Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Дипломна робота
магістра

з теми: **«ДОСЛІДЖЕННЯ МОДЕЛЕЙ ДЕЦЕНТРАЛІЗОВАНИХ ПЛАТФОРМ СОЦІАЛЬНИХ МЕРЕЖ»**

Виконав: студент KN1-M22 групи
спеціальності 122 Комп’ютерні науки
Літвін Роман Юрійович

Керівник: **Смалько О.А.,**
кандидат педагогічних наук,
доцент кафедри комп’ютерних наук

Рецензент: **Тулашвілі Ю.Й.,**
доктор педагогічних наук, професор
кафедри комп’ютерних наук Луцького
національного технічного університету

Кам’янець-Подільський – 2023

ЗМІСТ

ВСТУП

Децентралізовані соціальні мережі стають стратегічно важливим напрямком розвитку у сфері інформаційно-комунікаційних технологій. Необхідність вирішення сучасних викликів, таких як забезпечення конфіденційності даних, безпеки взаємодії та прагнення до децентралізованого контролю над інформацією акцентує увагу на потребі розробки нових способів віртуального спілкування, які враховують ці аспекти.

Актуальність обраної теми зумовлена необхідністю впровадження нових програмно-апаратних платформ, комунікаційних середовищ та інноваційних технологій захисту конфіденційності для підтримки зручних і безпечних форматів віртуального спілкування, які зможуть враховувати всі запити, що постійно з'являються в умовах швидкоплинних тенденцій. Саме децентралізований підхід до побудови соціальних мереж наразі вбачається перспективним рішенням, що може забезпечити якісно новий рівень взаємодії користувачів у віртуальному просторі. Однією з ключових ідей цього розвитку може стати поєднання піринговых технологій та блокчейну для створення безпечних мереж, які дозволять користувачам максимально комфортно, вільно та конфіденційно користуватися інформаційними каналами, забезпечуючи при цьому ефективний та надійний обмін інформацією.

Об'єкт дослідження — децентралізовані соціальні мережі.

Предмет дослідження — архітектура, принципи та технічні аспекти функціонування, а також соціальний вплив децентралізованих соціальних мереж.

Мета кваліфікаційної роботи полягає у комплексному дослідженні архітектурних рішень і технологій, що лежать в основі децентралізованих платформ соціальних мереж, а також у розробці робочого прототипу простої розподіленої соціальної мережі, в якій поєднується дві найбільш поширені у наш час технологій (блокчейну та peer-to-peer).

Досягнення мети передбачає виконання таких *завдань*:

1. Дослідити теоретичні основи та етапи розвитку децентралізованих соціальних мереж, оцінити їхні переваги і недоліки.
2. Проаналізувати функціональні можливості доступних для використання децентралізованих соціальних мереж та оцінити діапазон реалізованих у них соціальних взаємодій.
3. Спроєктувати архітектуру соціальної мережі з використанням передових технологій децентралізації, криптографії та блокчейну.
4. Розробити проєкт простої децентралізованої соціальної мережі, в якій поєднується модель розподіленого зберігання даних у вигляді блокчейну та пірингових протоколів, використання яких дозволяє безпечно обмінюватися інформацією.

Методи дослідження. Для реалізації мети та завдань кваліфікаційної роботи було використано наступні загальнонаукові та спеціальні методи: теоретичне дослідження, історичний і логічний методи, індуктивне дослідження, порівняння, емпіричний аналіз і синтез, описовий метод, структурно-функціональний аналіз, аналогія, структурно-генетичний аналіз і синтез, експериментальне моделювання.

Наукова новизна кваліфікаційної роботи полягає у розробці прототипу децентралізованої соціальної мережі, в якому поєднується використання технології блокчейну для забезпечення прозорості операцій інформаційної взаємодії, а також архітектурна пірингова модель для підтримки високого рівня розподіленості мережевих вузлів та анонімності користувачів,

Практичне значення результатів дослідження. Представлені у роботі основні теоретичні положення, фактичний матеріал та приклад реалізації децентралізованої соціальної мережі можуть бути використані під час опанування сучасних технологій комунікаційних мереж, вивчення відповідних спеціалізованих навчальних дисциплін у ЗВО, а також для всіх зацікавлених осіб, які прагнуть знайти в інформаційному просторі зручне та безпечне середовище обміну інформацією для особистого та/або професійного спрямування.

Апробація результатів дослідження здійснена у вигляді тез доповіді у збірнику матеріалів наукової конференції здобувачів вищої освіти фізико-

математичного факультету Кам’янець-Подільського національного університету імені Івана Огієнка (1 листопада 2023 року) [1].

Структура роботи: робота складається з вступу, трьох розділів, висновків, двох додатків та списку використаної літератури. Загальний обсяг роботи — 76 сторінок, з них 60 сторінок основного тексту. Текст містить 11 рисунків. Список використаних джерел на 6 сторінках складається з 64 позицій.

РОЗДІЛ 1.
АНАЛІЗ ДЕЦЕНТРАЛІЗОВАНИХ СОЦІАЛЬНИХ МЕРЕЖ: ТЕОРІЯ РІЗНОВИДІВ ПЛАТФОРМ

1.1. Теоретичні основи децентралізованих соціальних мереж

Активна глобалізація та трансформація інформаційного світу диктує нові правила інтернет-користувачам, тому прагнення людей посилити конфіденційність свого спілкування є природним, особливо в останні роки. З появою технологій Web 3.0, які стоять в основі принципу децентралізації, світ цифрових мереж постійно змінюється. Децентралізація в контексті Web 3.0 — відхід від централізованих структур, де повноваження та контроль зосереджені в одних руках, серверах тощо. Така зміна парадигми розділяє дані, обчислювальну потужність і мережеві сховища, а також надає контроль в руки користувачів. Фактично Web 3.0 — концепція нової ітерації розвитку інтернет-середовища, згідно з якою мережа стає децентралізованої і здебільшого базується на блокчейнах [53].

Централізовані мережі характеризуються схильністю до цензури та втрати даних, тоді як децентралізація Web 3.0 робить дані більш стійкими до хакерських атак і збоїв системи. Завдяки відсутності єдиної точки контролю децентралізовані мережі стають надійними, цілком сумісними з іншими способами зберігання даних та забезпечують їх надійне збереження, закладаючи основу для більш надійної цифрової інфраструктури [23].

Наприклад, такі рішення як IPFS, Filecoin і GhostDrive широко використовуються для децентралізованого зберігання даних й пропонують ефективну заміну централізації завдяки використанню однорангових мереж і розподілених обчислювальних ресурсів [59].

Переваги децентралізованого зберігання даних насправді численні. Адже цей спосіб зберігання не тільки забезпечує надійність даних, усуваючи централізовані точки контролю, але й покращує взаємодію між компонентами

систем, забезпечуючи гнучкий доступ через різні робочі процеси, кодові бази та інструменти. При цьому резервування є ключовою функцією процесів, коли кілька вузлів мережі одночасно зберігають і отримують файли, забезпечуючи доступність даних, навіть якщо окремі вузли виходять з ладу. Виникнення децентралізованих віртуальних середовищ — це закономірність, а не лише парадигма сучасності, це реальна потреба для цифрового суспільства.

Децентралізована соціальна мережа — служба соціальних мереж, яка децентралізована та розподілена між різними постачальниками послуг (подібно до електронної пошти, але для соціальних мереж), таких як Fediverse або IndieWeb [19]. З суспільної точки зору цю концепцію можна порівняти з концепцією того, що соціальні медіа є суспільно корисними. Наприклад, в тому випадку, коли кількість послідовників ідеології тан пінг або хікікоморі раптом збільшиться, постане питання комунікації. Тоді, за аналогією із комунальним підприємством, яке вважається монополією, бо «не може працювати ефективно та економічно, якщо не користується монополією на своєму ринку», комунікацію будуть забезпечувати соцмережі. Теоретично вважається, що комунальне підприємство обслуговує 100% свого ринку. Якщо соцмережа теж володітиме подібною монополією, таким чином соціальна корисність децентралізованих соцмереж збільшиться, оскільки власники звичних соцмереж іноді блокують окремих користувачів (на їхню думку, порушників, приклад Венесуели, Японії).

У децентралізованих соцмережах:

- немає єдиного центру управління;
- немає багатосторінкових моральних та етичних кодексів, яких ви зобов’язані дотримуватися;
- інформація зберігається на нодах (незалежних вузлах) — численних комп’ютерах, які підтримують роботу певної соціальної мережі;
- особисті дані не зберігаються (або зберігаються у зашифрованому вигляді) і не передаються третім особам — так зберігається анонімність під час використання.

Принцип розподіленості в соціальних мережах забезпечує більшу свободу, конфіденційність та безпеку для користувачів, а також покращує стійкість та ефективність всієї системи. Принцип розподіленості означає, що різні фрагментовані частини соціальних мереж забезпечують спілкування користувачів окремих їхніх компонентів завдяки широко використовуваним та відкритим стандартизованим протоколам зв'язку [33].

Загалом для належної візуалізації зв’язків та відношень компонентів комп’ютерних соціальних мереж можна використовувати дослідницький метод *аналіз децентралізованих соціальних мереж* (англ. social network analysis, SNA), що є міждисциплінарним інструментарієм математики (теорія графів), теорії складних систем, науки про статистику, системного аналізу, соціології та навіть психології.

На основі багатьох інформаційних джерел проаналізовано методологію мережевого аналізу (рис. 1.1), основні концепції пов’язані з аналізом соціальних мереж і сучасні тенденції у дослідженні цієї області [16].

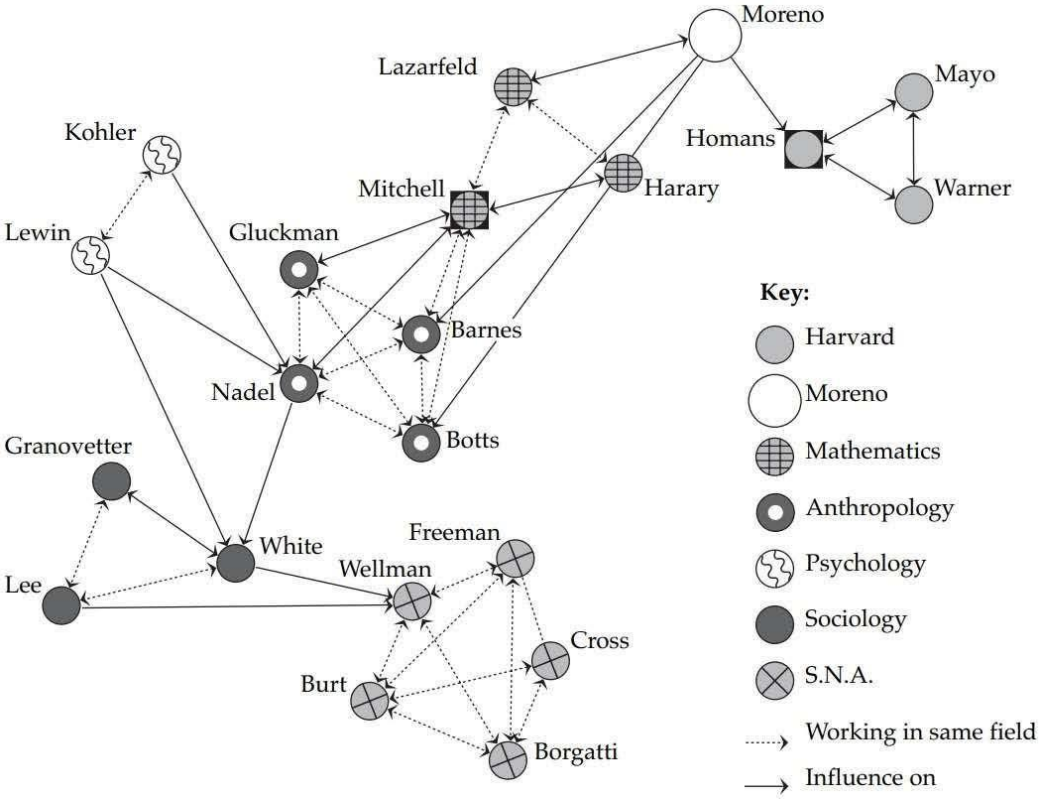


Рис. 1.1. Історія та впливові особи
в аналізі децентралізованих соціальних мереж (SNA)

Зважаючи на зростання обсягу інформації та розвиток технологій, мережний аналіз стає необхідним інструментом для розуміння соціальних структур та взаємодій. Спільно з тим, аналіз децентралізованих соціальних мереж відкриває нові можливості для дослідження, розширюючи традиційні методи та розкриваючи потенціал для подальших інновацій у цій галузі.

У висновку можна зазначити, що розподілені соціальні мережі не лише трансформують спосіб спілкування, але і відкривають нові перспективи для дослідження та розуміння складних соціальних структур, забезпечуючи простір для подальшого розвитку та інновацій у галузі вивчення взаємодій між людьми.

1.2. Переваги та недоліки децентралізованих соціальних мереж у порівнянні з традиційними

Недоліки традиційних платформ таких як Facebook були достатньо висвітлені протягом останніх років. Останні обговорення підняли рівень уваги до безпеки зберігання особистих даних та додали додаткові питання щодо бренду Facebook, особливо у контексті експлуатації приватності. Відомо, що Facebook використовує так звану бульбашку фільтрів, тобто весь контент, що бачить користувач залежить від того контенту, який йому більше до вподоби [35]. Як наслідок, користувачі відділяються від інформації, яка не відповідає їхнім точкам зору, фактично вони ізольовані у власних культурних або ідеологічних бульбашках. Відповіддю на це стала розробка децентралізованих соціальних мереж.

Децентралізовані соціальні мережі стійкі до цензури й відкриті для всіх [20]. Це означає, що користувачів не можна заблокувати, видалити дані чи довільно обмежити. Децентралізовані соціальні мережі побудовані на ідеалі відкритого вихідного коду й роблять вихідний код програм доступним для загального огляду. Усуваючи реалізацію непрозорих алгоритмів, поширених у традиційних соціальних медіа, соціальні мережі на основі блокчейну можуть узгоджувати інтереси користувачів і творців платформи. Децентралізовані соціальні мережі усувають «посередника». Творці контенту мають безпосереднє право власності на

свій контент і взаємодіють безпосередньо з підписниками, шанувальниками, покупцями та іншими сторонами, не маючи нічого, крім розумного контракту між ними.

Децентралізовані соціальні платформи пропонують покращену систему монетизації для творців контенту за допомогою невзаємозамінних токенів (NFT), криптоплатежів у програмі тощо. Також вони забезпечують користувачам високий рівень конфіденційності й анонімності. Децентралізовані соціальні мережі покладаються на децентралізоване сховище, яке значно краще захищає дані користувачів, а не на централізовані бази даних.

Хоча платформи соціальних медіа Web2.0 мають переваги та виклики, технологія Web3.0 може значно покращити простір. Ключовим флагманом цієї зміни є децентралізовані мережі соціальних медіа — новий тип соціальних мереж, які працюють децентралізовано. Це забезпечує більшу конфіденційність і безпеку та надає користувачам контроль над своїми даними, цифровою ідентифікацією та вмістом, сприяючи прозорості, оскільки будь-хто може переглядати дані в будь-який час.

Соціальні платформи, засновані на блокчейні, мають на меті сприяти свободі слова та забезпечувати опір цензурі, при цьому жодна центральна влада не контролює та не маніпулює вмістом. Крім того, жодна третя сторона не може володіти, збирати або продавати дані користувачів [4].

Крім того, соціальні мережі Web3.0 часто використовують взаємозамінні та незамінні токени (NFT) як нові способи монетизації вмісту. Таким чином, децентралізовані соціальні мережі — це не просто зміна інфраструктури централізованих платформ Web2.0; вони також змінюють метод того, як компанії децентралізованих соціальних мереж заробляють гроші. Соціальні мережі Web3.0 використовують блокчейни для зберігання та керування платформою, її даними та вмістом.

До *переваг децентралізованих соціальних мереж* можна віднести вищий рівень конфіденційності та анонімності. Тобто користувачі мають можливість контролювати доступ до своєї особистої інформації завдяки розподіленню даних

між різними вузлами мережі. Це дозволяє уникнути концентрації особистих даних на центральних серверах, зменшуючи ризик несанкціонованого доступу. Також, децентралізовані соціальні мережі надають користувачам більше можливостей для залишення анонімними чи використання псевдонімів, що важливо для тих, хто цінує свою приватність та не хоче розкривати свою особистість під час взаємодії в мережі. Такий підхід забезпечує не лише вищий рівень захисту особистої інформації, а й стимулює довіру користувачів до платформи, оскільки вони відчувають більше контролю над тим, як їхні дані використовуються.

Окрім цього, забезпечується високий рівень безпеки від цензури та втручання. Однією з ключових переваг децентралізованих соціальних мереж є їхня стійкість до цензури та втручання. Оскільки дані розподілені по різних вузлах, централізоване втручання або цензура стає значно складнішою задачею. Це особливо важливо в країнах з обмеженими свободами слова, де децентралізовані мережі можуть служити засобом вільного висловлення і обміну інформацією. Децентралізовані платформи можуть стати захистом від цензорських обмежень та забезпечити безпеку висловлювань користувачів, що сприяє розвитку відкритого обговорення і розмаїттю точок зору в мережі.

Ще однією важливою перевагою децентралізованих соціальних мереж є можливість активної участі користувачів у процесах управління та прийняття рішень. Деякі платформи використовують технології блокчейн для реалізації голосування за різні аспекти розвитку мережі. Це визначається як спроба надати спільноті більше влади над платформою та створити більш демократичне середовище для прийняття стратегічних рішень. Активна участь користувачів в управлінні мережею може сприяти виникненню більш адаптивної та відкритої платформи, яка враховує різноманітність потреб та поглядів спільноти [61].

Попри переваги, децентралізовані соціальні мережі також стикаються з недоліками, серед яких низька стійкість до різноманітних атак та зловживань. Мережі, побудовані на принципах децентралізації, можуть бути вразливі до 51%-атак, коли зловмисник отримує контроль над більше половини вузлів, що може веде до маніпуляції даними та порушення безпеки [45]. Також виникнення нових

технічних вразливостей чи брак адекватних захисних заходів може призвести до можливості зловживань та порушення безпеки особистих даних.

Ще однією проблемою є складніше впровадження деяких функцій у децентралізованих соціальних мережах. Розподілені структури можуть зробити важкими завдання, які легко реалізуються на централізованих платформах, такі як миттєве оновлення чи швидку передачу великої кількості даних. Складніше впровадження функцій може обмежувати зручність та функціональність децентралізованих соціальних мереж порівняно з традиційними аналогами.

Важливим аспектом дослідження переваг децентралізованих соціальних мереж є їх порівняння з традиційними соціальними мережами, що є корисним для визначення переваг та особливостей децентралізованих підходів у контексті соціальних мереж. Ось кілька ключових причин, чому це порівняння є важливим:

1. Інновації та передові технології: визначення переваг децентралізованих підходів сприяє використанню передових технологій, таких як блокчейн та peer-to-peer, що можуть принести інновації у сферу соціальних мереж.
2. Захист користувачів: розуміння відмінностей у рівні захисту та конфіденційності допомагає створювати мережі, які дозволяють користувачам краще контролювати свої дані та залишатися захищеними від можливих загроз.
3. Свобода вираження думок та приватність: забезпечення аналізу різниці у підходах допомагає створювати платформи, які сприяють свободі виразу та анонімності, що може бути важливим аспектом для користувачів.
4. Гнучкість та відкритість: порівняння дозволяє визначити, наскільки гнучкими та відкритими можуть бути децентралізовані соціальні мережі у порівнянні з традиційними платформами.
5. Вибір технологій: визначення ролі технологій, таких як блокчейн, у розбудові децентралізованих соціальних мереж, допомагає обирати оптимальні інструменти для реалізації конкретного проєкту.

Розуміння відмінностей привертає увагу дослідників, що може призвести до подальших наукових досліджень та розвитку нових підходів до соціальних мереж. Отже, порівняння визначає напрямки розвитку соціальних мереж, спираючись на

технологічні та концептуальні особливості децентралізованих систем. В цьому контексті слід виділити такі характеристики:

- Централізований контроль та менший рівень конфіденційності. У порівнянні з децентралізованими платформами, традиційні соціальні мережі характеризуються централізованим контролем, що може призводити до меншого рівня конфіденційності. Оскільки дані зазвичай зберігаються на центральних серверах, існує вищий ризик для безпеки та приватності особистої інформації користувачів. Централізований контроль також може стати причиною збільшення ризиків витоку інформації або її неправомірного використання з боку адміністраторів мережі.
- Зручність та швидкодія. Традиційні соціальні мережі відомі своєю високою швидкодією та зручністю використання. Оптимізовані для централізованого сервера, вони забезпечують швидку обробку запитань та ефективну передачу даних. Це забезпечує зручність користувачам та сприяє популярності традиційних соціальних мереж, особливо серед тих, хто цінує простоту та легкість використання платформи.
- Масовий доступ та популярність. Однією з головних переваг традиційних соціальних мереж є їхня масовість та висока популярність. Ці платформи мають широкий коло користувачів, що створює великий потенціал для соціальної взаємодії та обміну інформацією. Масовий доступ також означає, що традиційні соціальні мережі можуть служити важливим засобом комунікації та взаємодії для широкого кола користувачів, що робить їх важливими для побудови віртуальних спільнот та розвитку онлайн-культури.

Результати порівняльного аналізу традиційних та децентралізованих соціальних мереж визначають перспективні напрямки для майбутнього розвитку цих платформ. Однією з ключових відмінностей є рівень конфіденційності, де децентралізовані системи виходять переможцями завдяки відсутності централізованого контролю із ймовірним меншим ризиком витоку особистої інформації. Традиційні соціальні мережі вражають своєю швидкодією та зручністю використання, оптимізовані для централізованого сервера. Це

забезпечує швидку обробку запитань та ефективну передачу даних, але при цьому може обмежувати ступінь приватності користувачів.

З іншого боку, децентралізовані соціальні мережі надають користувачам більше контролю над їхніми даними і розподілом влади. Це стає ключовим аспектом для тих, хто приділяє велике значення конфіденційності та безпеці в онлайн-середовищі. Масовий доступ та популярність залишаються сильними сторонами традиційних соціальних мереж, адже широкий коло користувачів визначає їхню суспільну важливість та можливість формування великих спільнот. Проте, децентралізовані підходи також можуть привертати користувачів через більший рівень приватності та контролю.

Розуміння цих різниць визначає нові реалії для майбутнього розвитку соціальних мереж, підкреслюючи важливість досліджень у цьому напрямку та необхідність врахування користувацьких потреб і технологічних можливостей для створення ефективних та безпечних платформ для спілкування в онлайн-середовищі.

Висновок до розділу 1

В цьому розділі виконано глибокий огляд соціальних мереж, визначаючи їхню важливу роль у сучасному світі. Соціальні мережі стали не тільки засобом особистого спілкування, а й потужним інструментом для розвитку бізнесу та громадськості, розповсюдження інформації та формування соціальних зв'язків. Децентралізовані соціальні мережі представляють сучасну тенденцію, пропонуючи альтернативу традиційним мережам і підкреслюючи значення конфіденційності та безпеки даних користувачів. Метод аналізу концепцій соціальних мереж відкриває нові можливості для вивчення зв'язків та взаємодій в онлайн-середовищі. Важливою частиною цього аналізу є візуалізація структури мережі та вивчення основних концепцій, пов'язаних з дослідженням соціальних взаємозв'язків.

РОЗДІЛ 2.
ХАРАКТЕРИСТИКА МОДЕЛЕЙ ПОБУДОВИ ДЕЦЕНТРАЛІЗОВАНИХ СОЦІАЛЬНИХ МЕРЕЖ

2.1. Модель peer-to-peer

Модель peer-to-peer у контексті децентралізованих соціальних мереж являє собою унікальний підхід, де користувачі можуть спілкуватися напряму один з одним, обмінюючись даними без посередництва централізованого сервера [57].

Історія розвитку пірингової моделі налічує кілька ключових етапів, від зародження ідеї peer-to-peer моделі до сучасних реалізацій:

1. *Зародження ідеї peer-to-peer (1990-2000 рр.):* початкова концепція peer-to-peer виникла в середині 1990-х років, коли виникли технології, що дозволяли пристроям підключатися один до одного без централізованого посередника. У 2001 році було представлено протокол BitTorrent, який революціонізував обмін файлами, дозволяючи користувачам обмінюватися контентом напряму між собою. Цей протокол відрізняється від класичних методів завантаження файлів тим, що використовує підхід peer-to-peer (peer-to-peer), де користувачі, які завантажують файл, одночасно служать і як джерело для інших користувачів.
2. *Етап експансії (2000-2010 рр.):* у цьому десятилітті спостерігався значний розвиток peer-to-peer технологій, що призвело до появи різноманітних платформ, включаючи файлообмінні мережі, такі як eDonkey та Gnutella. Peer-to-peer почали використовувати не тільки для обміну файлами, а й для інших цілей, включаючи спільне використання обчислювальних ресурсів.
3. *Децентралізовані соціальні мережі (2010-2020 рр.):* з появою інтересу до децентралізації в соціальних мережах з'явилися проєкти, такі як Secure Scuttlebutt. Ця мережа дозволяє користувачам спілкуватися та обмінюватися даними напряму між вузлами, при цьому кожен користувач має свій власний журнал подій.
4. *Сучасні реалізації (з 2020 р.):* сьогоднішні децентралізовані соціальні мережі, наприклад Diaspora, використовують підходи peer-to-peer для

забезпечення безпеки та приватності користувачів. Ці платформи дозволяють створювати і управляти власним контентом, обмінюючись ним без посередництва централізованого сервера (рис. 2.1).

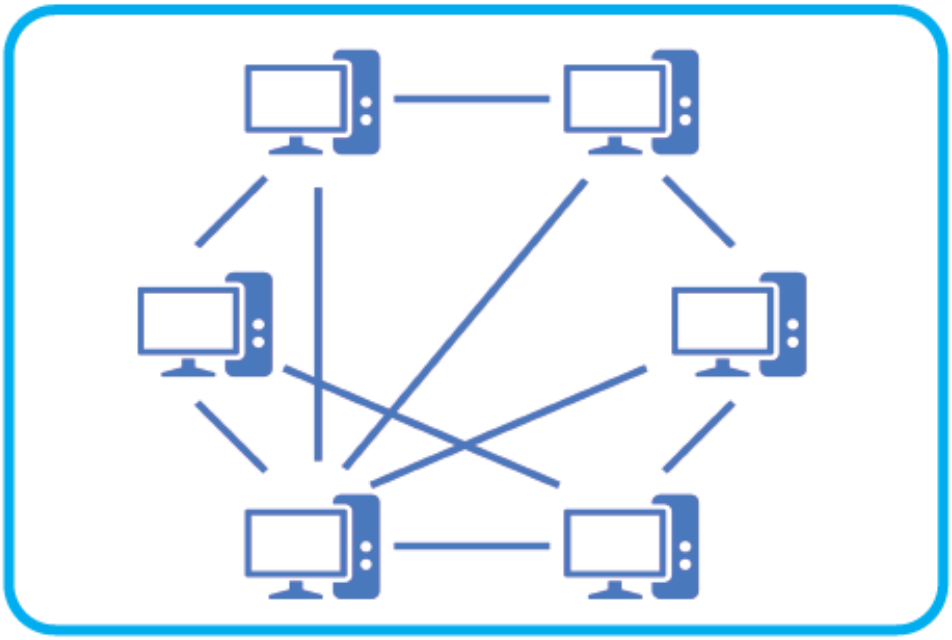


Рис. 2.1. Процес обміну даними між користувачами

Особливістю моделі peer-to-peer є відсутність центрального посередника, що дозволяє користувачам взаємодіяти безпосередньо. Масштабованість і надійність визначаються в традиційних термінах розподілених систем, таких як використання пропускної здатності — скільки систем може бути доступно з одного вузла, скільки систем може бути підтримано, скільки користувачів може бути підтримано і скільки пам'яті може бути використано. Надійність пов'язана з відмовами систем і мережі, відключенням, доступністю ресурсів тощо [31].

Кожен учасник може виступати як клієнт і сервер одночасно, що робить систему більш гнучкою та менш вразливою до відмов. Забезпечення безпеки визначається використанням шифрування та механізмів аутентифікації, що надає кожному користувачеві унікальний ключ для конфіденційності та цілісності інформації. Файли розділяються на шматки, які обмінюються паралельно між користувачами, що пришвидшує процес передачі та зменшує час завантаження. Окрім цього, використання механізмів кешування дозволяє зберігати та

використовувати локальні копії популярних ресурсів, що підвищує ефективність обміну даними.

Також peer-to-peer дозволяє забезпечити реалізацію систем рейтингів, що визначає довіру між користувачами, що допомагає уникнути неправдивих джерел та забезпечує безпечну комунікацію [55]. Ще однією перевагою peer-to-peer моделі є можливість резервного копіювання даних на різних вузлах, що допомагає уникнути втрати інформації та забезпечує надійність мережі. Модель peer-to-peer виявилася альтернативою моделі клієнт/сервер і перспективною парадигмою для грід-обчислень, обміну файлами, передачі голосу через IP, резервного копіювання та зберігання даних [18]. Деякі з недавніх спроб побудови високодоступного сховища або системи резервного копіювання на основі парадигми peer-to-peer включають OceanStore [39], CFS, Total Recall [17], [13] та UbiStorage. Вони є прикладом розподілених систем зберігання даних peer-to-peer, з більш ніж 100 мільйонами збережених файлів, де вузол може одночасно бути постачальником і клієнтом.

До особливостей цієї моделі дослідники також відносять й те, що у peer-to-peer відсутній централізований сервер. Така характеристика виключає проблему сінгл-пойнту-фейлу, що забезпечує більшу стійкість та надійність мережі. Peer-to-peer сприяє спільним зусиллям утримання та розвитку мережі, де кожен учасник відіграє активну роль у функціонуванні системи. Ці технічні особливості роблять peer-to-peer модель дуже привабливою для децентралізованих соціальних мереж, пропонуючи ефективний та безпечний обмін інформацією між користувачами.

Прикладом реалізації цієї моделі є платформа є Secure Scuttlebutt, де кожен користувач має власний журнал подій, а дані реплікуються між вузлами без втручання централізованого сервера. Secure Scuttlebutt (SSB) — децентралізована платформа для створення соціальних мереж, яка виникла як відповідь на прагнення створення безпечного та приватного спілкування в Інтернеті. Однією з таких альтернатив є проєкт під назвою Secure Scuttlebutt (SSB), який стартував у 2014 році та була розроблена Домініком Тар. SSB використовує концепції peer-to-peer для забезпечення обміну повідомленнями, контентом та даними між

користувачами. Такий підхід дозволяє забезпечити безпеку та приватність даних, оскільки вони не зберігаються централізовано та залежать від конкретного вузла. Деякі основні ідеї, що лежать в основі SSB, можна простежити ще з дев'яностих років, наприклад, безпечне ведення журналу [42] та безпечне відносне позначення часу [28]. Після кількох ітерацій розробки та впровадження протоколу та впровадження, SSB став стабільним сервісом, пропонуючи користувачам додатки для мультимедійної спільноти з потужним криптографічним захистом (наскрізним криптографічним захистом (наскрізне шифрування та метадані конфіденційність) і працює в чистому піринговому режимі [50]. Детальну реалізацію прикладу глобальної криптографічної соціальної мережі, що базується на SSB описано у Додатку Б.

Однією з ключових переваг моделі peer-to-peer є її стійкість до відмов та можливість працювати в умовах обмеженого мережевого доступу [30]. Також, вона сприяє створенню глобальних децентралізованих соціальних мереж, де кожен учасник має рівний статус та можливість взаємодіяти безпосередньо з іншими користувачами.

Завдяки поєднанню ідей peer-to-peer із децентралізацією соціальних мереж, створюються інноваційні платформи, спрямовані на забезпечення більшої автономії, прозорості та влади користувачів над їхніми особистими даними в цифровому просторі.

2.2. Модель на основі блокчейну

Модель на основі блокчейну в децентралізованих соціальних мережах являє собою технологічний фреймворк, в якому використовується блокчейн для організації та забезпечення функціональності в контексті соціальних мереж [38]. Децентралізовані соціальні мережі, засновані на блокчейні, пропонують розподілену структуру, де дані та контент керуються технологією блокчейн для забезпечення безпеки, прозорості та відсутності централізованого управління.

Блокчейн, англійська назва якого визначається як «зв'язаний список» (англ. blockchain) — це неперервний ряд блоків, що побудований відповідно до конкретних правил та містить інформацію [44]. Тобто, інформація групується в блоки, кожен з яких містить в собі унікальний хеш-код попереднього блоку. Це створює ланцюг блоків, де кожен блок тісно пов'язаний з попереднім, і будь-яка спроба змінити інформацію в одному блоку автоматично виявляється в інших блоках, забезпечуючи надійність та нередагованість даних. Безпека в блокчейні забезпечується криптографічними методами, такими як хеш-функції та електронні підписи, що дозволяє будь-яку спробу зміни даних легко простежити. Це надає впевненість у невід'ємності та конфіденційності інформації.

Попри те, що тема є відносно новою, на сьогодні оприлюднено значну кількість статей, присвячених блокчейну. У них досліджуються різноманітні сфери використання блокчейну, наприклад, такі як Інтернет речей (IoT), фінансові послуги, смартконтракти, управління ланцюгами поставок, ігри тощо [9].

Модель на основі блокчейну в контексті децентралізованих соціальних мереж є інноваційним підходом, який поєднує принципи блокчейн-технологій і соціальних мереж для створення безпечного, прозорого та децентралізованого середовища для користувачів.

Розвиток модель на основі блокчейну в соціальних мережах має свої коріння у відчутті необхідності забезпечення безпеки даних та виправлення проблем централізованих соціальних платформ, які часто порушують приватність користувачів та піддають їх особисті дані ризику.

Основні етапи розвитку включають період досліджень у галузі криптовалют та технологій блокчейну, де виникали ідеї про можливе використання цих концепцій для створення безпечних соціальних мереж. Перші спроби використання блокчейну у соціальних мережах датуються середини 2010-х років. Історія розпочалася з появи біткоїн у 2009 році, який використовував технологію блокчейн для створення децентралізованої криптовалюти. Цей період характеризується виникненням ідей та експериментів, спрямованих на

використання блокчейну для створення нових, безпечних і децентралізованих соціальних платформ.

1. Початки експериментів (2010-2015 рр). Перші спроби використання блокчейну у соціальних мережах можна відзначити навколо 2014-2015 років. Проєкти, такі як «Twister» та «Minds», стали піонерами у цьому напрямку, намагаючись створити соціальні мережі, де користувачі мають більший контроль над своїми даними і спілкуванням.

2. Виникнення блокчейн у соціальних мереж (2016-2018 рр). У цей період з'явилися перші блокчейн-соціальні мережі, такі як «Steemit» та «Yours.org. Steemit», які базуючись на технології блокчейну, запропонували користувачам винагороди за створення та взаємодію з контентом. Також було багато експериментів із застосуванням смартконтрактів для управління правами доступу та винагородами.

3. Зростання зацікавленості та диверсифікація (2019-2021 рр). Цей період характеризувався збільшеним зацікавленням індустрії у блокчейн-соціальних мережах. Проєкти, такі як «Voice» від компанії Block.one, спрямовували зусилля на поліпшення прозорості та безпеки в соціальних мережах. Також з'явилися нові підходи до використання технологій блокчейну для забезпечення анонімності та приватності користувачів.

З часом виникли платформи, такі як Ethereum, які надають можливість розробникам створювати програми, написані мовою програмування та розгорнуті на блокчейні, які автоматизовано виконують визначені умови або домовленості при виконанні певних умов (смартконтракти) та додатки, що використовують смартконтракти для своєї роботи та побудовані на децентралізованій інфраструктурі (DApps).

Децентралізовані соціальні мережі, які використовують блокчейн (рис. 2.2), часто вбирають у себе концепцію токеноміки, де використовують цифрові валюти або токени для заохочення участі, винагороди творців контенту та проведення економічних транзакцій в мережі [25].

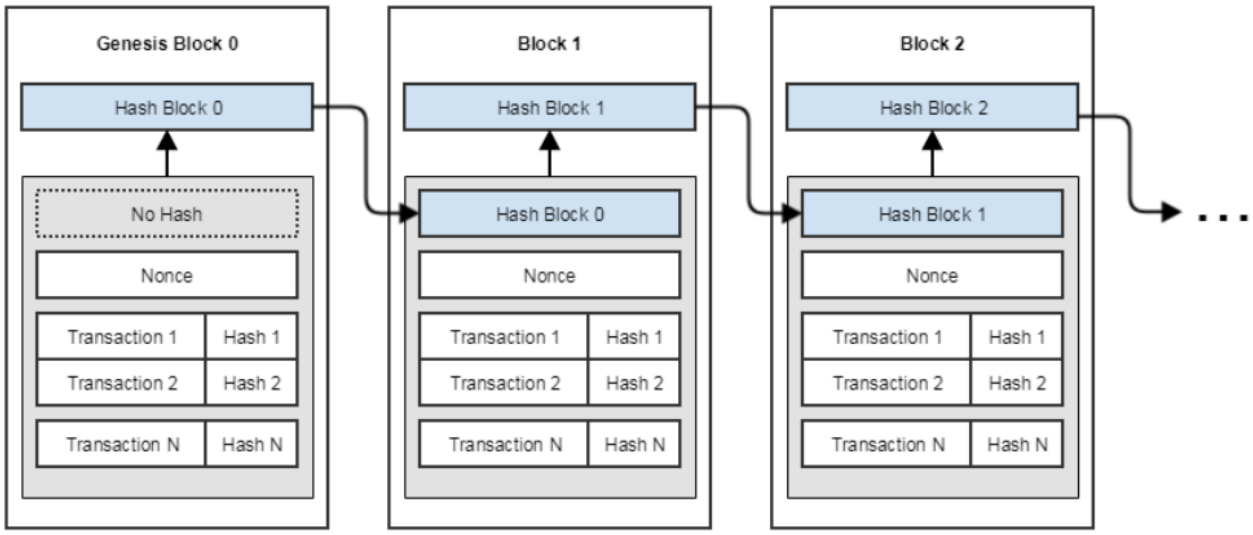


Рис. 2.2. Приклад архітектури блокчейн

Зацікавлені особи можуть заробляти ці токени через активну участь, створення контенту чи виконання інших бажаних дій. Система токенів створює стимули для користувачів приносити свій внесок у мережу, сприяючи формуванню живої та динамічної екосистеми [32].

Модель на основі блокчейну (рис. 2.3) в децентралізованих соціальних мережах є інноваційним підходом, який об'єднує технології блокчейну та соціальні мережі для створення безпечного, прозорого та контрольованого способу обміну інформацією та взаємодії користувачів. Основною особливістю моделі на основі блокчейну є використання розподіленої та нефальшивої бази даних для зберігання інформації про користувачів та їх взаємодії. Кожна дія або повідомлення може бути зафіксоване у блоку, що підвищує рівень безпеки та відкритості [60].

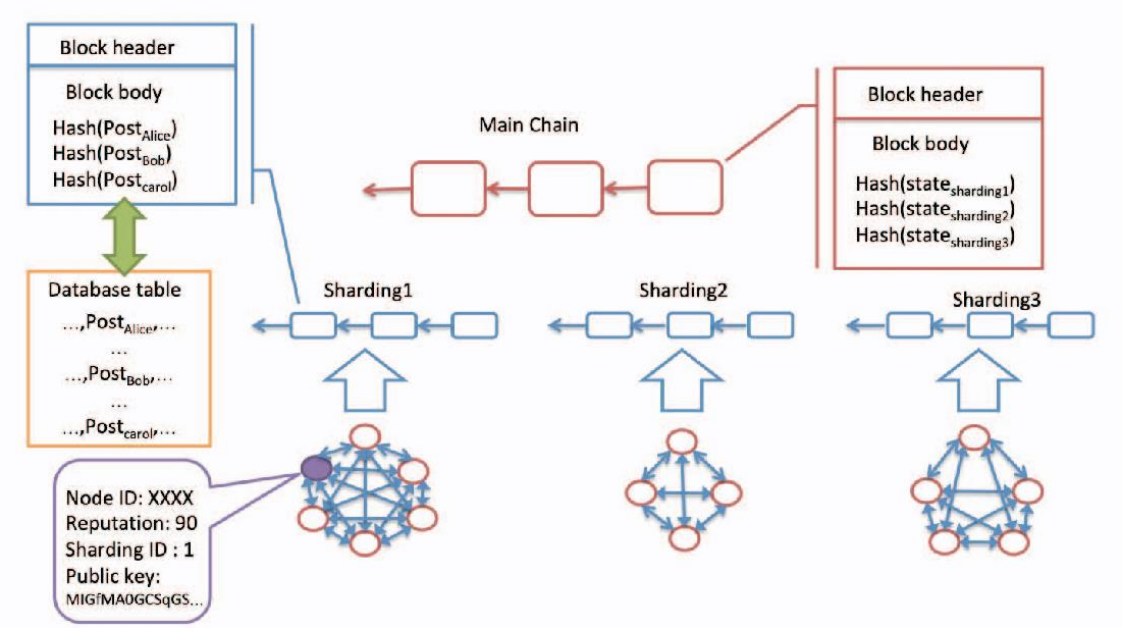


Рис. 2.3. Схема реалізації децентралізованої соціальної мережі на базі блокчейн

Ethereum став найпопулярнішою платформою для децентралізованих соціальних мереж завдяки своїй широкій функціональності, надійності та активній розробницькій спільноті. Його унікальність полягає у вбудованій можливості створення смартконтрактів, що надає розробникам гнучкість у реалізації різноманітних функціональностей в мережі. Ethereum визнаний за стандарти токенів, такі як ERC-20 та ERC-721, які дозволяють просту інтеграцію власних токенів та економічних моделей у соціальних мережах [56].

Децентралізована природа Ethereum забезпечує високий рівень безпеки та універсальності, а його розгалужена розробницька спільнота сприяє постійному розвитку та підтримці [5]. Крім того, можливість взаємодії з іншими додатками та смартконтрактами робить Ethereum ідеальним вибором для будівництва екосистеми децентралізованих соціальних мереж, де користувачі мають більше контролю над своїми даними та взаємодіють без посередників.

Ethereum було запущено у 2015 році Віталієм Бутеріним з метою створення універсальної платформи для розумних контрактів. Початково ця ідея не була прямо пов'язана з соціальними мережами, але з часом розширилася. Ethereum дозволяє розробникам створювати смартконтракти — програми, що

автоматизують виконання угод та умов. Фактично, основними характеристиками цієї технології, які відрізняють від інших, — це автономія, самодостатність і децентралізація [49]. Саме ці особливості відкрила можливості для створення децентралізованих соціальних мереж, де права та взаємодії можуть контролюватися розумними контрактами. Екосистема Ethereum підтримує децентралізовані ідентифікатори, які дозволяють користувачам володіти та контролювати свої особисті дані, що є важливим для забезпечення приватності в соціальних мережах.

Ethereum гарантує децентралізацію, оскільки його блокчейн побудований на різних вузлах, забезпечуючи стійкість та відсутність одного центрального контрольного пункту. Смартконтракти Ethereum дозволяють реалізувати системи голосування та управління платформою, де рішення приймається спільнотою користувачів. Застосування блокчейн-технологій для створення децентралізованих ідентифікаторів забезпечує власність та контроль користувачів над своєю особистою інформацією. Ethereum працює за принципом розподіленого консенсусу, де блоки транзакцій з'єднані в ланцюг, що робить неможливим зміну або вилучення інформації. Смартконтракти виконують угоди автоматично при виконанні умов, забезпечуючи безпеку та автономність управління.

Ethereum відіграв важливу роль у розвитку децентралізованих соціальних мереж, надаючи технічні засоби для створення інноваційних та безпечних платформ для взаємодії користувачів.

Прикладами реалізації цієї моделі є платформи, такі як Steemit (https://steemit.com), де користувачі отримують криптовалюту за створення та взаємодію з контентом, або Minds (https://minds.com), що використовує блокчейн для забезпечення безпеки та прозорості в обміні інформацією.

Steemit є платформою для блогінгу та соціальної мережі, яка використовує блокчейн Steem. Вона дозволяє користувачам створювати та розповсюджувати контент, отримувати винагороду в токенах STEEM за активність та залучення аудиторії. Модель винагороди на Steemit базується на голосах користувачів, що стимулює високоякісний та цікавий контент.

Steemit є ключовим учасником в екосистемі децентралізованих соціальних мереж, започаткованою у 2016 році Деніелом Ларимером та Недом Скоттом [15]. Тоді Steemit вперше представив STEEM — криптовалюту, яка використовується для винагородження користувачів за створення та взаємодію з контентом [58]. Steemit використовує технологію блокчейн для реєстрації та визначення власності контенту, а також винагородження користувачів за їхній внесок. Голосування та розподіл винагород базуються на кількості STEEM, яку користувачі утримують. Така система дозволяє створити децентралізоване середовище, де спільнота має великий вплив на платформу. Система голосування, базована на кількості у STEEM, надала користувачам можливість визначати популярність контенту. Платформа також надає можливість користувачам отримувати винагороди у вигляді STEEM за створення контенту та голосування за інші публікації. Користувачі також отримують так звані «Винагороди за кураторство» за те, що знаходять і голосують за контент, який потім підтримують інші користувачі. Це стимулює учасників активно співпрацювати та спільно визначати цінність матеріалів. З часом на платформі з'явилися різноманітні додатки, такі як DTube і DSound, які дозволяють завантажувати та обмінюватися відео та аудіо контентом [11]. Користувачі активно об’єднувалися в ком’юніті для спільного розвитку та підтримки. Steemit продовжує бути інноваційним гравцем у сфері децентралізованих соціальних мереж, розвиваючи свої можливості та пропонуючи учасникам унікальні способи взаємодії та отримання винагород за їхню активність. Ця модель визначає новий етап у розвитку соціальних мереж, забезпечуючи користувачам більший контроль над їхніми особистими даними та створюючи новий економічний стимул для участі в соціальної взаємодії.

Що стосується соціальної мережі Minds — це розповсюджена соціальна мережа з відкритим кодом. У Minds впроваджено систему монетизованого контенту через систему винагород токена Minds, які можуть використовуватися для просування своїх повідомлень або краудфандингу інших користувачів [37]. Minds більш орієнтовані на конфіденційність, ніж основні соціальні мережі. Повідомлення Minds з'являються у зворотному хронологічному порядку.

Заснована у червні 2015 року. Засновник і генеральний директор — Білл Оттман. Мережа Minds певний час була прикладом середовища в якому послаблення правил модерації й зведення до мінімуму цензури призвели до утворення груп, в яких культивувалася ненависть до людей певних поглядів, релігій, націй. Проте згодом у Minds сформувалася політика щодо того, щоб за допомогою голосування у форматі «журі» дозволити користувачам самостійно модерувати вміст, Таким чином кількість осередків «правих» звелася до мінімуму [36].

2.3. Модель Fediverse

Fediverse, що походить від словосполучення «Federation» (федерація) та «Universe» (всесвіт), являє собою децентралізоване об'єднання соціальних мереж, де користувачі можуть взаємодіяти між собою безперешкодно [24]. Завдяки обліковому запису на одному сервісі, користувач може взаємодіяти з іншими сервісами в межах Fediverse, не потребують реєстрації на них. За бажанням користувач може створити власний вузол в будь-якій федеральній мережі та стати повноправним та абсолютно незалежним учасником Fediverse.

Історія розвитку Fediverse почалася у 2008 році, коли розробник Еван Продрому заснував соціальну мережу identi.ca. Він оприлюднив вихідний код під ліцензією GNU Affero General Public License (AGPL), що визначило початок протоколу OStatus. GNU Affero General Public License (GNU AGPL) є вільною ліцензією, спеціально створеною для програм, зокрема вебдодатків (рис. 2.4). Вона дозволяє користувачам, які використовують модифіковану програму через глобальну мережу, отримувати доступ до її вихідного коду.

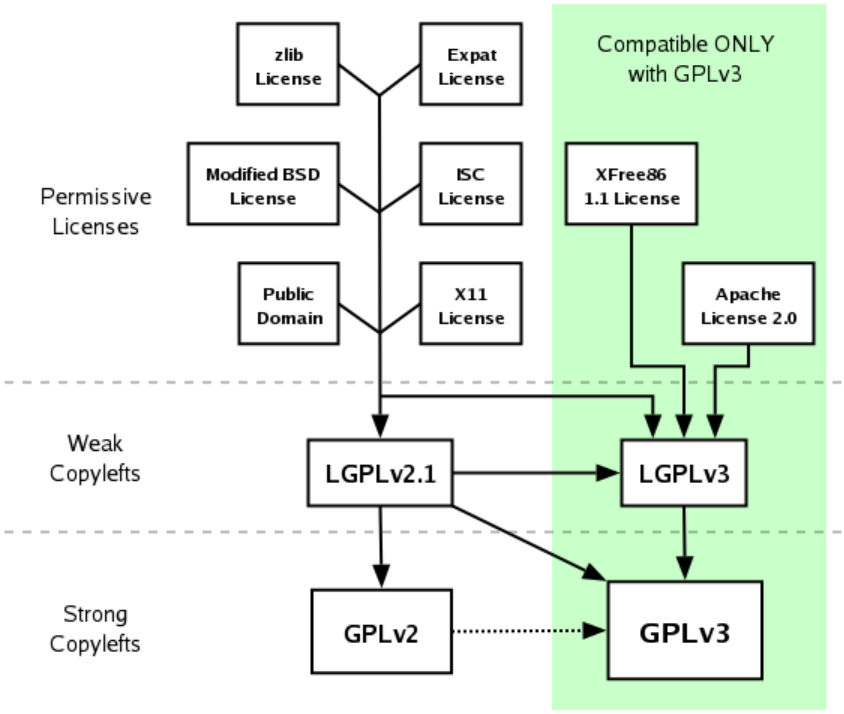


Рис. 2.4. Відносини сумісності між різними ліцензіями вільних програм

Фонд вільного програмного забезпечення (Free Software Foundation) розробив цю ліцензію базуючися на основі двох інших ліцензій — Affero General Public License (Affero GPL) та GNU General Public License [26]. Їх основна мета полягає в забезпеченні вільності користувачам, що використовують програми, особливо в контексті вебсервер та інтернет-застосунків, забезпечуючи доступ до вихідного коду при використанні через мережу.

Крім основного сервера identi.ca, Еван Продрому розробив декілька інших вузлів мережі та запустив їх для користувачів, які могли застосовувати модель для особистого використання. Зміни настали у 2011-2012 роках, коли розробник identi.ca перейшов на нове ПЗ pump.io. Таким чином з'явилося нове численне сімейство вузлів GNU social, і в той самий період інші проєкти, такі як Mastodon, Pleroma, Hubzilla розпочали використовувати новий ефективний протокол OStatus [52]. Його інтеграція значно розширила екосистему Fediverse.

Модель Fediverse у контексті децентралізованих соціальних мереж грунтується на ідеї об'єднання різних серверів (інстанцій) в одну мережу, при

цьому кожен сервер функціонує самостійно, зберігаючи контроль над своєю часткою користувацьких даних та правилами [62].

Завдяки цій моделі користувачі можуть використовувати наявні системи, роблячи свої дані більш узгодженими і легкодоступними, а отже, більш цінними. Платформа Fediverse, яка знаходиться на вершині системи оперативної підтримки, отримує дані з різних джерел і зводить їх в єдине ціле, що дозволяє соціальній мережі працювати більш ефективно, швидше реагувати і вирішувати проблеми з забезпеченням оптимізованих процесів (рис. 2.5).

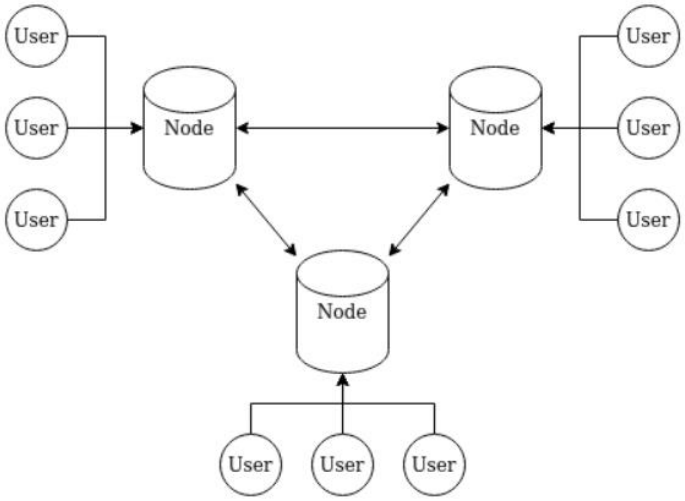


Рис 2.5. Децентралізована архітектура, яка дозволяє об'єднати декілька джерел даних

Модель Fediverse включає різні сервіси чи платформи, що працюють незалежно, але одночасно можуть взаємодіяти та обмінюватися інформацією між собою. У цій моделі кожен сервіс, чи то соціальна мережа, мікроблогінгова платформа чи інша, становить собою вузол (ноду) в одній великій мережі.

Основні риси моделі Fediverse включають:

1. Децентралізація: кожен вузол або сервіс функціонує незалежно від інших, і вони можуть розгортатися на різних серверах, підконтрольних різним особам або організаціям.

2. Протоколи взаємодії: щоб різні сервіси могли обмінюватися даними та взаємодіяти, вони використовують стандартизовані протоколи взаємодії. У світі децентралізованих соціальних мереж, наприклад, це може бути протокол типу ActivityPub.

3. Спільна мережа: попри те, що кожен сервіс діє самостійно, вони всі є частинами спільної мережі, що дозволяє користувачам взаємодіяти між різними сервісами, не обов'язково реєструючись окремо на кожному.

4. Спільний стандарт для ідентифікації: часто в моделі Fediverse використовуються спільні стандарти для ідентифікації користувачів, щоб забезпечити їхню розпізнаваність та взаємодію на різних сервісах.

Модель Fediverse швидко здобула популярність серед користувачів, які шукають більше контролю над своєю взаємодією в мережі [14]. Забезпечення окремих серверів дозволяє створювати специфічні спільноти та встановлювати власні правила.

Сервіси, що входять до складу Fediverse, базуються на вільному програмному забезпеченні. Кожен користувач сервісу, який є частиною Fediverse, може вільно обмінюватися повідомленнями, відео, аудіо та іншою інформацією з іншими користувачами свого або інших сервісів.

На серпень-вересень 2023 року в Fediverse нараховується 126 сервісів, які працюють на 15 різних протоколах і обслуговують майже 15 мільйонів користувачів [54].

Проте паралельно розвивалися інші протоколи взаємодії. За розвиток федераційних соціальних мереж також стоїть впровадження протоколу ActivityPub. У січні 2018 року Консорціум Всесвітнього павутиння (World Wide Web Consortium) представив ActivityPub. Новий протокол спрямований на значне покращення взаємодії між різними платформами. Цей протокол визначає стандарти взаємодії між серверами, що дозволяє їм обмінюватися інформацією та взаємодіяти через різні інстанції. Цей протокол підтримується тринадцятьма різними платформами.

ActivityPub — це протокол для соціальних мереж, що працює у децентралізованому режимі та ґрунтується на форматі даних ActivityStreams 2.0. Він забезпечує API для взаємодії між клієнтами та серверами, дозволяючи створювати, оновлювати та видаляти контент [6]. Крім того, він також має федераційний серверний API для передачі сповіщень та контенту. ActivityPub надає два рівні функціональності:

1. Протокол федерації між серверами: цей рівень дозволяє децентралізованим вебсайт обмінюватися інформацією. Він створює механізм взаємодії між різними серверами, щоб вони могли обмінюватися даними та спільною активністю.
2. Протокол клієнт-сервер: цей рівень надає можливість користувачам (реальним, ботам та іншим автоматизованим процесам) спілкуватися з ActivityPub. Користувачі можуть взаємодіяти з цим протоколом через свої акаунти на серверах, використовуючи різні пристрої та платформи [47].

Імплементації ActivityPub можуть охоплювати один з цих рівнів або обидва одночасно (рис. 2.6). Щоправда, після того, як один рівень реалізовано, виконання іншого виявляється нескладним, пропонуючи багато переваг, таких як включення вебсайт в децентралізовану соціальну мережу та можливість використовувати клієнти та бібліотеки, що працюють на різноманітних соціальних вебсайтів [63].

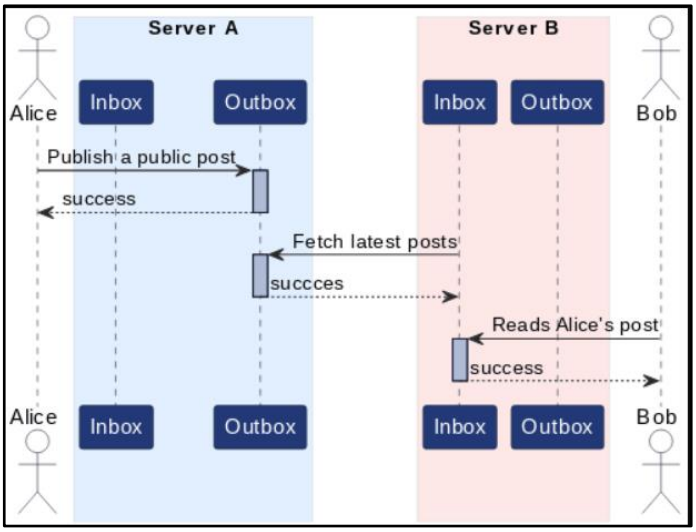


Рис. 2.6. Взаємодія користувачів з протоколом ActivityPub

У ActivityPub [8] кожен користувач представлений «акторами» через акаунти користувачів на серверах. Акаунти користувачів на різних серверах

відповідають різним акторам. Кожен актор має вхідну та вихідну скриньку, які визначають, звідки він отримує та надсилає повідомлення в межах мережі [7]. Нижче наведений приклад відображення даних в протоколі ActivityPub, котрий використовується для обміну даних в мережі (рис. 2.7):


```
{"@context": "https://www.w3.org/ns/activitystreams",
"type": "Person",
"id": "https://social.example/romanlitvin/",
"name": "Roman Litvin",
"preferredUsername": "romanlitvin",
"summary": "Passionate about technology",
"inbox": "https://social.example/romanlitvin/inbox/",
"outbox": "https://social.example/romanlitvin/outbox/",
"followers": "https://social.example/romanlitvin/followers/",
"following": "https://social.example/romanlitvin/following/",
"liked": "https://social.example/romanlitvin/liked/"}
```


Рис. 2.7. Приклад відображення даних в протоколі ActivityPub

Загалом це кінцеві точки, або просто URL-адреси, які перераховані в описі ActivityStreams актора ActivityPub.

У 2016 році платформа Mastodon визначила новий етап в розвитку соціальних мереж, впроваджуючи модель Fediverse. Ця модель забезпечує спільнотам можливість самостійного управління своєю інфраструктурою та забезпечує більші можливості вибору користувачів. Mastodon — це децентралізована соціальна мережа, створена у 2016 році Еугеном Рочаком. Система розвивалася як альтернатива централізованим платформам. Mastodon пропонує користувачам контроль над своїми даними та досвідом та ґрунтується на принципі федерації, де різні сервери (екземпляри) об'єднуються в одну мережу, забезпечуючи взаємодію між користувачами на різних екземплярах [34].

Основні характеристики Mastodon охоплюють можливість створення користувацьких профілів, обмін повідомленнями, фото та відео, а також перегляд стріму новин. Користувачі можуть вибирати екземпляр за своїми уподобаннями та політиками безпеки. Mastodon також пропонує можливість використання різних клієнтських програм та бібліотек.

Mastodon має кілька технічних особливостей, які роблять його унікальним в контексті децентралізованих соціальних мереж:

1. *Модель Fediverse.* Mastodon базується на принципі федерації, де різні сервери (інстанції) об'єднуються в одну мережу. Це дозволяє користувачам на різних серверах взаємодіяти та обмінюватися контентом.
2. *Протокол ActivityPub.* Mastodon використовує протокол ActivityPub для забезпечення взаємодії між різними серверами. Цей протокол дозволяє обмінюватися повідомленнями, статусами та іншим контентом між користувачами на різних інстанціях.
3. *Відкритий код.* Mastodon є проєктом з відкритим кодом, що означає, що його програмний код вільно доступний для перегляду, модифікації та розповсюдження спільнотою. Це сприяє розвитку та підтримці системи глобальною спільнотою розробників.
4. *Модульність та розширюваність.* Mastodon побудована з урахуванням модульності, що дозволяє розширювати функціональність за допомогою різних додатків та плагінів.
5. *Мультипротокольність***.** Окрім ActivityPub, Mastodon підтримує інші протоколи для взаємодії з іншими соціальними мережами, такі як OStatus та Diaspora.
6. *Локалізація та підтримка клієнтів.* Mastodon підтримує мовні файли для легкої локалізації, а також надає API для взаємодії з різними клієнтськими програмами та додатками.
7. *Система приватності.* Mastodon надає користувачам контроль над приватністю, включаючи можливість обирати рівень видимості для своїх повідомлень та обмежувати доступ до свого профілю.

Ці технічні особливості роблять Mastodon важливим гравцем у сегменті децентралізованих соціальних мереж, надаючи користувачам більший контроль та гнучкість у використанні платформи.

За час свого існування Mastodon набув значної популярності через свою сфокусованість на приватності, відкритий код, а також заходи щодо боротьби з

цензурою [29]. Система стала символом росту інтересу до децентралізованих соціальних мереж, розширюючи свою спільноту та поширюючи ідеї самоуправління та вільної комунікації в інтернеті.

Попри свої переваги, Fediverse-мережі також стикаються з викликами, такими як стандартизація та управління. Проте, шлях до децентралізації та федерації визначається постійними зусиллями спільноти та розвитком технологій.

Висновок до розділу 2

Модель Fediverse, peer-to-peer та блокчейну у контексті децентралізованих соціальних мереж є ключовими інноваціями, що революціонізують спосіб, яким користувачі спілкуються та обмінюються інформацією в цифровому просторі.

Модель Fediverse визначається сукупністю серверів, які працюють в тандемі, обмінюючись інформацією. Ця модель створює розподілену мережу, де користувачі можуть взаємодіяти, не обмежуючись одним централізованим сервером. Історія розвитку Fediverse свідчить про постійне удосконалення протоколів та стандартів для забезпечення сумісності та взаємодії між серверами.

Тоді як модель peer-to-peer дозволяє користувачам спілкуватися напряму, обмінюючись даними без посередництва централізованого сервера. Історія цієї моделі свідчить про її відмінність від традиційних підходів та постійне покращення технологій для забезпечення безпеки та швидкості обміну даними.

Модель на основі блокчейну дає можливість користувачам максимально контролювати свої особисті дані, забезпечуючи прозорість та безпеку. Застосування смартконтрактів дозволяє автоматизувати угоди та забезпечує безпосередню виконуваність угод, виключаючи посередників. Історія розвитку цієї моделі свідчить про постійні вдосконалення у напрямку більшої безпеки та ефективності.

Моделі Fediverse, peer-to-peer та блокчейну, представляють різні підходи до створення децентралізованих соціальних мереж і мають свої особливості та відмінності.

Модель Fediverse орієнтована на створення розподіленої мережі серверів, які обмінюються інформацією та співпрацюють між собою. Користувачі можуть спілкуватися через різні сервери, не обмежуючись однією централізованою платформою. Це робить систему менш вразливою до цензури та контролю, але вимагає розробки стандартів та протоколів для ефективної взаємодії між серверами.

Модель peer-to-peer передбачає прямий обмін даними між користувачами без централізованого посередника. Кожен користувач є вузлом, який спілкується з іншими вузлами мережі. Це забезпечує великий ступінь децентралізації та анонімності, але може виникнути проблеми щодо безпеки та швидкодії обміну даними.

Модель на основі блокчейну визначається використанням блокчейн-технології для зберігання та обробки даних. Кожен користувач має свій власний блокчейн, де вони можуть зберігати та контролювати свої особисті дані. Смартконтракти дозволяють автоматизувати угоди між користувачами без посередництва. Ця модель надає високий рівень прозорості та безпеки, але може виявитися складною в реалізації через технічні та масштабні виклики.

Основні відмінності полягають у способі обробки даних, масштабованості, безпеці та ефективності взаємодії. Кожна модель має свої переваги та обмеження, і вибір між ними залежить від конкретних потреб та цілей розробки соціальної мережі. Загалом, ці моделі позначають новий етап у розвитку соціальних мереж, де користувачі мають більший контроль над своєю інформацією, а економічні стимули заохочують активну участь у соціальній взаємодії. Всі вони спрямовані на створення більш безпечного, ефективного та учасницького цифрового середовища.

Отже, спираючись на результати проведення власних досліджень, мною було обрано поєднання моделі peer-to-peer та блокчейну для розробки децентралізованої соціальної мережі, оскільки симбіоз саме цих моделей має більші переваги. Реалізація моделі peer-to-peer дозволяє забезпечити спілкування між користувачами, зменшуючи їхню залежність від централізованих серверів.

Технологія блокчейну, своєю чергою, реалізує безпеку та прозорість даних, а також контроль користувачів над персональною інформацією. Це поєднання може покращити конфіденційність та надійність соціальної мережі.

РОЗДІЛ 3.
СТВОРЕННЯ ДЕЦЕНТРАЛІЗОВАНОЇ СОЦІАЛЬНОЇ МЕРЕЖІ НА ОСНОВІ МОДЕЛІ PEER-TO-PEER ТА БЛОКЧЕЙНУ

3.1. Розробка архітектури децентралізованої соціальної мережі Social Grab

Поява новітніх технологій, таких як блокчейн та моделі peer-to-peer, розширює горизонти можливостей для створення інноваційних та безпечних онлайн-платформ. Проведення комплексного аналізу взаємодії обраних моделей та їхній вплив на створення децентралізованої соціальної мережі дає можливість з'ясувати рівень забезпечення максимального контролю користувачів над їхніми даними, безпекою та новаторськими функціями. Обґрунтовуючи обрані моделі, проведено теоретичний огляд їхніх ключових аспектів, враховуючи специфіку використання в контексті соціальних мереж.

Створення децентралізованої соціальної мережі на базі моделі peer-to-peer та блокчейн-технологій визначається кількома важливими мотивами, які враховують сучасні виклики та потреби спільноти. По-перше, така мережа дозволяє користувачам здійснювати повний контроль над своєю особистою інформацією, уникати централізованого зберігання даних та потенційних порушень конфіденційності. Децентралізована природа гарантує, що користувачі мають владу над своєю власною інформацією та визначають, кому та за яких умов дозволено доступ до неї.

По-друге, така соціальна мережа створює інноваційні умови для обміну контентом та взаємодії, забезпечуючи аутентичну комунікацію без посередників. Модель peer-to-peer дозволяє користувачам обмінюватися інформацією напряму, зменшуючи вплив посередників та гарантуючи безпеку обміну.

По-третє, використання технології блокчейн в соціальних мережах впроваджує концепцію смартконтрактів, що дозволяє автоматизувати та безпечно виконувати угоди між користувачами. Це створює унікальні умови для

розгортання різноманітних сервісів та додаткових можливостей, наприклад, винагородження користувачів за активну участь чи створення нових спільнот.

Децентралізована соціальна мережа, яка поєднує в собі обидві моделі, не лише гарантує високий рівень конфіденційності й безпеки, але також стимулює інновації, взаємодію та творчість в онлайн-середовищі. Це створює екосистему, в якій користувачі мають повний контроль та стають активними учасниками.

Social Grab — це децентралізована соціальна мережа, спрямована на аудиторію населення України віком від 16 до 50+ років. Основною метою створення мережі є надання безпечного та ефективного засобу обміну інформацією серед користувачів, а також вирішення ключових викликів, пов'язаних з централізованим обміном даних та цензурою в інтернеті. Social Grab використовує технологію блокчейн для реалізації розподіленого зберігання даних. Кожен користувач мережі має свій власний блокчейн, що гарантує високий рівень цілісності та безпеки інформації. Застосування криптографічних принципів забезпечує конфіденційність інформації та відмову від централізованого зберігання паролів. Для забезпечення децентралізації спілкування між користувачами використовується технологія peer-to-peer (бібліотека libp2p). Це дозволяє взаємодіяти без посередництва централізованого сервера, підвищуючи ефективність та забезпечуючи стабільність мережі. Сприяючи принципам блокчейну, мережа заохочує активність користувачів через процес винагород, які спрямовані на підтримку інтеграції нових блоків та верифікацію інформації. Учасники отримують винагороду в токенах GrabCoins, стимулюючи взаємодію та обмін даними. Окрім цього користувачі отримують винагороду за перевірку та публікацію інформації, що стимулює залучення та перевірку контенту. Також Social Grab має вбудовані механізми для забезпечення високого рівня конфіденційності. Користувачі мають можливість анонімного обміну повідомленнями та інформацією, використовуючи криптографічні методи шифрування. З метою зменшення використання серверної частини та оптимізації витрат електроенергії, Social Grab використовує децентралізовану структуру, що

знижує навантаження на централізовані сервери та сприяє більш ефективному використанню ресурсів.

Створення децентралізованої соціальної мережі Social Grab можна розділити на 7 етапів:

1. *Визначення вимог:* на першому етапі проводиться аналіз функціональних та нефункціональних вимог до соціальної мережі. Це включає визначення основних можливостей, рівня безпеки, типів контенту, який може бути розміщений, та інших ключових параметрів.
2. *Проєктування структури:* на цьому етапі розробляється загальна структура соціальної мережі. Враховуються основні компоненти, такі як користувачі, профілі, дописи, коментарі, та взаємодія між ними. Застосовується модель peer-to-peer для забезпечення розподіленості, а також використовується блокчейн для забезпечення безпеки та невідкладності.
3. *Вибір технологій:* обираються технології для реалізації кожного компонента системи. Для мережевої частини використовується технологія peer-to-peer, така як libpeer-to-peer. необхідно розробити смартконтракти, які використовуються для управління та верифікації децентралізованих операцій, таких як створення постів, коментування, та взаємодія користувачів.
4. *Реалізація та тестування:* проходить розробка реальної системи з використанням обраних технологій. Проводиться тестування для перевірки працездатності, безпеки та відповідності вимогам.
5. *Впровадження та масштабування:* система вводиться в експлуатацію та взаємодіє з реальними користувачами. Поступово ведеться процес масштабування, який дозволяє підтримувати ріст користувачів та розширювати функціонал.
6. *Підтримка та оновлення:* після впровадження системи ведеться постійна підтримка, включаючи виправлення помилок, забезпечення безпеки та впровадження нових функцій відповідно до потреб користувачів. Цей процес забезпечить ефективне функціонування децентралізованої соціальної мережі, яка об'єднала переваги peer-to-peer та блокчейн-моделей.

Створення децентралізованої соціальної мережі починається з проведення аналізу функціональних та нефункціональних вимог до соціальної мережі. Це включає визначення основних можливостей, рівня безпеки, типів контенту, який може бути розміщений, та інших ключових параметрів. До основних функціональних вимог нової децентралізованої соціально мережі Social Grab можна віднести: можливість реєстрації нових користувачів та безпечна аутентифікація, додавання нового контенту (постів, фотографій, відео тощо), можливість коментування, лайків, та приватної взаємодії між користувачами. Окрім цього потрібно забезпечити нефункціональні вимоги: забезпечення конфіденційності та цілісності особистої інформації користувачів, здатність системи ефективно обслуговувати зростаючу кількість користувачів, зменшення енергоспоживання для підтримки децентралізованої інфраструктури.

Також розробка вимагає врахування додаткових параметрів:

- тип контенту: текстовий (можливість додавання та обміну текстовими постами), мультимедійний (підтримка зображень, аудіо та відео контенту;
- керування доступом: приватність (здатність користувачів контролювати доступ до свого контенту та особистої інформації), цензура (мінімізація цензури та обмежень для свободи вираження).

Децентралізована соціальна мережа Social Grab враховує також основні технічні вимоги — використання технології peer-to-peer для забезпечення розподіленості та використання технології блокчейн для гарантії безпеки, імутабельності та взаємодії з користувачами.

Визначення цих вимог відображає стратегічне бажання створити інноваційну соціальну мережу, яка забезпечить високу якість взаємодії, збереження приватності, та відповідає сучасним тенденціям в розробці платформ. Врахування різноманітних параметрів допомагає сформулювати повніші вимоги, що визначать ефективність та привабливість майбутньої соціальної мережі. Цей етап є важливим для створення концептуального фундаменту, який дозволяє точно визначити шлях розвитку проєкту та його позицію на ринку.

Наступним етапом у розробці децентралізованої соціальної мережі є розробка загальної структури вебспільноти. Social Grab — інноваційний вебспільнотний портал, в основі якого лежать моделі peer-to-peer та блокчейн. Вебспільнотний портал — це термін, який вказує на можливість взаємодії між користувачами, на створення спільнот та об'єднань людей за спільними інтересами або цілями. Ця структура спроєктована з урахуванням технічних вимог, забезпечуючи унікальні особливості та функціональні можливості. Система використовує криптографічні методи для безпечної аутентифікації користувачів за допомогою їхніх приватних ключів. Це дозволяє забезпечити високий рівень конфіденційності та захисту особистої інформації.

Мережа побудована на основі peer-to-peer архітектури, де кожен користувач є «вузлом». Задіяна технологія використання соціальних графів, які є абстрактними представленнями взаємодій та зв'язків між особами чи елементами в мережі та використовується для аналізу та моделювання цих взаємодій. Соціальні мережі, з іншого боку, являють собою реальні вебплатформи чи додатки, які дозволяють користувачам створювати профілі, знаходити друзів, обмінюватися інформацією та взаємодіяти один з одним. Дані про зв'язки між користувачами зберігаються в розподіленій базі даних, що дозволяє ефективно взаємодіяти та обмінюватися інформацією. Кожна операція, включаючи створення постів, коментарів та лайків, реєструється у блокчейні. Це забезпечує прозорість, непереборність та можливість перевірки історії взаємодії для кожного користувача.

Описувати та аналізувати соціальні мережі дуже зручно та ефективно саме за допомогою графа, ця технологія дозволяє розв’язувати багато різнотипних завдань, виявляти зв’язки між користувачами та аналізувати ступінь їх взаємодії. Саме завдяки можливості та доступності особистих даних користувачів можна розширити спектр отриманої інформації, отримати більше додаткових дані для кращого аналізу і сформувати певну статистику.

Графи набувають все більшої популярності. Головною їх перевагою є зручність та ефективність використання для розв'язання різноманітних задач з

аналізу та обробки даних, дослідження зв’язків, пошуку найкращих шляхів та наочного представлення даних [2].

У соціальних мережах суб’єкти групуються відповідно до схожості своїх взаємин, таких як спільні інтереси, членство у тих самих соціальних групах, спільне місце роботи чи проживання. Критерії подібності можуть бути різноманітними. Децентралізовані соціальні мережі надають можливість створювати соціальний граф користувача або граф інтересів на основі зібраних даних. Хоча обидва графи мають спільні принципи, вони відрізняються за деякими ключовими аспектами. У соціальному графі зв’язки формуються враховуючи дружбу між користувачами, тоді як у графі інтересів зв’язки створюються на основі подібності інтересів. Зв’язки в останньому можуть бути як між користувачами, так і між користувачем та певним інтересом.

Усі дані у соціальних мережах можна класифікувати як структуровані та неструктуровані. Структуровані дані у соціальних мережах найзручніше описувати завдяки графам, тому ці дані часто відображають графічно або моделюють у вигляді графів. Аналіз децентралізованих мереж спілкування та використання графічних аналітичних інструментів — дуже поширений метод обробки та структуризації інформації. Користувацький контент (UGC) — неструктуровані дані, які можна вимірювати за допомогою аналізу контенту, а також методів, що використовують алгоритми структурування даних.

Для опису, візуалізації та представлення загальної структури та взаємозв'язків усіх учасників соціальної мережі цілком доцільно використовувати контекстну соціограму — соціальний граф. Особливості соціального графа визначаються конкретними характеристиками, що характеризуються метрикою, яка спрямованих на розв'язання різноманітних завдань. Ці дані використовуються для аналізу децентралізованих платформ спілкування, оскільки вони завдяки числам можуть відобразити основні характеристики соціальних об'єктів.

Наведемо приклад архітектура децентралізованої соціальної мережі Social Grab на основі peer-to-peer, яка передбачає створення системи, де кожен

користувач є вузлом, і всі вони спільно утворюють мережу без централізованого управління. Загальна структура такої соціальної мережі:

1. *Peer-to-peer мережа.* Кожен користувач є вузлом мережі. Забезпечується пряме підключення між вузлами без посередництва центрального сервера.
2. *Розподілена база даних*. Інформація про користувачів, їхні зв'язки та контент зберігається в розподіленій базі даних. Кожен вузол зберігає лише обмежену частину даних, забезпечуючи децентралізований характер системи.
3. *Система ідентифікації та безпеки*. Застосовується система ідентифікації на основі криптографії для забезпечення безпеки та визначення власності даних. Кожен користувач має унікальний ідентифікатор та ключ для автентифікації.
4. *Алгоритми маршрутизації.* Використовуються peer-to-peer алгоритми маршрутизації для ефективного пошуку та передачі даних між вузлами.
5. *Контент та спільноти*. Забезпечується можливість створення та участі в спільнотах, які можуть бути тематичними чи заснованими на інтересах. Контент, як фотографії чи повідомлення, розповсюджується через мережу.
6. *Механізми взаємодії.* Реалізовано системи обміну повідомленнями, коментарів та взаємодії з контентом між користувачами.
7. *Пошук та рекомендації.* Використовуються алгоритми пошуку та рекомендацій на основі інтересів та зв'язків користувачів. Така архітектура дозволяє створити децентралізовану соціальну мережу, яка ефективно функціонує завдяки розподіленій природі зберігання даних та прямій взаємодії між користувачами.

Також мережа Social Grab використовує смартконтракти для автоматизації угод та взаємодії між користувачами. Наприклад, вони можуть регулювати доступ до контенту, розподіл рекламних прибутків чи винагородження за внесок. Кожен користувач має своє розподілене сховище для зберігання власних даних. Це розвиває концепцію децентралізованого зберігання та забезпечує надійність та доступність даних. Система розподіленого сховища в контексті децентралізованої соціальної мережі — ключовий аспект для забезпечення надійності, конфіденційності та доступності даних для кожного користувача. Кожен учасник

мережі має своє власне розподілене сховище, що розширює концепцію децентралізованого зберігання та вирішує ключові завдання, пов'язані із забезпеченням безпеки та надійності даних у розподіленому середовищі.

Основна мета розподіленого сховища — це забезпечити користувачам контроль над їхніми власними даними, враховуючи принципи децентралізації. Кожен користувач має свій унікальний ідентифікатор та асоційоване з ним розподілене сховище, яке може бути розподілено на вузлах peer-to-peer мережі або зберігати дані в блокчейні.

Технічно, розподілене сховище може використовувати різні стратегії для забезпечення високої доступності та безпеки даних. Також застосовується можливість використання реплікації даних для забезпечення копій у різних вузлах мережі та механізмів розподіленої бази даних для ефективного управління та пошуку інформації. Крім того, присутня інтеграція криптографічних методів для захисту конфіденційності та цілісності даних, зокрема, використання публічного та приватного ключів для шифрування та підпису інформації. Розподілене сховище в децентралізованій соціальній мережі є фундаментальним компонентом, який дозволяє забезпечити користувачам високий рівень захисту і контролю над їхніми особистими даними у світі, де приватність та безпека є критичними аспектами у сфері віртуальних спільнот.

У контексті структури соціальної мережі Social Grab, використання принципів блокчейну та механізму майнінгу відкриває новий рівень взаємодії та стимулювання активності користувачів. Система заохочення через майнінг, спрямована на створення нових блоків чи валідацію транзакцій, створює ефективний механізм для залучення та утримання учасників у соціальному середовищі.

Процес майнінгу в контексті соціальної мережі може охоплювати різноманітні дії та взаємодії, які додають цінність самій мережі. Наприклад, користувачі, які активно співпрацюють, створюють цікавий та важливий контент, можуть отримувати винагороду в токенах GrabCoins. Цей механізм стимулює творчість та активну участь, оскільки учасники отримують плату за свій внесок у

розвиток мережі. Кожна дія користувача, яка спрямована на покращення якості мережі, може бути визнана. Наприклад, коментування публікацій, розміщення цікавого контенту, чи взаємодія з іншими учасниками може бути враховано у механізмі отримання винагороди. Крім того, учасники мережі мають можливість заробляти та використовувати GrabCoins у внутрішній екосистемі мережі, наприклад, для розміщення реклами, отримання преміальних сервісів та розподілу прибутку від рекламних та інших доходів мережі. Цей підхід дозволяє створити демократичне та автономне середовище, де внесок кожного учасника є цінним та винагороджується, сприяючи створенню живої та динамічної соціальної мережі.

Також система дозволяє користувачам контролювати рівень конфіденційності, надаючи можливість анонімного обміну повідомленнями та інформацією. Всі дані, що передаються мережею, шифруються таким чином, що тільки власник відповідного ключа може розшифрувати і прочитати їх. Це забезпечує надійний захист від несанкціонованого доступу та забезпечує, що лише зазначені отримувачі матимуть доступ до конфіденційної інформації. Другий аспект, що впливає на рівень конфіденційності, це використання технології анонімізації. Система дозволяє користувачам обмінюватися повідомленнями та іншою інформацією, не розкриваючи особистої інформації. Алгоритми анонімізації видаляють або маскують ідентифікуючу інформацію, щоб забезпечити анонімність користувачів під час взаємодії в мережі.

Крім того, для забезпечення анонімного обміну повідомленнями, використовується технологія смартконтрактів. Вони гарантують, що обмін інформацією між користувачами відбувається безпечно та анонімно, відповідно до умов, визначених у контракті.

Усі ці технічні рішення разом створюють надійну систему, яка реалізує принципи децентралізації та анонімності, надаючи користувачам повний контроль над рівнем конфіденційності та приватності під час взаємодії у соціальній мережі.

Структура Social Grab враховує потужність peer-to-peer та блокчейн-технологій, надаючи користувачам безпеку, контроль та стимул для активної

участі в соціальній спільноті. Це є підґрунтям для створення інноваційного та децентралізованого середовища для соціального спілкування.

На етапі вибору технології розглянемо вибір технології peer-to-peer для реалізації мережевої частини децентралізованої соціальної мережі, зосереджуючись на технології libpeer-to-peer. Децентралізована соціальна мережа Social Grab розробляється з урахуванням специфічних потреб української аудиторії, що визначає важливість вибору оптимальної технології для спілкування та обміну даними. Libpeer-to-peer — це відкрите та модульне мережеве ядро, розроблене для забезпечення зручного та надійного peer-to-peer обміну даними. Ця технологія охоплює набір протоколів, які реалізують такі ключові функції, як ідентифікація вузла, шифрування, маршрутизація та обмін повідомленнями. Її модульна структура дозволяє легко вибирати лише необхідні компоненти для конкретного випадку використання.

```
const { createNode } = require('libp2p');
const PeerId = require('peer-id');
async function createLibp2pNode() {
  try {
    const node = await createNode();
    const nodeID = node.peerId.toB58String();
    console.log(`libp2p вузол створено. ID вузла: ${nodeID}`);
  } catch (error) {
    console.error('Помилка при створенні вузла libp2p:', error);
  }
}
createLibp2pNode();
```

Розглядаючи особливості українського користувача, намагаємося підійти до вибору технології з урахуванням особливостей мережевого з'єднання та інтересів користувачів. Libpeer-to-peer, завдяки своїй гнучкості та підтримці різноманітних пристроїв та платформ, дозволяє ефективно враховувати специфічність українського Інтернет-простору та забезпечує плавну інтеграцію з різними типами клієнтських пристроїв.

Обираючи libpeer-to-peer для мережевої частини децентралізованої соціальної мережі, ми отримуємо потужний інструментарій для побудови ефективної та надійної peer-to-peer комунікації. Ця технологія є ідеальним вибором для проєкту, спрямованого на задоволення потреб українських користувачів та створення інноваційного середовища для їхньої взаємодії.

В контексті блокчейн технології, соціальна мережа Social Grab базується на Ethereum, який є відкритою блокчейн-платформою, яка підтримує виконання смартконтрактів. Ця платформа надає гнучкість та розширюваність для створення розподілених додатків (DApps). Ethereum використовує мову програмування Solidity для розробки смартконтрактів. Технічні переваги Ethereum:

1. Ефективність та гнучкість: Ethereum відомий своєю широкою функціональністю та гнучкістю для створення різних видів смартконтрактів.
2. ERC-20 та ERC-721 стандарти: Ethereum підтримує стандарти токенів, такі як ERC-20 для функцій обміну та ERC-721 для унікальних токенів, що відкриває можливості для розширення функціонала соціальної мережі.
3. Розширюваність за допомогою Layer 2: Використання Layer 2 рішень, таких як Optimistic Rollup або zk-Rollup, дозволяє збільшити швидкість обробки транзакцій.

Приклад Solidity для створення токена у соціальній мережі Social Grab:

```
contract MyToken is ERC20 {
  constructor() ERC20("MyToken", "MTK") {
    _mint(msg.sender, 1000000 * (10 ** uint256(decimals())));
        }
        }
```

Після вибору технологій можна розпочати програмування функціонала соціальної мережі. На цьому етапі реалізується логіка системи, взаємодія між користувачами, зберігання та обробка даних на блокчейні. Інтеграція містить поєднання всіх компонентів в єдину функціональну систему. Забезпечується взаємодія фронтенду та бекенду, інтеграція блокчейн-технологій та налаштування мережі для ефективної передачі даних.

3.2. Модель децентралізованої соціальної мережі Social Grab

Архітектура децентралізованої соціальної мережі Social Grab, яка поєднує модель peer-to-peer та технологію блокчейну, розроблена для забезпечення максимального контролю користувачів над їхніми даними, безпеки та новаторських функцій.

Peer-to-peer протокол — використання peer-to-peer протоколів дозволяє безпечно обмінюватися даними без посередництва централізованого сервера. Кожен вузол мережі стає рівноцінним учасником. Розробка децентралізованої соціальної мережі Social Grab з використанням peer-to-peer протоколів охоплює використання бібліотеки libpeer-to-peer для забезпечення комунікації та обміну даними між різними вузлами мережі. Нижче наведено простий приклад коду мовою програмування JavaScript (Node.js), який демонструє створення мережевого вузла та обмін повідомленнями з використанням libpeer-to-peer:

```
const Libpeer-to-peer = require('libpeer-to-peer');
const TCP = require('libpeer-to-peer-tcp');
const WebSockets = require('libpeer-to-peer-websockets');
const PeerId = require('peer-id');
const multiaddr = require('multiaddr');
const createNode = async () => {
  const node = await Libpeer-to-peer.create({
    addresses: {
          listen:['/ip4/0.0.0.0/tcp/0','/ip6/::/tcp/0', '/dns4/wrtc-star1.par.dwebops.pub/tcp/443/wss/peer-to-peer-
          webrtc-star/'],
    },
    modules: {
      transport: [TCP, WebSockets],
    },
  });
  return node;
};
const sendMessage = async (node, targetPeerId, message) => {
  const targetAddr = `/ipfs/${targetPeerId.toB58String()}`;
```

```
  const connection = await node.dial(multiaddr(targetAddr));
  await connection.send(Buffer.from(message));
  await connection.close();
};
const startNode = async () => {
  const node = await createNode();
  await node.start();
  const ownPeerId = node.peerId.toB58String();
  console.log(`Node started. Own PeerId: ${ownPeerId}`);
  const targetPeerId = PeerId.createFromB58String('...');
 const message = 'Привіт, я відправляю тобі повідомлення через peer-to-peer  мережу!';
  await sendMessage(node, targetPeerId, message);
};
startNode();
```

У цьому прикладі ми створили мережевий вузол, запустили його та відправили привітання іншому вузлу у мережі через peer-to-peer з використанням libpeer-to-peer.

Однією з ключових особливостей цієї архітектури є розподілене *зберігання даних у вигляді блокчейну***.** Кожен користувач мережі має свій власний блокчейн, де зберігаються дані про їхні пости, фотографії та інші взаємодії. Використання принципів криптографії гарантує цілісність та безпеку даних, що важливо для захисту приватності користувачів. У соціальній мережі Social Grab кожен користувач має свій власний блокчейн, де зберігаються дані, такі як пости, фотографії та інші взаємодії. Блокчейн використовує принципи криптографії для гарантії цілісності та безпеки. Приклад демонструє простий блокчейн для зберігання даних у контексті соціальної мережі Social Grab.

```
const crypto = require('crypto');
class Block {
  constructor(index, timestamp, data, previousHash = '') {
    this.index = index;
    this.timestamp = timestamp;
    this.data = data;
    this.previousHash = previousHash;
    this.hash = this.calculateHash();
  }
```

```
  calculateHash() {
    return crypto
      .createHash('sha256')
      .update(
        this.index +
          this.previousHash +
          this.timestamp +
          JSON.stringify(this.data)
      )
      .digest('hex');
  }
}
class Blockchain {
  constructor() {
    this.chain = [this.createGenesisBlock()];
  }
  createGenesisBlock() {
    return new Block(0, new Date().toISOString(), 'Genesis Block', '0');
  }
  getLatestBlock() {
    return this.chain[this.chain.length - 1];
  }
  addBlock(newBlock) {
    newBlock.previousHash = this.getLatestBlock().hash;
    newBlock.hash = newBlock.calculateHash();
    this.chain.push(newBlock);
  }
  isValid() {
    for (let i = 1; i < this.chain.length; i++) {
      const currentBlock = this.chain[i];
      const previousBlock = this.chain[i - 1];
      if (currentBlock.hash !== currentBlock.calculateHash()) {
        return false;
      }
      if (currentBlock.previousHash !== previousBlock.hash) {
        return false;
      }
    }
```

```
    return true;
  }
}
const socialGrabBlockchain = new Blockchain();
socialGrabBlockchain.addBlock(
  new Block(1, new Date().toISOString(), { posts: ['Post 1', 'Post 2'] })
);
socialGrabBlockchain.addBlock(
  new Block(2, new Date().toISOString(), { photos: ['Photo 1', 'Photo 2'] })
);
console.log('Blockchain is valid:', socialGrabBlockchain.isValid());
console.log(JSON.stringify(socialGrabBlockchain, null, 2));
```

У цьому прикладі коду створюємо клас Block, який представляє блок у блокчейні, та клас Blockchain для управління цим блокчейном. Кожен користувач мережі має свій власний блокчейн, де зберігаються дані у вигляді блоків. Застосовані принципи криптографії для гарантії цілісності та безпеки даних.

Модуль ідентифікації та керування доступом у соціальній мережі Social Grab визначається децентралізованою системою автентифікації, спрямованою на забезпечення безпеки та конфіденційності користувачів. Цей модуль використовує криптографічні ключі для ідентифікації користувачів та забезпечення безпеки процесу входу в систему. В Social Grab кожен користувач отримує унікальний криптографічний ключ, який служить як основний засіб ідентифікації. Ці ключі створюються та зберігаються локально на пристрої кожного користувача, уникаючи централізованого зберігання чутливих даних на серверах. Також розроблено безпечний процес логіну. Під час процесу логіну користувач використовує свій криптографічний ключ для підпису цифрового запиту, який надсилається до блокчейну для верифікації. Цей процес гарантує безпеку та відсутність можливості перехоплення даних при автентифікації.

```
const crypto = require('crypto');
class User {
  constructor(userId) {
    this.userId = userId;
    this.cryptoKey = this.generateCryptoKey();
  }
```

```
    generateCryptoKey() {
        const currentTimestamp = new Date().getTime().toString();
        const randomValue = Math.random().toString();
        const uniqueString = currentTimestamp + randomValue;
                    return
            crypto.createHash('sha256').update(uniqueString).digest('hex');
    }
}
const user1 = new User(1);
console.log(`User ID: ${user1.userId}`);
console.log(`Crypto Key: ${user1.cryptoKey}`);
```

У цьому прикладі кожен користувач отримує свій унікальний криптографічний ключ при створенні облікового запису в мережі Social Grab. Цей ключ використовується для ідентифікації користувача та забезпечення безпеки входу в систему.

Користувачі мають повний контроль над своїми криптографічними ключами. Вони можуть генерувати нові ключі, відновлювати втрачені або створювати обмежені ключі для конкретних цілей, регулюючи рівні доступу. В разі втрати або компрометації криптографічного ключа користувача, система надає процедури безпечного відновлення доступу, забезпечуючи аутентифікацію на основі резервних ключів або інших методів підтвердження особи. Модуль ідентифікації та керування доступом в Social Grab враховує сучасні принципи криптографії та децентралізації, забезпечуючи користувачам надійний та безпечний доступ до соціальної мережі.

Смартконтракти у соціальній мережі Social Grab використовуються для автоматизації та управління правами доступу користувачів, забезпечуючи безпеку та прозорість в обміні інформацією. Цей модуль є невіддільною частиною архітектури мережі та забезпечує додатковий рівень безпеки. Смартконтракти визначають конкретні права доступу для кожного користувача. Це охоплює читання та запис на конкретних частках блокчейну, участь у певних групах чи обмін конкретними типами контенту. Використання смартконтрактів управління доступом дозволяє створювати різні ролі в мережі. Наприклад, адміністратори,

модератори, і звичайні користувачі можуть мати різні рівні доступу та повноважень.

У цьому прикладі визначено ролі «Адміністратор», «Модератор» та «Користувач», кожній з яких призначаються різні права доступу.

```
contract AccessControl {
    address public admin;
    mapping(address => string) public userRoles;
    event UserRoleChanged(address indexed user, string role);
    modifier onlyAdmin() {
        require(msg.sender == admin, "Only admin can perform this operation");  _; }
    modifier hasRole(string memory role) {
        require(keccak256(bytes(userRoles[msg.sender])) == keccak256(bytes(role)), "User does not have the required role");  _;  }
    constructor() {
        admin = msg.sender;
    }
    function changeUserRole(address user, string memory role) public onlyAdmin {
        userRoles[user] = role;
        emit UserRoleChanged(user, role);
    }
    function adminFunction() public onlyAdmin {
    }
    function moderatorFunction() public hasRole("Moderator") {
    }
}
```

Цей контракт містить елементи управління ролями та правами доступу. Модифікатори onlyAdmin та hasRole використовуються для обмеження доступу до певних функцій. Подія UserRoleChanged використовується для відстеження змін у ролях користувачів.

Користувачі можуть створювати групи або приєднуватися до існуючих. Смарт-контракти визначають правила взаємодії та обміну інформацією в групах, забезпечуючи прозорість та контроль. Смарт-контракти дозволяють ефективно використовувати ресурси мережі, бо вони визначають правила доступу та забезпечують автоматичне виконання цих правил без централізованого

управління. Кожен користувач може мати індивідуально налаштовані права доступу відповідно до його вибору та потреб. Це створює гнучкість та індивідуальний підхід до управління доступом. Смарт-контракти враховують динамічні зміни в мережі, такі як приєднання нових користувачів, створення нових груп чи зміна рівнів доступу. Це забезпечує сталу актуальність та ефективність управління доступом. Права доступу, визначені смартконтрактами, є відкритими та перевіреними для всіх користувачів. Це забезпечує прозорість та довіру у спільноті. Смартконтракти для керування доступом в соціальній мережі Social Grab демонструють високий рівень безпеки та індивідуалізації прав доступу, сприяючи безпечному та прозорому обміну інформацією в децентралізованому середовищі.

Модуль обміну даними в соціальній мережі Social Grab ґрунтується на ідеї децентралізованого сховища, що сприяє зберіганню даних користувачів у безпечному та доступному середовищі. Цей модуль гарантує надійність інформації та забезпечує контроль користувачів над своєю особистою інформацією. Усі дані користувачів, включаючи пости, фотографії, та інші взаємодії, зберігаються у децентралізованому сховищі. Це означає, що жоден централізований сервер не має повного контролю над інформацією, що покращує приватність та безпеку користувачів. Для забезпечення додаткового рівня безпеки, дані шифруються з використанням криптографічних методів. Тільки власник має ключ для розшифрування своїх особистих даних. Щоб забезпечити обмін даними у соціальній мережі Social Grab, використовується децентралізоване сховище для зберігання інформації користувачів. Нижче наведений приклад використання Node.js для роботи з децентралізованим сховищем та шифруванням даних з використанням криптографічних методів:

```
const CryptoJS = require('crypto-js');
const decentralizedStorage = {
  data: {},
  saveData: function (userId, encryptedData) {
    this.data[userId] = encryptedData;
  },
```

```
  retrieveData: function (userId) {
    return this.data[userId];
  },
};
function encryptData(data, encryptionKey) {
  return CryptoJS.AES.encrypt(data, encryptionKey).toString();
}
function decryptData(encryptedData, encryptionKey) {
  const bytes = CryptoJS.AES.decrypt(encryptedData, encryptionKey);
  return bytes.toString(CryptoJS.enc.Utf8);
}
const userId = '12345';
const userSecretKey = 'userSecretKey123';
const userData = {
  posts: ['Post 1', 'Post 2'],
  photos: ['Photo 1', 'Photo 2'],
};
const encryptedUserData = encryptData(JSON.stringify(userData), userSecretKey);
decentralizedStorage.saveData(userId, encryptedUserData);
const retrievedEncryptedData = decentralizedStorage.retrieveData(userId);
const decryptedUserData = decryptData(retrievedEncryptedData, userSecretKey);
console.log(JSON.parse(decryptedUserData));
```

Код надає огляд того, як виконується взаємодія з децентралізованим сховищем та використовувати криптографію для шифрування даних. Децентралізоване сховище передбачає систему реплікації, що гарантує наявність кількох копій даних. Це забезпечує надійність та доступність інформації в разі можливого відмову частини мережі. Кожен користувач має повний контроль над своєю особистою інформацією та керувати користувачами, з котрими може встановлювати зв’язок. Кожен користувач мережі має свій унікальний блок друзів, який знаходиться під його контролем. Це гарантує, що тільки сам користувач має доступ до свого списку друзів та вирішує, яка інформація про них буде доступна іншим користувачам.(рис. 3.1).

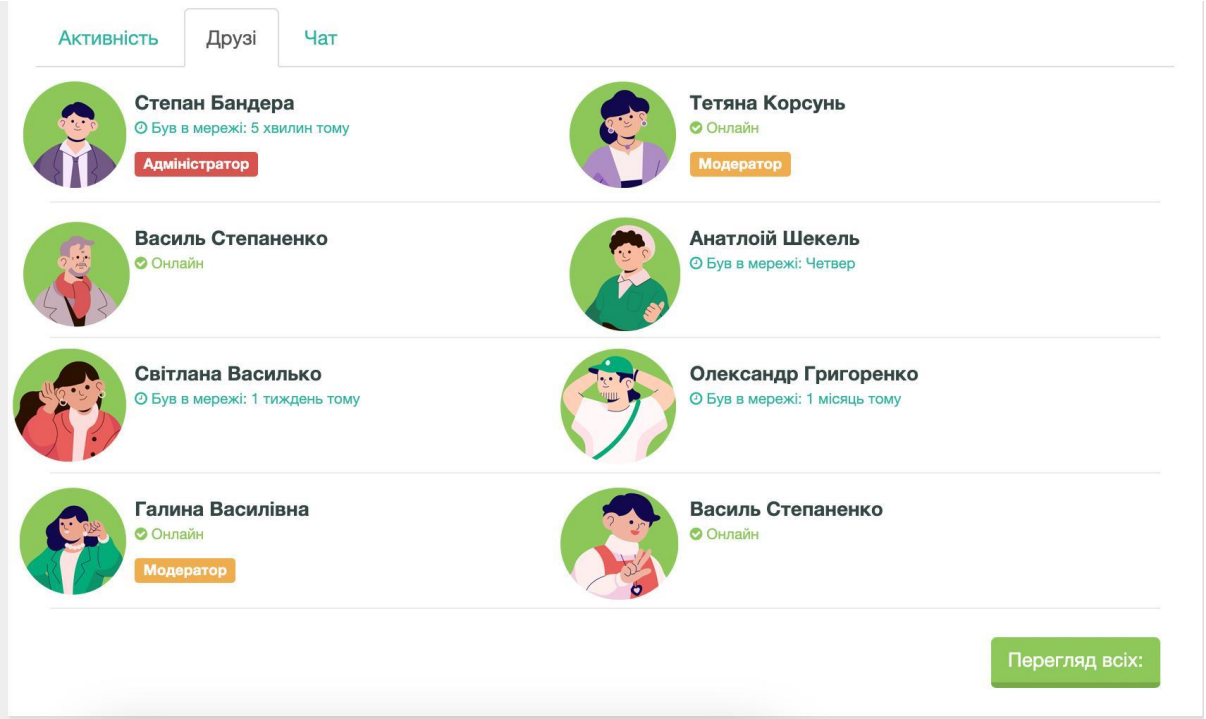


Рис. 3.1. Відображення панелі «Друзі»

Вони можуть встановлювати параметри доступу, визначати, хто може бачити їхні дані, і в будь-який момент видаляти або змінювати збережену інформацію. Модуль обміну даними також включає децентралізований пошук, що дозволяє користувачам знаходити інформацію в мережі без централізованого пошукового двигуна. Децентралізоване сховище дозволяє ефективно використовувати ресурси мережі, оскільки дані розподілені по вузлах, запобігаючи перевантаження та забезпечуючи стабільність системи.

У модулі «Винагородження за участь» соціальної мережі Social Grab використовується криптовалютна система для стимулювання та винагородження користувачів за активну участь у мережі. Ця система сприяє збільшенню залученості та розвитку спільноти. Кожна активність користувача, така як публікація постів, взаємодія з іншими користувачами, коментування та подібні, оцінюється системою, і користувачі отримують криптовалютні винагороди за ці дії. Для реалізації модуля «Винагородження за участь» у соціальній мережі Social Grab, використовується криптовалютна система. Нижче подано приклад коду мовою програмування Node.js, який ілюструє основні концепції цього модуля:

```
const crypto = require('crypto');
```

```
class User {
  constructor(userId, username) {
    this.userId = userId;
    this.username = username;
    this.balance = 0; // Баланс криптовалюти користувача
  }
  receiveReward(activityType) {
    const rewardAmount = this.calculateReward(activityType);
    this.balance += rewardAmount;
    console.log(`${this.username} отримав винагороду в розмірі ${rewardAmount} криптовалюти за ${activityType}.`);
  }
  calculateReward(activityType) {
    const randomReward = Math.floor(Math.random() * 10) + 1;
    return randomReward;
  }
}
const user1 = new User('1', 'JohnDoe');
user1.receiveReward('публікація поста');
user1.receiveReward('взаємодія з іншими користувачами');
console.log(`${user1.username} має баланс ${user1.balance} криптовалюти.`);
```

Отримані криптовалютні винагороди можуть бути використані у внутрішньому середовищі мережі. Користувачі можуть витрачати їх на покупку цифрових товарів, платити за підняття рівня, розміщення реклами чи інших послуг у межах екосистеми. Активні та творчі користувачі, які генерують цікавий та високоякісний контент, можуть отримувати більше винагороди, що стимулює розвиток творчості та інтересних ідей.

Криптовалютна система використовується для формування системи рейтингу користувачів. Високий рейтинг дозволяє отримати додаткові вигоди та привілеї у мережі. Використання криптовалютної системи в Social Grab сприяє активізації та розвитку спільноти, створюючи механізми винагородження за внесок кожного учасника.

Модуль «Взаємодії та спільноти» в Social Grab розроблений для поліпшення комунікації та взаємодії користувачів у децентралізованому середовищі. До

основних його компонентів входять децентралізований месенджер та система відслідковування активності. Вбудований децентралізований месенджер уніфікує засоби приватного спілкування та групових обговорень в одному інтерфейсі (рис. 3.2).

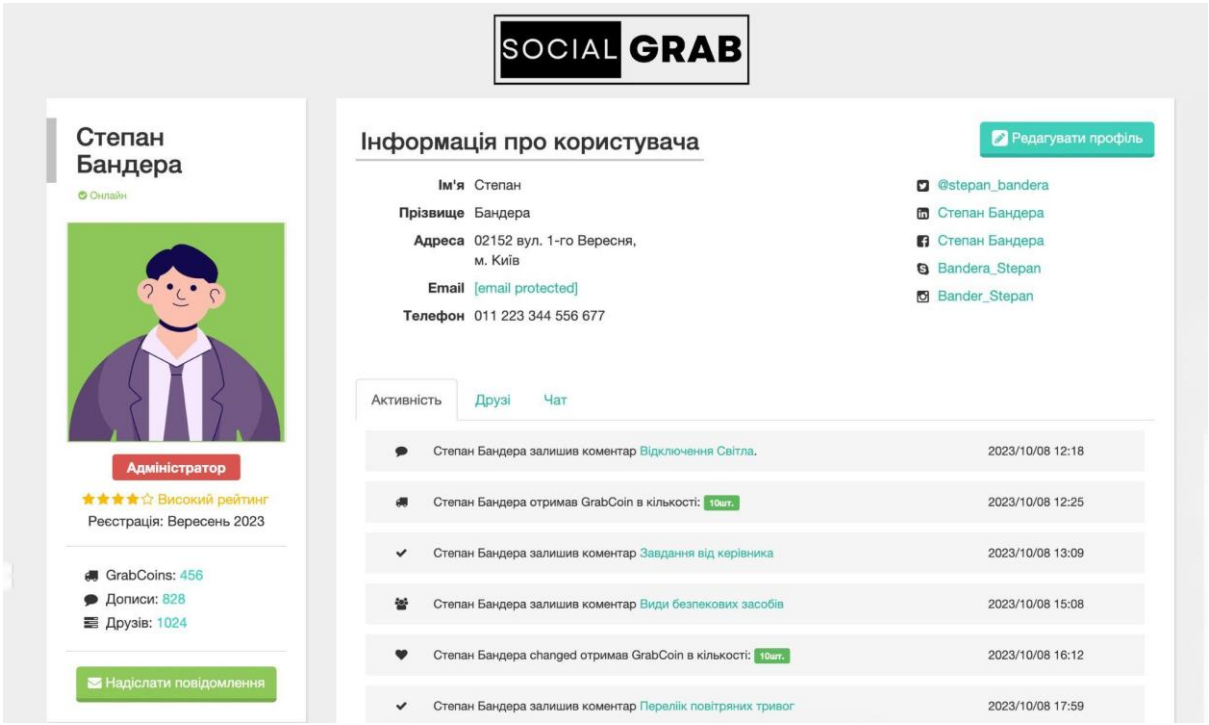


Рис. 3.2. Скріншот головної сторінки користувача

Кожен користувач отримує доступ до безпечних та шифрованих чатів, що забезпечує конфіденційність спілкування. Система відстежування активності дозволяє користувачам слідкувати за активністю інших учасників мережі та отримувати повідомлення про їхні нові пости, коментарі чи інші взаємодії. Ця система допомагає підтримувати актуальність контенту та сприяє збільшенню залученості.

Використання децентралізованого месенджера та системи відстежування активності в Social Grab підвищує рівень зручності та сприяє активній взаємодії користувачів в децентралізованому середовищі соціальної мережі (рис. 3.3).

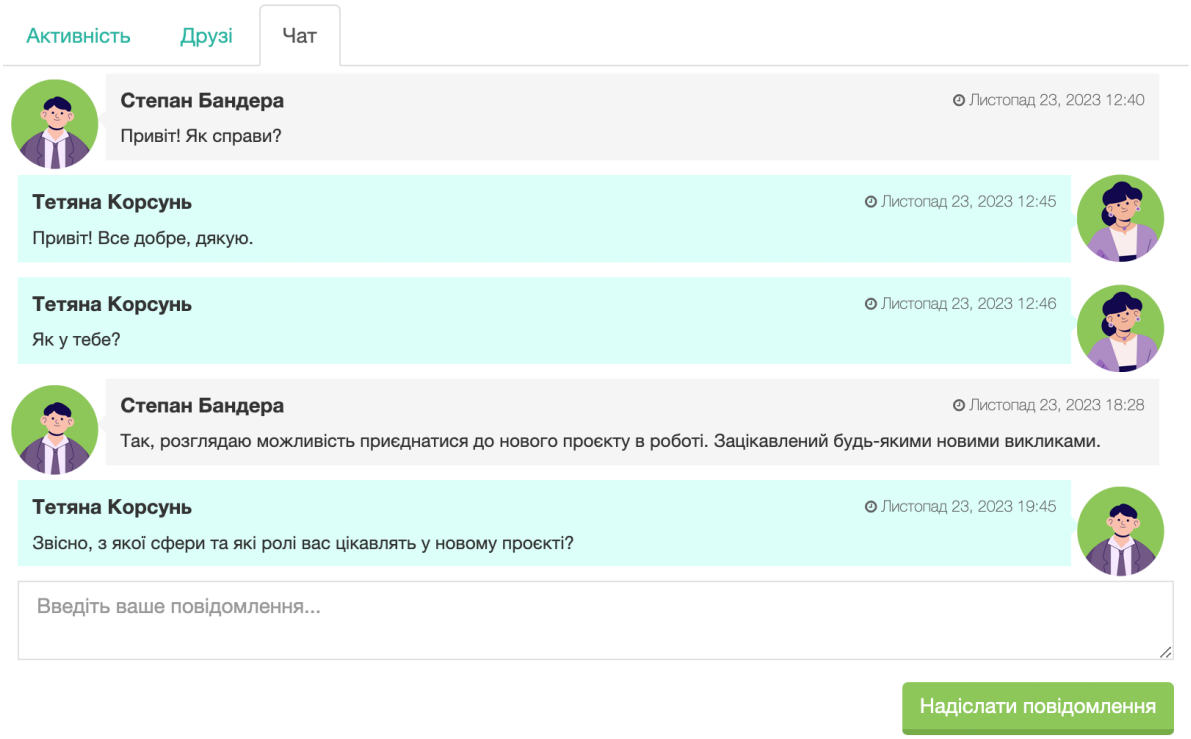


Рис. 3.3. Фрагмент месенджера соціальної мережі

Використання смартконтрактів у Social Grab не лише спрощує процес укладання угод, але й відкриває нові можливості для створення інноваційних сервісів та продуктів, що робить соціальну мережу більш динамічною та привабливою для користувачів.

Висновки до розділу 3

В цілому, сформована архітектура децентралізованої соціально мережі Social Grab націлена на реалізацію безпечного обміну інформацією між користувачами, відносного зменшення цензури, забезпечення прозорості обміну даними та створення різних інноваційних сервісів. Вона спирається на передові технології децентралізації та криптографії для досягнення цих цілей, створюючи безпечне та приватне віртуальне середовище для спілкування та обміну інформацією.

Зокрема реалізація концепції децентралізації дозволяє уникнути централізованого контролю та забезпечити високий рівень безпеки для

користувачів. Використання передових технологій криптографії допомагає захищати персональні дані користувачів та забезпечувати їхню конфіденційність у віртуальному середовищі.

Крім того, розробка Social Grab має на меті збалансоване зменшення цензури, дозволяючи користувачам вільно обмінюватися інформацією та виражати свої думки. Це важливо для створення невимушеного характеру спілкування у відкритій спільноті, де кожен має можливість вільно висловити свою точку зору.

Прозорість в роботі платформи гарантується за допомогою технології блокчейн, що дозволяє відстежувати всі операції та транзакції. Це сприяє відкритості та довірі в спільноті користувачів Social Grab, а також допомагає у запобіганні можливих конфліктів та непорозумінь.

ВИСНОВКИ

Децентралізовані соціальні мережі виявляються важливим етапом у розвитку інтернет-культури, приносячи значні переваги для користувачів та спільнот. Децентралізовані соціальні мережі надають користувачам більший контроль над їхніми особистими даними. Інформація розподіляється між учасниками, уникаючи централізованого зберігання даних, що робить систему менш вразливою до джерела інформації та несанкціонованого доступу. Децентралізовані мережі сприяють свободі висловлювання, зменшуючи можливість цензури. Користувачі можуть виражати свої думки та обмінюватися інформацією вільно, без обходження через централізований орган контролю. Окрім цього вони дозволяють уникнути великої концентрації влади в руках кількох великих компаній чи організацій. Це робить соціальні мережі більш різноманітними та менш вразливими до маніпуляцій владарів інформації.

Використання технології блокчейну в децентралізованих соціальних мережах дозволяє забезпечити прозорість операцій та транзакцій. Кожна дія може бути відстежена та перевірена, що сприяє довірі в спільноті. Користувачі мають більший контроль над власною інформацією та взаємодією в децентралізованих мережах. Вони можуть визначати правила, участь у прийнятті рішень та впливати на розвиток платформи.

Децентралізовані мережі стійкіші до цензури, оскільки дані та функції розподілені між багатьма вузлами. Це робить їх менш уразливими до атак та блокувань. Децентралізовані соціальні мережі створюють сприятливе середовище для інновацій та експериментів. Розподілена природа дозволяє впроваджувати нові ідеї та функції без необхідності одержання згоди від централізованого управління. Усі ці аспекти підкреслюють важливість децентралізованих соціальних мереж у створенні прозорого, безпечного та учасницького середовища для спілкування та обміну інформацією в онлайн-середовищі. Розроблена вебплатформа Social Grab — децентралізована соціальна мережа, в якій безпека, прозорість та свобода висловлювання є важливими пріоритетами.

Використовуючи передові технології децентралізації, криптографії та блокчейну, платформа створює безпечне та приватне віртуальне середовище для користувачів. Модель peer-to-peer, де користувачі можуть спілкуватися напряму, забезпечує високий рівень децентралізації та анонімності. Модель на основі блокчейну гарантує прозорість операцій та допомагає уникнути конфліктів.

Спрямованість на зменшення цензури вказує на бажання створення відкритого середовища, де кожен користувач має можливість висловлювати свої думки та обмінюватися інформацією вільно. Використання криптографії та технології блокчейну підсилює приватність та прозорість у спілкуванні.

Усі ці аспекти дозволяють Social Grab стати інноваційною соціальною мережею, яка враховує потреби користувачів у безпеці, конфіденційності та відкритості. Вибір поєднання моделі peer-to-peer та технології блокчейну вказує на намір платформи забезпечити користувачам великий контроль над їхніми даними та висловлюваннями. Загальною метою Social Grab є створення безпечного, ефективного та учасницького цифрового середовища для спілкування та обміну інформацією в онлайн-середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Літвін Р. Дослідження моделей децентралізованих Інтернет-служб соціальних мереж. Збірник матеріалів наукової конференції здобувачів вищої освіти фізико-математичного факультету Кам'янець-Подільського національного університету імені Івана Огієнка. 1.11.2023 року. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. С. 38-39. URL: http://elar.kpnu.edu.ua/xmlui/handle/123456789/7648
2. Мазуренко В., Штовба С. Огляд моделей аналізу соціальних мереж. *Вісник Вінницького політехнічного інституту*, 2015. №2. С. 62-74.
3. Муджирі Є. Якими соцмережами користуються українці під час війни: статистика. 2022. URL: https://speka.media/yakimi-socmerezami-koristuyutsya-ukrayinci-pid-cas-viini-doslidzennya-p22nyp (дата звернення: 24.11.2023).
4. Фронцкевич М. Роль блокчейну в децентралізованих соціальних мережах: як він допомагає покращити конфіденційність і контроль. URL: https://ts2.space/uk/роль-блокчейну-в-децентралізованих-с/#gsc.tab=0 (дата звернення: 24.11.2023).
5. Abiodun M. How a truly decentralized ethereum ensures the security and integrity of the network, 2023. URL: https://www.cryptopolitan.com/a-truly-decentralized-ethereum-network (дата звернення: 24.11.2023).
6. Activity Vocabulary. URL: https://www.w3.org/TR/activitystreams-vocabulary/ (дата звернення: 24.11.2023).
7. ActivityPub. URL: https://www.w3.org/TR/activitypub/ (дата звернення: 24.11.2023).
8. ActivityPub: from decentralized to distributed social networks. https://socialhub.activitypub.rocks/t/activitypub-from-decentralized-to-distributed-social-networks/46
9. Adere E. Blockchain in healthcare and IoT: A systematic literature review. *Array*, 2022. №14.

10. Ahlgren B., Dannewitz C., Imbrenda C., Kutscher D., Ohlman B. A Survey of Information-Centric Networking. *IEEE Communications Magazine*, 2012. №50. P.26-36.
11. Appify to Grow - Steemit, Dtube and Dsound. URL: Appify to Grow - Steemit, Dtube and Dsound. https://peakd.com/@nick-write-vegan/appify-to-grow-steemit-dtube-and-dsound (дата звернення: 24.11.2023).
12. Barnes, J. Class and Committees in a Norwegian Island Parish. *Human Relations*, 1954. №7. P. 39-58.
13. Bhagwan R. Tati K., Cheng Y., Savage S., Voelker G. Total Recall: System Support for Automated Availability Management. *Proc. of ACM/USENIX NSDI*, 2004. San Francisco. 350 p.
14. Cava L., Greco S., Tagarelli A. Understanding the growth of the Fediverse through the lens of Mastodon. Applied Network Science, 2021. № 6.
15. Cimpanu C. Steemit Social Network Hacked, User Funds Stolen, DDoS Attack Ensued. 2016. URL: https://news.softpedia.com/news/steem-social-network-hacked-user-funds-stolen-ddos-attack-followed-after-506417.shtml (дата звернення: 24.11.2023).
16. Curtin K. GIS Methods and Techniques. Comprehensive Geographic Information Systems, 2018. URL: https://www.sciencedirect.com/topics/social-sciences/network-analysis (дата звернення: 24.11.2023).
17. Dabek F., Kaashoek F., Karger D., Morris R., Stoica I. Wide-area cooperative storage with CFS. *SOSP'01: Proceedings of the eighteenth ACM symposium on Operating systems principles*, 2001. P. 202-215.
18. Dandoush A., Alouf S., Nain P. Lifetime and availability of data stored on a P2P system: Evaluation of redundancy and recovery schemes. *Computer Networks*, 2014, №64. P. 243-260.
19. Decentralized Social Networks. URL: https://www.horizen.io/academy/decentralized-social-networks/ (дата звернення: 24.11.2023).
20. Decentralized Social Networks 101. URL: https://klaytn.foundation/decentralized-social-networks-101 (дата звернення: 24.11.2023).

21. EdDSA and Ed25519. URL: https://cryptobook.nakov.com/digital-signatures/eddsa-and-ed25519 (дата звернення: 24.11.2023).
22. Electron docs. URL: https://www.electronjs.org/docs/latest/
23. Explained: What Is Web 3.0? URL: https://www.bybit.com/uk-UA/web3/raiders/learn1?id=74&from=detail&chainCode=undefined (дата звернення: 24.11.2023).
24. Fediverse: A Decentralized Network That's Reshaping the Web. URL: https://medium.com/@nickyrp/fediverse-a-decentralized-network-thats-reshaping-the-web-425ff7917303 (дата звернення: 24.11.2023).
25. Freni P., Ferro E., Moncada R. Tokenomics and blockchain tokens: A design-oriented morphological framework. Blockchain. *Research and Applications*, 2022. №3. DOI:10.1016/j.bcra.2022.100069.
26. GNU Affero General Public License. URL: https://www.gnu.org/licenses/agpl-3.0.en.html (дата звернення: 24.11.2023).
27. Greenwood W. The state of social media. How has social media evolved over the past year and what does the future look like. URL: https://browsermedia.agency/blog/state-of-social-media-2022 (дата звернення: 24.11.2023).
28. Haber S., Stornetta S. How to time-stamp a digital document. *Conference on the Theory and Application of Cryptography*. Springer, 1990. P. 437-455.
29. Huang K. What Is Mastodon and Why Are People Leaving Twitter for It? The New York Times, 2022. URL: https://www.nytimes.com/2022/11/07/technology mastodon-twitter-elon-musk.html (дата звернення: 24.11.2023).
30. Kanade V. What Is Peer-To-Peer? Meaning, Features, Pros, and Cons, 2023. URL: https://www.spiceworks.com/tech/networking/articles/what-is-peer-to-peer (дата звернення: 24.11.2023).
31. Iamnitchi A., Trunfio P. Peer-to-peer Computing. Euro-Par, 2010. URL: https://www.researchgate.net/publication/220767278_peer-to-peer_Computing (дата звернення: 24.11.2023).

32. Lipusch N., Dellermann D., Ebel P., Ghazawneh A. Token-Exchanges as a Mechanism to Create and Scale Blockchain Platform Ecosystems. *SSRN Electronic Journal*, 2019. DOI:10.2139/ssrn.3434941
33. Liu H., Zhang Y., Zhao D. Distributed Mechanism Design in Social Networks, 2023. URL: https://www.researchgate.net/publication/369035792_Distributed_Mechanism_Design_in_Social_Networks (дата звернення: 24.11.2023).
34. Mastodon: The Alternative Social Network Gaining Popularity Among Disenchanted Twitter Users. URL: https://www.todaysesquire.com/mastodon-the-alternative-social-network-gaining-popularity-among-disenchanted-twitter-users (дата звернення: 24.11.2023).
35. McNamee R. Zucked: waking up to the Facebook catastrophe. New York: Penguin Press, 2019. 352 p.
36. Minds, the 'Anti-Facebook,' Has No Idea What to Do About All the Neo-Nazis. URL: https://www.vice.com/en/article/wjvp8y/minds-the-anti-facebook-has-no-idea-what-to-do-about-all-the-neo-nazis (дата звернення: 24.11.2023).
37. Minds Features and Reviews. URL: https://thinkbiganalytics.com/minds
38. Murimi R. A Blockchain Enhanced Framework for Social Networking. *Ledger*, 2019. № 4. DOI:10.5195/ledger.2019.178.
39. Nurmi D., Brevik J., Wolski R. Modeling Machine Availability in Enterprise and Wide-Area Distributed Computing Environments. *European Conference on Parallel Processing*, 2005. p. 432–441.
40. O'Reilly T. What Is Web 2.0. 2005. URL:https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (дата звернення: 24.11.2023).
41. Popovych V., Ragimov F., Kornienko V., Ivanova I. Development of social and communicative paradigm of public administration in the field of social networks, 2020. DOI:10.5267/j.ijdns.2020.6.001.
42. Schneier B. Kelsey J. Cryptographic support for secure logs on untrusted machines. *USENIX Security Symposium*, 1998, №98. P. 53–62.

43. Scuttlebot. URL: https://scuttlebot.io/more/protocols/secure-scuttlebutt.html (дата звернення: 24.11.2023).
44. Shrimali B., Patel H. B. Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University — Computer and Information Sciences*, 2022. №34. P. 6793-6807.
45. Singh S., Hosen S., Yoon B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network., 2021. DOI: 10.1109/ACCESS.2021.3051602.
46. Social networking service? URL: https://www.ictea.com/cs/index.php?rp=%2Fknowledgebase%2F3356%2FiQue-es-una-Red-Social.html&language=english (дата звернення: 24.11.2023).
47. Social Web Protocols. URL: https://www.w3.org/TR/social-web-protocols/ (дата звернення: 24.11.2023).
48. Sociogram. URL: https://www.techtarget.com/whatis/definition/sociogram. (дата звернення: 24.11.2023).
49. Swan M. Blockchain: Blueprint for a New Economy 1st Edition. O'Reilly, 2015. P.130.
50. Tarr D., Lavoie E., Meyer A., Tschudin C. Secure Scuttlebutt: An Identity-Centric Protocol for Subjective and Decentralized Applications. *Proceedings of the 6th ACM Conference on Information-Centric Networking*, 2019. P. 1-11.
51. Tarr D. Designing a Secret Handshake: Authenticated. Key Exchange as a Capability System. Computer Science, 2015. URL: https://dominictarr.github.io/secret-handshake-paper/shs.pdf (дата звернення: 24.11.2023).
52. The Idea of #Decentralizing the #SocialMedia. URL: https://tech.anoopsavio.com (дата звернення: 24.11.2023).
53. The Rise of Web3: Navigating the Decentralized Frontier. URL: https://medium.com/@Zurlin_pro/the-rise-of-web3-navigating-the-decentralized-frontier-3bbb6a4d1a21 (дата звернення: 24.11.2023).

54. The Federation. Welcome to the new social web. URL: https://the-federation.info (дата звернення: 24.11.2023).
55. Tian Y., Wu D. On Distributed Rating Systems for Peer-to-Peer Networks. *The Computer Journal*, 2008, № 51. P. 162-180. DOI:10.1093/comjnl/bxm045
56. Token standards: ERC20 vs ERC721 vs ERC1155. URL: https://www.leewayhertz.com/erc-20-vs-erc-721-vs-erc-1155/ (дата звернення: 24.11.2023).
57. Tran M., Nguyen S., Ha S. Decentralized Online Social Network Using Peer-to-Peer Technology. *REV Journal on Electronics and Communications*, 2016, №5. P. 1-2. DOI:10.21553/rev-jec.95
58. Understanding Steem (STEEM): An In-Depth Look at the Project, 2023. URL: https://gncrypto.news/news/understanding-steem-steem-an-in-depth-look-at-the-project (дата звернення: 24.11.2023).
59. Unlocking the Power of Distributed Storage. URL: https://medium.com/@mhmt_dnc/ghost-drive-b86843bacdae (дата звернення: 24.11.2023).
60. What are blocks in a blockchain? URL: https://www.theblock.co/learn/245697/what-are-blocks-in-a-blockchain (дата звернення: 24.11.2023).
61. What is decentralized social media? Pros and Cons. URL: https://www.flatlineagency.com/blog/what-is-decentralized-social-media (дата звернення: 24.11.2023).
62. What Is Federation? URL: https://www.blueplanet.com/resources/What-Is-Federation.html (дата звернення: 24.11.2023).
63. W3c Activitypub Protocol. URL: https://dev.to/juliancantillo/w3c-activitypub-protocol-1e9g (дата звернення: 24.11.2023).
64. W3C Launches Push for Social Web Application Interoperability. URL: https://www.w3.org/news/2014/w3c-launches-push-for-social-web-application-interoperability (дата звернення: 24.11.2023).

ДОДАТКИ

Додаток А

Історія створення концепції соціальних мереж

Зародження концепції візуального представлення комунікаційних мереж бере витоки з 1934 року, коли відомий австрійсько-американський психіатр та соціальний психолог Джейкоб Леві Морено створив соціограми — абстракції соціальних взаємодій. Соціограма — це граф, у якому кожен вузол представляє компонент мережі (людину), а ребра візуалізують взаємодію між учасниками [48]. Морено використовував соціограми для вивчення поведінки невеликих груп людей, оскільки в епоху, в яку він працював, було важко отримати детальну інформацію про велику кількість особистих взаємодій. Усе змінилося з появою соціальних онлайн-мереж, таких як Facebook, Twitter, Instagram, кількість яких щороку динамічно зростає.

Термін «соціальна мережа» (англ. social network) уперше запровадив соціолог манчестерської школи Джеймс Барнс у 1954 році, задовго до появи Інтернету і сучасних мереж [41]. Він розглядав «соціальні мережі» як соціальну структуру, що охоплювала групу вузлів — соціальних об'єктів і зв'язків між ними [12]. Барнс прийшов до висновку, що розмір соціальної мережі навколо однієї людини становить приблизно 150 осіб.

Якщо говорити про поняття «соціальна мережа» в контексті інтернет-спільноти, то цей термін вперше використав Тім О’Рейлі — основоположник концепції Web 2.0 у 2005 році [40]. Першою соціальною мережею вважається Classmates.com, що з’явилася у 1995 році (США). На початку 2000-х років народились такі відомі платформи як MySpace, LinkedIn і Facebook, які і сприяли розвитку, поширенню та популяризації тренду соціальних мереж серед людей.

Як відомо, соціальні мережі в основному відрізняються одна від одної складом аудиторії (віковий параметр, гендерна приналежність, сфера інтересів). З початком повномасштабної війни в Україні, за даними GlobalLogic значно зросла кількість користувачів соціальних мереж. Це пояснюється тим, що соціальні

мережі використовують перш за все як джерело новин. Так, на основі відкритих даних з’ясовано, що у липні 2022 року соцмережами користувалися приблизно 76,6% українців, серед них 66% є користувачами Telegram, 61% — YouTube, 58% — Facebook. Більшість українців надають переваги розважальним соцмережам, і, лише 3,6 млн аккаунтів зареєстровані у LinkedIn — платформі для бізнес-комунікацій та пошуку роботи. У таких опитуваннях брала участь досить значна кількість людей з різних професійних сфер [3].

У світовому масштабі, згідно з даними Meltwater за 2022 рік «переможцями» серед усіх соціальних мереж стали Facebook, Twitter, Instagram, TikTok, LinkedIn та YouTube. Фактично, 90% користувачів використовують Facebook як частину своєї соціальної поведінки, що робить цю мережу найпопулярнішою. За ним у порядку спадання популярності використання слідують LinkedIn, Instagram, YouTube і Twitter [27].

У поняття «соціальні мережі» зараз перш за все вкладають зміст, що це інтернет-сервіси, які забезпечують формування, впорядкування, відображення відношень між учасниками мережі. Дані сервіси дозволяють створювати профілі для спілкування з іншими. Соціальні мережі характеризуються тим, що мають безліч різного контенту та дуже великі масиви даних про користувачів та їх зв’язки, які доцільно використовувати для аналізу.

Головними особливостями соціальних мереж зазвичай є наступні: широкий спектр можливостей для обміну інформацією між користувачами мережі, профілі користувачів містять певний персональний контент, реальні «друзі» у соціальних мережах переважають віртуальних.

Вебресурс соціальної мережі дозволяє користувачам взаємодіяти через основні функціональні можливості [46], такі як активне спілкування та створення профілю, який може мати публічний або закритий характер, включаючи особисті дані. Користувач також може керувати списком друзів, здійснювати взаємодію з ними через обмін повідомленнями, перегляд профілів та надсилання файлів. Додатково, є можливість перегляду взаємозв'язків між користувачами всередині соціальної платформи, а також можливість створення груп на основі спільних

інтересів для досягнення певних цілей, таких як ведення групового блогу. Користувач також має можливість управляти вмістом у межах власного профілю, використовувати синдикацію контенту, підключати різноманітні додатки та обмінюватися ресурсами, такими як покликання на дописи чи сайти.

Соціальна мережа визначається як узагальнена структура, що об'єднує множину агентів [2], представлених суб'єктами, такими як особи, спільноти, групи чи організації. Ще один компонент соціальної мережі формується через множину відносин, що включає різноманітні взаємозв'язки між учасниками, такі як знайомства, комунікація, дружба та інші форми взаємодії.

Термін «соціальна мережа» у своєму сучасному контексті визначається як віртуальна платформа чи сервіс, який дозволяє людям об'єднуватися в онлайн-спільноти, ділитися інформацією та взаємодіяти один з одним через мережу інтернет. Розподілена або децентралізована соціальна мережа — це така соціальна інтернет-мережа, яка працює децентралізовано та розподілена між різними провайдерами та спрямована на полегшення створення та інтеграції соціальних програм із відкритою вебплатформою[64]. Вона може складатися з кількох вебсайтів, на яких користувачі можуть спілкуватися з іншими авторизованими в цій мережі користувачами, які також знаходяться на будь-якому сайті цієї мережі. З соціальної точки зору, цю концепцію можна порівняти з поняттям «соціальні медіа як суспільна користь». Згідно з цією теорією сайти соціальних мереж таких, як Facebook, Twitter, YouTube, Google, Instagram, Tumblr, Snapchat тощо, є сервісами, які регулюються урядами країн, подібно до того, як регулюються послуги громадського електропостачання та телефонного зв’язку. При цьому, не дивлячись на те, що до платформ соціальних мереж застосовано монопольне керування, вони мають широку популярність серед населення та спричиняють значний соціальний вплив на різні сфери діяльності країн. Саме тому останнім часом люди все більше приділяють увагу необхідності зменшення цензури та контрольованості урядом в контексті соціальних мереж.

Загалом, глобальний вплив соціальних мереж очевидний, вони стали основним засобом комунікації та взаємодії для мільйонів користувачів. Особливо

це актуально в умовах кризи (війна, соціальні заворушення, протести), де соціальні мережі виступають основним джерелом новин та зв'язку. Загальний функціонал соціальних мереж, включаючи створення профілів, обмін повідомленнями та аналіз взаємозв'язків, робить їх універсальними інструментами для різних цілей, від розваг до бізнесу та аналізу великих обсягів даних.

Соціальні мережі визначають сучасну інтернет-культуру, що дозволяє різним спільнотам людей, окремим індивідам з різних країн світу ділитися своїми поглядами на різні події, сучасні наукові явища, висловлювати власну думку в будь-якому контексті, об'єднуватися в тематичні групи, інтернет-спільноти, вільно обмінюватися інформацією та взаємодіяти в онлайн-середовищах.

Додаток Б

Реалізація глобальної криптографічної соціальної мережі

Secure Scuttlebutt — це протокол бази даних для каналів повідомлень, які важко скомпрометувати. «Неможливо скомпрометувати» означає, що лише власник каналу може оновлювати цей канал, і це забезпечується цифровим підписом. Ця властивість робить протокол Secure Scuttlebutt корисним для однорангових додатків та мереж. Secure Scuttlebutt також дозволяє легко шифрувати повідомлення.

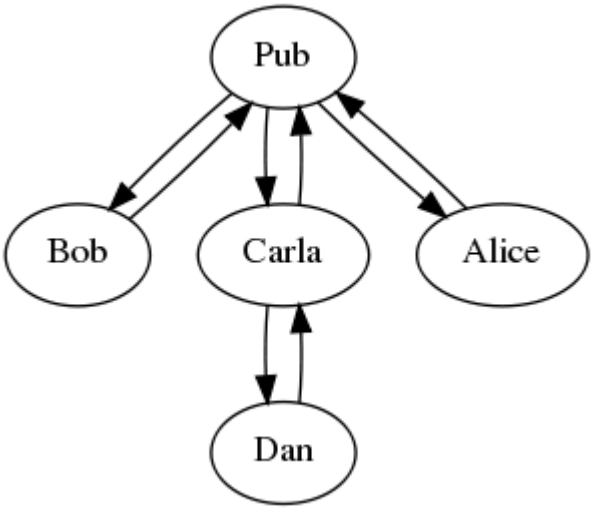
Scuttlebot формує глобальну розподілену криптографічну соціальну мережу зі своїми аналогами. Кожен користувач ідентифікується за відкритим ключем і може публікувати журнал підписаних повідомлень, за яким інші користувачі мають можливість стежити за ним у соціальних мережах.

Scuttlebot шукає в сітці peer-to-peer нові повідомлення та файли від користувачів-підписників. Повідомлення та файли зберігаються локально на невизначений термін, щоб програми могли їх читати.

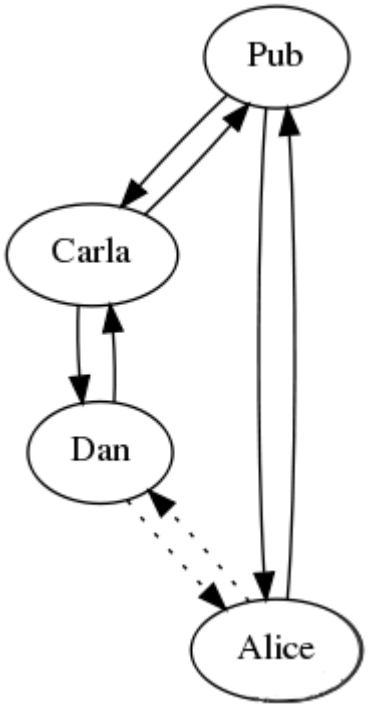
Користувачі ідентифікуються за підтвердженнями та сигналами в соціальному графі. В браузерах це надбудова категорії «Web-of-Trust» — служби онлайн-репутації та безпеки в Інтернеті, яка аналізує показники довіри до існуючих вебсайт. Рівень надійності базується як на рейтингах користувачів, так і на використанні засобів виявлення шкідливих програм, фішингу, шахрайств та спаму.

Процес викриття відбувається шляхом аналізу соціального графу або за допомогою зовнішнього обміну. Як ідентифікатора використовується відкритий ключ, сертифікатом є пара ключів, захищений криптографічною схемою цифрового підпису з відкритим ключем EdDSA [21] (Edwards-curve Digital Signature Algorithm), засновану на еліптичній кривій Едвардса. Користувачі обмінюються публічними ключами, розміщуючи їх у своїх каналах або деінде.

Протокол SSB формує глобальну мережу «пліток». Це означає, що інформація може розподілятися між кількома машинами, не вимагаючи прямих з’єднань між ними.



На схемі проілюстровано те, що «Аліса» та «Ден», не маючи «прямого зв’язку», все одно можуть обмінюватися стрічками новин:



Це відбувається тому, що плітки створюють «перехідні» зв’язки між комп’ютерами. Повідомлення «Дена» проходять через «Карлу» та центральний вузол («Pub»), щоб дістатися «Аліси», і навпаки.

Кожен ідентифікатор має лише один канал. Канал дозволяє додавати нові дані до сховища, але при цьому наявні дані залишаються незмінними і більше того ніхто не можете видалити наявне повідомлення або змінити історію. Це забезпечується блокчейном для кожного каналу та необхідно для того, щоб уся мережа сходилася в одному стані.

Система SSB базується на ідеї локального зберігання даних та можливості обміну цими даними між вузлами мережі. Кожен користувач має свій власний локальний журнал подій (log), де зберігаються всі його дані. Даний підхід сприяє децентралізації та підвищує захист від цензури [10]. Особливості Secure Scuttlebutt охоплюють безпеку та криптографічний захист даних, асинхронні повідомлення, а також можливість розміщення контенту, такого як зображення чи текст, в мережі. Інтерфейс SSB надає зручний спосіб переглядати та спілкуватися з іншими користувачами. Контент, створений користувачем у SSB, систематизований як незмінна послідовність повідомлень, доступних лише для додавання. Кожне повідомлення у цій послідовності підписується криптографічно, щоб гарантувати непідробленість усіх зв'язаних повідомлень під час їх передачі між вузлами. Вузли SSB взаємодіють, обмінюючись своїми публічними ключами та накладаючи захищене з'єднання один з одним за допомогою протоколу Authenticated Key Exchange [51]. Кожне повідомлення містить: підпис, відкритий ключ підпису, хеш вмісту попереднього повідомлення, порядковий номер, мітку часу, ідентифікатор використовуваного алгоритму хешування (наприклад, «SHA256»), контентний елемент. Наведемо приклад повідомлення на JavaScript:

```
{
  "previous": "%26AC+gU0t74jRGVeDY01...MnutGGHM=.sha256",
  "author": "@hxGxqPrplLjRG2vtjQL87...0nNwE=.ed25519",
  "sequence": 216,
  "timestamp": 1442590513298,
  "hash": "sha256",
  "content": {
    "type": "vote",
    "vote": {
      "link": "%WbQ4dq0m/zu5jxll9zUb...KjZ80JvI=.sha256",
      "value": 1
    }
  },
```

```
  "signature": "Sjq1C3yiKdmi1TWvNqxI...gmAQ==.sig.ed25519"
}
```

Secure Scuttlebutt (SSB) спеціалізується на локальному зберіганні та обміні даними, але багато користувачів використовують різноманітні клієнти з графічним інтерфейсом для спрощення використання [43]. Це призводить до розмаїття реалізацій, інтерфейсів та взаємодії з графічними елементами. Розгляньмо приклад простої взаємодії з графічним інтерфейсом у SSB на базі JavaScript:

```
const { app, BrowserWindow } = require('electron');
const path = require('path');
const sbot = require('scuttlebot/client');
const ssbClient = sbot({ appKey: require('ssb-keys') });
let mainWindow;
function createWindow() {
 mainWindow = new BrowserWindow({
 width: 800,
 height: 600,
 webPreferences: {
 preload: path.join(__dirname, 'preload.js'),
 },
 });
 mainWindow.loadFile('index.html');
 // Визначення дії при закритті вікна
 mainWindow.on('closed', function () {
 mainWindow = null;
 });
}
// Відправлення повідомлення через SSB
function sendMessage(message) {
 ssbClient.publish({ type: 'post', text: message }, (err, msg) => {
 if (err) throw err;
 console.log('Message sent:', msg);
 });
}
// Отримання з графічного інтерфейсу та відправлення повідомлення
app.whenReady().then(() => {
 createWindow();
 app.on('activate', function () {
 if (mainWindow === null) createWindow();
 });
});

// Закриття додатка при закритті всіх вікон (для платформ, які підтримують цю функцію)
app.on('window-all-closed', function () {
 if (process.platform !== 'darwin') app.quit();
});

// Отримання повідомлення з графічного інтерфейсу та відправлення
// через визначену раніше функцію sendMessage
ipcMain.on('send-message', (event, message) => {
```

```
 sendMessage(message);
});
```

У цьому прикладі використовується Electron [22], який є фреймворком для створення настільних додатків з вебтехнологій. Взаємодія з графічним інтерфейсом здійснюється через вікно, а саме відправка повідомлення у SSB під час натискання на кнопку чи введення тексту.

На основі Secure Scuttlebutt розроблено такі децентралізовані соціальні мережі:

- Manyverse, яка дозволяє користувачам створювати та переглядати контент, обмінюватися повідомленнями та взаємодіяти з іншими учасниками мережі SSB;
- Patchwork — мобільний клієнт, який дозволяє користувачам обмінюватися повідомленнями та контентом в режимі офлайн, а також створювати інтернет-спільноти навіть тоді, коли користувачі перебувають в автономному режимі.