

АНОТАЦІЯ

ЗМІСТ

Вступ	7
1 Теоретичні основи та аналіз сучасних підходів до організації електронних голосувань	9
1.1 Основи блокчейн-технології	9
1.2 Методи досягнення консенсусу у розподілених системах	10
1.3 Інноваційні підходи у технологіях електронного голосування	12
1.4 Огляд та аналіз існуючих рішень для організації голосувань	13
1.5 Висновки до розділу	14
2 Постановка завдання розробки системи та обґрунтування вибору технологій	15
2.1 Мета та завдання розробки	15
2.2 Обґрунтування вибору технологій та методів	15
2.3 Специфікація вимог	17
2.3.1 Загальний опис	17
2.3.2 Характеристики системи	18
2.3.3 Вимоги зовнішніх інтерфейсів	19
2.3.4 Інші нефункційні вимоги	20
2.4 Висновки до розділу	20
3 Проектування децентралізованого застосунку для проведення голосувань	21
3.1 Проектування загальної архітектури застосунку	21
3.2 Проектування функціональних модулів клієнтської частини	22
3.3 Проектування безпеки та конфіденційності	23

3.4	Висновки до розділу	24
4	<Розділ програмної реалізації та тестування>	26
4.1	26
4.2	Висновки до розділу	26
5	<Розділ з економіки>	27
5.1	27
5.2	Висновки до розділу	27
	Висновки	28
	Список літератури	28
А	Діаграма компонентів	31
Б	Діаграма прецедентів	32
В	Приклад інтерфейсу користувача	33

ВСТУП

У сучасному світі цифрові технології відіграють ключову роль у забезпеченні прозорості, достовірності та довіри в різних сферах суспільного життя. Однією з таких сфер є електронне голосування — інноваційний підхід до організації виборів, який дедалі частіше використовується як альтернатива традиційним паперовим методам. Електронне голосування дозволяє зменшити витрати часу та ресурсів, підвищити зручність участі, а також розширити коло учасників. Однак широке впровадження таких систем стикається з рядом викликів, серед яких — забезпечення цілісності даних, запобігання фальсифікаціям, гарантування конфіденційності виборців, а також підтвердження легітимності результатів.

Сучасні централізовані електронні системи голосування залишаються вразливими до низки загроз, включно з технічними збоями, зовнішніми атаками, внутрішніми маніпуляціями та недовірою з боку користувачів. Відсутність повної прозорості процесу створює передумови для спотворення результатів, що у свою чергу знижує рівень довіри суспільства до інституцій, які організовують такі голосування. Одним із перспективних напрямів розв’язання цих проблем є використання технології блокчейн. Блокчейн знаходить застосування в багатьох галузях, включаючи фінанси, логістику, охорону здоров’я та управління ланцюгами поставок. У контексті електронного голосування він дозволяє забезпечити прозорість, конфіденційність і захищеність голосів: кожен голос у такій системі зберігається у вигляді транзакції, яка є незмінною та відкритою для перевірки всіма учасниками. Завдяки цьому досягається високий рівень довіри до процесу голосування навіть без централізованого контролю.

Актуальність теми цієї роботи зумовлена потребою у створенні сучасних електронних систем голосування, які забезпечуватимуть високий рівень безпеки та довіри. З розвитком технологій все більше організацій, компаній та державних

установ прагнуть впроваджувати цифрові рішення для голосування, що потребує детального аналізу існуючих підходів, а також розробки нових моделей, що враховуватимуть їх переваги та недоліки.

Метою роботи є проектування системи для проведення голосувань та опитувань, яка відповідатиме вимогам прозорості, безпеки та достовірності результатів. Для забезпечення поставленої мети розроблено архітектуру системи голосування, яка відповідає вимогам безпеки, надійності та ефективності.

Для досягнення поставленої мети необхідно виконати низку задач, зокрема провести комплексне дослідження існуючих рішень у сфері електронного голосування, зосередивши увагу на системах, побудованих із використанням технології блокчейн. На основі цього слід визначити ключові переваги та недоліки таких рішень і сформулювати вимоги до безпечної, прозорої та зручної у використанні платформи для голосування. Далі потрібно спроектувати архітектуру майбутньої системи, що передбачає механізми створення голосувань, автентифікації користувачів, захисту даних і прозорої обробки результатів. Після цього необхідно реалізувати основні компоненти системи та провести тестування з метою перевірки її функціональності, стабільності роботи й відповідності визначеним вимогам безпеки.

Результати цієї роботи можуть бути використані для подальшого розвитку електронних систем голосування, а також як основа для впровадження подібних рішень у різних сферах діяльності — від державного управління до корпоративних голосувань та соціальних опитувань.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ОРГАНІЗАЦІЇ ЕЛЕКТРОННИХ ГОЛОСУВАНЬ

1.1. Основи блокчейн-технології

Блокчейн є децентралізованою технологією зберігання даних, яка дозволяє створювати надійні розподілені системи без потреби в довіреному централізованому органі. Основною її особливістю є здатність забезпечувати незмінність і прозорість інформації завдяки використанню криптографічних методів та особливої структури зберігання.

Кожен блок у блокчейні містить перелік транзакцій, хеш попереднього блоку та часову позначку [1]. Транзакції в мережі спочатку накопичуються, після чого об'єднуються в блоки — це дозволяє підвищити ефективність обробки та масштабованість системи. Блоки пов'язані між собою у послідовний ланцюг. Якщо змінити хоча б одну транзакцію в блоці, це призведе до зміни його хеша, порушить цілісність усього ланцюга й така спроба буде одразу виявлена. Завдяки цьому блокчейн є стійким до фальсифікацій і несанкціонованого втручання.

Функціонування блокчейну забезпечується одноранговою (peer-to-peer, P2P) мережею, в якій кожен вузол має власну копію ланцюга і з'єднаний безпосередньо з іншими учасниками. Вузли взаємодіють між собою, обмінюючись інформацією про транзакції та нові блоки, синхронізуючи свої копії ланцюга. Така архітектура усуває потребу в центральному сервері, забезпечуючи стійкість до збоїв, а також підвищуючи надійність і прозорість системи: усі транзакції доступні для перегляду кожному учаснику, що дозволяє перевіряти достовірність інформації без довіри до окремого адміністратора.

Таким чином, децентралізація, прозорість і незмінність — це основні риси блокчейн-систем, які роблять їх надійним фундаментом для побудови цифрових інфраструктур, включно з фінансовими платформами, ланцюгами постачання та

електронним голосуванням.

1.2. Методи досягнення консенсусу у розподілених системах

Однією з ключових складових технології блокчейн є механізм досягнення консенсусу, необхідний для узгодження єдиного порядку транзакцій та додавання нових блоків у децентралізовану мережу. У розподілених системах, де дані зберігаються та обробляються незалежними вузлами без центрального органу управління, виникає ризик розбіжностей між учасниками через одночасне надходження кількох транзакцій або через можливість недобросовісної поведінки окремих вузлів. Без механізму консенсусу система може стати вразливою до атак або втратити свою цілісність, оскільки вузли не зможуть дійти згоди щодо єдиного стану ланцюжка блоків. Ефективний механізм консенсусу вирішує ці проблеми, забезпечуючи синхронізацію дій вузлів, незмінність даних та довіру між учасниками мережі [2].

Один із найпоширеніших алгоритмів консенсусу — Proof of Work (PoW), або доказ виконаної роботи [3]. У цьому алгоритмі вузли мережі змагаються за право додати новий блок до ланцюжка, розв'язуючи складну криптографічну задачу. Перший вузол, який успішно знаходить розв'язок, отримує винагороду, а його блок додається до ланцюжка. PoW забезпечує безпеку системи завдяки високій обчислювальній складності, проте має значні недоліки, включаючи високе енергоспоживання та обмежену масштабованість.

Інший популярний алгоритм — Proof of Stake (PoS), або доказ частки володіння [4]. У цьому підході вузол, що додає новий блок, обирається пропорційно до кількості криптовалюти, яку він утримує. PoS значно знижує енергоспоживання порівняно з PoW та забезпечує вищу продуктивність, проте може викликати занепокоєння щодо концентрації влади у власників великої кількості криптовалюти.

Серед сучасних альтернативних підходів виділяється Proof of History (PoH) [5]. PoH впроваджує механізм впорядкування подій у часі за допомогою криптографічних міток часу. Це дозволяє вузлам мережі перевіряти порядок транзакцій

незалежно від інших вузлів, що значно підвищує швидкість обробки даних і забезпечує високу пропускну здатність. PoH унікальний тим, що додає часовий компонент до процесу консенсусу, що знижує необхідність тривалих узгоджень між вузлами.

Окрім основних методів консенсусу, існують інші підходи, як-от Delegated Proof of Stake (DPoS), де делегати обираються для прийняття рішень; Practical Byzantine Fault Tolerance (PBFT), який застосовується в приватних блокчейнах для забезпечення консенсусу при наявності шахраїв; Proof of Authority (PoA), де валідатори обираються на основі їх авторитету; Proof of Elapsed Time (PoET), який використовує випадковий час очікування для визначення лідера блоку; Proof of Space (PoSpace) і Proof of Capacity (PoC), що залучають вільне місце на диску для досягнення консенсусу з меншими енергетичними витратами.

Таблиця 1.1.

Порівняння алгоритмів консенсусу

Критерій	PoW	PoS	PoH
Безпека	Висока	Висока	Висока
Енергоспоживання	Високе	Низьке	Низьке
Масштабованість	Низька	Середня	Висока
Швидкість	Низька	Середня	Висока

Таким чином, різні алгоритми консенсусу забезпечують баланс між безпекою, продуктивністю та енергоспоживанням. Вибір конкретного механізму залежить від особливостей застосування блокчейну. У контексті електронного голосування важливими факторами є швидкість обробки транзакцій, масштабованість, низькі витрати та захищеність, що впливає на вибір найбільш відповідного алгоритму для створення ефективної системи. З огляду на це, для реалізації системи електронного голосування найбільш доцільним є використання алгоритму Proof of History (PoH). На відміну від PoW і PoS, PoH забезпечує високу швидкість обробки транзакцій, високу масштабованість та низьке енергоспоживання завдяки вбудованому

часовому компоненту, який дозволяє вузлам незалежно та швидко верифікувати порядок подій. Це зменшує затримки при досягненні консенсусу та є критично важливим для забезпечення швидкодії та доступності системи.

1.3. Інноваційні підходи у технологіях електронного голосування

Електронне голосування є одним із ключових напрямів цифровізації суспільства, який дозволяє підвищити зручність та доступність виборчих процесів. Традиційні електронні системи, хоч і широко використовуються, стикаються з численними викликами, зокрема щодо забезпечення прозорості, безпеки та захищеності від маніпуляцій. Сучасні інноваційні підходи у цій сфері спрямовані на вирішення цих проблем за рахунок використання новітніх технологій.

Одним із таких підходів є застосування блокчейн-технології, яка забезпечує децентралізоване зберігання даних і гарантує незмінність записів. У системах голосування на основі блокчейну кожен голос реєструється як транзакція, яка зберігається у ланцюжку блоків. Це дозволяє кожному учаснику перевірити правильність підрахунку голосів, зберігаючи при цьому конфіденційність виборців. Крім того, блокчейн унеможливорює зміну результатів голосування без відома більшості учасників, що підвищує рівень довіри до системи.

Іншим важливим напрямом є використання криптографічних методів для забезпечення безпеки та анонімності виборців. Зокрема, технології шифрування даних і цифрового підпису дозволяють гарантувати, що голос може бути зарахований лише від авторизованого виборця, а його зміст залишається недоступним для третіх сторін. Ці методи також забезпечують захист від дублювання голосів або спроб втручання у виборчий процес.

Застосування інноваційних підходів дозволяє вирішити ключові проблеми, притаманні традиційним електронним системам голосування. Проте впровадження цих технологій вимагає подолання ряду викликів, таких як висока вартість розробки, необхідність адаптації до юридичних норм та забезпечення масштабованості системи. Незважаючи на ці труднощі, інноваційні рішення відкривають нові

можливості для створення прозорих, безпечних та доступних виборчих процесів.

1.4. Огляд та аналіз існуючих рішень для організації голосувань

Системи електронного голосування існують у різних формах, починаючи від централізованих рішень, які використовуються у державних та корпоративних виборах, і закінчуючи децентралізованими платформами на основі блокчейн-технології. Кожен із цих підходів має свої переваги, недоліки та сферу застосування.

Одним із прикладів централізованих систем є використання спеціалізованих апаратних рішень. Ці системи забезпечують швидкий підрахунок голосів і зручність для виборців, але залежать від надійності та чесності центрального оператора. Недоліком таких систем є низький рівень прозорості, адже виборці не можуть незалежно перевірити результати голосування.

Системи віддаленого голосування через інтернет є ще одним поширеним централізованим рішенням. Вони дозволяють виборцям брати участь у процесі з будь-якого місця, використовуючи комп'ютер чи смартфон. Однак ці системи стикаються з проблемами кібербезпеки, включаючи ризик зламу серверів, підміни результатів голосування та витоку даних виборців.

Серед децентралізованих рішень особливе місце займають системи на основі блокчейн-технології. Наприклад, така платформа, як Voatz, використовує розподілений реєстр для реєстрації голосів [6]. Ці рішення забезпечують прозорість та незмінність даних, що підвищує довіру до процесу голосування. Водночас вони можуть стикатися з обмеженнями масштабованості, високими витратами на впровадження та складністю для кінцевих користувачів.

Уряд Естонії є лідером у сфері електронної демократії, успішно впровадивши систему i-Voting [7]. Завдяки цьому, естонські громадяни можуть голосувати онлайн, маючи електронну ID-картку. Хоча ця система не використовує блокчейн, вона демонструє ефективність і масштабованість електронного голосування у національних виборах.

Аналіз існуючих рішень показує, що централізовані системи, попри свою популярність, мають значні проблеми з безпекою та прозорістю. Натомість децентралізовані рішення на основі блокчейн-технології пропонують значні переваги, хоча й вимагають подальшого розвитку для подолання технічних і економічних бар'єрів [8].

Таблиця 1.2.

Порівняння централізованих та децентралізованих систем голосування

Критерій	Централізовані системи	Децентралізовані системи
Прозорість	Низька	Висока
Безпека	Середня	Висока
Масштабованість	Висока	Залежить від реалізації
Енергоспоживання	Низьке	Залежить від реалізації
Швидкість	Висока	Залежить від реалізації

1.5. Висновки до розділу

У цьому розділі було розглянуто основні аспекти технології блокчейн, методи досягнення консенсусу у розподілених системах, інноваційні підходи до електронного голосування та існуючі рішення для організації виборчих процесів. Аналіз існуючих рішень продемонстрував, що децентралізовані платформи на основі блокчейн-технології мають значний потенціал для вирішення ключових проблем електронного голосування. Подальший розвиток цих технологій, спрямований на подолання технічних і організаційних бар'єрів, дозволить створити прозорі, безпечні та доступні системи голосування, які відповідають сучасним вимогам.

РОЗДІЛ 2. ПОСТАНОВКА ЗАВДАННЯ РОЗРОБКИ СИСТЕМИ ТА ОБҐРУНТУВАННЯ ВИБОРУ ТЕХНОЛОГІЙ

2.1. Мета та завдання розробки

Метою цієї роботи є створення системи електронного голосування, яка забезпечує прозорість, безпеку та довіру до результатів. Система має вирішити проблеми централізованих рішень, такі як залежність від операторів і ризик маніпуляцій.

Завдання розробки включають аналіз існуючих систем для визначення вимог, розробку архітектури з ключовими модулями, реалізацію програмної частини та перевірку системи на відповідність вимогам. Вхідними даними для системи є реєстраційна інформація, параметри голосування та подані голоси, а вихідними — результати голосування, зашифровані записи та сповіщення про статус голосу. Основною метою є створення надійної системи, що відповідає сучасним стандартам прозорості та захищеності.

2.2. Обґрунтування вибору технологій та методів

Як видно з таблиці 1.2., децентралізовані системи голосування мають значні переваги порівняно з централізованими, зокрема високу прозорість та безпеку. Саме тому для розробки системи обрано блокчейн як технологічну основу. Однак для ефективного використання цих переваг необхідно обрати блокчейн-платформу, яка забезпечує високу масштабованість, низьке енергоспоживання та швидкість обробки транзакцій. Саме тому для реалізації системи було обрано платформу Solana, яка завдяки інноваційному механізму консенсусу Proof of History (PoH) демонструє високу продуктивність і стабільну роботу навіть за великого навантаження, що є критично важливим для системи голосування з великою кількістю учасників. Solana здатна обробляти до 65,000 транзакцій за секунду (TPS) [9], що значно перевищує показники багатьох інших блокчейн-платформ.

Мову програмування для розробки смарт-контрактів було обрано Rust. Однією з основних причин вибору Rust є його висока продуктивність та безпека. Rust дозволяє контролювати управління пам'яттю без використання збирача сміття, що дозволяє досягати кращої ефективності та передбачуваності в порівнянні з іншими мовами. Мова забезпечує гарантії безпеки пам'яті через систему власності і запозичення, що дозволяє уникати багатьох типових помилок, таких як витоки пам'яті або доступ до неініціалізованої пам'яті, зберігаючи високу продуктивність. Такий підхід є особливо важливим при розробці смарт-контрактів для блокчейн-платформи, де потрібно обробляти великі обсяги транзакцій і зберігати ефективність виконання програм при обмежених ресурсах. Завдяки цьому Rust є ідеальним вибором для розробки смарт-контрактів на Solana.

Для спрощення процесу розробки смарт-контрактів на Solana було обрано використання бібліотеки Anchor. Anchor - це фреймворк для розробки смарт-контрактів, який забезпечує більш високий рівень абстракції і значно спрощує роботу з Solana, дозволяючи швидше і безпечніше створювати смарт-контракти. Anchor також допомагає в автоматизації багатьох аспектів розробки, таких як перевірка транзакцій, підписання і виконання, що дозволяє зосередитися на бізнес-логіці, а не на низькорівневих деталях взаємодії з блокчейном.

Важливою частиною застосунку є інтеграція з криптовалютним гаманцем для забезпечення безпечного доступу користувачів до системи. Вибір Phantom Wallet зумовлений не лише його популярністю серед користувачів Solana, а й зручністю для розробників. Phantom надає простий інтерфейс для взаємодії зі смарт-контрактами, що значно спрощує інтеграцію з блокчейном і пришвидшує розробку. Він також підтримує безпечне зберігання ключів і легке підтвердження транзакцій, що робить його оптимальним вибором для системи голосування.

Для клієнтської частини застосунку обрано React, що дозволяє створювати зручні та інтерактивні веб-додатки. Завдяки своїй популярності і широкій підтримці бібліотек, React забезпечує гнучкість і масштабованість, необхідні для розробки інтерфейсу користувача для системи голосувань.

2.3. Специфікація вимог

Призначенням застосунку є забезпечення прозорого, безпечного та незмінного процесу голосування завдяки використанню технології блокчейну. Він дозволяє організаторам ініціювати голосування, визначати варіанти вибору та переглядати результати, а учасникам безпечно віддавати свої голоси.

2.3.1. Загальний опис

2.3.1.1. Характеристики продукту

Продукт складається з двох основних модулів. Один з них реалізує функціонал голосування на блокчейні, що охоплює створення, участь та підрахунок результатів голосувань із забезпеченням прозорості та незмінності даних. Інший модуль надає інтерфейс для взаємодії користувачів із системою, з можливістю налаштування голосувань, подачі голосів та перегляду результатів.

2.3.1.2. Класи користувачів та їх характеристики

Користувачі системи поділяються на два класи:

- Організатор голосування – користувач, який створює та налаштовує голосування, визначає варіанти для голосування та переглядає результати. Організатор може також брати участь у голосуванні, голосуючи за один з варіантів, як звичайний учасник.
- Учасник голосування (виборець) – користувач, який бере участь у голосуванні, подає голос за обраний варіант та переглядає результати. Учасник має доступ лише до голосування та результатів, без можливості управління голосуванням.

2.3.1.3. Середовище функціонування

Програмний продукт функціонує у децентралізованому середовищі блокчейну Solana. Клієнтська частина розроблена для роботи у сучасних веб-браузерах, взаємодіє зі смартконтрактом через RPC-сервіси Solana.

2.3.2. Характеристики системи

2.3.2.1. Створення голосування

Опис: Організатор може створювати голосування з заданими параметрами.

Пріоритет: Високий.

Послідовність дія/відгук:

1. Організатор входить у застосунок.
2. Вибирає опцію створення голосування.
3. Вводить параметри голосування (назва, опис, варіанти, час до завершення).
4. Підтверджує створення голосування.
5. Система перевіряє дані та публікує голосування у блокчейні.
6. Система повідомляє організатора про успішне створення.

Функціональні вимоги:

REQ-1.1: Система має забезпечувати форму для параметрів голосування.

REQ-1.2: Система перевіряє коректність введених даних.

REQ-1.3: Система інтегрується зі смартконтрактом для запису даних у блокчейн.

2.3.2.2. Участь у голосуванні

Опис: Виборець може подати свій голос за один із варіантів голосування.

Пріоритет: Високий.

Послідовність дія/відгук:

1. Виборець входить у систему.
2. Вибирає активне голосування.
3. Обирає варіант голосування.
4. Підтверджує вибір.
5. Система перевіряє валідність голосу (уникнення повторного голосування).
6. Система записує голос у блокчейн.
7. Виборець отримує підтвердження успішного голосування.

Функціональні вимоги:

REQ-2.1: Система має дозволяти вибір варіанту голосування.

REQ-2.2: Система перевіряє валідність голосу перед його подачею.

REQ-2.3: Система записує голос через смартконтракт у блокчейн.

2.3.2.3. Перегляд результатів голосування

Опис: Учасники можуть переглядати результати після завершення голосування.

Пріоритет: Середній.

Послідовність дія/відгук:

1. Користувач входить у систему.
2. Вибирає завершене голосування.
3. Вибирає опцію перегляду результатів.
4. Система зчитує дані з блокчейну.
5. Відображає результати голосування у графічному вигляді.

Функціональні вимоги:

REQ-3.1: Система має дозволяти доступ до завершених голосувань.

REQ-3.2: Система інтегрується зі смартконтрактом для отримання даних.

REQ-3.3: Система візуалізує результати у зручному форматі.

2.3.3. Вимоги зовнішніх інтерфейсів

2.3.3.1. Користувацькі інтерфейси

Користувач взаємодіє із системою через веб-інтерфейс, що включає:

- Екран створення голосування (форма з введенням параметрів голосування).
- Екран участі у голосуванні (вибір варіанта і підтвердження).
- Екран перегляду результатів (графічна візуалізація результатів голосування).
- Екран авторизації за допомогою Phantom Wallet для підтвердження особи користувача перед участю у голосуванні.
- Екран вибору кластеру мережі Solana.
- Екран управління акаунтом у мережі Solana.

2.3.4. Інші нефункційні вимоги

2.3.4.1. Вимоги продуктивності

- Час підтвердження голосу не повинен перевищувати 3 секунд (Не враховуючи час на взаємодію з гаманцем Phantom Wallet).
- Час відображення результатів голосування не повинен перевищувати 5 секунд.
- Система має підтримувати одночасну участь до 1000 користувачів без значного зниження продуктивності.

2.3.4.2. Вимоги безпеки

- Доступ до адміністрування голосувань дозволено лише організаторам.
- Користувачі не можуть проголосувати більше одного разу в межах одного голосування.
- Голоси, подані користувачами, повинні бути перевірені на валідність перед записом у блокчейн.

2.3.4.3. Атрибути якості програмного продукту

- Код повинен бути модульним і читабельним, щоб спрощувати майбутню розробку та підтримку.
- Система повинна залишатися працездатною при втраті з'єднання з блокчейном і коректно відновлювати роботу після повторного з'єднання.
- Усі функції мають бути покриті автоматичними тестами для забезпечення відповідності вимогам.

2.4. Висновки до розділу

У цьому розділі було сформульовано мету та завдання розробки, а також обґрунтовано вибір технологій, алгоритмів і інструментів, які використовуються для реалізації системи голосування. Проаналізовано вимоги до системи, включаючи функціональні та нефункціональні аспекти, що дозволило визначити ключові параметри, необхідні для забезпечення її надійності, безпеки та зручності використання.

РОЗДІЛ 3. ПРОЄКТУВАННЯ ДЕЦЕНТРАЛІЗОВАНОГО ЗАСТОСУНКУ ДЛЯ ПРОВЕДЕННЯ ГОЛОСУВАНЬ

3.1. Проєктування загальної архітектури застосунку

Архітектура застосунку для проведення голосувань базується на принципах децентралізації, прозорості та безпеки, що є фундаментальними вимогами для сучасних електронних систем голосування. Застосунок складається з трьох основних компонентів: клієнтської частини, смарт-контракту та блокчейн-платформи Solana. Кожен компонент виконує визначені функції у процесі голосування, забезпечуючи ефективну та безпечну взаємодію між користувачами та блокчейном.

Клієнтська частина, реалізована з використанням фреймворку React, надає користувачам інтуїтивно зрозумілий інтерфейс. Організатори за допомогою клієнтської частини створюють голосування, а учасники - подають свої голоси та переглядають результати. Взаємодія із блокчейном здійснюється через RPC-інтерфейс платформи Solana. Кожна дія користувача, така як голосування чи перегляд результатів, ініціює транзакцію, яка передається на обробку до смарт-контракту.

Смарт-контракт, розгорнутий у мережі Solana, виконує функції логічного ядра системи. Він відповідає за реєстрацію голосів, перевірку їхньої валідності та підрахунок результатів. Кожен голос фіксується у блокчейні у вигляді транзакції, що гарантує його незмінність і можливість перевірки будь-яким учасником мережі, забезпечуючи прозорість процесу та неможливість маніпулювання результатами.

Інтеграція з гаманцем Phantom Wallet є критичним елементом архітектури, що забезпечує безпечне зберігання приватних ключів користувачів та підпис транзакцій. Підписання транзакцій приватним ключем є обов'язковою умовою для подачі голосу, що гарантує автентичність кожного голосу. Таким чином, Phantom Wallet виконує роль безпечного посередника між користувачем і смарт-контрактом.

Децентралізована архітектура дозволяє уникнути централізованого контролю

над процесом голосування, забезпечуючи високий рівень довіри до системи. Зберігання голосів у блокчейні унеможливорює їхню зміну або видалення, що створює надійний механізм підтвердження результатів голосування.

Взаємодія між клієнтською частиною, смарт-контрактом та гаманцем Phantom Wallet організована таким чином, щоб забезпечити надійність, безпеку та прозорість кожного етапу голосування. Схематичне відображення взаємодії між компонентами представлено на діаграмі компонентів у Додатку А.

3.2. Проєктування функціональних модулів клієнтської частини

Функціональні можливості клієнтської частини застосунку організовані навколо п'яти основних модулів, які забезпечують повний життєвий цикл голосування та управління обліковим записом користувача. Кожен модуль взаємодіє зі смарт-контрактом або безпосередньо з блокчейн-платформою Solana, що гарантує високий рівень безпеки, прозорості та ефективності роботи системи. Детальну взаємодію модулів відображено на діаграмі прецедентів у Додатку Б. Приклад інтерфейсу користувача зображено у Додатку В

Перший модуль призначений для створення голосувань. Організатори можуть вводити параметри голосування, включно з назвою, описом, варіантами відповідей та часом до завершення. Після перевірки правильності введених даних інформація про голосування записується у блокчейн, що забезпечує її незмінність і відкритість для всіх користувачів мережі.

Другий модуль реалізує процес подання голосів. Він дозволяє користувачам вибирати один із запропонованих варіантів та подавати свій голос, одночасно контролюючи унікальність кожного голосування. Кожен голос фіксується як окрема транзакція у блокчейні, що гарантує його достовірність і захист від підробки або багаторазового голосування.

Третій модуль забезпечує перегляд результатів голосування. Учасники можуть отримувати результати безпосередньо з блокчейну, що виключає можливість їх фальсифікації. Додатково модуль підтримує візуалізацію даних у графічному

вигляді, що полегшує сприйняття інформації та її подальший аналіз.

Четвертий модуль відповідає за перегляд інформації про обліковий запис користувача. Він надає можливість переглядати баланс облікового запису у валюті SOL, а також переглядати історію транзакцій, пов'язаних із цим обліковим записом. Це дозволяє користувачам контролювати свої кошти та відстежувати всі операції, здійснені через застосунок.

П'ятий модуль реалізує функціональність вибору кластеру блокчейн-мережі Solana. Користувачі можуть вибирати між основними доступними кластерами або додавати власні адреси кластерів для роботи з приватними або тестовими мережами. Це забезпечує гнучкість у використанні застосунку в різних середовищах.

3.3. Проєктування безпеки та конфіденційності

Забезпечення безпеки та конфіденційності є фундаментальним елементом архітектури застосунку для голосувань, оскільки саме ці аспекти формують базову довіру користувачів до легітимності та незворотності результатів. У рамках розробки системи було впроваджено багатошарову модель захисту, яка використовує передові методи криптографії, протоколи шифрування та алгоритмічні механізми валідації даних.

Для унеможливлення повторного голосування застосовується система валідації унікальності транзакцій. Кожен голос супроводжується унікальним криптографічним маркером, що генерується на основі комбінації відкритого ключа користувача, даних про голосування та випадкового доповнення. Смарт-контракт на рівні Solana Runtime Environment аналізує ці маркери і здійснює детерміновану валідацію автентичності кожного голосу у режимі реального часу.

Щодо перевірки валідності голосу, перед його зарахуванням виконується перевірка підпису транзакції приватним ключем користувача. Додатково, перед надсиланням транзакції у мережу, відбувається локальна верифікація за допомогою Phantom Wallet SDK, що гарантує збереження приватного ключа у зашифрованому середовищі пристрою користувача без жодної можливості його витоку в мережу.

Анонімність учасників забезпечується шляхом використання псевдонімізації, де кожному користувачеві призначається унікальний криптографічний ідентифікатор. Ідентифікатор створюється на основі випадково згенерованого ентропійного значення та додаткових криптографічних операцій, що не дозволяють встановити зв'язок із особистими даними користувача. Відповідність голосу певному ідентифікатору перевіряється без розкриття особистості голосуючого, що забезпечує приватність даних у процесі голосування.

Блокчейн-технологія забезпечує високий рівень захисту від кібератак та маніпуляцій з даними завдяки своїм властивостям. Після того як голос зареєстрований у блокчейні, його неможливо змінити або видалити. Це забезпечується завдяки структурі блокчейну, що гарантує незмінність і стійкість до маніпуляцій завдяки криптографічному зв'язку блоків через унікальні хеші. Кожна зміна будь-якого елемента даних миттєво призводить до розриву зв'язності у мережі, що робить підробку практично неможливою без повного контролю над переважною більшістю вузлів (чого досягти надзвичайно складно через географічну та інституційну децентралізацію мережі).

Крім того, блокчейн Solana застосовує унікальну модель консенсусу Proof of History (PoH) у комбінації з Tower BFT - гібридний механізм, що забезпечує високу пропускну здатність транзакцій без зниження безпеки. Proof of History синхронізує події у часовій шкалі за допомогою криптографічних часових міток, що унеможливорює атаки типу "подвійного витрачання" навіть при високих навантаженнях на мережу. Ця властивість дозволяє системі підтримувати мілісекундні затримки обробки та мільйонні обсяги транзакцій на годину.

3.4. Висновки до розділу

У цьому розділі було розглянуто архітектуру децентралізованого застосунку для проведення голосувань, яка побудована на основі блокчейн-технології Solana. Кожен компонент системи взаємодіє з іншими через смарт-контракт, що забезпечує прозорість, безпеку та незмінність результатів голосування. Клієнтська части-

на застосунку, розроблена з використанням React, надає користувачам інтуїтивно зрозумілий інтерфейс для участі в голосуванні, а інтеграція з Phantom Wallet дозволяє здійснювати безпечну авторизацію та підпис транзакцій.

Важливими аспектами проектування є забезпечення високої безпеки та конфіденційності голосів. Використання криптографічних методів і анонімних ідентифікаторів гарантує, що голоси не можуть бути підроблені чи змінені після їх реєстрації в блокчейні. Усі транзакції зберігаються в Solana, що дозволяє забезпечити їх незмінність завдяки механізму консенсусу Proof of History. Це робить застосунок ефективним і надійним інструментом для проведення прозорих та безпечних голосувань.

РОЗДІЛ 4. <РОЗДІЛ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ ТА ТЕСТУВАННЯ>

4.1.

4.2. Висновки до розділу

РОЗДІЛ 5. <РОЗДІЛ 3 ЕКОНОМІКИ>

5.1.

5.2. Висновки до розділу

ВИСНОВКИ

СПИСОК ЛІТЕРАТУРИ

- [1] Awosika E. What Is Blockchain Voting?. URL: <https://second-pocket-shoot-73.hashnode.dev/what-is-blockchain-voting>
(дата звернення 22.01.2025)
- [2] PoH, PoS, PoW - Explained. *Helius*. URL: <https://www.helius.dev/blog/proof-of-history-proof-of-stake-proof-of-work-explained>
(дата звернення 22.01.2025)
- [3] Porat, A., Pratap, A., Shah, P. Blockchain Consensus: An analysis of Proof-of-Work and its applications. *Stanford University*. URL: https://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf
(дата звернення 22.01.2025)
- [4] C. T. Nguyen, D. T. Hoang, D. N. Nguyen. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access*. 2019. Ст. 5-9. DOI: 10.1109/ACCESS.2019.2925010.
- [5] Victor S. Proof of history: what is it good for? URL: <https://www.shoup.net/papers/poh.pdf>
(дата звернення 22.01.2025)
- [6] Security and technology. *Voatz*. URL: <https://voatz.com/security-and-technology/>
(дата звернення 22.01.2025)
- [7] Introduction to i-voting. *Valimised*. URL: <https://www.valimised.ee/en/internet-voting/more-about-i-voting/introduction-i-voting>

(дата звернення 17.01.2025)

- [8] Almeida, R. L., Baiardi, F., Maesa, D. D. F., & Ricci, L. Impact of Decentralization on Electronic Voting Systems: A Systematic Literature Survey. *IEEE Access*. 2023. Ст. 31. DOI: 10.1109/ACCESS.2023.3336593.

- [9] Network Performance Report - October 2022. *Solana*. URL: <https://solana.com/news/network-performance-report-october-2022>

(дата звернення 18.03.2025)

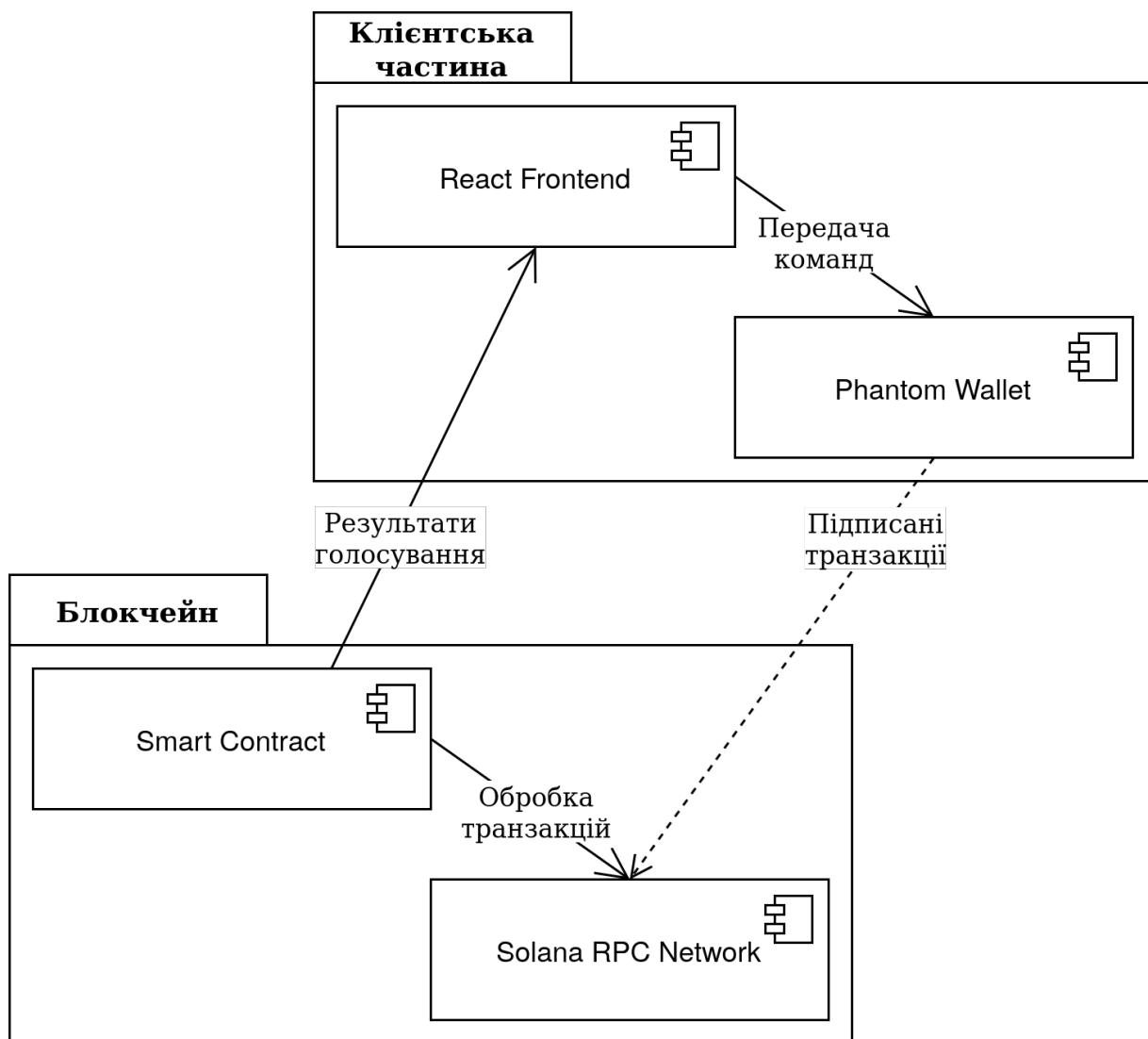
ДОДАТОК А. ДІАГРАМА КОМПОНЕНТІВ

Рис. А.1 Діаграма компонентів

ДОДАТОК Б. ДІАГРАМА ПРЕЦЕДЕНТІВ

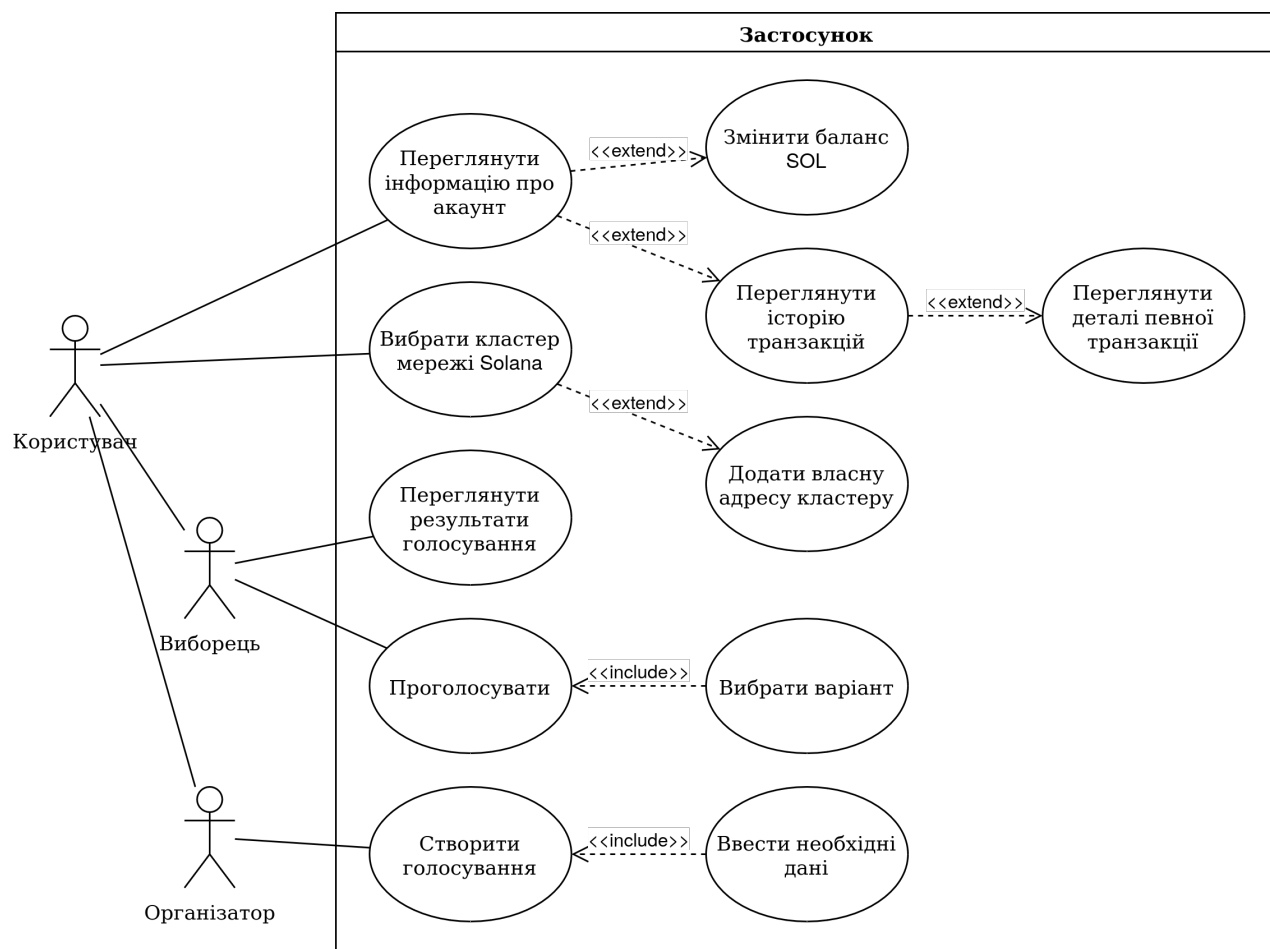


Рис. Б.1 Діаграма прецедентів

ДОДАТОК В. ПРИКЛАД ІНТЕРФЕЙСУ КОРИСТУВАЧА

Votingdapp

Create a new poll by clicking the "Create" button. The state of a poll is stored on-chain.

2VmZ...S7at

Create Poll

A or B

Рис. В.1 Перегляд списку голосувань

Poll Name

Description

Poll Duration

Minutes

Candidate 1

Candidate 2

Add Candidate

Create Poll

Close

Рис. В.2 Форма для створення голосування

A or B

Choose one
Time left: 13m 58s

Candidates

A
0 votes

Vote

B
0 votes

Vote

Close

Рис. В.3 Форма для подачі голосу

2.99018 SOL

3E7J...jsbB

Airdrop Send Receive

Token Accounts

No token accounts found.

Transaction History

Signature	Slot	Block Time	Status
<u>3ksEbDsY...mw9zyEe3</u>	<u>20170</u>	2025-04-26T16:10:12.000Z	Success

Рис. В.4 Відображення інформації про баланс акаунту та історії транзакцій

Clusters

Manage and select your Solana clusters

Add Cluster




Name/ Network / Endpoint	Actions
devnet Network: devnet https://api.devnet.solana.com	
local Network: custom http://localhost:8899	
testnet Network: testnet https://api.testnet.solana.com	

Рис. В.5 Сторінка зі списком кластерів мережі