацій.

Використання цих концепцій є надійним та технічно зрілим рішенням, через їхню ефективність у використанні іншими платформами. Імплементація даних концепцій значно підвищить ефективність роботи розробленої системи, підсилить захист від атак, а також збільшить залученість, довіру та інтерес користувачів.

1.3 Огляд блокчейн платформи CEDRA

Обґрунтування вибору блокчейн-платформи CEDRA

Cedra - це блокчейн нового покоління на базі коду відкритої платформи Aptos. Cedra містить в собі найкращі технології успадковані від блокчейн платформи Aptos, додаючи нові технологічні рішення. Завдяки чому блокчейн наділений повним функціоналом для створення надійної інфраструктури DAO.

1.3.1. Забезпечення гарантій безпеки завдяки MVM

Для забезпечення надійності та безпеки було обрано працювати в екосистемі блокчейну Cedra, який функціонує на базі мови програмування Move. Блокчейн побудований на Move та працює на Move Virtual Machine (MVM) та імплементує ресурсно-орієнтовану парадигму програмування. Порівняємо з акаунт-орієнтованою парадигмою, яку імплементують традиційні блокчейни, наприклад на базі Ethereum Virtual Machine (EVM), де основною моделлю даних є акаунти, а не ресурси. Тобто цифрові активи зберігаються як записи балансів акаунтів в хеш-таблицях, що дозволяє змінювати дані балансів активів користувача у смарт-контракті. У блокчейні Cedra ж ресурс існує лише в одному місці в певний період часу і не може бути перекопійованим. Завдки MVM також неможливе неявне знищення даних, що унеможливлюється саме мовою програмування Move. Resource-oriented модель забезпечує гарантії безпеки ще на рівні компіляції завдяки використанню лінійних типів та системи власності мови Move, а не покладається лише на runtime перевірки.

Саме цей підхід надзвичайно важливий в сфері DeFi та ідеально підходить для реалізації смарт-контрактів DAO. Адже архітектура Cedra визначає, що безпека активів є відповідальністю компілятора та віртуальної машини, а не людського фактору. Мінімізація багів в такому випадку є критичною, оскільки помилки в управлінні активами призводять до незворотних фінансових витрат.

1.3.2. Паралельне виконання транзакцій

Cedra використовує технологію Block-STM, забезпечуючи паралельне виконання транзакцій. Цю технологію Cedra імплементувала від Aptos, що забезпечило блокчейну більшу пропускну здатність мережі в транзакціях за секунду. Block-STM працює таким чином, що динамічно виявляє залежності та уникає конфліктів. Такий детермінований алгоритм також гарантує, що кінцевий

результат буде таким самим, якби транзакції виконувались послідовно без використання паралельності.

1.3.3. Використання модульної топології

Важливою архітектурною особливістю блокчейну також є використання модульної топології мережі. Що надає можливість розгорнути власну підмережу, де розробники можуть налаштувати власну економіку газу, правила управління чи консенсусу та інше. Порівнюючи з монолітними блокчейнами, модульний має кілька значних переваг:

- масштабованість (Кожен модуль є ізольованим і може налаштовувати власні параметри, які не впливають на інших, що дозволяє краще масштабувати);
- ізоляція (Активність одного не впливає на інші DAO);
- гнучкість (Завдяки модульному типу кожен окремий модуль може бути налаштований під певну спеціалізацію. Відповідно і мати різні економічні моделі та правила управління);

Саме модульний тип підходить найкраще для створення DAO платформи, адже надає повну ізоляцію для організацій, які мають право абсолютно незалежно встановлювати правила. До того ж Move Object Model вирішує вагому проблему класичних смарт-контрактів - надмірне навантаження (State Bloating) глобального стану, що збільшує ризик серйозних DoS атак. Завдяки тому, що кожна організація ізольована та розташована за унікальною адресою, транзакції та дії пов’язані з функціональністю організацій обробляються паралельно. Це підвищує пропускну здатність системи, а також допомагає під час маштабованості.

1.4 Аналіз архітектурних підходів до зберігання даних (off-chain / on-chain)

Сучасні приклади проєктів DAO реалізують різні підходи до збереження та маніпулювання даними. Їх поділяють на три категорії: on-chain, off-chain та гібридну форму. Важливість вибору моделі для реалізації застосунку критична, адже це впливає на економічну складову структури її витрат, збільшення капіталовкладень, а також залученість стейкхолдерів та інвесторів.

1.4.1. On-chain

Архітектурний підхід на блокчейні дозволяє керувати організацією, голосувати та зберігати інформацію прозоро та безпечно. Ця модель реалізується безпосередньо на блокчейні завдяки смарт-контрактам, а її головна мета це забезпечити децентралізацію та прозоре прийняття рішень. Правила, які визначає смарт-контракт, наприклад володіння токенами управління, правила мультипідпису, баланс гаманця чи його поповнення автоматично перевіряються вузлами мережі блокчейну, забезпечуючи безпечний контроль над ресурсами без втручання людей.

До того ж смарт-контракти забезпечують дотримання обмежень основного балансу DAO та ведуть ретельні аудити. Ще однією перевагою використання блокчейн технологій для реалізації DAO механізмів є інкапсуляція від зовнішнього впливу людей на ресурси, що вже записані на блокчейні. Таким чином віддавши свій голос один раз, ніхто вже не зможе змінити його, якщо так передбачено правилами смарт-контракту.

Такий підхід є традиційним для управління DAO, а також DeFi платформ та підходить для великих організацій, де важливо зберегти прозорість та незмінність даних. Прикладом серед відомих платформ, що використовують блокчейн для організації ресурсів та управління є Uniswap. Система управління DAO on-chain

дозволяє членам спільноти голосувати за зміни в протоколі чи рішення, пов’язані з операціями блокчейну. З точки зору обліку, on-chain управління забезпечує кращий аудит. Оскільки транзакції є незмінними, мають часові мітки та захищені від маніпуляцій, постійна гарантія може потенційно замінити більш традиційні періодичні аудити. З економічної точки зору, це підвищує ефективність капіталу, зменшує адміністративне навантаження та дозволяє впроваджувати програмовані системи винагород як стимули.

Однак така реалізація має і свої недоліки і погано підходить для організацій з частим голосуванням або обмеженими ресурсами. Реалізація DAO on-chain, може стати економічно не вигідною. Так як кожна транзакція потребує сплати газу, такий підхід може бути недоступним для деяких учасників. Також існує ризик втрати користувачів або малої залученість. Якщо члени DAO не отримують винагороди за свою участь або мають сплачувати високі комісії за транзакції в блокчейні, щоб проголосувати, це може відлякувати їх від участі в управлінні. Потенційним рішенням стане дозвіл на делегування голосу. До того ж в залежності від пропускної здатності блокчейну швидкість надсилання та обробки транзакцій може бути незадовільна.

1.4.2. Off-chain

На противагу on-chain механізму існує стандартний підхід зберігання у базах даних або децентралізованих сховищах, наприклад IPFS. Формування пропозицій, обговорення, угоди, управління та голосування зберігається поза блокчейном, для цього можуть бути використані зовнішні форуми. Часто такий підхід у системі DAO реалізують до основного голосуванн on-chain. Наприклад Uniswap та Aave DAO проводять off-chain перегляд пропозицій та обговорення для того, щоб зрозуміти настрій учасників. Якщо пропозиція не актуальна чи не популярна, то не буде зберігатися на блокчейні.

Прикладом є платформа Snapshot, яка дозволяє учасникам голосувати off-chain. Їхні голоси записуються як криптографічно підписані повідомлення, які зберігаються у децентралізованій мережі IPFS.

Перевагами такої реалізації є зручність та простота у використання для будь-яких веб платформ чи додатків. До того ж на відміну від блокчейн транзакцій такий підхід не потребує витратів газу. Даний підхід також є швидшим порівняно з on-chain транзакціями і сприяє більшій участі.

Проте реалізація off-chain не має такої історичної постійності голосування як on-chain, тобто якщо вебзастосунок, на якому проводиться голосування, вирішить видалити інформацію про голосування або ж станеться якась атака чи збій, вона буде втрачена. Ще одним недоліком є брак прозорості та ризик до маніпуляцій, складність проведення незалежних аудитів. Off-chain найкраще підходить для організацій з великою кількістю голосувань та пропозицій, що не несуть прямих фінансових ризиків.

1.4.3. Гібридний підхід

Гібридна модель поєднує переваги on-chain та off-chain механізмів, що надає більш гнучку та справедливу структуру управління DAO. Цей метод дозволяє членам спільноти подавати та голосувати за пропозиції.Такий підхід може бути реалізований по різному.

1. off-chain обговорення відбуваються на соціальних платформах, а для сприяння прийняттю рішень вже використовуються смарт-контракти. Завдяки цьому прийняті рішення базуються на думці спільноти, та є гарантування прозорості.
2. Критичні дані (результати голосування, транзакції скарбниці, розподіл токенів) фіксуються on-chain, тоді як допоміжні дані (описи пропозицій, коментарі, метадані) зберігаються off-chain у реляційній або документоорієнтованій базі даних.

Такий підхід на даний момент є найпрактичнішим як форма організації управління DAO, адже забезпечує як і ефективність так і прозорість. Його реалізують Uniswap Governance та Aave Governance V3.

Для реалізації даного дипломного проєкту було обрано саме гібридний підхід, де смарт-контракт на блокчейні визначає всі правила та логіку управління, голосування, мультипідпис, розподіл токенів, а PostgreSQL використовується для кешування подій, метаданих пропозицій та забезпечення ефективного UX. Таким чином розроблена платформа гарантує захищеність фінансових операцій завдяки консенсусу блокчейна, проте швидкість та доступність завдяки off-chain даним.

1.5 Механізми управління та децентралізованого контролю активами

Успіх DAO перш за все залежить від правильно налаштованої токеноміки та імплементованих механізмів управління. Проаналізувавши приклади успішних реалізацій DAO, було обрано найкращі підходи для розробки повноцінної функціональності роботи платформи.

1.5.1. Механізм пропозицій та голосування в DAO

За зразок механізму створення пропозиції було взято протокол Uniswap Governance, де пропозиція проходить декілька етапів перед тим як бути виконаною. Перед усім механізм створення пропозиції спочатку ретельно валідує вхідні дані. Однією з критичних умов створення пропозиції є дотримання порогу токенів (proposal threshold) - це конкретна кількість токенів управління, яку користувач повинен мати. Наявність цього обмеження зменшує ризик спаму не корисних пропозицій, через які хакери можуть здійснювати атаку. Адже якщо пропозиція пройшла успішну валідацію з балансу користувача списується плата,

яка надсилається на адресу DAO - комісія за створення пропозиції (proposal fee), створюючи таким чином економічний цикл і підтримку для організацій.

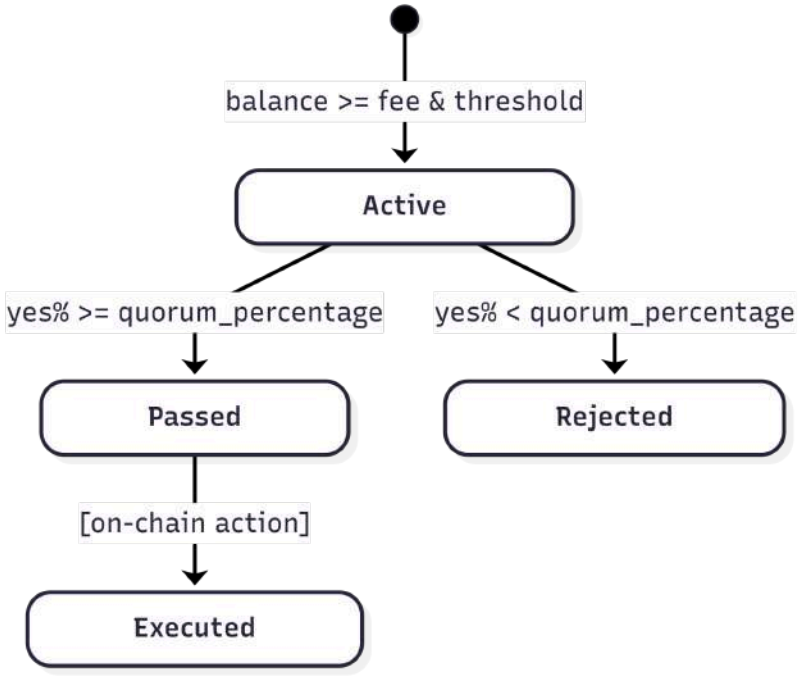

Рис.1.2.1 Життєвий цикл пропозиції

На рисунку 1.2.1 зображено стани в яких може знаходитись пропозиція на блокчейні. З початку пропозиція ініціалізується станом “Active”, тобто користувачі можуть брати активну участь у голосуванні обираючи один з трьох варіантів “за”, “проти” або “утриматися”. Після завершення відповідного терміну голосування, будь-хто, може викликати завершення пропозиції. Система перевіряє результати голосування за подвійним кворумом. Це означає, що крім основних перевірок на час, баланс та стан, наявні ще дві важливі перевірки для прийняття пропозиції. Подвійний кворум (dual quorum) полягає у перевірці двох незалежних умов:

1. Token-based quorum - мінімальна кількість токенів управління, що взяли участь у голосуванні.
2. Participant-based quorum - мінімальна кількість користувачів, які брали участь у голосуванні.

Такий підхід частково бореться з проблемою “китів” або великих власників активів. Таким чином навіть, якщо один користувач чи певна група осіб матиме на

меті взяти під одноосібний контроль владу децентралізованої організації і захоче самостійно прийняти якесь рішення він не зможе це зробити. Смарт-контракт працює автоматично та передбачувано, тому пропозиція буде прийнята тільки в тому випадку, якщо буде досягнуто подвійного кворуму. Проте варто зазначити, що кворум встановлює творець DAO під час її реєстрації на платформі.

Після фіналізації пропозиції наступає завершальний етап - виконання пропозиції. Цей етап використовує принцип сигнальної пропозиції (signaling proposal), тобто після її завершення, стан пропозиції змінюється на Executed та емітиться подія. Завдяки цьому патерну можна прослідкувати настрої спільноти отримати рекомендації та реалізувати пропозицію безпечно і без ускладнень, наприклад, якщо це стосується змін в якомусь протоколі чи зміни активів. А також використання такого підходу запобігає випадковому або спірному виконанню незворотних дій. Таким чином DAO захищене від виконання шкідливих пропозицій, а якщо пропозиції є безпечними та стосуються переказу активів це делагується модулю multisig.

Підсумовуючи, весь процес голосування на рівні смарт-контракту супроводжується постійними перевірками на різних етапах, що гарантує безпеку та прозорість голосування. Завдяки використанню сучасних архітектурних патернів та розробленої економічної моделі голосування з подвійним кворумом, механізм голосування є не лише стійким до атак та маніпуляцій, а ще й економічно вигідний для DAO та її учасників.

Якщо пропозиція стосується виконання фінансових операцій, наприклад переказ коштів чи розподілення активів, то її виконання делегується механізму multisig, де фінансові операції проходять додаткову перевірку для кращого захисту активів організації від несанкціонованих транзакцій.

1.5.2. Механізм спільного управління активами: multisig

У класичних централізованих системах усе управління може бути сконцентроване в руках однієї довіреної особи, що створює ризики для спільних активів організації: від людських помилок до навмисної крадіжки. Саме тому виникла потреба розробити механізм Multisig, логікою якого є виконання транзакції лише тільки тоді, коли зібрана потрібна кількість підписів. Система реалізується за стандартом M-of-N, де M - кількість обов'язкових голосів "за", а N - загальна кількість всі учасників Multisig. Стандартні налаштування такого механізму розраховані на загальну кількість учасників від трьох до п'яти, 2-of-3, 3-of-4 та 3-of-5 відповідно. Саме такий діапазон (від 3 до 5 управлінців) було визначено як базовий для забезпечення балансу між швидкістю прийняття рішень та рівнем безпеки. Це обмеження базується на аналізі Squads. Такий підхід відповідає головному принципу Multisig: рішення приймає більшість, якщо не досягнуто консенсусу - транзакцію буде відхилено.

Процес спільного прийняття рішення поділяється на декілька етапів.

1. *Ініціалізація фінансової пропозиції:* Будь-хто з управлінців може створити пропозицію транзакції, вказавши адресу токена, який хоче надіслати, адресата, опис та кількість.
2. *Обмежений період прийняття рішення:*Кожна пропозиція має чіткий термін придатності, по закінченню якого, транзакцію вже більше не можливо виконати чи підписати.
3. *Збір підписів:* Довірені особи незалежно розглядають транзакцію та надають свій криптографічний підпис.
4. *Виконання:* Результатом успішного виконання Multisig є відправлення транзакції за вказаною адресою після отримання всіх підписів.

Окремо варто наголосити на можливості переказувати не лише токени управління чи CedraCoin, а будь-які активи мережі. Таким чином застосунок

забезпечує нативну підтримку stablecoins. Використання таких активів є важливою складовою для повноцінної роботи організації (видача грантів, оплата праці).

Наявність реалізованої логіки усуває проблему з довірою та управлінням спільних активів. А завдяки розширеній підтримці інших цифрових активів в тому числі стейблкоїнів функціональність смарт-контракту розширюється та стає більш гнучкою.

1.6 Обґрунтування вибору рішення

Після проведеного дослідження основних принципів функціонування DAO та порівняльного аналізу успішних протоколів децентралізованих організацій, у даному підрозділі сформовано чіткі вимоги та особливості архітектури вебзастосунку.

Для збереження даних було обрано гібридний підхід, зважаючи на економічні фактори та вимоги до швидкості та зручності користувацького інтерфейсу. Критична бізнес-логіка реалізується on-chain за допомогою смарт-контракту, що гарантує незмінність та децентралізацію. Водночас допоміжні та дубльовані дані з блокчейна зберігатимуться off-chain у реляційній базі даних, для забезпечення швидкого інтерфейсу. Для синхронізації даних було вирішено розробити індексатор із серверної частини, який отримуватиме події смарт-контратку для подальшого кешування.

Основою управління децентралізованої організації обрано модель голосування, зваженого за токенами (token-weighted voting). Задля посилення безпеки обрано механізм подвійного кворуму. Для управління спільної скарбницею DAO та її активами імплементується механізм мультипідпису за стандартом M-of-N, що спирається на досвід протоколу Squads. Причому було обрано жорсткий поріг кількості управлінців від трьох до п’яти, включаючи засновника DAO. Адже занадто низький поріг знижує захист, тоді як занадто

високий ускладнює швидке реагування у невідкладних ситуаціях, тому було обрано оптимальні умови для всіх організацій на платформі.

Задля створення повноцінної фінансової інфраструктури скарбниця DAO має підтримувати різноманітні активи. Тому було вирішено використовувати типовий стандарт Cedra - Fungible Asset, що дозволить організація оперувати як нативними токенами, так і стейблкоїнами. Крім того аналіз успішних DAO також довів важливість в активному використанні токенів управління. Саме тому у застосунку реалізовано можливість автоматичного створення унікальних токенів управління для кожної нової організації.

Отже, обрані архітектурні рішення поєднують найкращі практики провідних DAO протоколів та інтегровані до особливостей та обмежень обраного блокчейну Cedra. Використання описаних концепцій та механізмів є надійним та технічно зрілим рішенням, що поєднує також інноваційні підходи до управління організаціями. Таким чином, комплексне дослідження предметної області дозволило сформувати архітектурну стратегію та вимоги до майбутнього застосунку, проєктування, розробка та тестування якого детально описані в наступному розділі кваліфікаційної роботи.

Розділ 2. Аналіз технічного завдання та проєктування застосунку

2.1 Аналіз технічного завдання та постановка задачі

Головною метою застосунку є створення повноцінної платформи для функціонування децентралізованих автономних організацій, яка надає можливість користувачам створювати власні DAO в межах єдиної екосистеми. Платформа дозволяє персоналізувати параметри організацій відповідно до своїх потреб: налаштовувати параметри управління, проводити голосування, обмінюватися ідеями стосовно пропозицій та безпечно керувати спільними активами без єдиного централізованого управління. Процес децентралізації відбувається завдяки інтеграції з блокчейном Cedra.

Відповідно до поставленої мети роботи, було сформовано основні завдання розробки:

1. Програмна реалізація смарт-контракту мовою Move з ключовою бізнес-логікою застосунку.
2. Проєктування та розробка серверної частини застосунку, яка містиме індексатор блокчейну для синхронізації on-chain даних з реляційною базою даних.
3. Розробка інтуїтивно зрозумілого інтерфейсу користувача, що забезпечить підтримку Web3.
4. Інтеграція компонентів системи, для забезпечення надійності та швидкому обміну даними.
5. Тестування платформи.

Для досягнення поставленої мети було сформовано основні вимоги до системи. Перш за все, функціональні вимоги до вебзастосунку включать:

- *авторизація та аутентифікація:* користувач має змогу увійти в систему декількома способами. По-перше завдяки електронній пошті та паролю, по-друге завдяки підключенню криптогаманця.
- *редагування профілю:* користувач має змогу редагувати профіль, проте має обмежений доступ до зміни власної ролі в структурі управлінні DAO.
- *створення DAO:* на платформі має бути реалізована можливість створення організації з власними параметрами, такими як: назва організації, опис, початкова емісія токенів управління, мінімальний кворум голосів, мінімальний відсоток схвальних голосів, тривалість періоду голосування, кількість управлінців тощо. Для створення DAO користувач має підтвердити свої наміри криптографічним ключем та оплатити комісію платформи за створення. Засновник DAO та його управлінці автоматично отримують початкову емісію токенів управління на свої адреси.
- *створення пропозиції та її обговорення:* користувачі платформи мають змогу створити пропозицію для конкретного DAO, лише при наявності встановленої кількості токенів управління. До того ж охочі користувачі платформи можуть залишати коментарі під пропозицією для висловлювання своїх думок та більш детального обговорення.
- *голосування за пропозиції:* користувачі мають мати змогу голосувати за пропозицію лише один раз. Вага голосу визначається кількістю токенів управління на балансі користувача на момент голосування.
- *децентралізоване управління активами:* користувач з роллю governor (управлінець) має змогу ініціювати надсилання коштів зі скарбниці DAO. Для цього він має зазначити адресу отримувача, тип активу (CedraCoin, токен управління, stablecoin), кількість та опис операції.

Також управлінці організації мають змогу незалежно голосувати за схвалення або відхилення транзакції.

- *статистика користувача:* кожен зареєстрований користувач системи має змогу переглядати власну активність на своєму профілі. А також користувач має змогу підключати криптогаманець для взаємодії з блокчейном.

До нефункціональних вимог системи входять:

- *безпека активів:* смарт-контракт повинен бути захищеним від несанкціонованого виведення коштів, атак повторного відтворення чи повторного голосування. До того ж транзакції мають виконуватися з дотриманням принципу атомарності. Вся взаємодія користувача з критичними операціями вимагає автентифікації користувача через підпис приватним ключем Web3-гаманця.
- *швидкість та надійність обробки подій:* серверна частина, а саме індексатор має обробляти події з блокчейну асинхронно. Система має бути відмовостійкою: у разі проблем з підключенням до блокчейну, система має продовжувати роботу без втрати важливих даних.
- *масштабованість:* архітектура системи має передбачати можливість подальшого розширення без необхідності повної зміни системи.

Результатом виконання поставлених вимог стане надійний програмний продукт, який вирішує проблеми децентралізованого управління активами та відповідає сучасним стандартам Web3.

2.2 Опис загальної архітектури системи

Архітектура розробленої системи поділяється на чотири основні логічні рівні: клієнтський (Frontend), серверний (Backend), рівень зберігання даних

(Database) та блокчейн-рівень (On-chain). Схему взаємодії всіх компонентів системи продемонстровано на рис. 2.1.

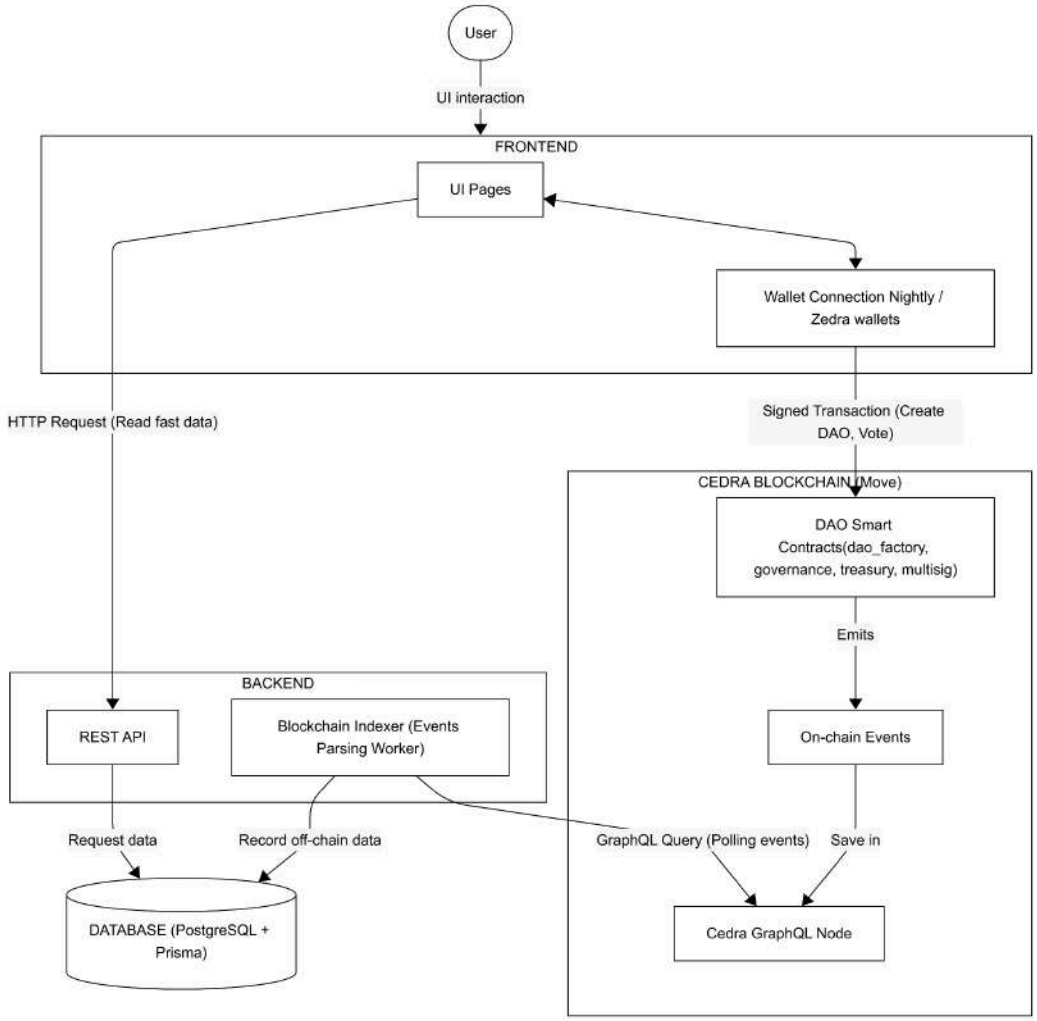

Рис. 2.1 Діаграма архітектури системи

Клієнтський рівень (Frontend) реалізований як Single Page Application на React і забезпечує користувацький інтерфейс для взаємодії з платформою. Цей рівень відповідає за відображення даних, обробку користувацьких дій, надсилання транзакцій з криптографічним підписом користувача.

Серверний рівень (Backend) складається з двох основних компонентів: REST API для обробки HTTP-запитів від клієнта та блокчейн індексатора для синхронізації блокчейн подій з базою даних. REST API надає швидкий доступ до

даних з бази даних, тоді як індексатор забезпечує актуальність off-chain даних on-chain стану через періодичний polling подій з Cedra GraphQL Node.

Блокчейн рівень складається зі смарт-контракту, де реалізована основна бізнес-логіка. Всі фінансові операції і результати голосувань фіксуються на блокчейні через емісію подій, які потім індексуються на бекенді.

Рівень зберігання даних представлений PostgreSQL базою даних з Prisma ORM.

Завдяки розробленій архітектурі система працює зі зваженим розподілом відповідальності.

2.3 Технологічний стек та обґрунтування вибору засобів розробки та їхнє використання

Для реалізації розробленого веб-застосунку було обрано наступні інструменти:

Cedra

Як було обґрунтовано в підрозділі 1.4, для реалізації смарт-контракту було обрано блокчейн Cedra, що базується на Move Virtual Machine. Ключовими факторами вибору стали: ресурсно-орієнтована парадигма програмування для гарантій безпеки активів на рівні компіляції, паралельне виконання транзакцій через Block-STM для високої пропускної здатності, та модульна топологія для ізоляції організацій.

Move

Для розробки смарт-контакту було обрано основну мову програмування блокчейну - Move. Дана мова програмування імплементує ресурсно-орієнтовану парадигму, тобто ресурси не можуть бути скопійованими чи неявно знищеними, що підвищує безпеку активів і зменшує ризик класичних вразливостей.

Node.js та TypeScript

Для розробки серверної частини було обрано середовище виконання Node.js у поєднанні з мовою TypeScript. Зважаючи на те, що робота з блокчейном та фінансовими транзакціями є критичною частиною системи, існує потреба у дотриманні типізації коду задля своєчасного виявлення архітектурних та логічних помилок на етапі розробки. Крім того, використання спільної мови для розробки як клієнтської, так і серверної частини значно оптимізує та спрощує процес розробки всього застосунку.

Безпосередня взаємодія серверної частини з блокчейном була реалізована за допомогою використання офіційного SDK - **@cedra-labs/ts-sdk**. Ця бібліотека дозволяє бекенду зчитувати глобальний стан MVM, викликати методи контрактів та відстежувати on-chain події для їх подальшого кешування.

TSOA

До того ж було використано бібліотеку TSOA (TypeScript OpenAPI) для проєктування та документування архітектури API. Її інтеграція дозволила автоматизувати процес генерації OpenAPI-специфікації (Swagger) та маршрутизаторів на основі TypeScript-декораторів, гарантуючи, що документація завжди відповідає актуальній бізнес-логіці сервера.

PostgreSQL та Prisma ORM

Для збереження off-chain даних була використана PostgreSQL. Це об'єктно-реляційна система управління базами даних з відкритим кодом. Сучасні версії включають велику кількість допоміжних функцій для розробки повноцінних додатків з відмовостійким середовищем для управління даними незалежно від обсягу. До того PostgreSQL відповідає принципам ACID, що гарантує безпечне та надійну обробку транзакцій в базі даних. База даних має великий вибір ORM, інструментів для міграцій і моніторингу, проте для взаємодії з базою даних було використано Prisma ORM. Це сучасний інструмент для об’єктно-реляційного відображення, який спрощує доступ до баз даних у додатках на Node.js та

TypeScript. Перевагами конкретної ORM є автоматична перевірка типів на етапі розробки, що зменшує кількість помилок у роботі з даними.

GraphQL

Під час написання блокчейн індексатора було використано GraphQL API для складних запитів до блокчейну. Використання цього інструмента дозволяє розробникам здійснювати запити до даних без необхідності писати складний код для отримання та фільтрування, що робить розробку більш ефективною. GraphQL безперешкодно відстежує взаємозв'язки між даними, усуваючи необхідність у численних викликах API. Для робити з великою мережею блокчейн GraphQL має значні переваги над іншими API, адже індексатор отримує всі необхідні дані за допомогою одного запиту. Після чого отримані дані обробляються і зберігаються у PostgreSQL для швидкого доступу з клієнтської частини без повторних звернень до блокчейну. Використання GraphQL покращує продуктивність і масштабованість децентралізованих додатків.

React

Для розробки клієнтського інтерфейсу було обрано бібліотеку React , що є одним із найпопулярніших UI-інструментів з компонентою архітектурою для розробки SPA (Single Page Application). ЇЇ компонентна архітектура надає можливість повторного використання компонентів під час розробки інтерфейсу, що спрощує підтримку великих проєктів. Завдяки декларативному підходу React дозволяє створювати інтерактивні інтерфейси завдяки зміні станів компоненту, що автоматично оновлює DOM-дерево (Document Object Model) без необхідності перезавантаження сторінки.

Для стилізації інтерфейсу було застосовано комбінований підхід з використанням препроцесора SCSS - це найдосконаліша, найстабільніша та найпотужніша мова розширення CSS професійного рівня. Та фреймворку Tailwind CSS, що надає набір готових класів для швидкого створення адаптивних та сучасних інтерфейсів.

Docker

Під час розробки вебзастосунку було використано Docker. Це відкрита платформа для розробки та запуску додатків в ізольованому середовищі. Використання Docker полегшує процес обміну та передачі проєктами між розробниками і гарантує однаковий код для всіх завдяки контейнеризації коду. А також спрощує розгортання проєкту як у development, так і у production середовищі.

Git

Під час розробки проєкту було використано Git, що є прикладом DVCS (розподілена система контролю версій) з відкритим кодом. Git забезпечує контроль над версіями коду для можливості роботи у розподілених командах та відстеження всіх змін у проєкті, а також надає можливість повернення попередніх станів коду, що є важливим для забезпечення надійності та цілісності під час розробки складних проєктів.

2.4. Опис ролей в системі та їхні можливості

Платформа передбачає дві основні ролі користувачів відповідно до їхнього статусу в організації: управлінець (governor) та учасник (member).

Управлінець (governor) - користувач, який призначається засновником DAO як довірена особа. Управлінці мають ширші повноваження для управління спільними активами спільноти. Крім того, вони володіють усіма можливостями звичайних учасників.

Учасник (member) - користувач, який володіє токенами управління конкретної організації. За дотримання всіх вимог, можуть створювати нові пропозиції, голосувати та коментувати.

Розділ 3. Розробка застосунку

3.1 Розробка логіки смарт-контрактів

Для забезпечення надійності, прозорості та децентралізації у функціонуванні застосунку, було реалізовано on-chain бізнес-логіку, відповідно на блокчейні Cedra. Для цього було розроблено смарт-контракт на мові програмування Move, який є основою всього застосунку. З моменту розгортання смарт-контракту на блокчейн, він працює автоматично, самостійно та децентралізовано, тобто ніхто не може критично змінювати його структуру або впливати на роботу DAO чи транзакції користувачів. У смарт-контакті було реалізовано таку функціональність для застосунку:

1. всі структури даних необхідні для успішного функціонування DAO та легшого пошуку даних для бекенду;
2. ініціалізовано константи можливих помилок для валідації;
3. логіка створення DAO;
4. логіка створення, фіналізація та виконання пропозиції;
5. система multisig для головних управлінців DAO з метою керуванням спільним балансом DAO;
6. механізм створення токенів управління відповідно до запитів користувача стандарту блокчейна - Fungible Asset та їхнє розподілення користувачам;
7. механізм голосування за пропозицію з подвійним кворумом.

Саме в смарт-контракті було визначено всі правила для можливості взаємодії та керуванням всього процесу життєдіяльності децентралізованої автономної організації.

3.1.1 Огляд архітектури смарт-контракту

Архітектурно смарт-контракт використовує модульний підхід для організації коду, в такому випадку кожен об’єкт має свою окрему адресу на блокчейні та може володіти іншими вкладеними ресурсами, що полегшує роботу з складними типами даних. Для мого застосунку це означає, що кожне DAO матиме свою унікальну криптографічну адресу і не матиме доступу чи зв’язку з іншими і буде повністю ізольованим. Кожен об’єкт DAO містить вкладені ресурси: список пропозицій, налаштування організації, конфігурацію multisig та інше. Використовуючи ресурсно-орієнтований підхід, завдяки MVM вся логіка смарт-контракту інкапсульована в єдиному модулі: dao_factory::dao, що забезпечує недоторканість та безпеку логіки.

Весь модуль смарт-контракту можна умовно розділити на чотири основні частини, які відповідають за різні функціональні особливості.

1. Управління DAO. Реалізує механізм створення нових організацій, за патерном “Фабрика” валідацію вхідних даних користувача під час створення, а також ведення реєстру з усіма організаціями.
2. Governance (Управління токенами). До цієї підсистеми належить створення унікального для кожного DAO токена управління, механізм безпечного та зваженого голосування token-weighted, де вага голосу дорівнює загальній кількості токенів, та обмеження подвійного голосування.
3. Життєвий цикл пропозиції. Для цього було реалізовано декілька окремих методів для створення пропозиції користувачем, завершення голосування за пропозицію, та її виконання.
4. Multisig. Механізм безпечного управління активами, де для здійснення транзакції з гаманця DAO, необхідна певна кількість підписів від управлінців. Цей етап включає створення транзакції, запуск голосування та його завершення успішим виконанням транзакції або відхиленням, через брак підписів.

Завдяки такій моделі проєкт можливо масштабувати в майбутньому, адже чітко окреслені межі відповідальності для кожного етапу функціонування організації.

3.1.2 Основні структури даних та їх призначення

Для реалізації логіки описаних попередньо підсистем було створено основні структури даних системи, які взаємопов’язані між собою і забезпечують повну функціональність децентралізованих організацій.

Структура DAO є основною і містить всю необхідну конфігурацію для коректної роботи організації (опис, назва унікальний числовий ідентифікатор, адреса токена управління, список управлінців multisig, загальні налаштування токена та інше). Окремо варто виділити наявність ExtendRef - це спеціальний механізм Move для генерації signer. Його мета надати можливість організації підписувати і надсилати транзакції. Завдяки чому смарт-контракт автоматично створює підпис лише після проходження всіх етапів multisig консенсусу. Наявність такого механізму є критично важливим архітектурним рішенням, що посилює безпеку організації і унеможливлює генерацію підпису будь-ким, що може призвести до узурпування чи крадіжки коштів. До складу даної структури також вкладений ресурс - DAOSetting, в якому описані параметри проведення голосування та обмеження, а саме quorum_votes, quorum_percentage, min_voters_count, proposal_threshold, voting_period.

Структура DAORegistry створена для глобального зберігання всіх DAO, які будуть створені в застосунку. Вона зберігається на адресі розробника і ініціалізується єдиний раз під час розгортання смарт-контракту. Реєстр всіх організацій потрібний для швидкого пошуку за ідентифікатором або унікальним кодом DAO.

Структура DAOGovernanceTokenControl зберігає важливі посилання для забезпечення повної функціональності токенів: MintRef та TransferRef. Створення нових токенів та їхнє розподілення відповідно.

Для реалізації логіки голосування було створено декілька структур найважливішими з яких є: ProposalStore та Proposal. ProposalStore зберігає всі пропозиції, які були створені користувачами організації, необхідна для управління та пошуку пропозицій. Кожна окрема пропозиція описується структурою Proposal.

Реалізація системи multisig було створена за допомогою трьох структур. MultisigConfig - зберігає визначену попередньо та незмінну конфігурацію, щодо кількості необхідних голосів для прийняття рішення і загальну кількість учасників multisig. PendingTransaction описує окрему транзакцію, що очікує схвалення. MultisigTransactions - структура, що містить транзакції (PendingTransaction), які лежать в листі очікування на підпис всіх учасників мультисіг.

Варто наголосити, що структури даних розроблені з урахуванням економії газу для оптимізації збереження даних.

3.1.3 Створення DAO

Процес створення акаунту DAO на блокчейні супроводжується автоматичною генерацією токена управління з параметрами metadata: назва, символ, 8 десяткових знаків, URL іконки та URL проєкту. Після успішного створення токена система карбує відповідну кількість токенів зазначену користувачем і розподіляє її у відсотковому співвідношенні, яке вказує засновник організації під час створення. Певний відсоток токенів одразу надсилається усім вказаним управлінцям рівномірно, таким чином вони одразу отримують баланс для участі після створення організації. Важливо зазначити, що весь процес створення DAO супроводжується перевірками, якщо будь-яка з валідацій не пройшла і виникає помилка - DAO не буде створена. Це гарантує правильну структуру для всіх DAO, запобігає створенню вразливих та незахищених

організацій, а також зменшує ймовірність помилок на наступних етапах. Важливо зазначити, що за створення DAO користувач платить 5 CEDRA платформі, це розроблено для підтримки економіки застосунку.

3.1.4 Технічна реалізація життєвого циклу пропозиції та етапи голосування

Як описано в підрозділі 1.5.1, життєвий цикл пропозиції включає декілька станів та механізм подвійного кворуму. Технічна реалізація всього циклу вимагала реалізації декількох архітектурних завдань, а саме:

- забезпечити атомарність операцій голосування,
- захист від повторного голосування,
- оптимізація газу для великих DAO.

Життєвий цикл пропозиції відбувається з виклику відповідної функції смарт-контракту, яка безпосередньо взаємодіє з ресурсом “ProposalStore”. Ця структура містить вектор всіх пропозицій та лічильник для генерації унікальних ідентифікаторів. Таким чином пропозиції ізольовані в різних DAO завдяки об’єктній моделі блокчейну Cedra. Отже, під час створення пропозиції смарт-контракт перевіряє поточний баланс користувача, що підписував виклик контракту своїм криптографічним ключем. Це перший з трьох основних етапів перевірок для протидії атакам та забезпечення якості пропозицій. Значення порогу (proposal threashold) визначається творцем на етапі створення організації. Під час аналізу існуючих протоколів було виявлено, що оптимальний діапазон становить 0.5-2% від загальної емісії токенів. Наприклад, Uniswap використовує поріг у один мільйон UNI, що становить 1%. Проте для платформи на блокчейні Cedra реалізована можливість обрати поріг для кращої гнучкості. Другий етап це списування комісії за створення пропозиції, як вже зазначалось кошти надсилаються на скарбницю організації, які можуть бути використані для

прийняття фінансових рішень. Після чого нова пропозиція записується на блокчейн зі статусом “Active” та обмеженням щодо періоду голосування.

Наступним логічним етапом після створення пропозиції є механізм голосування. Він реалізується завдяки методу vote, який вимагає криптографічного підпису. Вага голосу визначається за моделлю token-weighted voting, де voting_power дорівнює поточному балансу токенів управління користувача на момент голосування. Атомарність процесу голосування полягає в оновлені лічильників в рамках однієї транзакції. Якщо всі перевірки були успішно пройдені відповідно адреса користувача, що проголосував додається до загального вектору, а лічильники кількості голосів збільшуються відповідно до вибору користувача.

Фіналізація пропозиції є важливим етапом, під час якої встановлюється остаточний статус пропозиції на основі результатів голосування. Технічною інновацією цього процесу є розроблений механізм подвійного кворуму, що відрізняє розроблену систему від інших односторонніх моделей, як в Uniswap чи Aave.

Завершенням повного життєвого циклу є виконання пропозиції, тут важливо зазначити, що реалізований підхід дещо відрізняється від інших протоколів з автоматичним виконанням коду (executable proposals). В таких підходах виконання пропозиції ініціює виклик змін в смарт-контракті чи переказ активів. Проте підхід сигнальних пропозицій (signaling proposals) не передбачає негайне виконання транзакцій автоматично. Це архітектурне рішення було розроблено навмисно через безпекові фактори.

3.1.5 Технічна реалізація механізму спільного управління активами multisig

Як було описано в підрозділі 1.5.2 механізм спільного управління активами організації вимагає строгого контролю та жорстких перевірок. Реалізація цього механізму ставила перед собою деякі архітектурні виклики. Серед них:

- генерація криптографічного підпису від імені DAO без приватного ключа (для надсилання транзакцій безпосередньо з адреси організації);
- підтримка різних типів активів, в тому числі і stablecoin;
- розробити весь життєвий процес multisig голосування повністю атомарним.

Для вирішення цих та інших задач під час розробки даного механізму програмна логіка смарт-контракту базувалась на специфічних можливостях MVM.

Головною архітектурною задачею децентралізованої скарбниці є можливість безпечно ініціювати фінансові транзакції без приватного ключа, повністю автономно з адреси самої організації. Для вирішення цього завдання було використано розширене посилання (ExtendRef) з бібліотеки ‘cedra framework’. Логіка механізму полягає в тому, що під час створення DAO на блокчейні система генерує унікальне посилання, яке інкапсулюється в захищений ресурс. Цей об’єкт не може бути видаленим або скопійованим ззовні, проте він може конвертуватися в криптографічний об’єкт signer завдяки розробленій логіці смарт-контракту. Даний процес відбувається лише за умови наявності схвальних голосів всіх управлінців. Завдяки такому підходу скарбниця організації повністю захищена від крадіжки активів ззовні, адже валідний підпис для транзакції генерується безпосередньо MVM в runtime виключно за умови досягнення заданого консенсусу.

Наступним важливим етапом було реалізувати можливість зберігати та транспортувати різні типи активів для забезпечення гнучкості скарбниці. Цю функціональність було реалізовано шляхом побудови смарт-контракту за сучасним стандартом Cedra - Fungible Asset. Завдяки цьому DAO може акумулювати та безпечно переказувати CedraCoin, унікальні токени управління або стейблкоїни (USDC, USDT), не потребуючи написання окремих модулів під кожен тип активу.

Для завершення повноцінного процесу механізму multisig було важливо забезпечити атомарність та передбачуваність життєвого циклу пропозицій. Сама

функція виконання працює атомарно: вона зчитує масив підписів, перевіряє кворум, генерує signer, здійснює фінансовий переказ і змінює стан об'єкта. У випадку помилки на якомусь із етапів уся транзакція відхиляється на рівні віртуальної машини, а стан смарт-контракту повністю повертається до початкового. Це повністю виключає можливість часткового виконання операцій або незворотньої втрати активів внаслідок помилки. Додатково, для запобігання засмічення стану смарт-контракту неактуальними транзакціями, було реалізовано механізм обмеження часу життя пропозиції (Time-To-Live). Кожній новій транзакції присвоюється часова мітка, яка блокує можливість збору підписів чи виконання через 7 діб після її ініціалізації.

3.1.6 Система розподілення токенів

У логіці смарт-контракту і всього застосунку відповідно токени управління відіграють важливу роль - надають право голосу. Саме тому була створена відповідна система розподілу токенів з урахуванням децентралізації та розробленої системи управління.

Як вже зазначалось частина токенів одразу розподіляється рівномірно між управлінцями. Проте ця частина токенів не має перевищувати половини викарбуваних токенів. Завдяки такому ліміту організація захищена від надмірної концентрації влади на початкових етапах. Решта токенів залишається на рахунку організації, для їхнього розподілення створений окремий механізм.

Для того, щоб надати токени управління новим учасникам організації, один із управлінців має викликати відповідну функцію смарт-контракту, для користувача це реалізовано через клієнтський інтерфейс. Важливо зазначити, що існує обмеження в кількості токенів, які можуть бути надіслані один раз на одну адресу (оптимально 1000). Цей ліміт встановлюється під час створення DAO на блокчейні. Використання такого ліміту зменшує ризик помилок та бюрократичних маніпуляцій. Для більших сум варто використати Multisig, щоб забезпечити

кращих контроль. Отже, такий підхід дозволяє відповідальним особам швидко розподілити токени серед нових учасників, наприклад співробітників компанії.

3.1.7 Підсумок розробленого смарт-контракту

Було розроблено смарт-контракт з використанням модульної архітектури та об’єктно-орієнтованої парадигми програмування, завдяки чому успішно досягнуто повної ізоляції окремих децентралізованих організацій, безпеку активів та автоматизованість виконання правил. Було реалізовано та оптимізовано основну on-chain логіку для інтеграції з блокчейном Cedra, зважаючи на економіку газу.

Інтегровано механізм multisig з можливістю передачі stablecoin, повний цикл життєдіяльності пропозицій від створення до завершення з використанням перевірки подвійного кворума, голосування за системою token-weighted, створення унікальних токенів управління їхнє розподілення. Всі процеси супроводжуються постійними валідаціями даних в разі порушення правил смарт-контракту користувач отримує кастомну помилку з унікальним кодом. Розроблена функціональність відповідає вимогам децентралізованим організацій та DeFi протоколів у мережі Web-3 та підтримує масштабованість. Математичний обрахунок в управлінні організаціями посилює захист від маніпуляції даними та узурпування владою “китів”.

3.2 Реалізація серверної частини та клієнтського інтерфейсу

Наступним етапом після розгортання смарт-контракту у розробці вебдодатку стала розробка off-chain інфраструктури, яка відповідає за взаємодію користувача з блокчейном. Програмна реалізація цієї частини складається з двох модулів: блокчейн індексатора на серверній частині з REST API та клієнтського інтерфейсу.

3.2.1 Програмна реалізація індексатора блокчейн-подій

Блокчейн являє собою розподілену машину станів, де вузли (nodes) виконують роль, яку раніше виконували централізовані сервери. Вони забезпечують консенсус, валідацію транзакцій, зберігають дані та взаємодіють один з одним. Проте блокчейн не адаптований для складних реляційних вибірок, а пряма взаємодія фронтенд-частини з вузлами блокчейну через стандартні RPC-запити має суттєві обмеження. Саме тому для вирішення цих архітектурних викликів було розроблено власний блокчейн-індексатор.

Технічна необхідність індексатора зумовлена потребою у трансформації сирих даних блокчейну у структурований реляційний вигляд. Програмна реалізація процесу полягає у встановлені постійного з‘єднанні з Cedra Node та періодичного опитування (polling) вузла на наявність нових подій, емітованих шляхом виклику власного смарт-контракту. Polling здійснюється завдяки GraphQL запитам.

Практична значущість такого підходу полягає у його відмовостійкості та повній синхронізації з блокчейном. Така функціональність реалізується шляхом збереження в базі даних унікального ідентифікатора останньої успішно обробленої події. До того ж, якщо індексатор повертає помилку він не припиняє свою роботу, помилка логується через бібліотеку Winston, а механізм повторює спробу через декілька секунд. Після трьох невдалих спроб індексатор переходить у режим exponential backoff зі збільшенням інтервалів викликів, щоб не перевантажувати недоступний вузол. Таким чином, якщо серверна частина тимчасово втрачає зв’язок з мережею або перезавантажується, робота індексатора буде відновлена без втрати подій.

Під час розробки системи я дотримувалась стратегії Event-Driven Development (розробка на основі подій). EDD - це стратегія розробки, яка зосереджується на створенні смарт-контрактів з великим обсягом даних для децентралізованих додатків. Вона закладає основу для подій смарт-контрактів з

урахуванням кінцевого додатка або сценарію використання, що, у свою чергу, допомагає ефективно надавати користувачам як поточні, так і історичні дані. Принцип цього підходу полягає у наступному: коли смарт-контракт генерує подію, він створює повідомлення, яке зберігається в блокчейні. Зовнішні додатки можуть отримувати доступ до цих логувань і здійснювати запити до них, завдяки чому події стають зручним способом повідомлення про зміни стану та відповідного запуску дій.

Отриманні дані з блокчейну парсяться та валідуються і записуються в базу даних для швидкого UI виводу. Доступ до цих структурованих даних надається клієнтському застосунку через REST API, маршрутизація та документація якого автоматично генерується за допомогою декораторів TSOA.

3.2.2 Інтеграція Web3 у клієнтському інтерфейсі

Основна мета клієнтської частини - надати можливість користувачу зручно взаємодіяти з екосистемою.

Для побудови інтерфейсу було обрано Atomic Design методологію з розділенням компонентів на рівні. Навігація в межах застосунку реалізована за допомогою використання react-router-dom, що забезпечує клієнтський роутинг без переавантаження сторінок, підвищуючи продуктивність.

Програмна логіка розділена на два функціональні напрямки:

1. Читання та відображення даних: реалізується стандартними HTTP-запитами до розробленого REST API для миттєвого відображення. Завдяки індексатору, дані завантажуються за мілісекунди, не перевантажуючи RPC-вузли блокчейну.
2. Інтеграція Web3: усі дії, що вимагають зміни системи (створення пропозиції, голосуванн, ініціалізація витрат), реалізовані через інтеграцію з Web3-гаманцем, а саме Nightly Wallet.

3.3 Тестування застосунку та результати роботи

Тестування застосунку поділялось на декілька етапів, охоплюючи як автоматизовану перевірку on-chain логіки, так і функціональне тестування off-chain інфраструктури.

Тестування смарт-контракту було проведено до його розгортання на блокчейн, адже після цього він є незмінним. Тому для тестування смарт-контракту було створено близько 50 unit-тестів, які включали перевірку на успішне виконання всіх реалізованих механізмів. А також окремо було протестовано випадки, завершення яких спричинило б помилку, це було необхідно для перевірки коректної валідації даних. Результати тестування підтвердили, що архітектура смарт-контракту працює успішно та захищена від некоректних викликів зі сторони клієнта.

Тестування серверної частини здійснювалось відповідно до завершення окремих модулів. Тестування REST API проводилося у ручному режимі. Було перевірено коректність обробки клієнтських HTTP-запитів, валідацію вхідних даних та правильність формування JSON-відповідей. Важливим етапом тестування системи став саме процес тестування блокчейн-індексатора, який здійснювався шляхом маніпулювання його станом. Результати підтвердили, що механізм синхронізації працює коректно: індексатор успішно виявляв пропущені події та уникав дублювання транзакцій.

Фінальним етапом стало наскрізне функціональне тестування (End-to-End) клієнтського інтерфейсу з використанням тестової блокчейн-мережі Testnet.

3.4 Обмеження поточної реалізації та масштабування

Смарт-контракт був реалізований з урахуванням необхідної функціональності та складності виконання. Саме тому варто зазначити нереалізовані можливості, які в подальшому розвитку проєкту можуть бути допрацьовані.

1. *Децентралізований розподіл токенів.*

Реалізований механізм розподілення токенів найбільш оптимальний та безпечний варіант на даному етапі розробки застосунку MVP. Проте досвідчені та успішні DAO використовують інші підходи орієнтовані на мережу mainnet та залучення більшої кількості користувачів. Наприклад: продаж / купівля токенів на ланчпадах або маркетплейсах. Одна з найпоширеніших концепцій, за якою користувачі для того, щоб стати частиною спільноти DAO купують відповідні токени на доступних платформах. Такий підхід продажу токенів через пули ліквідності на даний момент обмежений у розробці, через потребу у взаємодії з іншими сторонніми сервісами блокчейну.

2. *Обмеження передачі активів у механізмі multisig.*

Механізм multisig на даному етапі підтримує передачу будь-якого токену стандарту Fungible Asset, наприклад унікальні токени організацій - governance token. Також є можливість працювати з CedraCoin, stablecoins (USDC, USDT). Проте не реалізована можливість передачі невзаємозамінних активів, як NFT або інші типи активів. Оскільки застосунок знаходиться на етапі MVP та розроблений для виконанні фінансових операцій і їх управлінні таке обмеження не впливає на функціональність та роботу DAO, проте може бути усуненим в подальшій розробці.

3. *Інтеграція системи винагород.*

Додатково в подальшому розвитку ще однією особливістю застосунку може стати нарахування бонусів за активність. Надання унікальних NFT чи додаткових токенів управління є позитивним досвідом для розвитку DAO, що збільшує активність користувачів спільноти.

4. *Розширення механізмів голосування (Delegation, Staking)*

Для підвищення залученості спільноти та захисту від фінансових маніпуляцій, у наступних ітераціях розробки передбачено впровадження механізмів делегування голосів та стейкінгу активів під час проведення голосувань.

Отже, описанні обмеження не є критичними для повноцінної роботи застосунку. Рішення щодо їхньої імплементації полягає у обмеженні взаємодії з іншими сервісами або важливістю для застосунку. Завдяки модульній архітектурі смарт-контракту розширення функціональності не буде проблемним на майбутніх етапах розвитку.

Висновки

У ході виконання кваліфікаційної роботи було визначено мету та актуальність розробки застосунку, а також сформовано основні завдання. Окрім того проведено дослідження принципів функціонування децентралізованих автономних організацій, виявлено ключові механізми управління активами та розподіленого контролю активами. Було визначено оптимальні архітектурні патерни та технічні рішення для розробки власної системи, завдяки порівняльному аналізу провідних протоколів DAO.

Обґрунтовано вибір блокчейн-платформи Cedra та мови програмування смарт-контрактів Move. Аналіз особливостей платформи довів доцільність розробки на даній платформі, завдяки використанню ресурсо-орієнтованої парадигми MVM для гарантій безпеки активів на рівні компіляції, а також виконання транзакцій через Block-STM для високої пропускної здатності та наявність модульною топологія для ізоляції організацій.

Результатом кваліфікаційної роботи став розроблений Web3 застосунок з гібридним підходом до зберігання даних. Платформа працює децентралізовано та підтримує фабричний підхід для створення DAO та має інтуїтивно зрозумілим інтерфейс, інтегрованим з криптогаманцем. Завдяки розробці в поєднанні з технологією блокчейн вдалось досягти незмінності критичних операцій, а розроблена серверна частина забезпечила швидкий та надійний доступ до даних.

Практична цінність роботи полягає у створенні повнофункціональної платформи, що може використовуватися для управління DeFi протоколами, колективного прийняття інвестиційних рішень, розподілу грантів та координації децентралізованих команд розробників.

Наукова новизна роботи полягає у комплексній адаптації механізмів децентралізованого управління для блокчейн-платформи Cedra, що на момент

виконання дослідження не мала власних DAO-рішень. По-перше, розроблено механізм подвійного кворуму для token-weighted voting. На відміну від класичних моделей голосування, де достатньо лише досягнення порогу токенів, запропонований механізм знижує ризик концентрації влади великими власниками токенів при збереженні принципу пропорційного впливу. По-друге, обґрунтовано та реалізовано гібридну архітектуру з blockchain індексатором для оптимізації взаємодії з Move Virtual Machine. По-третє, реалізовано повнофункціональну DAO-платформу на блокчейні Cedra з урахуванням специфіки MVM. Адаптовано кращі практики Ethereum-based DAO протоколів до архітектурних обмежень та можливостей Cedra.

У висновку, реалізований програмний продукт має високу практичну цінність та становить собою готовий MVP для створення і функціонування децентралізованих організацій в екосистемі Cedra. Завдяки модульній архітектурі платформа має значний потенціал до подальшого масштабування, зокрема шляхом майбутньої інтеграції механізмів стейкінгу, делегування голосів та розширених систем репутаційних винагород.

Список використаних джерел

1. A complete guide to different kinds of DAOs / Dr. Ravi Chamria, 2023. URL: https://www.zeeve.io/blog/a-complete-guide-to-different-kinds-of-daos/
2. Block-STM: Scaling Blockchain Execution by Turning Ordering Curse to a Performance Blessing / [Rati Gelashvili, Alexander Spiegelman, Zhuolun Xiang, George Danezis, Zekun Li, Dahlia Malkhi, Yu Xia, Runtian Zhou], 2022
3. Cedra Documentation. URL: https://docs.cedra.network/intro
4. Challenges of Effective Decision Making in Decentralized Autonomous Organizations (DAOs) / Rubhesh Jha, 2023. URL: https://www.researchgate.net/publication/373045869_Challenges_of_Effective_Decision_Making_in_Decentralized_Autonomous_Organizations_DAOs
5. Comparative Analysis of Major DeFi Protocols (Uniswap, Aave, MakerDAO, etc.) / Iyanuoluwa Blessing, Mary Blessing, Johnson FedrickDa, 2023. URL: https://www.researchgate.net/publication/391698881_Comparative_Analysis_of_Major_DeFi_Protocols_Uniswap_Aave_MakerDAO_etc
6. DAO(Decentralized Autonomous Organization) in Blockchain, 2025. URL: https://www.geeksforgeeks.org/computer-networks/daodecentralized-autonomous-organization-in-blockchain/
7. DAO Examples: Goals, Governance, and Soulbound Tokens, 2023. URL: https://supra.com/academy/dao-examples-goals-governance-and-soulbound-tokens/#Aave-DAO
8. Decentralized Autonomous Organizations As Emerging Economic Entities in Accounting and Governance Frameworks [Rajendra Vasantrao Patil, Dr. Vishakha Abhay Gaidhani, Dr. Pratibha Vivekanand Kashid, Dr. Indani Hazarika, Dr. Ramchandra Vasant Mahadik, Govind Mohanlal Pddoar, Shravani Rajendra Patil], 2025. URL: https://www.researchgate.net/publication/394304707_Decentralized_Autonomous_Organizations_as_Emerging_Economic_Entities_in_Accounting_and_Governance_Frameworks
9. Delegated voting in decentralized autonomous organizations: a scoping review / [Lukas Weidener, Fabio Laredo, Kishore Kumar, Karlin Compton], 2025

10. Evaluating DAO Sustainability and Longevity Through On-Chain Governance Metrics / [Silvio Meneguzzo,Claudio Schifanella, Valentina Gatteschi, Giuseppe Destefanis], 2025.
11. Event-Driven Development: Unlocking Optimized Dapps and Subgraphs / Denver Baumgartner, 2023. URL: https://thegraph.com/blog/event-driven-development-unlocking-optimized-dapps-and-subgraphs/
12. Exploring Decentralized Autonomous Organization (DAO) Governance: An integrative literature review / Carlos Santana, Patrick Mikalef, 2024. URL: https://www.researchgate.net/publication/385694204
13. Fortifying Decentralized Governance: Introducing Decentralized Autonomous Verification (DAVe) for Decentralized Autonomous Organization (DAOs) Security / Haya Altaleb, Beatrix Fregan, Zoltán Rajnai.
14. Governance for regenerative coordination: the evolution from DAO to DAO 3.0 / Kate Bennett, 2025
15. How to Protect Your Smart Contracts from State Bloating and Gas Griefing Attacks, Part 2, 2025. URL: https://medium.com/@ankitacode11/part-2-how-to-protect-your-smart-contracts-from-state-bloating-and-gas-griefing-attacks-2a0be91e249e
16. How to Use Multisig: A Guide for Individuals. URL: https://squads.xyz/blog/multisig-guide-for-individuals
17. Hybrid-DAOs: Enhancing Governance, Scalability, and Compliance in Decentralized Systems / Neil Shah, 2024. URL: https://www.researchgate.net/publication/385353426_Hybrid-DAOs_Enhancing_Governance_Scalability_and_Compliance_in_Decentralized_Systems
18. MakerDAO Technical Docs. URL: https://docs.makerdao.com/
19. Not just code: a framework for community governance and management in Decentralized Autonomous Organizations / Thomaz Henrique Viaro Bridi, Berislav Andrlić, Rodrigo Franco Gonçalves, 2025.
20. Top DAO Legal Wrappers & Jurisdictions – Global Guide, 2025. URL: https://daobox.io/blog/top-dao-legal-wrappers-jurisdictions-global-guide
21. Top DAO Platforms: Comparing Features and Benefits / Jesse Anglen. URL: https://www.rapidinnovation.io/post/top-dao-platforms-comparing-features-and-benefits#9-comparing-top-dao-platforms
22. Understanding decentralized autonomous organizations from the inside / Nils Augustin, Andreas Eckhardt, Alexander Willem de Jong, 2023.

23. Uniswap Documentation. URL: https://developers.uniswap.org/docs
24. Using The Graph for Indexing and Querying Blockchain Data / Lea Lobanov / 2023. URL: https://medium.com/@lea.lobanov/using-the-graph-for-indexing-and-querying-blockchain-data-2bd8d95b0ea2
25. Voting governance and value creation in decentralized autonomous organizations (DAOs) / Cristiano Bellavitis, Paul P. Momtaz, 2024.
26. Web3 in Ukraine: adoption that can teach the world / Diana King, 2025. URL: https://medium.com/cedra-network/web3-in-ukraine-adoption-that-can-teach-the-world-3a0553e49fce
27. What is a DAO & How Does it Work? / Sead Fadilpasic, 2022. URL: https://dappradar.com/blog/what-is-a-dao-how-does-it-work#What-do-DAO-members-do
28. What is a Signaling Proposal? URL: https://www.chainscorelabs.com/glossary/dao-governance-and-voting-systems/on-chain-vs-off-chain-governance/signaling-proposal
29. What is Docker? URL: https://docs.docker.com/get-started/docker-overview/#the-docker-platform
30. What is Git? URL: https://www.atlassian.com/git/tutorials/what-is-git
31. Що таке MakerDAO? (MKR) / Kraken Learn team, 2022. URL: https://www.kraken.com/uk/learn/what-is-maker-mkr#a88--makerdao