

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Інформаційних технологій

(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

на тему: «Анонімна соціальна мережа з використанням технології блокчейн.
Складання білого паперу та токекономіки»

Ткаченко Марина Олександрівна

(прізвище, ім'я та по батькові студента повністю)

Київ 2023 р.

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ**

Автоматизації і інформаційних технологій

(факультет)

Інформаційних технологій

(кафедра)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТ
д.т.н., професор Цюцюра С.В.

„___” _____ 2023 року

**ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»**

на тему: «Анонімна соціальна мережа з використанням технології блокчейн.
Складання білого паперу та токекономіки»

Виконала: студентка 4-го курсу, групи КН-42с

Спеціальності: 122 «Комп'ютерні науки»

Спеціалізація: «Інформаційні управляючі системи і технології»

(шифр і назва напряму підготовки, спеціальності)

_____ Ткаченко М.О. _____

(прізвище та ініціали)

Керівник

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Київ 2023 р

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій

Кафедра: інформаційних технологій

Освітній рівень: «бакалавр» за ОП

Спеціальність: 122 «Комп'ютерні науки»

Спеціалізація: Інформаційні управляючі системи і технології.

ЗАТВЕРДЖУЮ

Завідувач кафедри ІТ
д.т.н., професор Цюцюра С.В.

„10” лютого 2023 року

ЗАВДАННЯ

**ДО ВИКОНАННЯ АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»**

Ткаченко Марина Олександрівна

Тема роботи: Анонімна соціальна мережа з використанням технології блокчейн. Складання білого паперу та токекономіки

затверджена наказом ректора КНУБА № 1811/2 від «17» листопада 2022 р.

2. Керівник роботи:

3. Строк подання студентом роботи до захисту: 6 червень 2022 р.

4. Зміст пояснювальної записки за розділами:

Р.1. Аналіз та дослідження проблеми

Р.2. Проектування інформаційного забезпечення

Р.3. Практична реалізація

Р.4. Бізнес план

5. Інформаційні слайди:

C.1. Розробка підсистеми обліку студентів деканатом
C.2. Аналіз особливостей системи та дерево цілей
C.3. Аналіз існуючих рішень та дерево функцій
C.4. Визначення типу та вимог до підсистеми
C.5. Структурний та інформаційний аналіз
C.6. Мережа Петрі
C.7. Побудова моделей екранних форм та опис навігації
C.8. Архітектура та файлова структура системи
C.9. Проектування системи
C.10. Відображення програми

6. Календарний план виконання атестаційної випускної роботи

Види робіт та їх зміст	Дата виконання
P. 1. Аналіз та дослідження проблем	Лютий 2022 р.
P. 2. Проектування інформаційного забезпечення	Квітень 2022 р.
P. 3. Практична реалізація	Квітень 2022 р.
P. 4. Бізнес	Квітень 2022 р.
Остаточне оформлення роботи	Травень 2022 р.
Направлення роботи на рецензування	Червень 2022 р.
Попередній захист роботи на кафедрі	Червень 2022 р.

7. Консультанти розділів атестаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта, представника комісії	дата	підпис
Ергономіка інформаційних технологій	д.т.н. проф. Терентьев О.О.		
Прийом програмного продукту	к.т.н. доц., Єрукаєв А.В.		

8. Дата видачі завдання: 10 лютого 2022 р.

Керівник

(підпис)

Цюцюра С.В.

(прізвище та ініціали)

Бакалавр

(підпис)

Ткаченко М.О.

(прізвище та ініціали)

АНОТАЦІЯ

Ткаченко М.О. Анонімна соціальна мережа з використанням технології блокчейн. Створення білого паперу та токекономіки.

Дипломна бакалаврська робота за спеціальністю – «Комп’ютерні науки» – Київський національний університет будівництва та архітектури, Київ, 2023 рік.

Бакалаврська робота присвячена розробці анонімної соціальної мережі, що базується на технології блокчейн, з фокусом на збірці білого паперу та токекономіці. Метою проекту є створення платформи, яка забезпечить безпеку, приватність і винагороду користувачів за їхню активність і внесок у мережу.

У рамках дослідження буде проведено аналіз наявних анонімних соціальних мереж і технології блокчейн, з акцентом на їхні переваги та обмеження.

Ключовими словами є: "інформаційне забезпечення", "анонімна соціальна мережа", "блокчейн", "приватність", "функціональні можливості".

ABSTRACT

Tkachenko M.O. Anonymous social network using blockchain technology. Creating a white paper and token economy.

Bachelor's thesis in Computer Science – Kyiv National University of Construction and Architecture, Kyiv, 2023.

The bachelor's thesis is about developing an anonymous social network based on blockchain technology, with a focus on white paper collection and tokenization. The goal of the project is to create a platform that will provide security, privacy, and reward users for their activity and contribution to the network. *Key words are: "information support", "anonymous social network", "blockchain", "privacy", "functionality".*

ЗМІСТ

1	АНАЛІЗ ТА ДОСЛІДЖЕННЯ ПРОБЛЕМ.....	11
1.1	Загальні та теоретичні відомості, концепції та проблематика.....	11
1.2	Постановка та аналіз проблеми.....	12
1.3	Дерево основних цілей.....	13
1.4	Постановка задачі.....	15
2.	ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ....	19
2.1.	Технології блокчейн та їх застосування в соціальних мережах.....	19
2.2.	Аналіз наявних проєктів і досліджень у сфері блокчейн-соціальних мереж.	22
2.3.	Проблеми безпеки та приватності в існуючих соціальних мережах.	25
2.4.	Методи забезпечення анонімності та приватності в анонімних соціальних мережах.....	27
2.5.	Вибір інтерфейсу користувача.....	30
2.5.1.	Вимоги до інтерфейсу.....	30
2.5.2	Загальні можливості структури інтерфейсу.....	31
2.6	Створення діаграми випадків використання (UseCase).....	33
2.7	Створення діаграми класів (Class Diagram).....	35
2.8	Створення діаграми послідовності (Sequence Diagram).....	37
2.9	Створення діаграми станів (State Diagrams).....	40
2.10	Створення діаграми кооперацій (Collaboration Diagram).....	42
3.	ПРАКТИЧНА РЕАЛІЗАЦІЯ.....	44
4.	БІЗНЕС ПЛАН.....	69
4.1.	Опис проєкт.....	69
4.1.1.	Цілі і задачі.....	70
4.1.2.	Ключові переваги.....	71
4.2	Аналіз ринку соціальних мереж.....	72

4.2.1	Ідентифікація цільової аудиторії	72
4.2.2	Конкурентний аналіз	73
4.2.3	Позиціонування на ринку	74
4.2.4	Попередня оцінка реалізації ціни реалізації продукту.....	75
4.3	Опис функціональності	75
4.3.1	Анонімність та безпека	76
4.3.2	Модель монетизації.....	77
4.4	Команда проекту	78
4.5	Фінансовий план	79
4.6	Прогноз доходів.....	79
4.7	Аналіз ризиків	80
4.8	Висновок.....	81
	ВИСНОВОК	84
	СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	87

ВСТУП

Соціальні мережі стали невід'ємною частиною сучасного суспільства, надаючи людям унікальну можливість спілкування, обміну інформацією, створення контенту і знаходження однодумців. Однак, зі зростанням популярності соціальних мереж виникли серйозні проблеми, пов'язані з приватністю і безпекою користувачів. Часто особиста інформація користувачів стає об'єктом зловмисників і може бути використана в небажаних цілях, як-от крадіжка особистих даних, шахрайство або навіть шантаж.

У світлі цих проблем, технологія блокчейн набуває дедалі більшої актуальності як потужний інструмент для забезпечення безпеки та анонімності в онлайн-середовищі. Блокчейн, як децентралізована та неруйнівна система зберігання даних, дає змогу покращити приватність користувачів, гарантувати цілісність інформації та забезпечити прозорість взаємодій у мережі.

Вибір теми "Анонімна соціальна мережа з використанням технологій блокчейн" має значну актуальність і наступні аспекти допоможуть більш детально розібратися в цій актуальності:

Приватність і безпека: Захист особистих даних і приватність в онлайн-середовищі стають дедалі важливішими питаннями. Багато користувачів соціальних мереж стикаються з проблемою витоку і зловживаннями своїми персональними даними. Анонімні соціальні мережі, засновані на технології блокчейн, пропонують нові можливості для захисту і контролю над своїми даними. Завдяки децентралізації та шифруванню, блокчейн може забезпечити безпечне зберігання і передачу інформації, а також дозволити користувачам визначити, яку інформацію вони хочуть розкрити.

Децентралізація і прозорість: Технологія блокчейн відрізняється від централізованих систем, таких як традиційні соціальні мережі, де всі дані зберігаються на центральних серверах. Блокчейн пропонує децентралізовану модель зберігання даних, де інформація розподілена по

безлічі вузлів мережі. Це дає змогу підвищити прозорість і надійність, оскільки інформація може бути перевірена і підтверджена кількома учасниками мережі. Така модель також дає змогу користувачам мати більший контроль над своїми даними, виключаючи проблему централізованого контролю і зловживання з боку посередників.

Стійкість до цензури і цінність анонімності: Анонімні соціальні мережі на основі блокчейна мають потенціал бути стійкими до цензури і втручання з боку державних або комерційних організацій. Такі мережі можуть надавати користувачам можливість вільно висловлювати свої думки, спілкуватися і ділитися інформацією, мінімізуючи ризик переслідувань або репресій. Анонімність також дає змогу користувачам бути більш відвертими і почуватися більш захищеними в онлайн-середовищі.

Нові економічні моделі та стимулювання участі: Запровадження токеноміки та створення економічної системи на основі блокчейна може стимулювати активну участь користувачів в анонімних соціальних мережах. Токени можна використовувати як винагороду за внесок у мережу, створення і споживання контенту, участь у голосуваннях і ухваленні рішень. Це дає змогу створити стійку економічну модель, яка заохочує активність і взаємодію в мережі.

Інновації та розвиток: Тема анонімних соціальних мереж на базі блокчейна являє собою область активних досліджень і розробок. Провідні компанії та стартапи в усьому світі вже працюють над реалізацією таких мереж, досліджують нові підходи до безпеки та приватності, розробляють нові технологічні рішення та економічні моделі. Це створює можливості для інновацій, розвитку та комерційного успіху.

Таким чином, вибір теми "Анонімна соціальна мережа з використанням технологій блокчейн" є актуальним у контексті підвищеного інтересу до приватності та безпеки в онлайн-середовищі, прагнення до децентралізації та прозорості, а також появи нових економічних моделей і можливостей, які блокчейн може надати.

1 АНАЛІЗ ТА ДОСЛІДЖЕННЯ ПРОБЛЕМ

1.1 Загальні та теоретичні відомості, концепції та проблематика

Анонімна соціальна мережа є актуальною і захоплюючою темою в сучасному цифровому світі. В епоху загальної цифровізації, користувачі шукають нові способи взаємодії та спілкування, водночас зберігаючи свою анонімність і захищаючи свої особисті дані від витоків і зловживань. В останні роки технологія блокчейн стала особливо цікавою в контексті анонімних соціальних мереж, оскільки вона може забезпечити безпеку, приватність і прозорість даних користувачів.

Традиційні соціальні мережі, такі як Facebook, Instagram і Twitter, хоч і надають можливість спілкування та обміну інформацією, часто стикаються з проблемами, пов'язаними з конфіденційністю та безпекою. Багато користувачів мають побоювання щодо витоків особистої інформації, масового стеження і небажаного використання їхніх даних. У цьому контексті анонімні соціальні мережі на основі технології блокчейн можуть запропонувати революційне рішення.

Технологія блокчейн являє собою розподілену базу даних, де інформація зберігається у вигляді блоків, пов'язаних між собою ланцюжком. Кожен блок містить хеш попереднього блоку і дані, забезпечуючи цілісність і безпеку зберігання інформації. Блокчейн також працює в децентралізованому режимі, що означає відсутність центрального управління і контролю, що важливо для анонімних соціальних мереж.

У даній дипломній роботі ми розглянемо переваги та виклики використання технології блокчейн в анонімних соціальних мережах, а також їхній потенціал для створення нових форм взаємодії та обміну інформацією. Ми також проаналізуємо вплив цієї технології на безпеку,

анонімність, управління даними та приватність користувачів у контексті анонімних соціальних мереж.

1.2 Постановка та аналіз проблеми.

Під час формулювання проблем, пов'язаних із розробленням анонімної соціальної мережі з використанням технології блокчейн, важливо уточнити такі аспекти:

Анонімність: Однією з головних проблем при розробці анонімної соціальної мережі є забезпечення анонімності користувачів. Виникає питання про те, як гарантувати конфіденційність і захист персональних даних користувачів, водночас надаючи їм можливість спілкуватися і ділитися інформацією в мережі. Розробники повинні враховувати різні загрози безпеці, такі як можливість ідентифікації користувачів через аналіз даних або злом системи.

Масштабованість: Створення анонімної соціальної мережі, що використовує блокчейн, являє собою складне завдання в плані масштабованості. Технологія блокчейн має свої обмеження у швидкості обробки транзакцій і зберігання даних. У разі соціальної мережі, де велика кількість користувачів може виконувати безліч операцій одночасно, необхідно розробити ефективні механізми масштабування блокчейн-мережі, щоб забезпечити плавну роботу платформи.

Децентралізація та управління: Блокчейн-технологія будується на принципі децентралізації, що означає, що немає центрального керівного органу. Однак у соціальній мережі може бути необхідність в ухваленні рішень, модерації контенту або управлінні розвитком платформи. Виникає питання про те, як досягти балансу між децентралізацією і необхідністю ефективного управління, щоб створити безпечну і зручну соціальну мережу.

Користувацький досвід: Успіх будь-якої соціальної мережі значною мірою залежить від зручності використання і функціональності для користувачів. При розробці анонімної соціальної мережі з використанням

блокчейн необхідно забезпечити плавну навігацію, швидкий відгук системи, зручний інтерфейс і функції, які привернуть і утримають користувачів. Водночас, необхідно балансувати користувацький досвід із безпекою та анонімністю.

Соціальний вплив: Соціальні мережі мають значний вплив на поведінку та менталітет користувачів. Розробляючи анонімну соціальну мережу з використанням блокчейн, важливо враховувати потенційні негативні наслідки та забезпечувати заходи безпеки, щоб запобігти поширенню незаконного або шкідливого контенту. Необхідно створити систему моніторингу та модерації, яка буде ефективно боротися з негативним впливом і забезпечувати безпечне оточення для користувачів.

Загалом розробка анонімної соціальної мережі з використанням технології блокчейн є складним завданням, що вимагає уважного аналізу і вирішення безлічі проблем, пов'язаних з анонімністю, масштабованістю, управлінням і безпекою. Однак, правильна реалізація та врахування цих чинників може призвести до створення інноваційної та захищеної платформи для анонімного спілкування та обміну інформацією.

1.3 Дерево основних цілей

Метою досліджень в роботі є розробка інформаційного забезпечення системи та баз даних "розумного" дому.

Дерево цілей опису даної мети наведено на рисунку 1.1.

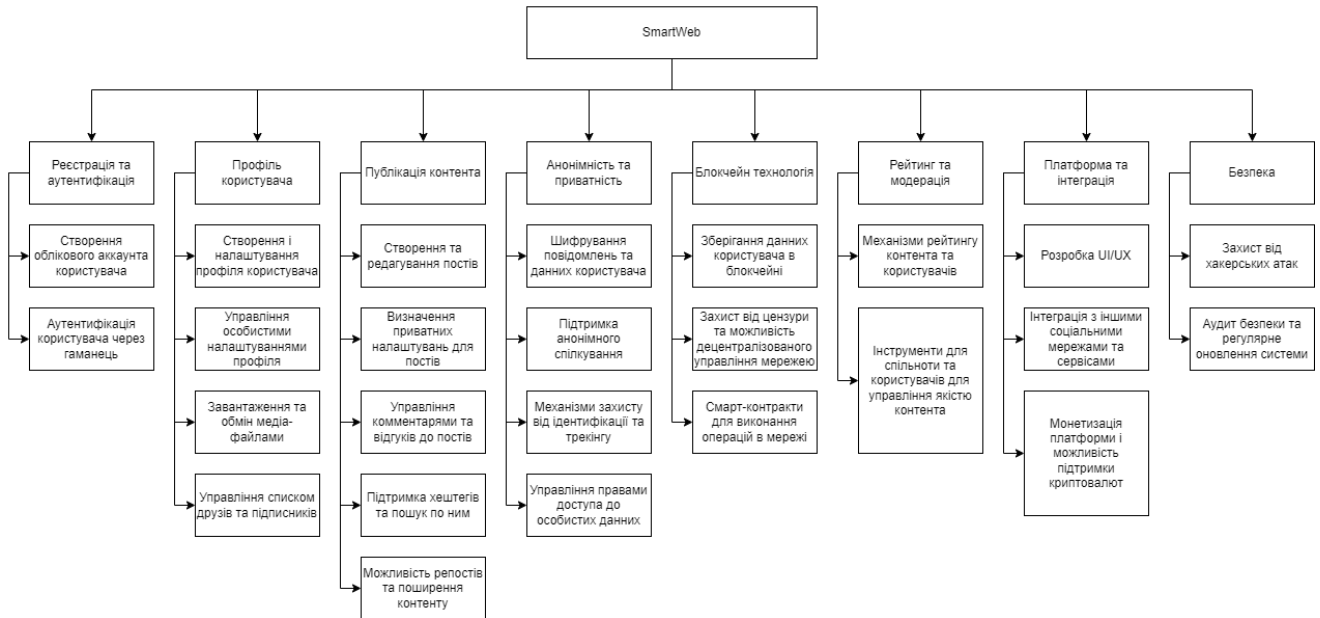


Рисунок 1.1 – Дерево цілей досліджень роботи.

Реєстрація та аутентифікація

- 1.1 Створення облікового запису користувача
- 1.2 Аутентифікація користувача
- 1.3 Керування особистими даними користувача

Профіль користувача

- 2.1 Створення та налаштування профілю користувача
- 2.2 Керування особистими налаштуваннями профілю
- 2.3 Завантаження та обмін медіа-файлами (фото, відео тощо)
- 2.4 Керування списком друзів і підписок

Публікація контенту

- 3.1 Створення та редагування постів
- 3.2 Визначення налаштувань приватності для постів
- 3.3 Управління коментарями та відгуками до постів
- 3.4 Підтримка хештегів і пошук за ними
- 3.5 Можливість репостів і поширення контенту

Анонімність і приватність

- 4.1 Шифрування повідомлень і даних користувачів

- 4.2 Підтримка анонімного спілкування
- 4.3 Механізми захисту від ідентифікації та трекінгу
- 4.4 Управління правами доступу до особистих даних

Блокчейн-технологія

- 5.1 Розробка власної блокчейн-мережі або використання наявної
- 5.2 Зберігання даних користувача в блокчейні
- 5.3 Захист від цензури та можливість децентралізованого управління мережею
- 5.4 Смарт-контракти для виконання специфічних операцій у мережі

Рейтинг і модерація

- 6.1 Механізми рейтингу контенту та користувачів
- 6.2 Модерація контенту та боротьба з небажаною поведінкою
- 6.3 Інструменти для спільноти та користувачів для управління якістю контенту

Платформа та інтеграції

- 7.1 Розробка користувацького інтерфейсу (UI) і користувацького досвіду (UX)
- 7.2 Інтеграція з іншими соціальними мережами та сервісами
- 7.3 Монетизація платформи та можливість підтримки криптовалюти

Безпека

- 8.1 Захист від хакерських атак і зломів
- 8.2 Аудит безпеки та регулярне оновлення системи
- 8.3 Опрацювання скарг на порушення безпеки та небажаний контент

1.4 Постановка задачі .

Метою цього дипломного проекту є створення анонімної соціальної мережі з використанням технології блокчейн. Головною метою цього

проєкту є надання користувачам безпечного та анонімного простору для спілкування та обміну інформацією.

Існуючі соціальні мережі зазвичай вимагають від користувачів надання особистої інформації, яка може бути використана третіми особами без їхньої згоди. Шляхом застосування технології блокчейн у рамках цього проєкту ми прагнемо розв'язати цю проблему, надаючи користувачам можливість спілкуватися і ділитися інформацією, не розкриваючи свою особистість

Переваги анонімної соціальної мережі на базі блокчейн включають:

Анонімність: Користувачі можуть створювати і використовувати облікові записи без розкриття своєї особистої інформації.

Безпека даних: Використання технології блокчейн дає змогу забезпечити захист даних і запобігання несанкціонованому доступу.

Децентралізація: Блокчейн-технологія дає змогу створювати децентралізовані соціальні мережі, які не залежать від централізованої керівної структури.

Прозорість: Усі операції в анонімній соціальній мережі, як-от пости, коментарі та голосування, записуються в блокчейн, що забезпечує прозорість і недвозначність.

Платформа має забезпечувати безпечне зберігання даних користувачів і підтримку транзакцій та смарт-контрактів. Це може бути реалізовано шляхом розроблення власного блокчейн-протоколу або використання наявних платформ, таких як Ethereum, EOS або Hyperledger. Блокчейн-платформа має бути децентралізованою, щоб учасники мережі могли взаємодіяти безпосередньо, минаючи централізовані сервери.

Аутентифікація та ідентифікація:

Для забезпечення анонімності та безпеки входу в соціальну мережу необхідні механізми аутентифікації та ідентифікації. Це може бути досягнуто з використанням криптографічних протоколів і алгоритмів. Наприклад, користувачі можуть створити облікові записи, засновані на криптографічних ключах, які слугуватимуть їхніми ідентифікаторами в

мережі. Під час входу в мережу вони можуть використовувати свої ключі для аутентифікації без розкриття своєї реальної особистості.

Анонімний обмін повідомленнями:

Механізм обміну повідомленнями має забезпечувати анонімність і конфіденційність. Повідомлення можуть бути зашифровані з використанням криптографічних алгоритмів, щоб запобігти можливості перехоплення або розкриття інформації третіми особами. Децентралізована мережа блокчейна дає змогу безпосередньо передавати повідомлення між користувачами, минаючи централізовані сервери.

Публікація контенту:

Користувачі повинні мати можливість завантажувати і обмінюватися контентом, таким як текст, зображення і відео, з іншими користувачами. Важливо забезпечити анонімність і безпеку публікації контенту. Контент може зберігатися в блокчейні або децентралізованій файлової системі, де кожен користувач має унікальний ідентифікатор і контроль над своїми даними. Завантажений контент також може бути зашифрований для забезпечення додаткової приватності.

Підтримка комунікації:

Соціальна мережа повинна надавати можливість комунікації між користувачами, включно з коментуванням, лайками та репостами. Усі комунікаційні дії мають бути анонімними та безпечними. Коментарі та зворотний зв'язок можуть бути збережені в блокчейні або децентралізованій базі даних для забезпечення прозорості та стійкості.

Монетизація та винагорода:

Для заохочення активності користувачів і створення якісного контенту можна використовувати механізм монетизації та винагороди. Це може бути реалізовано за допомогою токенів на блокчейні, які користувачі можуть отримувати за свої внески в мережу, як-от публікація цікавого контенту або участь у комунікації. Токени можуть бути використані для доступу до додаткових функцій або обмінювані на реальні активи.

Управління контентом і модерація:

Необхідно передбачити систему управління контентом і модерації, щоб запобігти публікації неприйнятної або незаконної контенту. Це може бути здійснено через децентралізований підхід до модерації, де учасники мережі можуть брати участь у процесі ухвалення рішень про контент. Смарт-контракти на блокчейні можуть використовуватися для автоматичної фільтрації або рейтингу контенту.

Мобільний додаток:

Розробка мобільного застосунку дасть змогу користувачам зручно отримувати доступ до анонімної соціальної мережі на своїх мобільних пристроях. Додаток має надавати зручний та інтуїтивно зрозумілий інтерфейс для обміну повідомленнями, публікації контенту та комунікації з іншими користувачами.

Тестування та оптимізація:

Після розробки анонімної соціальної мережі необхідно провести ретельне тестування, щоб виявити і виправити можливі вразливості або помилки. Також потрібна оптимізація системи для забезпечення високої продуктивності та масштабованості при збільшенні кількості користувачів і обсягу контенту.

Розвиток і підтримка:

Анонімна соціальна мережа має підтримуватися і розвиватися надалі. Необхідно впроваджувати нові функції та поліпшення, реагувати на відгуки користувачів, виправляти помилки й оновлювати безпеку системи. Регулярні оновлення та підтримка допоможуть зберегти актуальність і привабливість анонімної соціальної мережі.

2. ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

2.1. Технології блокчейн та їх застосування в соціальних мережах

Блокчейн (або ланцюжок блоків) - це розподілена база даних, яка зберігає інформацію у вигляді блоків даних, що безперервно розширюються, пов'язаних між собою за допомогою криптографічних хешів. Вона є основною технологією, що лежить в основі криптовалют, таких як Біткойн, але має і ширше застосування в різних галузях і сферах діяльності.

У блокчейн існує чотири основні типи децентралізованих або розподілених мереж:

Публічний блокчейн

Публічні блокчейни не потребують дозволів і дають змогу будь-кому, хто бажає, приєднатися до мережі. Усі учасники блокчейну мають рівні права на читання, редагування та перевірку інформації. Для обміну та майнінгу таких криптовалют, як Bitcoin, Ethereum і Litecoin, в основному використовують публічні блокчейни.

Приватний блокчейн

Приватні блокчейни, які також можна назвати керованими, контролюються однією організацією. Уповноважений орган визначає, хто може бути учасником і якими правами в мережі вони володіють. Приватні блокчейни децентралізовані лише частково, оскільки включають обмеження доступу. Прикладом приватного блокчейна є Ripple - платформа для обміну цифрової валюти.

Гібридний блокчейн

Гібридний блокчейн поєднує в собі функції як приватних, так і публічних мереж. Компанії можуть створювати як приватні, так і публічні системи дозволів. Таким чином, вони контролюють доступ до певних даних у блокчейні, але при цьому підтримують загальнодоступний доступ

до інших даних. Вони використовують смарт-контракти, що дають змогу публічним учасникам упевнитися в проведенні приватних транзакцій. Наприклад, гібридні блокчейни можуть надавати публічний доступ до цифрової валюти, зберігаючи приватний доступ до банківської валюти.

Блокчейн-консорціуми

Блокчейн-консорціумами управляє група організацій. Обрані заздалегідь організації розділяють відповідальність за функціонування блокчейна і визначення прав доступу до даних. Блокчейн-консорціумам часто віддають перевагу компанії-однорумці, які отримують вигоду від спільної відповідальності. Наприклад, Global Shipping Business Network - це некомерційний блокчейн-консорціум, що спеціалізується на цифровізації судноплавної галузі та розширенні співпраці між операторами морських перевезень.

Принцип роботи блокчейна заснований на децентралізації та консенсусі між учасниками мережі. У блокчейні кожен блок містить набір транзакцій або записів, а також хеш попереднього блоку. Це створює ланцюжок блоків, де кожен блок пов'язаний з попереднім і містить інформацію про всю історію транзакцій. Кожен блок також має унікальний ідентифікатор, званий хешем, який гарантує цілісність даних.

Одна з ключових переваг блокчейна - це його надійність і стійкість до злому. Оскільки блокчейн децентралізований і зберігається на безлічі комп'ютерів (вузлів), зміна одного блоку вимагає зміни всіх наступних блоків, що робить його дуже складним і витратним процесом. Це забезпечує захист від підробки даних і забезпечує довіру між учасниками мережі.

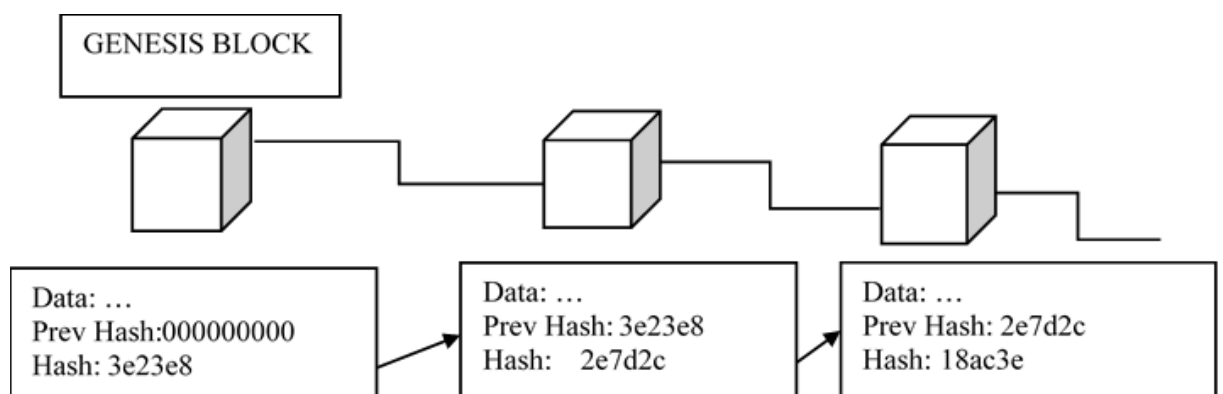


Рисунок 2.1 –Блокові посилання.

Останніми роками технологія блокчейн привернула велику увагу в різних сферах, починаючи від фінансів і закінчуючи логістикою. Однією з областей, де блокчейн може мати значний вплив, є соціальні мережі. У цій статті ми розглянемо, як технологія блокчейн може поліпшити безпеку, приватність і прозорість у соціальних мережах, а також переваги та виклики, пов'язані з її впровадженням.

Покращення безпеки даних:

Соціальні мережі сьогодні стали невід'ємною частиною нашого життя, і безліч користувачів ділиться особистою інформацією на платформах соціальних медіа. Однак, уразливість у централізованій системі управління даними може призвести до витоку персональної інформації. Блокчейн пропонує рішення цієї проблеми, забезпечуючи безпеку даних через децентралізацію і шифрування. Кожен користувач може контролювати свої дані і дозволяти доступ тільки обраним особам, виключаючи можливість несанкціонованого доступу і зміни інформації.

Зміцнення приватності:

Традиційні соціальні мережі можуть збирати величезну кількість персональних даних користувачів для цілей реклами та аналітики. Це викликає стурбованість з точки зору приватності. Блокчейн пропонує рішення, що дає змогу користувачам зберігати повний контроль над своїми даними і вирішувати, кому і яку інформацію вони хочуть надавати. Користувачі можуть обирати, яку інформацію ділитися з іншими учасниками мережі, анонімно або ідентифіковано.

Прозорість і боротьба з фейковими новинами:

У соціальних мережах часто виникають проблеми з фейковими новинами та недостовірною інформацією. Блокчейн може забезпечити прозорість і достовірність контенту, зберігаючи інформацію про кожну зміну і джерело. Користувачі зможуть перевіряти справжність публікацій і контенту, а також простежити всі зміни, зроблені в записі. Це може

допомогти боротися з поширенням дезінформації та підвищити довіру до інформації, що публікується в соціальних мережах.

Нагороди та монетизація контенту:

Блокчейн може змінити економічну модель соціальних мереж, даючи змогу користувачам отримувати винагороду за створення і поширення контенту. З використанням токенів або криптовалюти, користувачі можуть отримувати винагороду за свою активність і вплив, залучаючи більше підписників або отримуючи позитивні оцінки від інших учасників мережі. Це може стимулювати активну участь користувачів і сприяти створенню високоякісного та цікавого контенту.

2.2. Аналіз наявних проєктів і досліджень у сфері блокчейн-соціальних мереж.

У сучасному цифровому світі соціальні мережі відіграють важливу роль у нашому повсякденному житті. Вони надають можливість людям з усього світу обмінюватися інформацією, комунікувати і ділитися своїми ідеями і творчістю. Однак, зі зростанням стурбованості приватністю і безпекою даних, а також цензурою в соціальних медіа, багато користувачів шукають альтернативні платформи, які пропонують анонімність і захист.

У цьому аналізі розглянуто три популярні анонімні соціальні мережі, засновані на технології блокчейн: Steemit, Minds і Sola. Кожна з цих платформ надає унікальні можливості та функції, забезпечуючи анонімність користувачів, захист даних і можливість заробітку криптовалюти за активність на платформі.

Steemit була створена у 2016 році і є однією з найпопулярніших блокчейн-платформ соціальних медіа. Вона працює на блокчейні Steem, який був розроблений спеціально для цієї платформи. Steemit надає користувачам можливість створювати і ділитися контентом, включно зі статтями, блогами, фотографіями та відео. Однак, на відміну від традиційних соціальних мереж, користувачі можуть заробити винагороду в

криптовалюті Steem за свою активність, включно з отриманням голосів і коментарів від інших користувачів. Винагорода розподіляється на основі системи голосування, де вага голосу визначається кількістю Steem Power, якою володіє користувач. Це дає змогу користувачам заробляти гроші за свій контент і привертати більше уваги до своїх публікацій.

Steemit забезпечує анонімність користувачів, оскільки вони можуть реєструватися і взаємодіяти під псевдонімами. Блокчейн-технологія Steem забезпечує прозорість і безпеку даних, а також запобігає можливості цензури або зміни контенту після його публікації. Крім того, Steemit має вбудовану систему репутації, яка дає змогу оцінювати надійність і якість контенту користувачів.

Minds - це соціальна мережа, заснована на блокчейні Ethereum. Ця платформа ставить на перше місце приватність і безпеку користувачів, а також забезпечує анонімність під час реєстрації та взаємодії. Minds дає змогу користувачам ділитися контентом, включно з текстами, фотографіями і відео, і отримувати винагороду в криптовалюті, званій "токенами мізків" (Minds tokens), за свою активність і залучення нових користувачів на платформу. Ці токени можна використовувати для просування контенту і посилення видимості всередині платформи.

Одним із ключових аспектів Minds є надання повного контролю над даними користувача. Користувачі мають можливість зберігати свої дані локально або вибрати, щоб вони зберігалися на блокчейні Ethereum. Це надає користувачам більшу конфіденційність і захист від централізованого збору даних. Minds також використовує систему голосування на основі блокчейна, щоб запобігати цензурі та забезпечувати прозорість в алгоритмах відображення контенту.

Sola - це блокчейн-платформа соціальних медіа, яка прагне створити децентралізовану спільноту для обміну інформацією та ідеями. Платформа використовує алгоритми машинного навчання для персоналізації стрічки новин кожного користувача. Користувачі можуть ділитися контентом, таким як тексти, зображення та відео, і отримувати оцінку цього контенту

від інших користувачів, що впливає на його популярність і видимість у стрічці новин. Крім того, Sola використовує систему токенів для винагороди користувачів за активність і участь у платформі.

Voice - це анонімна соціальна мережа, створена на базі блокчейна EOS. Платформа прагне створити простір, де голос кожного користувача має рівну цінність, і запобігає можливості маніпуляції та цензури. Voice дає змогу користувачам створювати і ділитися контентом, і їхня активність нагороджується токенами, які можуть бути використані всередині платформи.

Aether - це анонімна соціальна мережа, яка прагне забезпечити безпеку і приватність користувачів. Платформа не вимагає реєстрації і не збирає особисті дані. Aether дає змогу користувачам створювати спільноти та спілкуватися з іншими користувачами через анонімні та зашифровані повідомлення. Такий підхід забезпечує високий ступінь конфіденційності та захисту особистої інформації.

Obsidian - це анонімна соціальна мережа, заснована на блокчейні Stratis. Платформа дає змогу користувачам створювати профілі, ділитися контентом і спілкуватися в зашифрованих чатах. Особливістю Obsidian є використання системи ідентифікації, що дозволяє користувачам підтверджувати свою анонімність, а також вбудована функція анонімного голосування.

Incognito - це анонімна соціальна мережа, яка надає користувачам можливість спілкуватися, ділитися контентом і залишатися анонімними. Платформа використовує протоколи шифрування і блокчейн-технологію для забезпечення безпеки даних і приватності користувачів. Incognito не вимагає обов'язкової ідентифікації та не зберігає особисту інформацію користувачів.

Ghost - це анонімна соціальна мережа, яка ставить акцент на приватності та анонімності користувачів. Платформа дає змогу користувачам створювати профілі та ділитися контентом, при цьому ідентифікація користувачів залишається анонімною. Ghost використовує

технологію блокчейн для забезпечення безпеки даних і запобігання цензурі.

Попри те, що всі ці платформи використовують технологію блокчейн і підтримують анонімність користувачів, кожна з них має свої особливості та функції. Під час вибору анонімної соціальної мережі важливо враховувати параметри, як-от популярність, безпека, зручність використання та спільнота користувачів, щоб обрати платформу, що найкраще відповідає вашим потребам та вподобанням.

2.3. Проблеми безпеки та приватності в існуючих соціальних мережах.

У наше сучасне інформаційне суспільство соціальні мережі міцно увійшли в повсякденне життя багатьох людей. Вони стали невід'ємною складовою нашої комунікації, обміну інформацією, пошуку нових знайомств і підтримки зв'язків з друзями, сім'єю та колегами. Однак, разом з усіма перевагами, які вони приносять, ми також стикаємося з серйозними проблемами безпеки та приватності, які не можна просто ігнорувати.

Проблеми безпеки та приватності в соціальних мережах мають значний вплив на саму сутність використання їх користувачем. Велика кількість персональної інформації, яку користувачі добровільно розміщують на своїх профілях, створює загрозу конфіденційності та безпеки даних. Особисті дані, такі як ім'я, фотографії, місце розташування, дата народження, інтереси та інші деталі життя користувача, стають доступними для різноманітних акторів, включно з самою соціальною мережею, рекламодавцями, а також зловмисниками, які мають недобрі наміри.

Однією з основних проблем є витік персональних даних. У зв'язку зі зростаючою кількістю інформації, яку збирають і зберігають соціальні мережі, виникає загроза безпеці цих даних. Витік персональних даних може статися через недостатній захист інформаційної інфраструктури

соціальних мереж або внаслідок злому акаунтів користувачів. У разі витоку даних, користувачі стають уразливими перед кіберзлочинцями та шахраями, які можуть використати отримані дані для вчинення злочинів, таких як ідентифікаційна крадіжка, фінансові шахрайства або навіть шантаж.

Недостатній захист особистих акаунтів також є серйозною проблемою. Зловмисники активно шукають способи злому акаунтів користувачів, щоб отримати доступ до їхньої персональної інформації та контролювати акаунт. Підбір паролів, фішингові атаки, використання слабких механізмів автентифікації - все це методи, які зловмисники можуть використовувати для злому акаунтів і нанесення шкоди користувачам. Коли акаунт зламується, зловмисники отримують можливість змінювати налаштування приватності, поширювати шкідливий контент або навіть видавати себе за користувача, що може призвести до негативних наслідків для репутації та особистої безпеки користувача.

Крім того, соціальні мережі стикаються з проблемою поширення негативного контенту, включно з кібербулінгом, онлайн-жорстокістю і неприйнятною поведінкою. Анонімність і віддаленість, які надають соціальні мережі, створюють сприятливе середовище для такої поведінки. Користувачі можуть стати жертвами образ, погроз, дискримінації та інших форм цифрового насильства, що негативно позначається на їхньому психологічному стані та благополуччі. Це особливо актуально для підлітків і молодих людей, які є однією з найбільш уразливих груп в онлайн-просторі.

Ще однією серйозною проблемою є поширення неправдивої інформації та фейкових новин у соціальних мережах. Завдяки свободі публікації контенту, яку надають соціальні мережі, неправдива інформація може швидко поширюватися і впливати на громадську думку. Фейкові новини можуть бути використані для маніпуляції масами, спотворення фактів, створення конфліктів і дезінформації. Це загрожує довірі до інформаційних джерел і демократичним принципам суспільства.

У світлі цих проблем стає очевидною необхідність вжиття заходів щодо забезпечення безпеки та приватності користувачів у соціальних мережах. Компанії-розробники соціальних мереж повинні активно працювати над удосконаленням систем безпеки, захисту даних і забезпечення конфіденційності користувачів. Для вирішення цих проблем необхідно вживати заходів, таких як поліпшення політик безпеки та приватності, забезпечення надійної автентифікації користувачів, розроблення ефективних інструментів для боротьби з кібербулінгом, унеможливлення фейкових акаунтів і забезпечення прозорості у збиранні та використанні даних користувачів. Також важливо освічувати користувачів щодо можливих загроз і проблем, пов'язаних із використанням соціальних мереж.

2.4. Методи забезпечення анонімності та приватності в анонімних соціальних мережах

Для забезпечення приватності в анонімних соціальних мережах використовують такі методи:

Розподілене зберігання даних у блокчейні означає, що інформація не зберігається на одному центральному сервері, а копії даних зберігаються на безлічі вузлів, які є частиною мережі. Кожен вузол містить повну копію блокчейна і перевіряє правильність даних. Це робить блокчейн більш стійким до атак і витоків інформації, оскільки для зміни або підробки даних необхідно отримати контроль над більшістю вузлів у мережі.

Алгоритми шифрування:

Блокчейн використовує різні алгоритми шифрування для забезпечення безпеки даних. Ці алгоритми перетворюють інформацію в зашифрований вигляд, який не може бути прочитаний без відповідних ключів. Шифрування даних у блокчейні допомагає захистити інформацію від несанкціонованого доступу та підробки. Хеш-функції

використовуються для зв'язку блоків даних, забезпечуючи цілісність блокчейна.

Псевдоніми та анонімні ідентифікатори:

В анонімних соціальних мережах, заснованих на блокчейні, користувачі можуть використовувати псевдоніми або анонімні ідентифікатори замість реальних імен. Це дає їм змогу залишатися анонімними і зберігати свою приватність. Завдяки технології блокчейн, можна упевнитися в унікальності ідентифікатора без розкриття особистої інформації. Наприклад, у блокчейні Ethereum існують контракти реєстрації імені, які дають змогу користувачам зареєструвати унікальне псевдоіменне ім'я.

Смарт-контракти:

Смарт-контракти - це програми, записані в блокчейн, які автоматично виконуються при виконанні певних умов. В анонімних соціальних мережах на базі блокчейна, смарт-контракти можуть використовуватися для визначення та управління правами доступу до інформації. Наприклад, можна створити смарт-контракт, який дозволяє доступ до певної інформації тільки для конкретних користувачів або груп користувачів. Це допомагає контролювати розкриття інформації та забезпечує приватність користувачів.

Транзакційна приватність:

Технологія блокчейн надає можливість забезпечити приватність транзакцій в анонімних соціальних мережах. У разі використання криптовалюти або токенів на базі блокчейна, інформація про транзакції може бути захищена за допомогою криптографічних протоколів. Кільцеві підписи та нульові докази знання (Zero-Knowledge Proofs) - це деякі з протоколів, які забезпечують анонімність і приватність у блокчейн-мережах. Ці протоколи дають змогу довести виконання умов транзакції без розкриття деталей самої транзакції.

Міксери та протоколи анонімності:

Міксери (mixers) і протоколи анонімності є додатковими інструментами для забезпечення анонімності в анонімних соціальних мережах на базі блокчейна. Міксери приймають токени від різних користувачів і перемішують їх перед відправленням на кінцеву адресу, що ускладнює відстеження та ідентифікацію відправника й одержувача транзакції. Протоколи анонімності, такі як ZeroLink і CoinJoin, пропонують різні методи комбінування транзакцій і змішування коштів для забезпечення анонімності.

Розподілені та анонімні мережі:

Анонімні соціальні мережі на базі блокчейна можуть використовувати розподілені й анонімні мережі, такі як Tor (The Onion Router) або I2P (Invisible Internet Project), для обміну інформацією між користувачами. Ці мережі маршрутизують мережевий трафік через кілька вузлів, що робить його складним для відстеження та ідентифікації. Користувачі можуть спілкуватися в таких мережах, зберігаючи свою анонімність і приватність.

Децентралізовані та самокеровані системи:

Технологія блокчейн дає змогу створювати децентралізовані та самокеровані системи, де рішення та ухвалення рішень здійснюються колективно учасниками мережі. Це включає голосування за правила використання даних, контроль за доступом до інформації та ухвалення рішень про протоколи анонімності. Такі системи забезпечують більшу прозорість і довіру, виключаючи можливість зловживання і цензури.

Децентралізовані та незалежні ідентифікаційні системи:

Для забезпечення анонімності та приватності в анонімних соціальних мережах на базі блокчейна можуть використовуватися децентралізовані та незалежні ідентифікаційні системи. Ці системи дозволяють користувачам мати унікальні ідентифікатори, які можуть бути підтверджені іншими учасниками мережі без розкриття особистої інформації. Прикладом такої системи є децентралізований ідентифікаційний протокол Sovrin.

Конфіденційні смарт-контракти:

Конфіденційні смарт-контракти - це різновид смарт-контрактів, які забезпечують конфіденційність даних, пов'язаних із виконанням контракту. Вони використовують різні методи шифрування і протоколи, такі як Zero-Knowledge Proof (ZKP), для забезпечення конфіденційності інформації, пов'язаної з виконанням контракту. Це дає змогу користувачам виконувати складні операції в анонімних соціальних мережах, не розкриваючи деталі своїх дій.

2.5. Вибір інтерфейсу користувача

2.5.1. Вимоги до інтерфейсу

Вимоги інформаційного забезпечення для анонімної соціальної мережі з використанням технології блокчейн включають такі аспекти:

1. Зберігання даних: Розподілене зберігання даних з використанням технології блокчейн, щоб забезпечити децентралізацію і стійкість до відмов. Безпечне і шифроване зберігання користувацької інформації, щоб запобігти несанкціонованому доступу до даних.
2. Анонімність: Розробка механізмів для забезпечення анонімності користувачів, щоб запобігти ідентифікації особистості через дані в блокчейні.
3. Безпека: Використання криптографічних методів для забезпечення безпеки даних і транзакцій у блокчейні. Механізми виявлення і запобігання атак, таких як шкідливі програми, фішинг і DDoS-атаки. Резервне копіювання даних і механізми відновлення системи для забезпечення безперервності роботи.
4. Масштабованість: Розробка блокчейн-системи, здатної обробляти велику кількість транзакцій і зберігати зростаючий обсяг даних. Використання механізмів масштабування, таких як шардинг, побічні ланцюжки або смарт-контракти, щоб забезпечити високу продуктивність і ефективність роботи системи.

5. Інтеграція з іншими системами: Взаємодія з іншими блокчейн-платформами або сервісами для розширення функціональності та можливостей соціальної мережі. Інтеграція із зовнішніми сервісами та АРІ для забезпечення сумісності та взаємодії зі сторонніми додатками і платформами.
6. Швидкість і продуктивність: Оптимізація алгоритмів та архітектури блокчейна для забезпечення високої швидкості обробки транзакцій та операцій. Поліпшення продуктивності мережі та зменшення часу підтвердження транзакцій, щоб забезпечити плавний і чуйний користувацький досвід.

2.5.2 Загальні можливості структури інтерфейсу

Структура інтерфейсу для анонімної соціальної мережі з використанням технології блокчейн:

1. Реєстрація та вхід у систему: Користувачі повинні мати можливість зареєструватися та увійти в систему. При анонімній соціальній мережі ви можете розробити механізм реєстрації, який не вимагає від користувачів надання особистих даних, але може знадобитися створення облікових записів для аутентифікації.
2. Профіль користувача: Кожен користувач повинен мати свій профіль, де вони можуть додавати інформацію про себе, таку як нікнейм, фотографію і коротку біографію. Важливо зберігати анонімність користувачів, тому краще уникати вимоги надання особистих даних.
3. Стрічка новин: Головна сторінка або стрічка новин має відображати актуальні пости або повідомлення від користувачів. Користувачі можуть бачити повідомлення від тих, на кого вони підписалися, або популярні повідомлення в загальній стрічці. Крім текстових повідомлень, можна передбачити можливість публікації зображень, відео або інших медіафайлів.

4. Пошук користувачів і контенту: Користувачі повинні мати можливість шукати інших користувачів або контент, використовуючи пошукову функцію. Це може включати пошук за ключовими словами, хештегами або іншими критеріями.
5. Взаємодія з контентом: Користувачі можуть коментувати, оцінювати (лайкати) або ділитися контентом інших користувачів. Також можна передбачити можливість збереження контенту для перегляду пізніше.
6. Приватні повідомлення: Користувачі повинні мати можливість надсилати приватні повідомлення іншим користувачам. Важливо забезпечити безпеку та конфіденційність цих повідомлень.
7. Налаштування та безпека: Розділ налаштувань має давати змогу користувачам керувати своїми налаштуваннями конфіденційності, безпекою облікового запису та уподобаннями відображення контенту.
8. Управління підписками: Користувачі можуть підписуватися на інших користувачів, щоб отримувати оновлення про їхню активність. Інтерфейс має надавати можливість управління підписками та відписки.
9. Управління блокуваннями: Користувачі повинні мати можливість блокувати інших користувачів, якщо вони не хочуть бачити їхній контент або отримувати від них повідомлення.
10. Управління гаманцем і транзакціями: Якщо ваша соціальна мережа використовує технологію блокчейн, користувачі можуть мати цифровий гаманець, пов'язаний з обліковим записом, і можливість виконувати транзакції всередині мережі (наприклад, для передплати платних контентних матеріалів).

Графічне представлення вимог зображено на рисунку 2.5.2

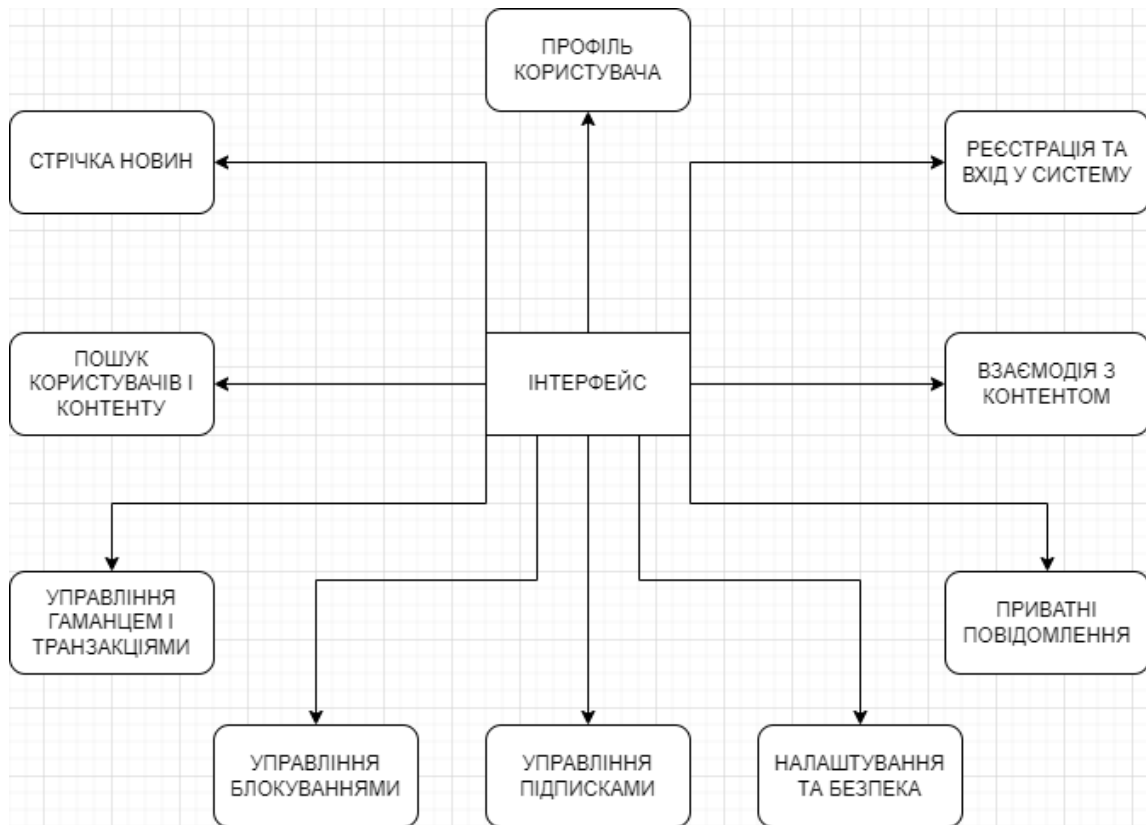


Рисунок 2.5.2 – графічне представлення загальних можливостей структури інтерфейсу

2.6 Створення діаграми випадків використання (UseCase)

Під час проєктування інформаційних систем (ІС) із застосуванням UML (Unified Modeling Language) для анонімної соціальної мережі з використанням технології блокчейн і токеноміки можна виокремити кілька типів діаграм, які можуть бути корисними. Нижче представлено деякі з них:

Діаграма випадків використання (Use Case Diagram): Ця діаграма допомагає ідентифікувати акторів (користувачів) системи та функціональні вимоги, які вони мають виконувати. Наприклад, в анонімній соціальній мережі акторами можуть бути користувачі, а функціональні вимоги можуть включати створення профілю, публікацію повідомлень, перегляд стрічки новин та інші функції. Ця діаграма представляє основні варіанти

використання, пов'язані з акторами (користувач, адміністратор) і блокчейном в анонімній соціальній мережі.

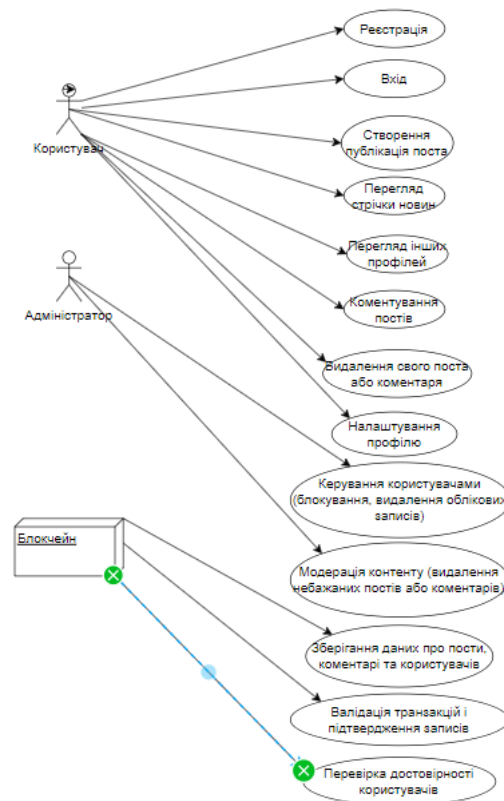


Рисунок 2.2 – Графічне зображення діаграми використання(UseCase)

На діаграмі представлено:

Користувач виходить з анонімної соціальної мережі та має доступ до таких варіантів використання: реєстрація, вхід до системи, створення та публікація посту, перегляд стрічки з постами, перегляд профілів інших користувачів, коментування постів, видалення посту або коментаря, зміна налаштувань профілю.

Адміністратор виходить з анонімної соціальної мережі та має доступ до управління користувачами (блокування, видалення облікових записів) і модерації контенту (видалення небажаних постів або коментарів).

Блокчейн виходить з анонімної соціальної мережі і виконує функції зберігання даних про пости, коментарі та користувачів, валідації транзакцій і підтвердження записів.

2.7 Створення діаграми класів (Class Diagram)

Діаграма класів (Class Diagram): Ця діаграма представляє структуру системи, визначаючи класи об'єктів, їхні атрибути та методи. У разі анонімної соціальної мережі вона може включати класи, такі як "Користувач", "Пост", "Токен" тощо.

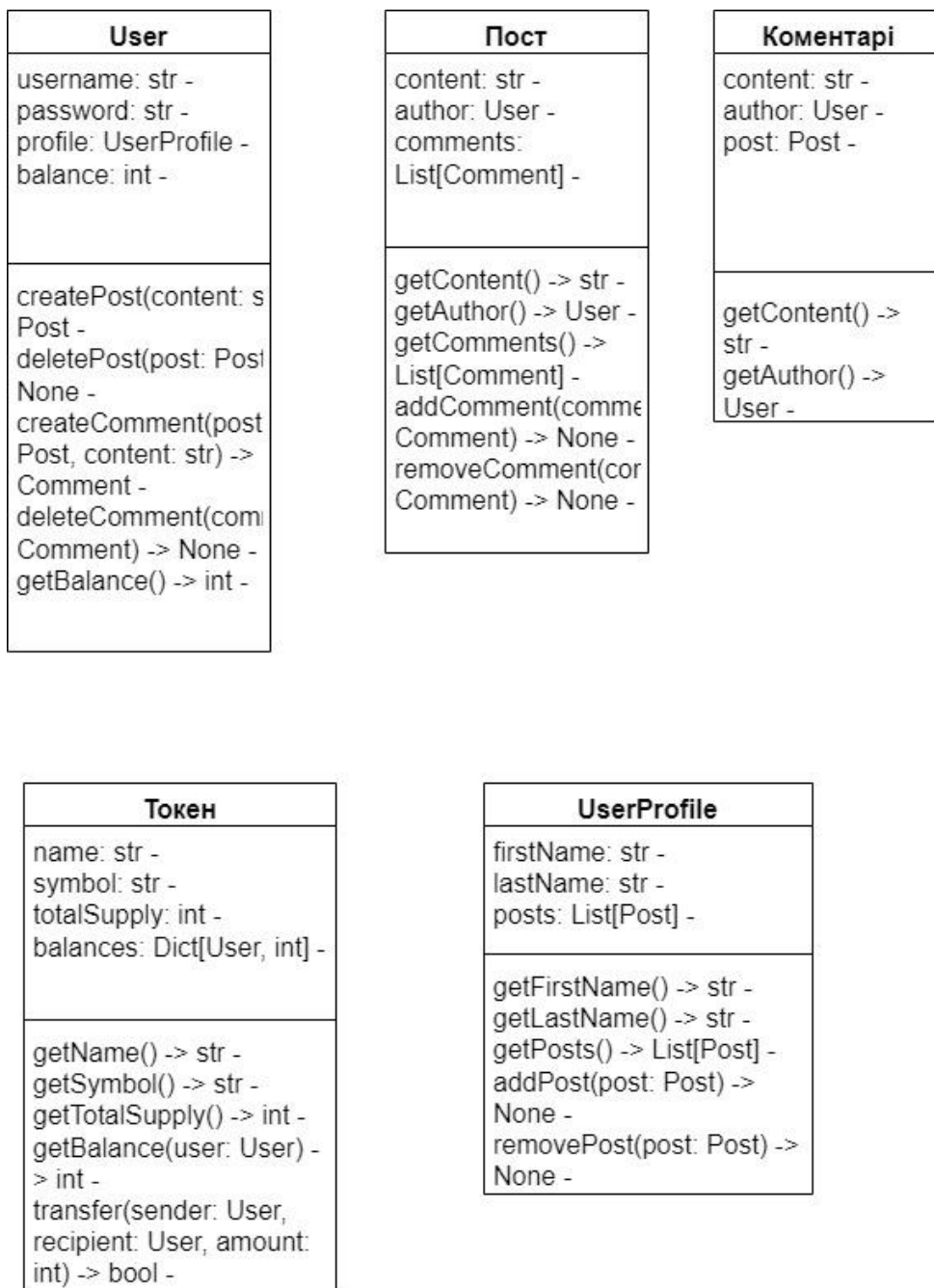


Рисунок 2.2 – Графічне зображення діаграми класів (Class Diagram)

У класі "Анонімна соціальна мережа" (AnonymousSocialNetwork):

Атрибути, пов'язані зі станом мережі, такі як користувачі (users), пости (posts), коментарі (comments), токени (tokens) тощо.

У класі "Користувач" (User):

Атрибути, пов'язані з даними користувача, такі як ім'я користувача (username) і пароль (password).

Методи, пов'язані з управлінням профілем користувача, як-от отримання імені користувача (getUsername()), зміна імені користувача (setUsername(username)), зміна пароля (setPassword(password)) тощо.

Методи, пов'язані з діями користувача, такі як створення постів (createPost(user, content)), створення коментарів (createComment(user, post, content)), видалення постів (deletePost(user, post)), видалення коментарів (deleteComment(user, comment)) тощо.

У класі "Пост" (Post):

Атрибути, пов'язані з даними поста, такі як вміст (content) і автор (user).

Методи, пов'язані з отриманням і встановленням даних поста, такі як отримання вмісту (getContent()), зміна вмісту (setContent(content)), отримання автора (getUser()), встановлення автора (setUser(user)) тощо.

Методи, пов'язані з коментарями до посту, як-от отримання коментарів (getComments()), додавання коментаря (addComment(comment)) і видалення коментаря (deleteComment(comment)).

У класі "Коментар" (Comment):

Атрибути, пов'язані з даними коментаря, такі як вміст (content), автор (user) і пов'язаний пост (post).

Методи, пов'язані з отриманням і встановленням даних коментаря, як-от отримання вмісту (getContent()), зміна вмісту (setContent(content)), отримання автора (getUser()), встановлення автора (setUser(user)),

отримання пов'язаного поста (`getPost()`), установлення пов'язаного поста (`setPost(post)`) і т.д.

У класі "Токен" (Token):

Атрибути, пов'язані з даними токена, такі як ім'я (`name`), символ (`symbol`), загальна кількість (`totalSupply`) і баланси користувачів (`balances`).

Методи, пов'язані з отриманням і встановленням даних токена, такі як отримання імені (`getName()`), зміна імені (`setName(name)`), отримання символу (`getSymbol()`), зміна символу (`setSymbol(symbol)`), отримання загальної кількості (`getTotalSupply()`), зміна загальної кількості (`setTotalSupply(totalSupply)`) тощо.

Методи, пов'язані з управлінням балансами користувачів і передачею токенів, як-от отримання балансів (`getBalances()`), зміна балансу користувача (`setBalance(user, amount)`), отримання балансу користувача (`getBalance(user)`), передача токенів (`transfer(sender, recipient, amount)`) тощо.

У класі "UserProfile" (UserProfile):

Атрибути, пов'язані з даними профілю користувача, такі як ім'я (`firstName`), прізвище (`lastName`) і список постів (`posts`).

Методи, пов'язані з отриманням і встановленням даних профілю, як-от отримання імені (`getFirstName()`), зміна імені (`setFirstName(firstName)`), отримання прізвища (`getLastName()`), зміна прізвища (`setLastName(lastName)`), отримання списку постів (`getPosts()`), додавання посту (`addPost(post)`) та видалення посту (`removePost(post)`).

2.8 Створення діаграми послідовності (Sequence Diagram)

Діаграма послідовності (Sequence Diagram): Ця діаграма моделює взаємодію між об'єктами в певній послідовності. Вона може допомогти візуалізувати, як користувачі взаємодіють із системою і як повідомлення та транзакції передаються між ними в анонімній соціальній мережі.

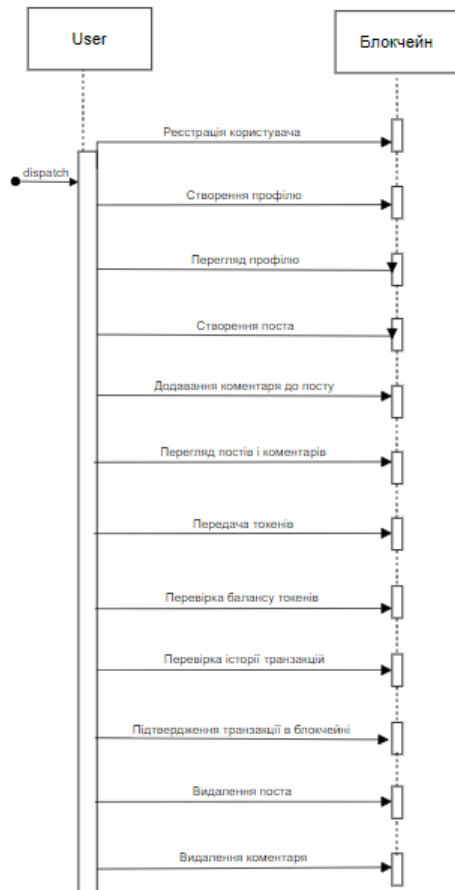


Рисунок 2.2 – Графічне зображення діаграми послідовності

Реєстрація користувача:

Користувач запитує реєстрацію в анонімній соціальній мережі. Мережа блокчейн створює обліковий запис користувача і присвоює унікальний ідентифікатор. Мережа блокчейн повертає ідентифікатор користувачеві.

Створення профілю:

Користувач створює профіль, вказуючи інформацію про себе, таку як ім'я, фотографія, опис та інші деталі. Користувач відправляє інформацію про профіль у мережу блокчейн для збереження. Мережа блокчейн зберігає інформацію про профіль користувача.

Перегляд профілю:

Користувач запитує перегляд профілю іншого користувача, вказуючи його ідентифікатор. Мережа блокчейн шукає інформацію про профіль користувача і повертає її користувачеві для перегляду.

Створення поста:

Користувач створює новий пост, вказуючи зміст, теги та інші деталі. Користувач відправляє інформацію про пост у мережу блокчейн для збереження. Мережа блокчейн зберігає інформацію про пост і присвоює йому унікальний ідентифікатор.

Додавання коментаря до посту:

Користувач обирає певний пост, до якого він хоче додати коментар. Користувач створює коментар і відправляє його в мережу блокчейн для збереження. Мережа блокчейн зберігає коментар і пов'язує його з відповідним постом.

Перегляд постів і коментарів:

Користувач запитує перегляд списку постів або вибирає конкретний пост. Мережа блокчейн повертає список постів або інформацію про обраний пост.

Користувач може переглянути зміст постів, коментарі та іншу пов'язану інформацію.

Передача токенів:

Користувач вибирає іншого користувача і вказує кількість токенів, які він хоче передати. Користувач надсилає запит на передачу токенів у мережу блокчейн. Мережа блокчейн перевіряє доступність токенів у відправника, виконує передачу і оновлює баланс токенів у відправника та одержувача.

Перевірка балансу токенів:

Користувач запитує свій поточний баланс токенів. Мережа блокчейн повертає інформацію про баланс токенів користувача.

Перевірка історії транзакцій:

Користувач запитує історію своїх транзакцій. Мережа блокчейн повертає список транзакцій, які були виконані користувачем, включаючи деталі кожної транзакції.

Підтвердження транзакції в блокчейні:

Після виконання транзакції, користувач може підтвердити її в мережі блокчейн. Мережа блокчейн обробляє підтвердження і включає транзакцію в блок, щоб вона стала незмінною частиною блокчейн.

Видалення поста:

Користувач вибирає пост, який він хоче видалити. Користувач відправляє запит на видалення поста в мережу блокчейн. Мережа блокчейн видаляє пост і всі пов'язані з ним коментарі з блокчейну.

Видалення коментаря:

Користувач вибирає коментар, який він хоче видалити. Користувач відправляє запит на видалення коментаря в мережу блокчейн. Мережа блокчейн видаляє коментар із блокчейну.

2.9 Створення діаграми станів (State Diagrams)

Діаграми станів (State Diagrams) є одним із типів діаграм UML, які можуть бути корисними під час проектування анонімною соціальною мережі з використанням технології блокчейн і токеноміки. Діаграма станів допомагає описати різні стани, переходи між ними та дії, які відбуваються в системі залежно від цих станів.

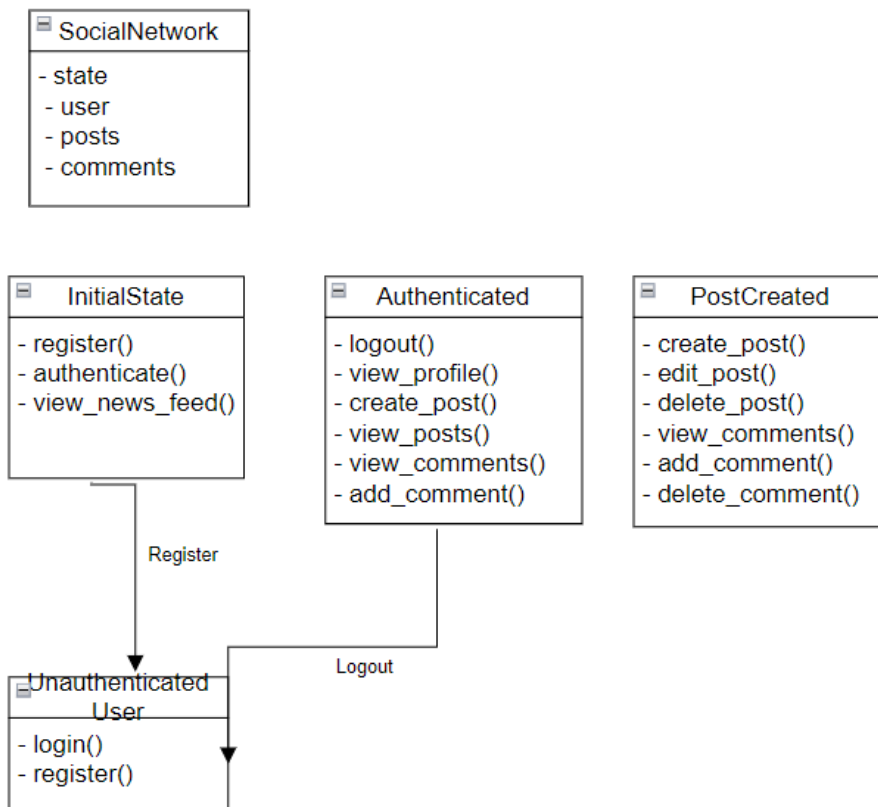


Рисунок 2.2 – Графічне зображення діаграми станів(State Diagrams)

InitialState (Початковий стан):

Це початковий стан під час запуску програми.

Реєстрація: користувач може зареєструватися в системі, вказавши ім'я користувача та пароль. Аутентифікація: користувач може увійти в систему, надавши свої облікові дані.

AuthenticationState (Стан аутентифікації):

Користувач успішно аутентифікований і має доступ до основних функцій соціальної мережі. Перегляд профілю: користувач може переглядати свій профіль, включно з інформацією про себе та своїми постами. Створення поста: користувач може створювати нові пости, додавати текст і медіа-матеріали. Перегляд новинної стрічки: користувач може переглядати пости інших користувачів, відсортовані за часом. Перегляд коментарів: користувач може переглядати коментарі до своїх постів і постів інших користувачів. Додавання коментаря: користувач може додавати коментарі

до постів. Лайки і репости: користувач може ставити лайки і робити репости на пости, що його цікавлять.

PostCreationState (Стан створення поста):

Користувач перебуває в стані створення нового поста. Введення вмісту поста: користувач може вводити текст і медіа-матеріали для нового поста. Додавання тегів: користувач може додати теги для пошуку і класифікації поста. Публікація поста: користувач може опублікувати створений пост і зробити його видимим для інших користувачів.

AnonymousState (Стан анонімності):

Користувач може вибрати режим анонімності, в якому його ідентичність прихована від інших користувачів. Перегляд профілів: користувач може переглядати профілі інших користувачів, але не може дізнатися їхні реальні імена. Перегляд постів: користувач може переглядати пости інших користувачів без можливості визначити, хто їх створив.

2.10 Створення діаграми кооперацій (Collaboration Diagram)

Діаграма кооперацій (Collaboration Diagram), також відома як діаграма комунікації, представляє взаємодію між об'єктами та компонентами системи. У контексті анонімної соціальної мережі з використанням блокчейн і токеноміки, діаграма кооперацій може допомогти візуалізувати обмін інформацією та токенами між різними компонентами системи.

В наступних розділах будуть наведені графічні зображення даних діаграм

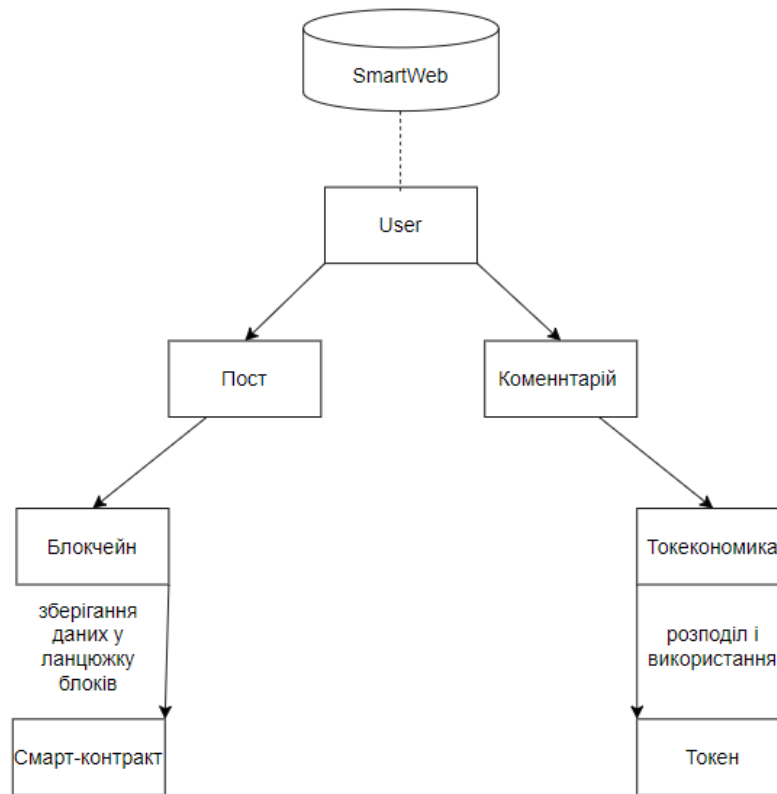


Рисунок 2.2 – Графічне зображення кооперацій (Collaboration Diagram)
 Користувач взаємодіє з Постою і Коментарями, відправляючи запити на створення або перегляд контенту.
 Пости і Коментарі використовують функціональність Блокчейна для зберігання даних у ланцюжку блоків.
 Блокчейн використовує розумні контракти для виконання логіки та перевірки умов доступу до даних.
 Токеноміка забезпечує розподіл і використання токенів у системі, можливо, для винагороди користувачів за активність або підтримку контенту.

3. ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Вибір програмного інструментарію

Для створення анонімної соціальної мережі на блокчейні існує кілька варіантів програмного інструментарію. Ось кілька популярних та ефективних засобів, які можна використовувати для цього:

1. **Ethereum**: Ethereum є одним з найбільш популярних блокчейнів для створення децентралізованих додатків (DApps). Він має власну віртуальну машину Ethereum (EVM), яка дозволяє запускати розумні контракти. Ви можете розглянути розробку вашої анонімної соціальної мережі в Ethereum, використовуючи мови програмування, такі як Solidity або Vyper.
2. **EOS**: EOS є іншим блокчейном, який підтримує розробку DApps. Він має швидку транзакційну швидкість та гнучку систему контрактів. EOS пропонує свою власну мову програмування - C++ або Python, що може бути корисним для розробки соціальної мережі.
3. **Hyperledger Fabric**: Hyperledger Fabric є приватним блокчейном, розробленим для використання у корпоративних середовищах. Він надає розширені можливості приватності та контролю доступу, що можуть бути важливими для анонімної соціальної мережі. Ви можете використовувати Hyperledger Fabric, розробляючи вашу мережу з використанням мови програмування, такої як Go або Java.
4. **IPFS**: InterPlanetary File System (IPFS) - це протокол для розподіленого зберігання і обміну файлами. Ви можете використати IPFS для зберігання анонімних повідомлень та медіафайлів у вашій соціальній мережі. IPFS можна поєднати з іншим блокчейном, наприклад, Ethereum, для керування доступом та ідентифікації користувачів.

3.1.1 Мови програмування

При розробці анонімної соціальної мережі на блокчейні можна використовувати різні мови програмування залежно від платформи блокчейну, яку ви обираєте. Ось декілька популярних мов програмування для таких проектів:

1. **Solidity**: Це мова програмування, що використовується в блокчейні Ethereum. Вона спеціально розроблена для розумних контрактів і підтримується Ethereum Virtual Machine (EVM). Solidity є популярним вибором для розробки DApps на Ethereum.

2. **Vyper**: Це інша мова програмування, спеціально призначена для розумних контрактів на блокчейні Ethereum. Vyper пропонує простий синтаксис та більш високий рівень безпеки, порівняно з Solidity. Вона може бути хорошим вибором, якщо ви прагнете до безпеки та аудитування коду.

3. **C++ та Python**: Якщо ви розглядаєте платформу EOS для розробки своєї анонімної соціальної мережі, то мови програмування, такі як C++ та Python, є популярними виборами для розробки на EOS. Ви можете використовувати C++ для розробки контрактів, а Python для розробки додатків, які взаємодіють з цими контрактами.

4. **Go та Java**: Якщо ви розглядаєте Hyperledger Fabric для розробки вашої соціальної мережі, то мови програмування, такі як Go та Java, є популярними виборами для розробки на цій платформі. Ви можете використовувати Go або Java для розробки ланцюжка блоків, розумних контрактів та додатків, які взаємодіють з Hyperledger Fabric.

5. **JavaScript**: Якщо ви розглядаєте використання платформи, яка підтримує розробку DApps на блокчейні, як Ethereum або EOS, ви також можете розглянути JavaScript. JavaScript має широку підтримку та багато ресурсів, які допоможуть вам в розробці фронтенду та взаємодії з розумними контрактами через веб-інтерфейси.

3.1.2 Переваги та недоліки мов програмування

Solidity:

Плюси:

- Створена спеціально для розумних контрактів на блокчейні Ethereum, тому має широку підтримку та активну спільноту розробників.
- Широкий набір інструментів та бібліотек для розробки на Ethereum.
- Хороша документація та ресурси для навчання.

Мінуси:

- Менш безпечна в порівнянні з іншими мовами програмування, оскільки може бути складно уникнути пасток безпеки.
- Синтаксис може бути складним для розуміння для розробників, які не мають досвіду з мовами, що базуються на C++.

Vyper:

Плюси:

- Більш високий рівень безпеки порівняно з Solidity, оскільки має обмежені можливості та виразність мови.
- Простий синтаксис, що полегшує розуміння та аудитування коду.

Мінуси:

- Менша популярність та менша кількість доступних ресурсів та інструментів порівняно з Solidity.
- Обмежені можливості мови можуть призвести до складнішої реалізації певних функціональностей.

C++ та Python:

Плюси:

- Широко використовувані та популярні мови програмування з багатим екосистемою та великою кількістю ресурсів.
- Висока продуктивність та швидкодія для обробки великого обсягу даних.
- Здатність до розробки складних та потужних додатків.

Мінуси:

- Вимагають більше ресурсів та часу для розробки порівняно з іншими мовами.
- Можуть бути складнішими для вивчення, особливо для початківців.

Go та Java:

Плюси:

- Швидкодія та ефективність виконання програм.
- Мають потужні функції та розширені бібліотеки.
- Хороша масштабованість та здатність до розробки розподілених систем.

Мінуси:

- Можуть мати вищий поріг вхідного рівня для розробників з меншим досвідом.
- Можуть бути більш обсяжними та складними для розробки порівняно з деякими іншими мовами.

JavaScript:

Плюси:

- Широко використовувана мова з великою спільнотою розробників та багатим вибором фреймворків та бібліотек.
- Ідеальна для розробки фронтенду та веб-інтерфейсів.
- Здатність до взаємодії з блокчейнами, такими як Ethereum, через бібліотеки, такі як Web3.js.

Мінуси:

- Менш ефективна в розрахунку швидкодії та обробці великого обсягу даних порівняно з деякими іншими мовами.
 - Потребує додаткових заходів безпеки та обережності при розробці розумних контрактів.

3.1.3 Програмне середовище

При створенні анонімної соціальної мережі на блокчейні знадобиться програмне середовище, яке підтримує розробку для вибраної блокчейн-платформи. Ось кілька популярних програмних середовищ, які можуть бути використані для розробки такого проекту:

1. Ethereum Studio: Це інтегроване середовище розробки, спеціально створене для платформи Ethereum. Воно надає зручний веб-інтерфейс, де ви можете розробляти розумні контракти, компілювати та розгортати їх на тестовій мережі Ethereum. Ethereum Studio також має вбудований генератор шаблонів контрактів та підтримку мови Solidity.

2. Remix: Це ще одне веб-середовище для розробки розумних контрактів на платформі Ethereum. Воно пропонує повний набір інструментів для розробки, налагодження та тестування контрактів. Remix також має інтегровану консоль, яка дозволяє взаємодіяти з розумними контрактами безпосередньо через веб-інтерфейс.

3. Truffle: Це розширене програмне середовище для розробки на платформі Ethereum. Воно надає набір інструментів для створення, тестування та розгортання розумних контрактів. Truffle має вбудовану систему управління міграціями контрактів, що полегшує розгортання та оновлення контрактів.

4. Ganache: Це локальна блокчейн-мережа, яка надає зручні засоби для розробки та тестування розумних контрактів. Ganache дозволяє швидко запускати локальну блокчейн-мережу, на якій ви можете розгортати та взаємодіяти з вашими контрактами. Воно також має графічний інтерфейс та зручні інструменти для відладки контрактів.

5. Hyperledger Composer: Якщо ми розглядаємо розробку на Hyperledger Fabric, Hyperledger Composer є програмним середовищем, що дозволяє швидко створювати, тестувати та моделювати мережі блокчейн. Воно має вбудований текстовий редактор та засоби візуального моделювання для створення бізнес-мереж та розумних контрактів.

3.2 Архітектура розроблюваного об'єкта

3.2.1 Автентифікація розробника

Хоча читати дані з SmartWeb API так само просто, як надіслати запит GraphQL, для публікації в мережі потрібно пройти автентифікацію або написати транзакцію безпосередньо в смарт-контрактах SmartWeb.

Це включає будь-яку зміну стану, наприклад підписку, відмову від підписки, створення публікації та створення дзеркала.

Хоча існує досить багато документації щодо запису транзакцій у блокчейні, ми подумали, що було б корисно надати повний посібник зі стеку для автентифікації за допомогою SmartWeb API для розробників, які дозволяють змінювати стан у своїх програмах.

Також важливо розуміти, як реалізувати автентифікацію, щоб мати можливість скористатися такими функціями SmartWeb API, як введені дані (спосіб показати користувачам те, що вони підписують, у більш зручному для читання форматі), безгазові транзакції або використовувати диспетчер.

Щоб почати створюємо нову програму Next.js:

```
npx create-next-app lens-app
```

- ✓ Would you like to use TypeScript with this project? No
- ✓ Would you like to use ESLint with this project? Yes
- ✓ Would you like to use Tailwind CSS with this project? Yes
- ✓ Would you like to use src/ directory with this project? No
- ✓ Use App Router (recommended)? Yes
- ✓ Would you like to customize the default import alias? No

Далі переходимо у новий каталог і встановлюємо такі залежності:

```
npm install @apollo/client graphql ethers@5.7.2
```

Далі ми налаштуємо клієнт GraphQL. Це те, що ми будемо використовувати для надсилання запитів до SmartWeb API.

Створіть файл з назвою api.js у корені проекту та додайте такий код:

```
import { ApolloClient, InMemoryCache, gql } from '@apollo/client'
```

```
const API_URL = 'https://api.lens.dev'

export const client = new ApolloClient({
  uri: API_URL,
  cache: new InMemoryCache()
})
```

Визначення запитів і мутацій GraphQL

У GraphQL операції читання відомі як запити, а операції запису (створення, оновлення, видалення тощо) відомі як мутації.

Тепер, коли ми створили клієнт GraphQL, давайте визначимо запити та мутації, які нам знадобляться для автентифікації.

Для автентифікації потрібні дві дії сервера. Перший - це генерація виклику з сервера (challenge). По-друге, користувач повинен підписати це завдання за допомогою свого гаманця Ethereum і надіслати підпис на сервер Lens для створення дійсного маркера доступу JWT і маркера оновлення (автентифікації).

Додаємо такий код до api.js:

```
'use client'
import { useEffect, useState } from 'react'
import { ethers } from 'ethers'
import { client, challenge, authenticate } from '../api'

export default function Home() {
  /* local state variables to hold user's address and access token */
  const [address, setAddress] = useState()
  const [token, setToken] = useState()
  useEffect(() => {
    /* when the app loads, check to see if the user has already connected their wallet */
    checkConnection()
  }, [])
  async function checkConnection() {
    const provider = new ethers.providers.Web3Provider(window.ethereum)
    const accounts = await provider.listAccounts()
    if (accounts.length) {
      setAddress(accounts[0])
    }
  }
  async function connect() {
    /* this allows the user to connect their wallet */
    const account = await window.ethereum.send('eth_requestAccounts')
    if (account.result.length) {
      setAddress(account.result[0])
    }
  }
  async function login() {
```

```

try {
  /* first request the challenge from the API server */
  const challengeInfo = await client.query({
    query: challenge,
    variables: { address }
  })
  const provider = new ethers.providers.Web3Provider(window.ethereum);
  const signer = provider.getSigner()
  /* ask the user to sign a message with the challenge info returned from the server */
  const signature = await signer.signMessage(challengeInfo.data.challenge.text)
  /* authenticate the user */
  const authData = await client.mutate({
    mutation: authenticate,
    variables: {
      address, signature
    }
  })
  /* if user authentication is successful, you will receive an accessToken and
refreshToken */
  const { data: { authenticate: { accessToken } } } = authData
  console.log({ accessToken })
  setToken(accessToken)
} catch (err) {
  console.log('Error signing in: ', err)
}
}

return (
  <div>
    { /* if the user has not yet connected their wallet, show a connect button */ }
    {
      !address && <button onClick={connect}>Connect</button>
    }
    { /* if the user has connected their wallet but has not yet authenticated, show them a
login button */ }
    {
      address && !token && (
        <div onClick={login}>
          <button>Login</button>
        </div>
      )
    }
    { /* once the user has authenticated, show them a success message */ }
    {
      address && token && <h2>Successfully signed in!</h2>
    }
  </div>
)
}

```

Далі запускаємо додаток щоб перевірити його:

```
npm run dev
```

Коли програма завантажиться, ми зможемо увійти, а `accessToken` має бути виведено з консолі після успіху.

3.2.2 Логін користувача

Щоб увійти, потрібно дві дії на сервері: перша — створити виклик із сервера, а друга — підписати цей виклик за допомогою вашого гаманця Ethereum і надіслати підпис на наш сервер для створення дійсного маркера доступу JWT і маркера оновлення.

Щоб отримати токен JWT, потрібно спочатку надіслати запит на виклик із сервера, який поверне певний текст для підпису в гаманці, щоб підтвердити право власності. Після того як ми скористалися викликом для створення маркера JWT, він більше не працюватиме.

```
query Challenge {
  challenge(request: { address: "0xdfd7D26fd33473F475b57556118F8251464a24eb" }) {
    text
  }
}
```

3.2.3. Автентифікація користувача

Після того, як ви отримаєте текст виклику від сервера, вам потрібно підписати виклик за допомогою свого гаманця Ethereum, а потім передати цей підпис кінцевій точці автентифікації, це створить вам `accessToken` і `refreshToken`.

`accessToken` – це триває 30 хвилин, перш ніж потрібно буде оновити

`refreshToken` – це триває 7 днів, щоб ви могли залишити їх увійшли в систему та створити новий `accessToken`, коли вони повернуться, і їм не потрібно знову підписувати виклик.

```
mutation Authenticate {
  authenticate(request: {
    address: "0xdfd7D26fd33473F475b57556118F8251464a24eb",
    signature:
"0x8f82e1a2c2cc35a2963c60eeb0a76aecc100686c4ffcb98fd522a90cba2f0b2642067c79cd6
d0c9d239ed28a6882818f77bf546e774410236c730988bd14de5d1c"
  }) {
    accessToken
    refreshToken
  }
}
```

3.2.4. Створення профілю користувача

`useCreateProfile` — це React Hook, який дозволяє створити новий профіль об'єктива, який належить підключеному гаманцю.

```
const { execute, error, isPending } = useCreateProfile();
```

Викликаємо `useCreateProfile` у компоненті, який відповідає за прийняття потрібного дескриптора.

```
import { isValidHandle, useCreateProfile } from '@lens-protocol/react-web';
```

```
const [handle, setHandle] = useState<string | null>(null);
```

```
const { execute: create, error, isPending } = useCreateProfile();
```

```
const onSubmit = async (e: FormEvent) => {  
  e.preventDefault();  
  if (!handle) return;  
  await create(handle);  
};
```

```
<form onSubmit={onSubmit}>  
  <input  
    minLength={5}  
    maxLength={31}  
    required  
    type="text"  
    disabled={isPending}  
    onChange={(e) => {  
      if (isValidHandle(e.target.value)) {  
        setHandle(e.target.value);  
      } else {  
        setHandle(null);  
      }  
    }}  
  />
```

```
<button type="submit">Create</button>
```

</form>

3.2.4.1 Визначення

useCreateprofile

Параметри

useCreateProfile не приймає жодних параметрів.

Повернення

Повертає об'єкт з:

execute: функція, за допомогою якої можна ініціювати створення нового профілю об'єктива.

isPending: логічне значення, яке сповіщає вас, коли операція все ще триває.

error: будь-яка помилка, яка може виникнути в нормальних умовах роботи, повертатиметься через цю властивість. Значення за замовчуванням null

DuplicatedHandleError - наданий маркер уже використано виконувати функцію

Щоб розпочати процес створення профілю, можна скористатися функцією виконання. Залежно від умов мережі це може зайняти деякий час, оскільки хук очікує виконання операції та її індексування за допомогою Smart Web API.

Параметри

Він приймає рядок із бажаним маркером. Дескриптор не повинен містити суфікс .test (ані .smart для розгортання протоколу SmartWeb main-net).

Повернення

Він повертає Promise<void> , який можна використовувати для синхронізації зі станом вашого компонента. Наприклад, ви можете очистити вміст будь-якого поля введення тексту, коли така обіцянка вирішується.

3.2.5 Підписка на інший профіль

Цей виклик API дозволяє отримати введені дані, щоб потім викликати метод withSig для відстеження профілів на SmartWeb.

Введені дані — це спосіб спробувати показати користувачам те, що вони підписують, у більш зручному для читання форматі.

Побудова такого типу даних зазвичай складна. У даних типу також потрібно отримати nonce, крайній термін, версію контракту, адресу контракту, ідентифікатор ланцюга та назву контракту, щоб підпис можна було підписати та перевірити.

Під час використання цього API сервер перевіряє кожен деталь, перш ніж генерувати введені дані. Наприклад: якщо ви спробуєте створити введені дані для транзакції, яка завжди завершується помилкою, сервер видасть помилку у формі, зрозумілій людині. Це чудово підходить для налагодження, але також усуває проблеми з користувачами, які постійно надсилають невдалі транзакції або невідповідність неправильного запиту. Покажемо підхід до типізованих даних, використовуючи ethers та API поруч. З типізованим підходом даних ми використовуємо методи withSig, які можна викликати за допомогою свого підпису або за допомогою цього підпису будь-який ретранслятор може викликати його за вас від вашого імені, дозволяючи безгазові транзакції.

```
mutation CreateFollowTypedData {
  createFollowTypedData(request: {
    follow: [
      {
        profile: "0x01",
        followModule: null
      }
    ]
  }) {
    id
    expiresAt
    typedData {
      domain {
        name
        chainId
        version
```

```

    verifyingContract
  }
  types {
    FollowWithSig {
      name
      type
    }
  }
  value {
    nonce
    deadline
    profileIds
    datas
  }
}
}
}
}

```

Запит

Давайте торкнемося цього запиту, щоб було надзвичайно зрозуміло.

Профіль - обов'язковий

Ми повинні передати profile, який є обов'язковим (це profileId).

FollowModule

Якщо ми стежимо за кимось, у кого визначено модуль стеження, ми повинні передати властивості, щоб викупити його. Ми змушуємо вас передавати властивості зі сторони клієнта, тому що, якби ми зчитували їх із сервера щоразу, коли хтось міг передати запит і змусити вас підписати щось, чого ваш клієнт не бачив під час створення підпису. Підписуватися на модулі можна будь-коли змінити за допомогою профілю. Якщо для цього профілю не налаштовано модуль відстеження, нам не потрібно нічого передавати.

За допомогою створеної нами схеми дуже легко визначити наступний модуль, який потрібно викупити:

Немає наступних налаштувань модуля

Якщо особа не налаштувала модуль стеження, нам не потрібно нічого передавати в модуль стеження.

```

mutation CreateFollowTypedData {
  createFollowTypedData(request: {

```

```

follow: [
  {
    profile: "0x01"
  }
]
}) {
id
expiresAt
typedData {
  domain {
    name
    chainId
    version
    verifyingContract
  }
  types {
    FollowWithSig {
      name
      type
    }
  }
  value {
    nonce
    deadline
    profileIds
    datas
  }
}
}
}
}

```

FollowModule

Людина, за якою ви хочете стежити, вимагає, щоб у вас був профіль, щоб стежити за нею. Ви повинні передати свій profileId у запит. Цей профіль може стежити за ними лише один раз, що зупиняє спам.

```

mutation CreateFollowTypedData {
  createFollowTypedData(request: {
    follow: [
      {
        profile: "0x01",
        followModule: {
          profileFollowModule: {
            profileId: "0x02"
          }
        }
      }
    ]
  })
}

```

```

    }
  }
}
]
}) {
  id
  expiresAt
  typedData {
    domain {
      name
      chainId
      version
      verifyingContract
    }
    types {
      FollowWithSig {
        name
        type
      }
    }
    value {
      nonce
      deadline
      profileIds
      datas
    }
  }
}
}
}
}

```

Плата за модулем

Особа, на яку ви підписані, має платний модуль підписки.

```

mutation CreateFollowTypedData {
  createFollowTypedData(request: {
    follow: [
      {
        profile: "0x01",
        followModule: {
          feeFollowModule: {
            amount: {
              currency: "0xD40282e050723Ae26Aeb0F77022dB14470f4e011",
              value: "0.01"
            }
          }
        }
      }
    ]
  })
}

```

```

    }
  }
}
]
}) {
  id
  expiresAt
  typedData {
    domain {
      name
      chainId
      version
      verifyingContract
    }
    types {
      FollowWithSig {
        name
        type
      }
    }
    value {
      nonce
      deadline
      profileIds
      datas
    }
  }
}
}
}
}

```

Як ви бачите вище, ми зіставили валюту, у якій профіль хоче отримати плату, разом із значенням, яке має бути передано як звичайну суму без зсуву до десяткових знаків, оскільки наш сервер робить це за вас. Отже, якщо вартість профілю, яку потрібно стежити, становить 1 WETH, ви повинні ввести 1 як значення.

Підключення без використання даних типу

Можливо, ви не захочете спускатися до введених даних із маршрутом підпису та просто надсилати транзакцію безпосередньо від клієнта до блокчейну без будь-якого виклику API для відображення даних для вас.

Вам потрібно буде виконати кодування та перевірку самостійно, якщо ви підете на цей підхід. Це виходить за рамки документації API, оскільки було б пояснено та показано, як це зробити в документах контракту. Це намагається порадити ту саму практику, яку роблять searport на OpenSea разом із багатьма іншими проектами, які намагаються покращити видимість того, що підписує користувач.

Використання SmartWebClient SDK

Ви можете використовувати SmartWebClient SDK, щоб стежити за профілем.

```
// SmartWebClient is an authenticated instance of SmartWebClient

// get recommended profiles to follow
const recommendedProfiles = await SmartWebClient.profile.allRecommended();

// request follow typed data
const followTypedDataResult = await
SmartWebClient.profile.createFollowTypedData({
  follow: [
    {
      profile: recommendedProfiles[0].id,
    },
  ],
});

// sign and broadcast the typed data
const data = followTypedDataResult.unwrap();

// sign with the wallet
const signedTypedData = await wallet._signTypedData(
  data.typedData.domain,
  data.typedData.types,
  data.typedData.value
);

const broadcastResult = await SmartWebClient.transaction.broadcast({
  id: data.id,
  signature: signedTypedData,
});
```

3.2.6. Публікація контенту

Створення власного завдання

Я впевнений, що ви вже звикли до цього; ми почнемо зі створення нового файлу під назвою `post.ts` у каталозі `tasks/`.

Ми також включимо наш звичайний імпорт і базову ініціалізацію. Ми також будемо використовувати `FreeCollectModule`, який дозволяє будь-якому підписнику безкоштовно збирати нашу публікацію назавжди. Ось як має виглядати файл:

```
import { defaultAbiCoder } from 'ethers/lib/utis';
import { task } from 'hardhat/config';
import { SmartWebHub__factory } from '../typechain-types';
import { PostDataStruct } from '../typechain-types/SmartWebHub';
import { getAddrs, initEnv, waitForTx, ZERO_ADDRESS } from './helpers/utis';

task('post', 'publishes a post')
  .setAction(async ({}, hre) => {
    const [governance, , user] = await initEnv(hre);
    const addrs = getAddrs();
    const freeCollectModuleAddr = addrs['free collect module'];
    const SmartWebHub = SmartWebHub__factory.connect(addrs['SmartWebHub proxy'], governance);
  });
```

Додавання модуля `Collect` до білого списку

Протокол дозволяє використовувати в дописах і коментарях лише модулі збору з білого списку (дзеркала не мають модуля збору, пов'язаного з ними), тому ми повинні включити в білий список наш безкоштовний модуль збору:

```
...
  await waitForTx(lensHub.whitelistCollectModule(freeCollectModuleAddr, true));
...
```

Створення публікації

Тепер, коли ми внесли модуль збирання в білий список, ми готові створити нашу публікацію! Як і створення профілю, функції публікації (у нашому випадку ми розглядаємо лише `post()`) використовують структуру вхідних даних. Ось як виглядає структура даних, яка нам потрібна (з `contracts/libraries/Datatypes.sol`):

```
// NOTE: This struct is defined in the contracts/libraries/Datatypes.sol library

/**
 * @notice A struct containing the parameters required for the post() function.
 *
 * @param profileId The token ID of the profile to publish to.
 * @param contentURI The URI to set for this new publication.
 * @param collectModule The collect module to set for this new publication.
 * @param collectModuleInitData The data to pass to the collect module's
initialization.
 * @param referenceModule The reference module to set for the given publication,
must be whitelisted.
 * @param referenceModuleInitData The data to be passed to the reference module for
initialization.
 */
struct PostData {
    uint256 profileId;
    string contentURI;
    address collectModule;
    bytes collectModuleInitData;
    address referenceModule;
    bytes referenceModuleInitData;
}
```

Тепер ми готові приступити до створення нашої вхідної структури! Ми хочемо, щоб ідентифікатор профілю був 1, оскільки ми володіємо єдиним існуючим профілем. URI вмісту можна імітувати. Модуль збирання буде нещодавно включеним у білий список FreeCollectModule, який не приймає даних, і, нарешті, довідковий модуль і пов'язане з ним поле даних є безкоштовними.

```
...
const inputStruct: PostDataStruct = {
    profileId: 1,
    contentURI:
'https://ipfs.io/ipfs/Qmby8QocUU2sPZL46rZeMctAuF5nrCc7eR1PPkooCztWPz',
    collectModule: freeCollectModuleAddr,
    collectModuleInitData: defaultAbiCoder.encode(['bool'], [true]),
    referenceModule: ZERO_ADDRESS,
    referenceModuleInitData: [],
};
...
```

Гаразд, тепер ми майже готові до виконання транзакції. Подібно до створення профілю, ми підключимо екземпляр SmartWebHub до нашого

підписувача user та надішлемо транзакцію! Щоб бути впевненим, ми також збираємося додати деякі протоколи, щоб переконатися, що все працює саме так, як ми очікуємо:

```
...
  await waitForTx(SmartWebHub.connect(user).post(inputStruct));
  console.log(await SmartWebHub.getPub(1, 1));
...
```

Підведення підсумків

Створюємо файл tasks/post.ts із таким кодом:

```
import { defaultAbiCoder } from 'ethers/lib/utis';
import { task } from 'hardhat/config';
import { SmartWebHub__factory } from '../typechain-types';
import { PostDataStruct } from '../typechain-types/SmartWebHub';
import { getAddr, initEnv, waitForTx, ZERO_ADDRESS } from './helpers/utis';

task('post', 'publishes a post').setAction(async ({}, hre) => {
  const [governance, , user] = await initEnv(hre);
  const addr = getAddr();
  const freeCollectModuleAddr = addr['free collect module'];
  const SmartWebHub = SmartWebHub__factory.connect(addr['SmartWebHub proxy'],
governance);

  await waitForTx(SmartWebHub.whitelistCollectModule(freeCollectModuleAddr,
true));

  const inputStruct: PostDataStruct = {
    profileId: 1,
    contentURI:
'https://ipfs.io/ipfs/Qmby8QocUU2sPZL46rZeMctAuF5nrCc7eR1PPkooCztWPz',
    collectModule: freeCollectModuleAddr,
    collectModuleInitData: defaultAbiCoder.encode(['bool'], [true]),
    referenceModule: ZERO_ADDRESS,
    referenceModuleInitData: [],
  };

  await waitForTx(SmartWebHub.connect(user).post(inputStruct));
  console.log(await SmartWebHub.getPub(1, 1));
});
```

Нарешті запускаємо завдання:

```
$ npx hardhat post --network localhost
```

Якщо все пройшло за планом, консоль повинна вивести щось на зразок цього:

```
BigNumber { _hex: '0x00', _isBigNumber: true },
  BigNumber { _hex: '0x00', _isBigNumber: true },
  'https://ipfs.io/ipfs/Qmby8QocUU2sPZL46rZeMctAuF5nrCc7eR1PPkooCztWPz',
  '0x0000000000000000000000000000000000000000000000000000000000000000',
  '0x20Ce94F404343aD2752A2D01b43fa407db9E0D00',
  '0x0000000000000000000000000000000000000000000000000000000000000000',
  profileIdPointed: BigNumber { _hex: '0x00', _isBigNumber: true },
  pubIdPointed: BigNumber { _hex: '0x00', _isBigNumber: true },
  contentURI:
'https://ipfs.io/ipfs/Qmby8QocUU2sPZL46rZeMctAuF5nrCc7eR1PPkooCztWPz',
  referenceModule: '0x0000000000000000000000000000000000000000000000000000000000000000',
  collectModule: '0x20Ce94F404343aD2752A2D01b43fa407db9E0D00',
  collectNFT: '0x0000000000000000000000000000000000000000000000000000000000000000'
]
```

Операция поиска #1



[9:02:09] **Yah**Найдено 1% совпадений по адресу:

https://uk.wikipedia.org/wiki/Теорія_мереж [Исключить](#)

[9:02:31] **Yah**Найдено 1% совпадений по адресу:

https://tech.vernadskyjournals.in.ua/journals/2021/3_2021/22.pdf [Исключить](#)

[9:02:43] **Yah**Найдено 1% совпадений по адресу: [https://dut.edu.ua/ua/news-1-626-7897-](https://dut.edu.ua/ua/news-1-626-7897-zastovuvannya-uml-chastina-2-diagrama-poslidovnosti---sequence-diagram_kafedra-kompyuternih-nauk-ta-informaciynih-tehnologiy)

[zastovuvannya-uml-chastina-2-diagrama-poslidovnosti---sequence-diagram_kafedra-kompyuternih-nauk-ta-informaciynih-tehnologiy](https://dut.edu.ua/ua/news-1-626-7897-zastovuvannya-uml-chastina-2-diagrama-poslidovnosti---sequence-diagram_kafedra-kompyuternih-nauk-ta-informaciynih-tehnologiy) [Исключить](#)

[9:02:44] **Yah**Найдено 1% совпадений по адресу: [http://www.tsatu.edu.ua/kn/wp-](http://www.tsatu.edu.ua/kn/wp-content/uploads/sites/16/laboratorna-robota-9-diahrama-poslidovnosti.pdf)

[content/uploads/sites/16/laboratorna-robota-9-diahrama-poslidovnosti.pdf](http://www.tsatu.edu.ua/kn/wp-content/uploads/sites/16/laboratorna-robota-9-diahrama-poslidovnosti.pdf) [Исключить](#)

[9:02:53] **Yah**Найдено 1% совпадений по адресу: [https://www.mindonmap.com/uk/blog/what-is-uml-](https://www.mindonmap.com/uk/blog/what-is-uml-sequence-diagram/)

[sequence-diagram/](https://www.mindonmap.com/uk/blog/what-is-uml-sequence-diagram/) [Исключить](#)

[9:02:54] **Yah**Найдено 1% совпадений по адресу:

http://www.economy.in.ua/pdf/9_2019/10.pdf [Исключить](#)

[9:03:19] **Yah**Найдено 1% совпадений по адресу: [https://elle.ua/crypto-guida/blokcheyn-shcho-vartoz-](https://elle.ua/crypto-guida/blokcheyn-shcho-vartoznati-novachkam/)

[znati-novachkam/](https://elle.ua/crypto-guida/blokcheyn-shcho-vartoznati-novachkam/) [Исключить](#)

[9:03:23] **Yah**Найдено 1% совпадений по адресу: [https://academy.binance.com/uk/articles/what-is-](https://academy.binance.com/uk/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners)

[blockchain-technology-a-comprehensive-guide-for-beginners](https://academy.binance.com/uk/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners) [Исключить](#)

[9:03:31] **Yah**Найдено 1% совпадений по адресу: [https://ua-referat.com/uploaded/socialeni-mereji-](https://ua-referat.com/uploaded/socialeni-mereji-v2/index1.html)

[v2/index1.html](https://ua-referat.com/uploaded/socialeni-mereji-v2/index1.html) [Исключить](#)

[9:04:08] **Yah**Найдено 1% совпадений по адресу: [https://search.oecd.org/eurasia/competitiveness-](https://search.oecd.org/eurasia/competitiveness-programme/eastern-partners/UKR_FINALSummary_Record_OECD_Decentralisation_Launch_11May2021_Proceedings_UKR.pdf)

[programme/eastern-partners/UKR_FINALSummary_Record_OECD_Decentralisation_Launch_11May2021_Proceedings_UKR.pdf](https://search.oecd.org/eurasia/competitiveness-programme/eastern-partners/UKR_FINALSummary_Record_OECD_Decentralisation_Launch_11May2021_Proceedings_UKR.pdf) [Исключить](#)

[9:04:37] **Yah**Найдено 1% совпадений по адресу:

<http://dspace.wunu.edu.ua/bitstream/316497/28732/1/374.PDF> [Исключить](#)

[9:04:52] **Yah**Найдено 1% совпадений по адресу:

https://ela.kpi.ua/bitstream/123456789/18035/1/30_p47.pdf [Исключить](#)

[9:05:03] **Yah**Найдено 1% совпадений по адресу: [https://futurenow.com.ua/shho-take-sotsialni-](https://futurenow.com.ua/shho-take-sotsialni-merezhi-vydy-klyasyfikatsiya-bezpeka/)

[merezhi-vydy-klyasyfikatsiya-bezpeka/](https://futurenow.com.ua/shho-take-sotsialni-merezhi-vydy-klyasyfikatsiya-bezpeka/) [Исключить](#)

[9:05:33] [Yah](#)Найдено 1% совпадений по адресу: <https://uk.wikipedia.org/wiki/Анонімність> [Исключить](#)

[9:05:50] [Yah](#)Найдено 1% совпадений по адресу: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_631067.pdf [Исключить](#)

[9:05:53] [Yah](#)Найдено 1% совпадений по адресу: [https://uk.wikipedia.org/wiki/Перелік_стандартів_для_ЕЦП_\(Україна\)](https://uk.wikipedia.org/wiki/Перелік_стандартів_для_ЕЦП_(Україна)) [Исключить](#)

[9:06:21] [Yah](#)Найдено 1% совпадений по адресу: http://philol.vernadskyyournals.in.ua/journals/2021/5_2021/part_2/27.pdf [Исключить](#)

[9:06:55] [Yah](#)Найдено 1% совпадений по адресу: https://uk.wikipedia.org/wiki/Безпека_мережі [Исключить](#)

[9:06:57] [Yah](#)Найдено 1% совпадений по адресу: <https://imi.org.ua/articles/bezpeka-v-sotsialnih-merejah-etika-povedinki-v-interneti-i1085> [Исключить](#)

[9:07:07] [Yah](#)Найдено 1% совпадений по адресу: <https://blockchainsummit.com.ua/shho-take-tehnologija-blokchejn/> [Исключить](#)

[9:07:32] [Yah](#)Найдено 1% совпадений по адресу: <https://webcase.com.ua/uk/blog/etapi-stvorennja-mobilnogo-dodatku/> [Исключить](#)

[9:08:11] [Yah](#)Найдено 1% совпадений по адресу: <https://majiclif.com/uk/scho-take-blokchejn-vse-scho-potr-bno-znati-pro-tehnolog-yu/> [Исключить](#)

[9:08:25] [Yah](#)Найдено 1% совпадений по адресу: <https://academy.binance.com/uk/articles/what-is-the-blockchain-trilemma> [Исключить](#)

[9:08:29] [Yah](#)Найдено 1% совпадений по адресу: <https://blog.whitebit.com/uk/what-is-blockchain-technology/> [Исключить](#)

[9:08:29] [Yah](#)Найдено 2% совпадений по адресу: <https://nenws.com/finansii/kriptoaljuti/shcho-take-blokchejn/> [Исключить](#)

[9:08:40] [Yah](#)Найдено 2% совпадений по адресу: <https://sharpay.net/uk/blokchejn-shho-cze-take-i-yak-jogo-vykorystovuyut-u-finansah/> [Исключить](#)

[9:09:16] [Yah](#)Найдено 1% совпадений по адресу: [https://www.obmenat24.com/blog/shcho-take-blokchejn\(Сохраненная копия\)](https://www.obmenat24.com/blog/shcho-take-blokchejn(Сохраненная копия)) [Исключить](#)

[9:09:27] [Yah](#)Найдено 1% совпадений по адресу: <https://uk.wikipedia.org/wiki/Інтернет-комунікація> [Исключить](#)

[9:09:29] [Yah](#)Найдено 1% совпадений по адресу: https://www.bbc.com/ukrainian/institutional/2013/10/000001_about_sharing [Исключить](#)

[9:10:06] Не загружена страница из запроса №144-1 (30107 миллисек., превышен таймаут в 30000 миллисек.): <https://support.google.com/youtube/answer/154235?hl=uk>

[9:10:06] Не загружена страница из запроса №144-2 (30090 миллисек., превышен таймаут в 30000 миллисек.): <https://support.google.com/admob/answer/7313578?hl=uk>

[9:10:31] [Yah](#)Найдено 1% совпадений по адресу: <https://academy.binance.com/uk/articles/what-is-ethereum> [Исключить](#)

[9:10:34] [Yah](#)Найдено 1% совпадений по адресу: [https://support.google.com/youtube/answer/154235?hl=uk\(Сохраненная копия\)](https://support.google.com/youtube/answer/154235?hl=uk(Сохраненная копия)) [Исключить](#)

[9:10:43] [Yah](#)Найдено 1% совпадений по адресу: <https://blog.trusteeglobal.com/uk/perspektyvni-tokeny-2021-2022/> [Исключить](#)

[9:10:59] [Yah](#)Найдено 1% совпадений по адресу: https://uk.wikipedia.org/wiki/Соціальне_павутиння [Исключить](#)

[9:11:12] [Yah](#)Найдено 1% совпадений по адресу: https://uk.wikipedia.org/wiki/Загальний_регламент_про_захист_даних [Исключить](#)

[9:11:40] [Yah](#)Найдено 1% совпадений по адресу: <https://www.unicef.org/ukraine/cyberbullying> [Исключить](#)

[9:12:15] [Yah](#)Найдено 1% совпадений по адресу: <https://www.kozaky.org.ua/ponyattya-prichini-formi-i-vidi-nasilstva-viznachennya-v-psixologii-naslidki-nasilstva-u-doroslix-profilaktika-ta-reabilitaciya/> [Исключить](#)

[9:12:44] [Yah](#)Найдено 1% совпадений по адресу: http://pev.kpu.zp.ua/journals/2021/1_24_ukr/35.pdf [Исключить](#)

- [9:12:49] **Yah** Найдено 1% совпадений по адресу: <https://avada-media.ua/ua/services/vnedreniye-blokcheyn-v-bazy-dannykh/> **Исключить**
- [9:13:09] **Yah** Найдено 1% совпадений по адресу: https://uk.wikipedia.org/wiki/Конфіденційність_в_Інтернеті **Исключить**
- [9:13:11] **Yah** Найдено 1% совпадений по адресу: https://elearning.sumdu.edu.ua/free_content/lectured:89b3d175c06a6b137e410cb14821d0e94549ad5a/last/44150/index.html **Исключить**
- [9:13:19] **Yah** Найдено 1% совпадений по адресу: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-access-control> **Исключить**
- [9:13:25] **Yah** Найдено 1% совпадений по адресу: https://ir.nmu.org.ua/bitstream/handle/123456789/151389/Шевченко_Д.І..pdf?sequence=1 **Исключить**
- [9:13:35] **Yah** Найдено 1% совпадений по адресу: <https://www.linkedin.com/pulse/sid-share-internet-data-огляд-проекту-alina-ryabets> **Исключить**
- [9:13:52] **Yah** Найдено 1% совпадений по адресу: https://uk.wikipedia.org/wiki/Цензура_в_Інтернеті **Исключить**
- [9:14:07] **Yah** Найдено 2% совпадений по адресу: <https://trufflesuite.com/guides/lens-protocol/> **Исключить**
- [9:14:08] **Yah** Найдено 1% совпадений по адресу: <https://stackoverflow.com/questions/72588459/passing-variables-through-to-graphql-queries-in-external-queries-ts-file-in-reac> **Исключить**
- [9:14:09] **Yah** Найдено 1% совпадений по адресу: <https://mon.gov.ua/storage/app/media/innovatsii-transfer-tehnologiy/2019/02/06/3metodichni-rekomendatsii-shchodo-zabezpechennya-konfidentsiynosti-vidomostey-povyazanikh-z-dogovorami-ndr.doc> **Исключить**
- [9:14:13] **Yah** Найдено 1% совпадений по адресу: https://wiki.legalaid.gov.ua/index.php/Конфіденційна_інформація **Исключить**
- [9:14:26] **Yah** Найдено 1% совпадений по адресу: <https://blockchain-media.org/uk/bezopasnost-decentralizovannaja-identifikacija-s-pomoshhju-civic-secure-identity/> **Исключить**
- [9:14:40] **Yah** Найдено 1% совпадений по адресу: [https://uk.wikipedia.org/wiki/Соціальна_мережа_\(Інтернет\)](https://uk.wikipedia.org/wiki/Соціальна_мережа_(Інтернет)) **Исключить**
- [9:14:49] **Yah** Найдено 1% совпадений по адресу: <https://pozovna.in.ua/zrazki-listiv/list-providomlennya/> **Исключить**
- [9:15:03] **Yah** Найдено 1% совпадений по адресу: <https://support.microsoft.com/uk-ua/office/докладніше-про-стандарти-спільноти-microsoft-teams-безкоштовної-dfcf8b69-6566-4182-a9aa-89f523714f84> **Исключить**
- [9:15:21] **Yah** Найдено 1% совпадений по адресу: <https://support.microsoft.com/uk-ua/office/створення-діаграм-0baf399e-dd61-4e18-8a73-b3fd5d5680c2> **Исключить**
- [9:15:28] **Yah** Найдено 1% совпадений по адресу: <https://policies.google.com/privacy?hl=uk> **Исключить**
- [9:15:47] **Yah** Найдено 1% совпадений по адресу: <https://www.samsung.com/ua/support/mobile-devices/remove-accounts-from-your-galaxy-phone-or-tablet/> **Исключить**
- [9:16:00] Не загружена страница из запроса №258-1 (30072 миллисек., превышен таймаут в 30000 миллисек.): <https://support.google.com/googlenews/answer/7688469?hl=uk&co=GENIE.Platform=Android>
- [9:16:01] **Yah** Найдено 1% совпадений по адресу: <http://pzs.dstu.dp.ua/DataMining/social/bibl/SNA.pdf> **Исключить**
- [9:16:17] **Yah** Найдено 1% совпадений по адресу: <https://helpx.adobe.com/ua/acrobat/using/commenting-pdfs.html> **Исключить**
- [9:16:40] Не загружена страница из запроса №274-2 (30070 миллисек., превышен таймаут в 30000 миллисек.): <https://support.google.com/admob/answer/1355699?hl=uk>
- [9:16:47] **Yah** Найдено 1% совпадений по адресу: [https://prog.bobrodobro.ru/88958\(Сохраненная_копия\)](https://prog.bobrodobro.ru/88958(Сохраненная_копия)) **Исключить**
- [9:16:53] **Yah** Найдено 1% совпадений по адресу: <https://dou.ua/forums/topic/40575/> **Исключить**

[9:17:03] Не загружена страница из запроса №282-3 (30004 миллисек., превышен таймаут в 30000 миллисек.): <https://support.google.com/accounts/answer/7162782?hl=uk&co=GENIE.Platform=Android>

[9:17:19] **Yah**Найдено 1% совпадений по адресу: <https://learn.microsoft.com/uk-ua/dynamics365/project-operations/project-accounting/project-adjustments> **Исключить**

[9:17:44] **Yah**Найдено 1% совпадений по адресу: <https://sendpulse.ua/blog/creating-a-content-plan-for-instagram> **Исключить**

[9:18:22] Не загружена страница из запроса №312-1 (30069 миллисек., превышен таймаут в 30000 миллисек.): <https://support.google.com/tagmanager/answer/6103696?hl=uk>

[9:18:22] Не загружена страница из запроса №312-2 (30086 миллисек., превышен таймаут в 30000 миллисек.): <https://support.google.com/tagmanager/answer/12329709?hl=uk>

[9:18:36] **Yah**Найдено 1% совпадений по адресу: <https://www.quicknode.com/guides/ethereum-development/smart-contracts/solidity-vs-vyper/> **Исключить**

[9:18:45] **Yah**Найдено 1% совпадений по адресу: <https://greg.jeanmart.me/2019/08/14/managing-storage-in-a-java-application-with-ipfs/> **Исключить**

[9:18:47] **Yah**Найдено 1% совпадений по адресу: <https://www.howtogeek.com/784295/what-is-the-interplanetary-file-system-ipfs/> **Исключить**

[9:18:49] **Yah**Найдено 1% совпадений по адресу: <https://developers.cloudflare.com/web3/ipfs-gateway/concepts/ipfs/> **Исключить**

[9:18:52] **Yah**Найдено 1% совпадений по адресу: <https://support.google.com/tagmanager/answer/12329709?hl=uk>(Сохраненная копия) **Исключить**

[9:18:58] **Yah**Найдено 1% совпадений по адресу: <https://ethereum.org/en/developers/docs/evm/> **Исключить**

[9:18:58] **Yah**Найдено 1% совпадений по адресу: <https://ethereum.org/en/developers/docs/ethereum-stack/> **Исключить**

[9:19:08] **Yah**Найдено 1% совпадений по адресу: <https://webcase.com.ua/uk/blog/razrobotka-veb-prilozhenij-s-ispolzovaniem-python-i-django/> **Исключить**

[9:19:10] **Yah**Найдено 1% совпадений по адресу: <https://www.coindesk.com/consensus-magazine/2022/12/12/ethereum-virtual-machine-evm-future/> **Исключить**

[9:20:04] **Yah**Найдено 1% совпадений по адресу: <https://merehead.com/ua/blog/how-develop-smart-contract/> **Исключить**

[9:20:10] **Yah**Найдено 1% совпадений по адресу: https://uk.wikipedia.org/wiki/Аналіз_вимог **Исключить**

[9:20:18] **Yah**Найдено 1% совпадений по адресу: <https://www.epravda.com.ua/columns/2021/09/24/678133/> **Исключить**

[9:21:15] **Yah**Найдено 1% совпадений по адресу: <https://www.freecodecamp.org/news/introduction-to-react-hooks/> **Исключить**

[9:21:36] **Yah**Найдено 1% совпадений по адресу: <https://stackoverflow.com/questions/15711127/express-passport-node-js-error-handling> **Исключить**

[9:22:16] **Yah**Найдено 1% совпадений по адресу: <https://stackoverflow.com/questions/50320055/react-handlesubmit-with-axios-post-with-e-preventdefault-still-refreshe> **Исключить**

[9:22:24] Не загружена страница из запроса №398-3 (30038 миллисек., превышен таймаут в 30000 миллисек.): <https://help.webex.com/uk-ua/article/av6oo3/RedSky-Emergency-911-Service-for-Webex-Calling>

[9:22:25] **Yah**Найдено 1% совпадений по адресу: <https://docs.lens.xyz/docs/use-create-profile> **Исключить**

[9:23:00] **Yah**Найдено 1% совпадений по адресу: <https://dev.to/olesmartyniuk/dynamodb-5grc> **Исключить**

[9:23:11] **Yah**Найдено 1% совпадений по адресу: <https://ethereum.stackexchange.com/questions/125425/solidity-cannot-verify-ethers-js-signed-data-signtypeddata> **Исключить**

[9:23:15] Не загружена страница из запроса №412-1 (30042 миллисек., превышен таймаут в 30000 миллисек.): <https://support.google.com/googleplay/android-developer/answer/9888170?hl=uk>

[9:23:21] **Yah**Найдено 1% совпадений по адресу: <https://fondy.ua/uk/knowledge/digital-signature/> **Исключить**

[9:23:26] **Yah**Найдено 2% совпадений по адресу: <https://docs.lens.xyz/docs/create-follow-typed-data> **Исключить**

[9:23:42] **Yah**Найдено 1% совпадений по адресу: <https://docs.lens.xyz/docs/create-burn-profile-typed-data> **Исключить**

[9:24:03] **Yah**Найдено 1% совпадений по адресу: <https://sendpulse.com/ua/knowledge-base/crm/settings/manage-task-attributes> **Исключить**

[9:24:13] **Yah**Найдено 2% совпадений по адресу: <https://docs.lens.xyz/docs/creating-publications> **Исключить**

[9:24:20] **Yah**Найдено 1% совпадений по адресу: <https://docs.lens.xyz/docs/collecting-publications> **Исключить**

[9:24:25] **Yah**Найдено 2% совпадений по адресу: <https://github.com/lens-protocol/core/issues/118> **Исключить**

[9:24:49] **Yah**Найдено 1% совпадений по адресу: <https://docs.lens.xyz/docs/functions> **Исключить**

[9:24:56] **Yah**Найдено 1% совпадений по адресу: <https://github.com/lens-protocol/core/blob/main/contracts/libraries/DataTypes.sol> **Исключить**

[9:25:13] Не загружена страница из запроса №458-2 (30080 миллисек., превышен таймаут в 30000 миллисек.): <https://gist.github.com/JamJomJim/c327e256c0ad4edc86da11490e7f729b>

[9:25:26] **Yah**Найдено 2% совпадений по адресу: <https://github.com/lens-protocol/lens-protocol/issues/118> **Исключить**

[9:25:27] **Yah**Найдено 1% совпадений по адресу: https://csbc-edu.github.io/programming-essentials/homework/hw06_Python_intro.pdf **Исключить**

[9:25:34] **Yah**Найдено 1% совпадений по адресу: <https://gist.github.com/JamJomJim/c327e256c0ad4edc86da11490e7f729b>(Сохраненная копия) **Исключить**

[9:25:34] Тип проверки: *Стандартная* (Поисковики = Vi, Yah)

[9:25:34] ВНИМАНИЕ! Уникальность может быть определена некорректно! (Обнаружено ошибок: 29%)

[9:25:34] **Уникальность текста 90%** © (Проигнорировано подстановок: 0%)

4. БІЗНЕС ПЛАН

4.1. Опис проект

Проект являє собою анонімну соціальну мережу, засновану на технології блокчейн і токеноміки. Ця платформа призначена для користувачів, які цінують конфіденційність, безпеку і свободу вираження своїх думок та ідей.

Основна мета нашого проекту - створити безпечний і надійний простір для спілкування, де користувачі можуть вільно обмінюватися інформацією, взаємодіяти один з одним і отримувати винагороди за свою активність. Анонімність є ключовою особливістю нашої соціальної мережі, що дає змогу користувачам зберігати свою особистість у таємниці та уникати небажаного спостереження чи цензури.

Технологія блокчейн відіграє важливу роль у нашому проекті, забезпечуючи прозорість, непідробність даних і децентралізацію. Завдяки блокчейн, ми можемо гарантувати збереження інформації та забезпечити безпеку користувацьких акаунтів. Кожна дія, зроблена користувачами, буде записана в блокчейні, що створює прозорість і неможливість фальсифікації даних.

Токеноміка є невід'ємною частиною нашої соціальної мережі. Ми впроваджуємо токени, які будуть використовуватися як засіб обміну, винагород і стимулювання активності користувачів. Користувачі можуть отримувати токени за створення контенту, взаємодію з іншими користувачами, а також за участь у різноманітних акціях і конкурсах. Токени можна буде використовувати всередині платформи для купівлі привілеїв, розширених функцій або обміну на інші цифрові активи.

Анонімна соціальна мережа буде розроблена з урахуванням високих стандартів безпеки та конфіденційності. Ми будемо використовувати передові технології шифрування і захисту даних, щоб забезпечити безпеку особистої інформації користувачів. Крім цього, завдяки децентралізованій

природі блокчейна, ми зможемо запобігти односторонньому контролю і цензурі з боку централізованих структур.

Наш проект прагне створити нове співтовариство, де користувачі зможуть вільно висловлювати свої думки та ідеї, обмінюватися інформацією і будувати взаємини, не побоюючись за свою безпеку і конфіденційність. Ми впевнені, що анонімна соціальна мережа з використанням технології блокчейн і токеноміки має великий потенціал і здатна залучити широку аудиторію користувачів.

4.1.1. Цілі і задачі

Цілі:

Створити безпечний і анонімний простір для користувачів, де вони можуть вільно висловлювати свої думки та ідеї, не турбуючись про небажане спостереження або цензуру.

Побудувати активну і залучену спільноту користувачів, які активно обмінюються інформацією, взаємодіють один з одним і підтримують різноманітність точок зору.

Створити економічну модель, засновану на токеноміці, яка стимулює активність користувачів і винагороджує їх за внесок у розвиток платформи.

Забезпечити високий ступінь безпеки і конфіденційності даних користувачів, використовуючи передові технології блокчейн і шифрування.

Завдання:

Розробити і запусити функціональну та інтуїтивно зрозумілу платформу анонімної соціальної мережі.

Гарантувати анонімність і безпеку користувачів, забезпечуючи захист і шифрування особистих даних.

Впровадити технологію блокчейн для забезпечення прозорості та надійності даних, а також для запобігання фальсифікації інформації.

Розробити економічну модель токеноміки, що визначає структуру винагород, стимулює активність користувачів і підтримує зростання спільноти.

Залучити й утримати активних користувачів, розробляючи функції, які відповідають їхнім потребам та інтересам.

Провести маркетингові кампанії для залучення нових користувачів і встановлення позиції на ринку анонімних соціальних мереж.

4.1.2. Ключові переваги

Анонімність: Наша соціальна мережа надає високий рівень анонімності, даючи змогу користувачам висловлювати свої думки та думки без страху небажаного спостереження або репресій. Анонімність є основоположною перевагою, яка приваблює користувачів, які цінують свою конфіденційність.

Безпека: Ми надаємо великого значення безпеці даних користувачів. За допомогою технології блокчейн і шифрування ми забезпечуємо захист особистої інформації та запобігаємо несанкціонованому доступу.

Токеноміка та винагороди: Наша економічна модель, заснована на токенах, стимулює активність користувачів і винагороджує їх за їхній внесок у розвиток платформи. Користувачі можуть заробляти токени за створення якісного контенту, активну участь і залучення нових користувачів.

Децентралізація: Завдяки технології блокчейн, наша соціальна мережа має децентралізовану природу. Це означає, що немає єдиної контролюючої структури, що запобігає односторонній цензурі та забезпечує прозорість і незалежність даних.

Різноманітність і свобода вираження: Ми цінуємо розмаїття точок зору і надаємо користувачам свободу висловлювати свої думки та ідеї. Наша платформа заохочує відкритий діалог та обмін інформацією між користувачами.

Ці ключові переваги роблять нашу анонімну соціальну мережу привабливою для користувачів, які шукають безпечний, вільний і конфіденційний простір для спілкування та обміну інформацією.

4.2 Аналіз ринку соціальних мереж

Сьогодні ринок соціальних мереж є конкурентним і динамічно розвивається. Анонімні соціальні мережі, засновані на технології блокчейн і токеноміці, представляють відносно новий напрямок, але вже мають потенціал для успіху. Ось деякі ключові аспекти аналізу ринку:

Тенденції зростання: Соціальні мережі стають дедалі популярнішими і широко використовуються в усьому світі. Люди шукають платформи, які пропонують нові можливості та безпечніші умови для спілкування. Анонімні соціальні мережі можуть задовольнити цей попит і запропонувати альтернативу традиційним платформам.

Проблеми конфіденційності та безпеки: Останніми роками дедалі більше користувачів висловлюють занепокоєння щодо конфіденційності та безпеки своїх даних у соціальних мережах. Анонімні соціальні мережі надають можливість зберігати особистість у таємниці, що може бути привабливим для користувачів, яким важлива приватність.

Потреби спільноти: Існує потреба в платформі, яка дає змогу користувачам вільно висловлювати свої думки та ідеї, спілкуватися з однодумцями та знаходити підтримку в спільноті. Анонімні соціальні мережі можуть створити простір для таких взаємодій, де користувачі почувуються комфортно і вільно.

Технологічний прогрес: Технологія блокчейн, хоча й відносно нова, вже привернула значну увагу в різних галузях. Використання блокчейну в соціальних мережах може покращити прозорість, безпеку та надійність даних, що є привабливим фактором для користувачів.

4.2.1 Ідентифікація цільової аудиторії

Цільова аудиторія анонімної соціальної мережі на основі блокчейн і токеноміки може бути різноманітною. Ось кілька категорій користувачів, які можуть бути зацікавлені в такій платформі:

Активісти та захисники приватності: Люди, які цінують конфіденційність і безпеку своїх даних, можуть бути зацікавлені в анонімній соціальній мережі, що надає їм можливість висловлювати свої погляди без страху відстеження.

Люди, які бажають обговорювати чутливі теми: Анонімність може бути привабливою для тих, хто хоче обговорити питання, які можуть бути непопулярними або такими, що викликають суперечки у звичайних соціальних мережах.

Криптоентузіасти: Люди, зацікавлені в технології блокчейн і криптовалютах, можуть бути зацікавлені в соціальній мережі, яка використовує ці технології та пропонує токеноміку.

Люди, які шукають підтримку та поради: Анонімна соціальна мережа може привабити користувачів, яким потрібен анонімний простір для обговорення проблем, отримання порад і підтримки від інших користувачів.

4.2.2 Конкурентний аналіз

Конкурентний аналіз допоможе визначити сильні та слабкі сторони інших анонімних соціальних мереж на ринку. Ось деякі відомі конкуренти та їхні характеристики:

Whisper: Whisper є анонімною соціальною мережею, заснованою на технології блокчейн. Вона надає користувачеві можливість анонімно публікувати повідомлення і взаємодіяти з іншими користувачами. Однак у Whisper є обмеження у функціональності та активності спільноти.

Minds: Minds - це соціальна мережа, яка дотримується принципів свободи вираження та конфіденційності. Вона використовує технологію блокчейн для забезпечення безпеки даних. Minds пропонує

користувацький контент, винагороджуючи користувачів за активність на платформі.

Steemit: Steemit - це блогова платформа, яка також використовує технологію блокчейн і винагороджує користувачів за публікації та взаємодію з контентом. Вона пропонує можливість анонімних публікацій і захищає особисті дані користувачів.

Memo.cash: Memo.cash - це соціальна мережа на основі блокчейна Bitcoin Cash. Вона дозволяє користувачам публікувати повідомлення і коментарі, зберігаючи їх у блокчейні. Memo.cash забезпечує анонімність і свободу вираження поглядів.

4.2.3 Позиціонування на ринку

Для успішного позиціонування на ринку анонімних соціальних мереж, необхідно визначити унікальні особливості та переваги вашої платформи. Ось деякі способи позиціонування:

Анонімність і безпека: Основним фокусом вашої платформи може бути високий рівень анонімності та безпеки, які забезпечуються використанням технології блокчейн і шифрування даних. Це може привабити користувачів, яким важлива приватність.

Активна спільнота і залученість: Створення активної та залученої спільноти користувачів може бути однією з ключових особливостей вашої платформи. Спеціальні функції, що стимулюють взаємодію і винагороду за активність, допоможуть створити позитивну атмосферу і залучити нових користувачів.

Зручність використання: Забезпечення простоти використання та інтуїтивного інтерфейсу платформи буде ключовим фактором для залучення користувачів. Приділіть увагу розробці зручних функцій, які дозволять користувачам легко створювати та обмінюватися контентом.

Різноманітність контенту: Надання різноманітних типів контенту, таких як тексти, фотографії, відео, аудіо тощо, дасть змогу залучити різні категорії користувачів і створити багату екосистему.

Розширення можливостей за допомогою токенів: Використання токенів та економічної моделі на платформі може запропонувати користувачам додаткові можливості, як-от отримання винагород за активність, участь у голосуваннях або доступ до ексклюзивного контенту.

4.2.4 Попередня оцінка реалізації ціни реалізації продукту

Попередня оцінка залежить від багатьох факторів, таких як складність проекту, трудомісткість його розробки та реалізації, кількість спеціалістів, які займатимуться розробкою та інші. Вартість витрат на виробництво продукту також залежить від багатьох чинників, таких як вартість компонентів, витрат на розробку та виробництво прототипу, витрат на тестування тощо. Так як проєкт виконано, суто в наукових та теоретичних рамках, точної ціни реалізації не буде наведено. Але по ходу просування розділу є певні приклади.

4.3 Опис функціональності

Анонімна соціальна мережа на основі технології блокчейн і токеноміки пропонує таку функціональність:

Реєстрація та створення профілю: Користувачі можуть зареєструватися на платформі, створити анонімний профіль і налаштувати свої вподобання та інтереси.

Публікація контенту: Користувачі можуть створювати і публікувати різні типи контенту, такі як текстові повідомлення, зображення, відео, аудіозаписи та інші формати.

Взаємодія з контентом: Користувачі можуть коментувати, лайкати, ділитися і відзначати контент інших користувачів. Це сприяє активній взаємодії та обміну інформацією в спільноті.

Групи та спільноти: Платформа дає змогу користувачам створювати групи та долучатися до спільнот, які відповідають їхнім інтересам і поглядам. Це полегшує спілкування та обмін досвідом з однодумцями.

Особисті повідомлення: Користувачі можуть обмінюватися особистими повідомленнями один з одним, зберігаючи при цьому анонімність і приватність.

Механізм винагород: Користувачі отримують винагороди у вигляді токенів за активність на платформі, як-от створення якісного контенту, залученість у спільноту або залучення нових користувачів.

4.3.1 Анонімність та безпека

Анонімність і безпека є важливими аспектами анонімної соціальної мережі на основі блокчейн і токеноміки. Ось деякі заходи, що вживаються для забезпечення цієї функціональності:

Псевдоніми: Користувачі можуть використовувати псевдоніми замість своїх реальних імен, що дає їм змогу зберегти анонімність і запобігти прямій ідентифікації.

Шифрування даних: Усі дані, що зберігаються на платформі, захищені з використанням сучасних методів шифрування, щоб запобігти несанкціонованому доступу та зберегти конфіденційність.

Децентралізація: Блокчейн-технологія забезпечує децентралізовану природу платформи, що означає, що немає єдиної контролюючої сторони, яка може отримати доступ до особистих даних користувачів.

Управління узгодженнями: Користувачі мають повний контроль над своїми даними і можуть обирати, яку інформацію ділитися з іншими користувачами або групами.

Анонімний блокчейн: Використання технології блокчейн дає змогу зберігати анонімність користувачів під час транзакцій та обміну токенами, забезпечуючи безпеку та конфіденційність фінансових операцій.

Модерація контенту: Незважаючи на анонімність, платформа повинна мати систему модерації контенту, щоб запобігти поширенню незаконного або шкідливого матеріалу. Це допомагає підтримувати безпечне та позитивне середовище для всіх користувачів.

4.3.2 Модель монетизації

Модель монетизації анонімної соціальної мережі на основі блокчейн і токеноміки може включати такі аспекти:

Рекламні платежі: Платформа може запропонувати рекламним компаніям можливість розміщення реклами на своїй платформі. Це може включати як традиційні формати реклами, так і інноваційні методи, пов'язані з використанням токенів і блокчейна.

Преміум-акаунти: Користувачі можуть мати можливість поліпшити свій досвід використання платформи, підписавшись на преміум-акаунт. Преміум-акаунти можуть пропонувати додаткові функції та привілеї, як-от доступ до ексклюзивного контенту або можливість управління групами.

Комісії за транзакції: Платформа може стягувати невеликі комісії за транзакції, пов'язані з використанням токенів на платформі. Наприклад, під час переказу токенів між користувачами або під час купівлі спеціальних послуг чи контенту.

Співпраця з брендами і партнерами: Платформа може встановити партнерські відносини з брендами, компаніями або організаціями, пропонуючи їм доступ до цільової аудиторії або спеціальні рекламні можливості. Це може включати спонсорство контенту, проведення акцій або партнерські програми.

ICO або токенсейл: Платформа може провести первинне розміщення монет (Initial Coin Offering, ICO) або токенсейл, де інвестори можуть придбати токени платформи з метою їхнього майбутнього використання або отримання вигоди від їхнього зростання в ціні.

4.4 Команда проекту .

Кожен член команди повинен мати чітко визначені ролі та відповідальності.

Генеральний директор (СЕО):

Розробка стратегії проекту і досягнення поставлених цілей.

Керівництво командою та координація роботи всіх відділів.

Представлення проекту перед інвесторами, партнерами та іншими зацікавленими сторонами.

Технічний директор (СТО):

Розробка технічної стратегії та архітектури платформи.

Керівництво розробкою і підтримкою блокчейн-інфраструктури.

Забезпечення безпеки та захисту даних користувачів.

Розробники блокчейну:

Розробка і тестування смарт-контрактів і блокчейн-протоколів.

Підтримка та оновлення блокчейн-інфраструктури.

Робота з безпекою та усунення вразливостей.

Веб-розробники:

Розробка і підтримка веб-платформи та користувацького інтерфейсу.

Інтеграція функціональності блокчейн веб-додатка.

Оптимізація продуктивності та поліпшення користувацького досвіду.

Маркетинговий фахівець:

Розробка і реалізація маркетингової стратегії.

Залучення нових користувачів і просування платформи.

Встановлення партнерських відносин і проведення рекламних кампаній.

Спеціаліст з токеноміки:

Розробка економічної моделі та токеноміки платформи.

Визначення параметрів токенів, їх розподіл і використання.

Аналіз ринку та прогнозування впливу токенів на екосистему.

Команда підтримки користувачів:

Відповідь на запитання і вирішення проблем користувачів.

Проведення навчальних програм і підтримка користувачів у використанні платформи.

Зворотний зв'язок з користувачами та надання звітів команді розробки.

4.5 Фінансовий план

Для успішної реалізації проекту анонімної соціальної мережі з використанням технології блокчейн і токеноміки необхідно врахувати такі проектні витрати:

Розробка і програмування: Включає в себе витрати на розробку платформи соціальної мережі, створення унікальної функціональності, розробку блокчейн-технології та створення смарт-контрактів. Ці витрати включають оплату розробників, програмістів і технічного персоналу.

Інфраструктура: Включає витрати на серверне обладнання, хостинг, мережеву інфраструктуру та забезпечення безпеки системи. Ці витрати можуть варіюватися залежно від розміру проєкту і його потреб у масштабуванні.

Маркетинг і просування: Включає витрати на рекламні кампанії, маркетингові дослідження, створення контенту, управління соціальними медіа та просування бренду. Ці витрати спрямовані на залучення користувачів і створення обізнаності про нову соціальну мережу.

Правова та юридична підтримка: Включає витрати на консультації юристів, реєстрацію та ліцензування проєкту, захист інтелектуальної власності та дотримання законодавства в галузі криптовалют і блокчейна.

Операційні витрати: Включають витрати на адміністративні витрати, оренду офісу, заробітну плату співробітникам, обслуговування і технічну підтримку системи.

4.6 Прогноз доходів

Прогнозування доходів у випадку анонімної соціальної мережі, заснованої на токеноміці, може бути складним завданням, оскільки це

залежить від активності користувачів, залучення рекламодавців та інших факторів. Однак, слід враховувати такі джерела доходів:

Продаж токенів: можна випустити свій власний токен і запропонувати його користувачам платформи. Продаж токенів може принести значні доходи, особливо якщо попит на вашу соціальну мережу буде високим.

Комісії за транзакції: Як анонімна соціальна мережа, стягувати комісії за транзакції, які користувачі здійснюють всередині платформи. Це може бути комісія за купівлю або продаж токенів, переказ коштів або інші дії.

Рекламні партнерства: Можливо залучити рекламодавців, які розміщуватимуть свої оголошення всередині платформи. За це можна стягувати плату за розміщення реклами або отримувати комісію від кліків або покупок, здійснених користувачем.

Платні послуги: Запропонувати додаткові платні послуги, такі як розширені функції, додаткове сховище або привілейований доступ до певних контентів. Користувачі, зацікавлені в цих послугах, платитимуть додаткову плату.

4.7 Аналіз ризиків

При розробці та впровадженні анонімної соціальної мережі існують певні ризики, на які слід зважати. Ось деякі з них:

Технічні ризики: Пов'язані з розробкою та інфраструктурою. Можливі затримки в розробці платформи, помилки в коді, непередбачувані технічні проблеми та вразливості безпеки блокчейна. Необхідно приділити особливу увагу тестуванню та забезпеченню безпеки системи.

Ризики конфіденційності та безпеки: Анонімність є ключовою особливістю вашої соціальної мережі. Однак, існує ризик порушення конфіденційності та витоку особистої інформації користувачів. Необхідно

розробити і застосувати суворі заходи безпеки, шифрування даних і механізми анонімності.

Регулятивні ризики: У сфері блокчейну та криптовалют можливі зміни в законодавстві та регуляторному середовищі. Вам слід бути готовими до змін у правовому оточенні та застосовувати відповідні практики з метою дотримання вимог законодавства.

Ризики низької користувацької активності: Успіх анонімної соціальної мережі залежить від активності користувачів. Існує ризик, що користувачі не будуть достатньо активно використовувати платформу або масово не приймуть нову концепцію анонімності. Важливо провести маркетингові дослідження та стратегії для залучення й утримання активної користувацької бази.

Конкурентні ризики: Ринок соціальних мереж є конкурентним, і ви стикатиметеся з конкуренцією від уже встановлених соціальних мереж. Необхідно розробити унікальну пропозицію і стратегію просування, щоб залучити користувачів і виділитися на тлі конкурентів.

Ризики ринкової волатильності: Криптовалюти і ринок блокчейна можуть бути схильні до значної волатильності. Зміни в цінах криптовалют можуть вплинути на доходи проєкту і попит на токени всередині платформи. Слід враховувати цей фактор під час розроблення фінансової стратегії та планування бізнесу.

4.8 Висновок

На закінчення, розробка і запуск анонімної соціальної мережі з використанням технології блокчейн і токеноміки представляє великі можливості для створення інноваційного та затребуваного продукту. Проєкт має низку переваг, як-от підвищена анонімність і безпека користувачів, можливість заробітку та обміну токенами, а також унікальна функціональність і досвід використання.

Аналіз ринку соціальних мереж показав постійне зростання попиту на анонімні та безпечні платформи для спілкування. Ідентифікована

цільова аудиторія складається з користувачів, яким важлива приватність і анонімність, а також тих, хто прагне нових можливостей заробітку та обміну цінностями всередині соціальної мережі.

Конкурентний аналіз виявив відсутність прямих конкурентів з подібними характеристиками і функціональністю. Це дає нашому проєкту перевагу на ринку і можливість зайняти позицію лідера.

Ми розробили стратегії монетизації, засновані на моделі токеноміки, які дадуть нам змогу генерувати доходи через продаж токенів, комісії за транзакції та платні послуги. Ми також розробили план залучення фінансування, який включає пошук інвесторів, залучення коштів через попередній продаж токенів (ICO) і залучення користувачів за допомогою маркетингових і рекламних ініціатив.

У фінансовому плані ми проаналізували проєктні витрати і прогнозовані доходи, а також оцінили рентабельність і окупність проєкту. Ми впевнені, що наша анонімна соціальна мережа має потенціал для досягнення стабільного прибутку і зростання.

Управління ризиками є важливим аспектом нашого проєкту, і ми розробили стратегії управління ризиками для мінімізації та пом'якшення впливу можливих негативних ситуацій. Також ми бачимо низку можливостей для зростання і розширення, включно з розширенням на нові ринки, встановленням партнерств і впровадженням нових функцій та інновацій.

Ми пишаємося нашою командою проєкту, до складу якої входять досвідчені фахівці в галузі розробки, блокчейн-технологій, маркетингу та управління. Ми розподілили ролі та відповідальності, і у нас є план найму додаткових членів команди для підтримки та прискорення розвитку проєкту.

Загалом, наш бізнес-план є важливим кроком у створенні та розвитку успішної анонімною соціальною мережі з використанням технології блокчейн і токеноміки. Ми впевнені в потенціалі проєкту і готові

реалізувати його за допомогою стратегічних кроків, інноваційних рішень і сильної команди. Ми з нетерпінням чекаємо можливості реалізувати цей проєкт і створити цінність для наших користувачів та інвесторів.

ВИСНОВОК

У цій дипломній роботі було досліджено створення та реалізацію анонімної соціальної мережі з використанням технології блокчейн. Під час дослідження було розглянуто різні аспекти блокчейн-технології та її застосування в соціальних мережах, а також розглянуто переваги та обмеження використання анонімності в цьому контексті. Метою роботи було розробити прототип анонімної соціальної мережі, що забезпечує безпеку і конфіденційність для користувачів, і представити його ефективність та аналіз результатів.

Під час розроблення було виконано такі завдання: аналіз наявних анонімних соціальних мереж та їхніх недоліків, вивчення принципів роботи блокчейн-технології, визначення вимог до анонімної соціальної мережі, проектування та розроблення архітектури системи, створення користувацького інтерфейсу та реалізація функціональності, пов'язаної з безпекою та конфіденційністю.

У розробці анонімної соціальної мережі було реалізовано такі функціональності: створення анонімних акаунтів, шифрування повідомлень і даних користувачів, а також зберігання даних у блокчейн реєстрі.

На закінчення, розробка та дослідження анонімної соціальної мережі з використанням технології блокчейн являє собою важливу галузь у сфері інформаційної безпеки. Розроблений прототип є значущим внеском у забезпечення безпеки та анонімності в мережі. Подальші дослідження та вдосконалення можуть сприяти розвитку цієї технології та призвести до створення більш ефективних і надійних анонімних соціальних мереж.

У результаті цієї роботи було отримано цінні практичні та теоретичні результати, які можуть бути використані дослідниками та розробниками в галузі інформаційної безпеки та приватності в мережі. Також прототип може бути корисним для користувачів, які прагнуть обмінюватися інформацією анонімно та безпечно в соціальних мережах.

У першому розділі дипломної роботи було проведено аналіз предметної області та здійснено постановку задачі розробки анонімної соціальної мережі з використанням технології блокчейн.

У процесі аналізу було вивчено основні аспекти наявних соціальних мереж, їхні переваги та недоліки. Особливу увагу було приділено питанням приватності та анонімності користувачів. Було виявлено, що в сучасних соціальних мережах часто виникають проблеми, пов'язані з витоком персональних даних і порушенням приватності користувачів. Це призводить до втрати довіри користувачів і обмеження свободи вираження думок.

У другому розділі дипломної роботи було проведено проектування інформаційного забезпечення. Основною метою проектування було створення надійної, безпечної та анонімної платформи для обміну інформацією між користувачами.

У процесі аналізу наявних анонімних мереж було виявлено та вивчено основні проблеми, з якими вони стикаються.

Як основу для проектування було обрано технологію блокчейн. Блокчейн має властивості прозорості, безпеки та непорушності даних, що робить його ідеальним кандидатом для створення анонімної соціальної мережі. Шляхом використання блокчейн-технології, ми можемо створити децентралізовану платформу, де користувачі матимуть повний контроль над своїми даними та анонімністю.

У результаті проектування інформаційного забезпечення було розроблено діаграми, що відображають основні компоненти та взаємодію системи.

Ці діаграми є важливим інструментом для розуміння і візуалізації проєктованої системи. Вони дають змогу наочно уявити функціональність і взаємодію різних компонентів, а також слугують основою для подальшого розроблення та реалізації системи.

В третьому розділі було описано програмний інструментарій для подальшого створення програмного забезпечення. Було розроблено модулі

для аутентифікації та ідентифікації користувачів, обміну повідомленнями, і тд.

Четвертий розділ забезпечує інформацією щодо впровадження продукту на ринок. Описує задачу проектування продукту, фінансовий план, прогноз доходів, аналіз ризиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Антонов, В. М., & Широченко, О. В. (2021). Блокчейн та його додатки у сфері соціальних мереж. Інформаційні технології, системи управління, автоматика, (3), 59-68.
2. Беляков, Д. В., & Болтоногов, А. В. (2020). Блокчейн-технології в соціальних мережах: проблеми та перспективи. Інформаційне суспільство, (3), 42-47.
3. Васильєв, А. А., & Зайцев, А. А. (2019). Розподілені реєстри в соціальних мережах на основі технології блокчейн. Комунікації, Обчислювальні, Управляючі Системи, (7), 18-27.
4. Дмитрієв, А. І., & Черняєв, В. А. (2019). Блокчейн-технології в соціальних мережах: можливості та ризики. Проблеми інформаційної безпеки, (2), 23-28.
5. Іванова, О. І., & Чернишов, О. М. (2020). Використання технології блокчейн у соціальних мережах. Молодий вчений, (66), 144-146.
6. Капустян, В., & Кузнєцов, Ю. (2018). Використання блокчейн-технології в соціальних мережах. Матеріали Міжнародної науково-практичної конференції "Інформаційні технології в науці, освіті, економіці і бізнесі", 6-9.
7. Коновалов, О., & Черняк, І. (2018). Розподілені реєстри та блокчейн-технології в соціальних мережах. Інформаційні технології в освіті, науці, техніці та технологіях, (3), 86-92.
8. Лозовой, А., & Соколов, А. (2020). Використання блокчейн-технологій в соціальних мережах як інструмент забезпечення конфіденційності інформації. Молодий вчений, (10(90)), 51-54.
9. Buterin, V. (2013). Ethereum White Paper: A Next-Generation Smart Contract & Decentralized Application Platform. <https://ethereum.org/whitepaper/>
10. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
11. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303.
12. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.
13. Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. Procedia Computer Science, 98, 461-466.

14. Swan, M. (2017). *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*. O'Reilly Media.
15. Герасимов, В. А. (2019). Блокчейн: революція, яка вже тут. Видавничий дім "Супутник+".
16. Гришаєв, І. В., & Долгих, С. В. (2018). Аналіз і розробка моделей консенсусу в блокчейн-технології. *Інформаційні технології та обчислювальні системи*, 2(1), 73-80.
17. Левін, М. Ю. (2017). Блокчейн-технології в соціально-орієнтованих проєктах. *Молодий вчений*, 6(156), 98-100.
18. Ломакін, М. І., & Суркіс, О. М. (2019). Застосування блокчейн-технологій у соціальних мережах. *Інноваційний розвиток економіки*, 3(49), 120-125.
19. Міщенко, О. В., & Толстобров, О. В. (2020). Блокчейн-технології: понятійний апарат, застосування у сфері фінансів та перспективи розвитку. *Молодий вчений*, 8(110), 50-54.
20. Назарова, О. В., & Караулов, І. І. (2019). Аналіз можливостей використання блокчейн-технології в соціальних мережах. *Наукові відомості БелГУ. Серія: Математика. Фізика*, 46(8), 88-93.
21. Пузиревський, М. Л. (2019). Розвиток соціальних мереж на основі блокчейн-технологій. *Вісник Російського університету дружби народів. Серія: Інформатизація освіти*, 23(3), 461-471.
22. Слишкін, С. В., & Рибakov, В. А. (2019). Дослідження блокчейн-технологій у соціальних мережах та їх застосування. *Науковий журнал КубДАУ*, 148(04), 1-12.
23. Тихонов, В. А., & Зарембо, О. П. (2020). Перспективи використання блокчейн-технології в соціальних мережах. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філософія. Соціологія*, 31(70), 200-205.
24. Хайрутдінов, Р. Ш., & Кіреєв, А. А. (2018). Використання блокчейн-технології в соціальних мережах для забезпечення безпеки інформації. *Інноваційний розвиток економіки*, 6(44), 111-116.
25. Zohar, A. (2015). Ethereum: State of knowledge and research perspectives. In *International Conference on Financial Cryptography and Data Security* (pp. 469-485). Springer.
26. Herrera-Joancomartí, J., Gyarmati, L., & Buttyán, L. (2017). Efficient decentralized revocation for anonymous users in blockchain. In *International Symposium on Foundations and Practice of Security* (pp. 108-125). Springer.