# АНОТАЦІЯ

# ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ, СИМВОЛІВ І СПЕЦІАЛЬНИХ ТЕРМІНІВ

**BFT** Byzantine Fault Tolerance.

**DPoS** Delegated Proof of Stake.

**HTTP** Hypertext Transfer Protocol.

**HTTPS** Hypertext Transfer Protocol Secure.

**P2P** Peer-to-Peer.

**PBFT** Practical Byzantine Fault Tolerance.

**PoA** Proof of Authority.

**PoC** Proof of Capacity.

**PoET** Proof of Elapsed Time.

**PoH** Proof of History.

**PoS** Proof of Stake.

**PoSpace** Proof of Space.

**PoW** Proof of Work.

**RPC** Remote Procedure Call.

**SDK** Software Development Kit.

**TPS** транзакції на секунду.

# 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 спроєктувати 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. На рис 1.1 зображено загальну структуру блокчейну, що ілюструє зв'язки між блоками, їхній вміст та хеш-значення попередніх блоків [1].

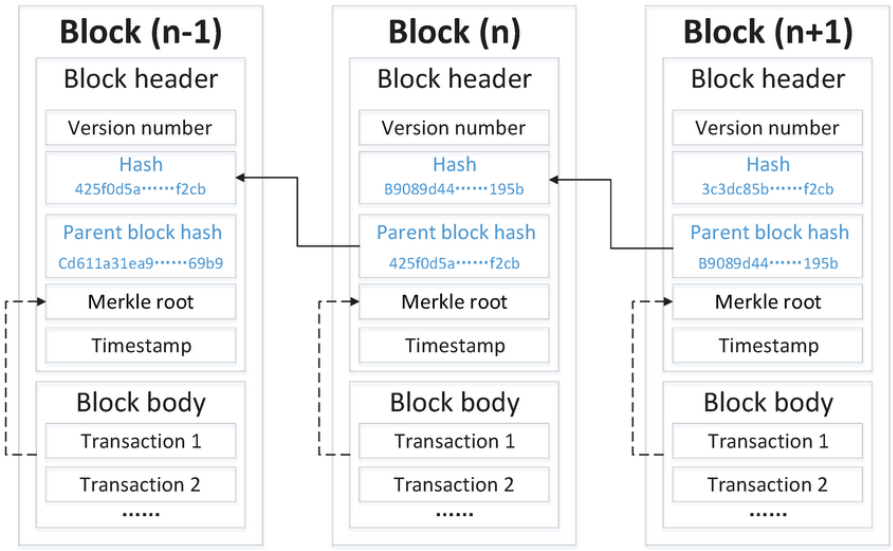


Рис. 1.1 Схема структури блокчейну

Кожен блок у блокчейні містить перелік транзакцій, хеш попереднього блоку та часову позначку [2]. 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 [3].

Один із найпоширеніших алгоритмів консенсусу — Proof of Work (PoW), або доказ виконаної роботи [4]. 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 [5]. 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) [6]. 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.

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 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.

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. Проте ці алгоритми не набули широкого використання, оскільки використовуються переважно в специфічних умовах.

### 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 пра-

вильність підрахунку голосів, зберігаючи при цьому конфіденційність виборців. Крім того, блокчейн унеможливлює 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 голосування постійно еволюціонують, охоплюючи як традиційні офлайн та онлайн централізовані моделі, так і новітні децентралізовані рішення. Вибір підходу залежить від цілей, масштабу, вимог до безпеки та ступеня довіри між учасниками процесу.

Одним із найпоширеніших підходів є централізовані офлайн-системи голосування, які використовуються на виборчих дільницях. Вони базуються на спеціалізованому апаратному та програмному забезпеченні (електронні урни, сканери бюлетенів), контрольованому єдиним оператором або групою довірених органів. Такі системи забезпечують високу швидкість обробки голосів і зручність для виборчих комісій. Проте вони мають суттєві недоліки: обмежена прозорість для виборців, потреба в повній довірі до адміністратора системи, ризики технічних збоїв або втручання в ланцюг постачання обладнання.

Іншим різновидом є централізовані онлайн-системи голосування, які забезпечують дистанційну участь виборців через інтернет. Вони реалізуються як веб- або мобільні додатки і особливо корисні в умовах пандемій чи для виборців за кордоном. Попри зручність, ці системи мають свої виклики: захист від кібератак, гарантія цілісності та конфіденційності голосів, запобігання повторному голосуванню, а також складність незалежної верифікації результатів.

У зв'язку з викликами, притаманними централізованим рішенням, зростає зацікавленість у децентралізованих системах голосування, зокрема на основі блокчейн-технологій. У таких системах дані про голоси зберігаються в розподіленому реєстрі, змінити який без консенсусу учасників мережі практично неможливо. Платформи на кшталт Voatz декларують використання блокчейну для досягнення прозорості, незмінності та довіри [7]. Водночас Voatz критикували за закритість вихідного коду та виявлені вразливості [8], що підкреслює важливість відкритості й незалежного аудиту в таких рішеннях.

Ще одним прикладом масштабного впровадження електронного голосування є система i-Voting в Естонії [9], яка з 2017 року дає громадянам змогу голосувати онлайн із використанням електронного підпису. Хоча ця система не базується на блокчейні, вона спирається на перевірену інфраструктуру електронної ідентифікації та шифрування й продемонструвала на практиці свою ефективність у загальнодержавному масштабі.

Для кращого розуміння відмінностей між централізованими та децентралізованими підходами у сфері електронного голосування, у таблиці 1.2. наведено порівняння ключових характеристик обох типів систем за основними критеріями, що впливають на їхню ефективність, надійність та придатність до практичного використання. Оскільки існують різні реалізації блокчейнів, кожен з яких має свої характеристики, показники децентралізованих систем можуть суттєво варіюватися в залежності від вибраної платформи.

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 |

Аналіз демонструє, що централізовані рішення переважають у зрілості та практичності, проте обмежені в прозорості та довірі. Натомість децентралізовані рішення пропонують привабливу альтернативу, що вимагає вирішення проблем масштабованості, складності впровадження, зручності для користувачів та юридичного регулювання [10]. Зважаючи на ці фактори, дослідження в напрямку побудови блокчейн-орієнтованих систем електронного голосування є актуальним і перспективним.

## 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 роботи є створення функціональної та надійної системи електронного голосування, яка забезпечить підвищення прозорості, безпеки та довіри до процесу волевиявлення шляхом застосування технології блокчейн. Розроблена система має вирішити існуючі проблеми централізованих рішень, зокрема залежність від операторів, потенційний ризик маніпуляцій з даними голосування та необхідність забезпечення високого рівня безпеки.

Для досягнення поставленої мети необхідно виконати наступні завдання:

1. Розробити деталізовану архітектуру системи електронного голосування, визначивши ключові модулі, їхню взаємодію та відповідальність. Архітектурне рішення має враховувати вимоги до безпеки, масштабованості та зручності використання.
2. Реалізувати програмну частину системи, включаючи смарт-контракти на блокчейн-платформі, а також клієнтський веб-інтерфейс для взаємодії користувачів із системою.
3. Забезпечити інтеграцію з криптовалютним гаманцем для безпечної аутентифікації користувачів та підписання транзакцій голосування.
4. Створити та провести тестування розробленої системи на відповідність визначеним функціональним та нефункціональним вимогам, включаючи перевірку безпеки, продуктивності та зручності використання.
5. Підготувати технічну документацію, що описує процес розробки, архітектуру системи, інструкції з використання та результати тестування.

## 2.2. Характеристика об'єкту проектування

Об'єктом проєктування є децентралізована система електронного голосування, що функціонує на основі блокчейн-технології.

Вхідними даними для розробленого програмного забезпечення є:

- Реєстраційна інформація користувачів (ідентифікатори, публічні ключі гаманців), що отримується з підключеного гаманця. Формат представлення – дані, що передаються через веб-форми та API гаманця.
- Параметри голосування, що задаються організатором через веб-інтерфейс (назва, опис, перелік варіантів вибору, тривалість голосування). Формат представлення – структуровані дані, що передаються через веб-форми.
- Подані голоси користувачів, що вибираються ними через веб-інтерфейс та підписуються за допомогою їхніх приватних ключів. Формат представлення – ідентифікатор обраного варіанту та криптографічний підпис транзакції.

Результатом роботи ПЗ є:

- Захищені та незмінні записи про проведені голосування та подані голоси, що зберігаються у блокчейні. Формат представлення – транзакції та дані у відповідних облікових записах блокчейну.
- Результати голосування, що агрегуються на основі даних з блокчейну та відображаються користувачам через веб-інтерфейс у текстовому та графічному форматах.
- Сповіщення про статус голосу (успішно подано, помилка), що відображаються користувачам у веб-інтерфейсі. Формат представлення – текстові повідомлення та візуальні елементи інтерфейсу.

## 2.3. 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 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 транзакції на секунду (TPS) [11], 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.

## 2.4. Аналіз вимог

На етапі аналізу вимог було проведено ретельне дослідження предметної області електронного голосування. Це дозволило визначити ключові потреби основних зацікавлених сторін: організаторів голосувань та учасників (виборців). Метою аналізу було формування чіткого переліку функціональних та нефункціональних вимог до розроблюваної системи, які стали підґрунтям для подальшої детальної специфікації.

Організатори голосувань мають потребу у зручному інструменті для створення та гнучкого налаштування голосувань, включаючи визначення назви, опису, варіантів вибору та терміну дії. Вони також зацікавлені у можливості контролювати процес голосування та, за необхідності (з урахуванням анонімності), переглядати проміжну статистику. Ключовою вимогою є забезпечення прозорості та незмінності результатів для зміцнення довіри до процесу волевиявлення, а також надання простого способу оголошення підсумків після завершення голосування. У перспективі, за потреби, можлива інтеграція системи з іншими платформами або системами обліку користувачів.

Учасники голосувань мають потребу в інтуїтивно зрозумілому інтерфейсі для зручної участі в голосуваннях. Для них критично важливим є забезпечення анонімності їхнього волевиявлення та захист від розкриття зробленого вибору. Виборці також зацікавлені у можливості ознайомлення з результатами голосування після його завершення. Безпека системи та неможливість фальсифікації результатів є

для них першочерговими вимогами, так само як і зручний спосіб ідентифікації та автентифікації для участі у голосуванні.

## 2.5. 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.

### 2.5.1. Загальний опис

#### 2.5.1.1. Характеристики продукту

Розроблена система електронного голосування надає наступні основні можливості:

- Організатори можуть ініціювати голосування, визначаючи назву, опис, перелік варіантів вибору та термін дії.
- Зареєстровані учасники можуть безпечно віддавати свої голоси за один із запропонованих варіантів протягом визначеного терміну.
- Після завершення голосування всі користувачі можуть переглядати підсумки голосування у наочному форматі.

#### 2.5.1.2. Класи користувачів та їх характеристики

Користувачі системи поділяються на два класи:

- Організатор голосування – користувач, який має право створювати, налаштовувати та контролювати параметри голосування (назва, опис, варіанти, час завершення). Організатор також може брати участь у створеному ним голосуванні як звичайний виборець.
- Учасник голосування (виборець) – користувач, який має право брати участь в активних голосуваннях, віддаючи свій голос за один із варіантів. Для участі виборець повинен мати встановлений та налаштований криптовалютний гаманець.

Як організатори, так і учасники голосування є пріоритетним класом користу-

вачів, оскільки без їхньої взаємодії функціонування системи є неможливим.

#### 2.5.1.3. Середовище функціонування

Програмний продукт функціонує у децентралізованому середовищі блокчейну Solana. Смарт-контракти, що реалізують основну логіку голосування, виконуються в мережі Solana. Клієнтська частина системи розроблена як веб-застосунок, що працює у сучасних веб-браузерах та взаємодіє зі смарт-контрактами через Remote Procedure Call (RPC)-сервіси Solana. Для взаємодії з користувачами використовується криптовалютний гаманець.

### 2.5.2. Характеристики системи

#### 2.5.2.1. 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.

#### 2.5.2.2. 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.

#### 2.5.2.3. 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.

### 2.5.3. Вимоги зовнішніх інтерфейсів

#### 2.5.3.1. 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 голосуван-

ня).

- 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.

#### 2.5.3.2. Програмні інтерфейси

Система взаємодіє з наступними програмними компонентами:

- Блокчейн Solana — через RPC-сервіси для запису та зчитування даних смарт-контрактів.
- Криптовалютний гаманець Phantom Wallet — через його API для аутентифікації користувачів та підписання транзакцій.
- Веб-браузери (сучасні версії Chrome, Firefox, Safari, Edge, тощо).
- Бібліотека Anchor для спрощення взаємодії зі смартконтрактами Solana.
- Бібліотека React для розробки клієнтського веб-інтерфейсу.

#### 2.5.3.3. Комунікаційні інтерфейси

Веб-застосунок використовує стандартні протоколи Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) для взаємодії з RPC-сервісами Solana. Для взаємодії з гаманцем Phantom Wallet використовуються специфічні методи, передбачені його API. Безпека комунікацій забезпечується використанням протоколу HTTPS.

### 2.5.4. Інші нефункційні вимоги

#### 2.5.4.1. 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 повинна підтримувати одночасну участь 1000 користувачів без значного зниження продуктивності (час відгуку на дії користувача не повинен збільшуватися більше ніж на 20

#### 2.5.4.2. Вимоги безпеки

- Доступ до функціональності створення та редагування голосувань повинен бути обмежений лише авторизованими організаторами.
- Система повинна гарантувати, що кожен користувач може проголосувати лише один раз в межах одного голосування.
- Голоси, подані користувачами, повинні бути перевірені на валідність перед записом у блокчейн.

#### 2.5.4.3. Атрибути якості програмного продукту

- Кодова база повинна мати модульну та читабельну структуру для полегшення подальшої розробки, тестування та підтримки.
- Система повинна бути стійкою до тимчасових втрат з'єднання з блокчейном та автоматично відновлювати свою роботу після відновлення з'єднання.
- Основна функціональність системи повинна бути покрита автоматизованими тестами (юніт-тести, інтеграційні тести) для забезпечення відповідності вимогам та виявлення потенційних помилок.
- Інтерфейс користувача повинен бути інтуїтивно зрозумілим та зручним у використанні для користувачів з різним рівнем технічної підготовки.

## 2.6. 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 та сформувати специфікацію вимог.

# 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 чотирьох основних компонентів: клієнтської частини, гаманця Phantom Wallet, смарт-контракту та блокчейн-платформи Solana. Кожен з них виконує окремі функції у процесі голосування, забезпечуючи ефективну, безпечну та прозору взаємодію між користувачем і блокчейном. Схематичне відображення взаємодії між компонентами представлено на діаграмі компонентів на рисунку 3.1.

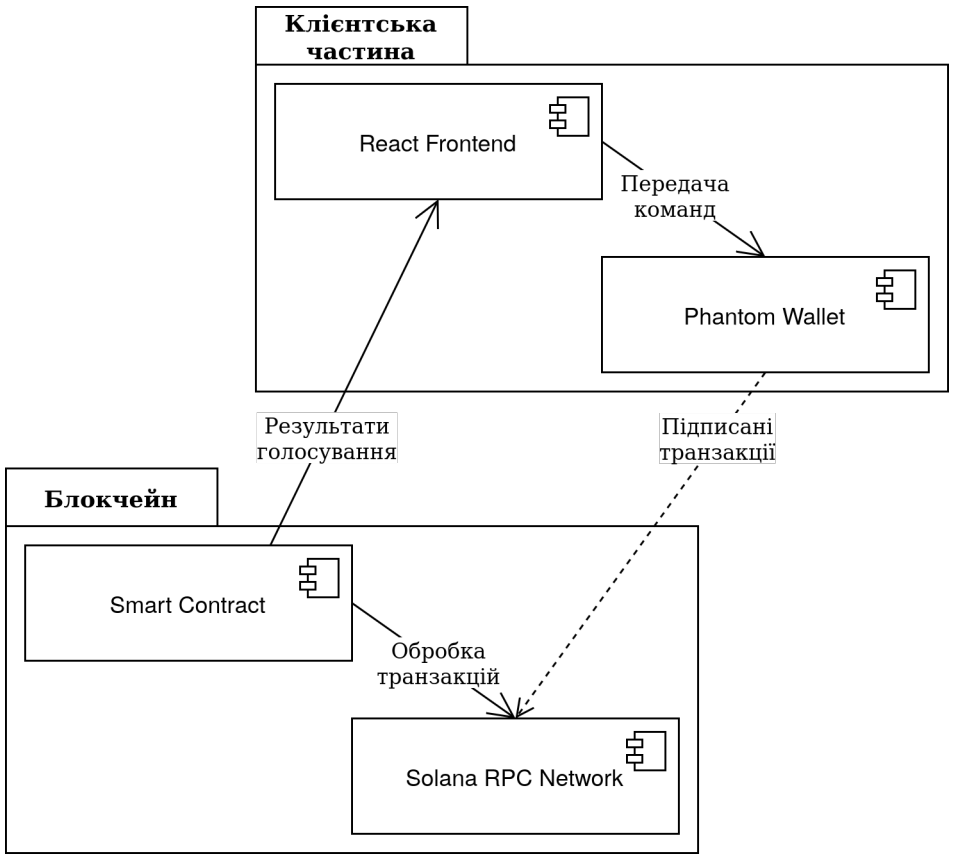


Рис. 3.1 Діаграма компонентів

Клієнт є основним інтерфейсом взаємодії користувача із системою. Реалізована за допомогою фреймворку React, вона забезпечує доступ до функціоналу як для організаторів, так і для учасників голосування. Організатори можуть створювати нові голосування, встановлювати варіанти відповідей і визначати дедлайни. Учасники мають змогу переглядати доступні голосування, обирати варіанти та відстежувати результати. Кожна дія користувача (створення голосування, голосування, перегляд результатів) ініціює транзакцію, яка формується у клієнті, підписується через Phantom Wallet та надсилається до смарт-контракту. Таким чином, клієнт виступає посередником між користувачем і блокчейн-інфраструктурою, забезпечуючи зручність та безпеку взаємодії.

Phantom Wallet — це браузерне розширення, яке забезпечує безпечне зберігання приватних ключів користувача та підпис транзакцій. Його використання є критично важливим для автентифікації та авторизації дій у системі. Під час голосування або створення нового голосування клієнтська частина формує транзакцію, яку користувач повинен підписати своїм приватним ключем через Phantom Wallet. Це гарантує, що жодна дія не може бути виконана від імені користувача без його згоди. Гаманець також забезпечує взаємодію з мережею Solana, виступаючи у ролі шлюзу між користувачем і блокчейном.

Смарт-контракт є логічним ядром системи голосування, розгорнутим у мережі Solana. Він реалізує повний життєвий цикл голосування: створення опитування, реєстрацію голосів, перевірку права голосу, виключення можливості повторного голосування, підрахунок голосів та збереження результатів. Смарт-контракт є детермінованим і не залежить від зовнішніх сервісів, що гарантує чесність та прозорість виконання логіки. Всі записи зберігаються безпосередньо в блокчейні, що унеможливлює їх зміну або видалення. Це забезпечує довіру до системи і дозволяє будь-кому перевірити достовірність результатів голосування.

У системі голосування блокчейн Solana виконує роль середовища для зберігання та обробки транзакцій. Кожна дія користувача — створення голосування, голос чи перегляд результатів — перетворюється на транзакцію, яка надсилається

до мережі Solana. Ці транзакції перевіряються, обробляються та фіксуються у блокчейні, що гарантує їхню незмінність і публічну доступність. Solana забезпечує високу швидкість обробки та масштабованість, що дозволяє системі працювати ефективно навіть при великій кількості користувачів.

Узгоджена взаємодія клієнта, гаманця Phantom, смарт-контракту та блокчейну Solana формує цілісну архітектуру, що забезпечує безпечний, прозорий і незмінний процес голосування. Такий підхід дозволяє реалізувати децентралізовану систему, якій можуть довіряти всі учасники, незалежно від їх ролі, забезпечуючи високий рівень надійності та масштабованості.

### 3.2. Проєктування функціональних модулів клієнтської частини

Функціональність клієнтської частини застосунку організована навколо шести ключових модулів, які забезпечують повний цикл взаємодії користувачів із системою електронного голосування, починаючи від перегляду інформації про власний обліковий запис до безпосередньої участі у голосуваннях та ознайомлення з їхніми результатами. Ці модулі побудовані таким чином, щоб забезпечити інтуїтивно зрозумілий процес для різних категорій користувачів, використовуючи при цьому можливості блокчейн-платформи Solana для гарантування безпеки та прозорості. Взаємодія між користувачами різних ролей та функціональними можливостями системи наочно представлена на діаграмі прецедентів, відображеній на рисунку 3.2.

Діаграма прецедентів ілюструє, як дві основні ролі користувачів – "Виборець"та "Організатор"– взаємодіють із застосунком. "Виборець"має можливість переглядати інформацію про свій обліковий запис, включаючи баланс та історію транзакцій, обирати кластер мережі Solana для роботи, переглядати результати вже завершених голосувань, додавати власну адресу кластеру та, що є його основною функцією, брати участь у голосуваннях шляхом вибору одного з доступних варіантів. Процес голосування є складною дією, яка включає попередній вибір варіанту.

Роль "Організатор"об’єднує в собі всі можливості "Виборця"та додає ключову функцію створення нових голосувань. Цей процес передбачає введення необхідних даних, таких як назва голосування, опис, перелік варіантів вибору та тривалість. Таким чином, діаграма прецедентів демонструє розподіл функціональних можливостей між різними ролями користувачів, підкреслюючи основні сценарії використання системи електронного голосування.

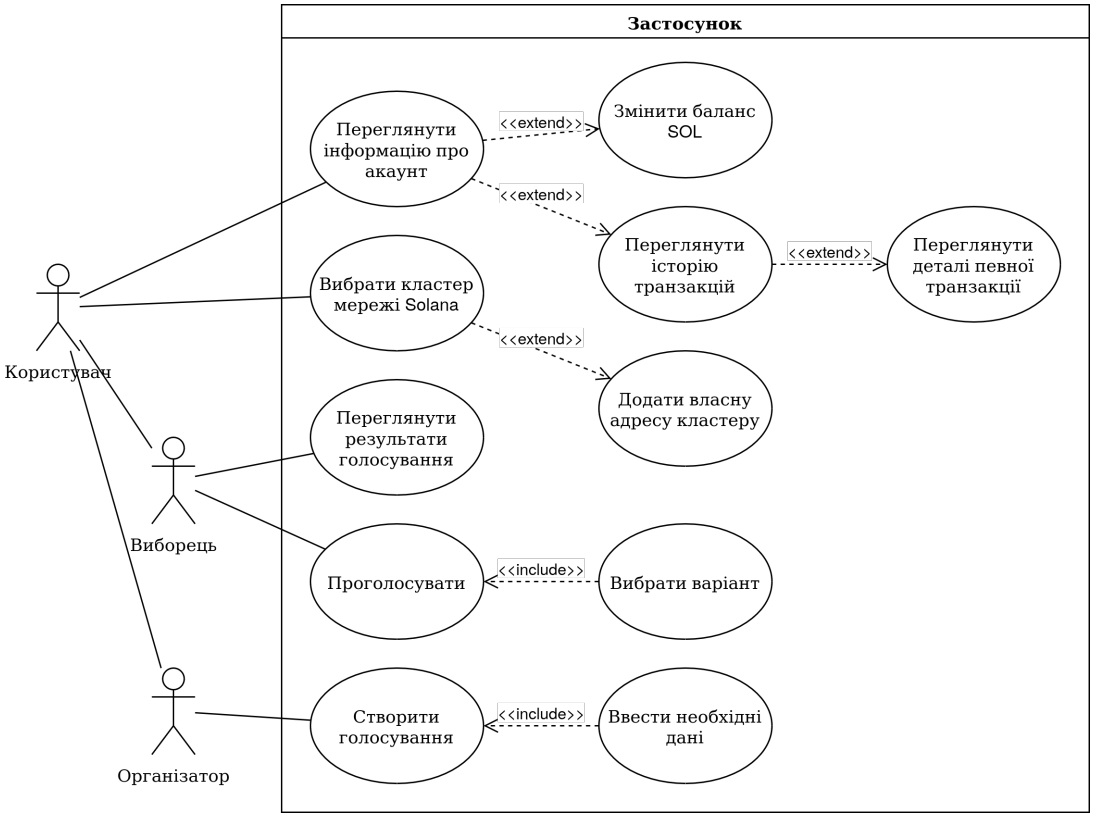


Рис. 3.2 Діаграма прецедентів

### 3.3. Проєктування інтерфейсу користувача та його елементів

Інтерфейс клієнтської частини застосунку розроблено з фокусом на зручність та інтуїтивність використання, щоб забезпечити ефективну взаємодію користувачів на всіх етапах роботи з системою електронного голосування.

На рисунку А.1 зображено головну сторінку застосунку, де відображаються доступні голосування. У верхній частині сторінки розміщено заголовок, та кнопки для вибору між управлінням акаунтом, вибором кластеру та додатком для голосувань. Нижче розташована коротка інструкція користувача для створення голосува-

ння та інформація про обліковий запис користувача, зокрема його ідентифікатор, що підкреслює важливість автентифікації у системі голосування. Центральне місце займає кнопка створення, яка є ключовим елементом для ініціювання процесу створення нового голосування організатором. Важливою частиною цієї сторінки є список доступних голосувань, представлених за їхніми назвами. Користувачі можуть переглядати цей список, щоб знаходити потрібні їм голосування. При натисканні на назву конкретного голосування відкривається діалогове вікно, що відображає детальну інформацію про це голосування та надає можливість взяти в ньому участь. Дизайн сторінки мінімалістичний, з акцентом на простоті та функціональності, щоб користувачі могли легко орієнтуватися та швидко знаходити потрібні опції.

На рисунку А.2 представлено форму для створення нового голосування. Для того, щоб потрапити на цю сторінку, користувач повинен натиснути кнопку "Create Poll"на головній сторінці застосунку. У верхній частині форми розташовані поля для введення назви голосування та його опису, що дозволяє організатору надати контекст та інформацію про предмет голосування. Нижче знаходиться поле для визначення тривалості голосування, де організатор вказує час, протягом якого голосування буде активним. Тривалість голосування може бути вказана у хвилинах, годинах та днях, що забезпечує гнучкість у плануванні голосування. Далі розташовані поля для введення кандидатів або варіантів вибору та кнопка для додавання нових варіантів. У нижній частині форми знаходяться дві кнопки: для підтвердження створення голосування та для закриття форми. Дизайн форми інтуїтивно зрозумілий, з чіткими підписами до полів введення, що полегшує процес заповнення.

На рисунку А.3 зображено форму, призначену для подачі голосу учасником голосування. У верхній частині форми відображається назва та опис голосування. Нижче розміщено таймер, який спливає в реальному часі та показує час, що залишився до завершення голосування, що створює відчуття терміновості та стимулює учасників до активності. Після завершення таймера проголосувати більше не мо-

жна. Далі представлені варіанти голосування з інформацією про кількість поданих голосів за кожен варіант. Праворуч від кожного варіанту розташована кнопка для подачі голосу. У нижній частині форми знаходиться кнопка для закриття форми. Якщо голосування переглядає організатор, йому також доступна кнопка для зміни параметрів голосування, а саме можливість збільшення тривалості часу до завершення. Дизайн форми зосереджений на простоті та зручності використання, з чітким відображенням варіантів вибору та таймером, що дозволяє учасникам швидко і легко зробити свій вибір.

На рисунку А.4 представлено вікно з результатами голосування. У верхній частині вікна розміщений заголовок, який одразу інформує користувача про призначення цього екрана. Нижче наведено варіанти відповідей. Для кожного варіанту відображається кількість отриманих голосів та їхній відсоток від загальної кількості. Візуально кількість голосів представлена горизонтальними смугами, довжина яких пропорційна кількості відданих голосів, що полегшує швидке порівняння результатів. Під результатами голосування підсумовується загальна кількість поданих голосів та вказано лідера голосування. У нижній частині вікна розміщено кнопку, яка дозволяє користувачеві закрити вікно з результатами та повернутися до попереднього екрана. Дизайн цього вікна лаконічний та інформативний, основний акцент зроблено на чіткому відображенні результатів голосування.

На рисунку А.5 відображено інтерфейс для управління кластерами Solana. У верхній частині сторінки знаходиться заголовок та коротка інструкція користувача, що пояснює призначення сторінки – управління та вибір кластерів Solana. Нижче розташована кнопка, що дозволяє користувачам додавати нові кластери. Основну частину сторінки займає таблиця з переліком доступних кластерів, де для кожного кластера відображаються його назва, мережа та кінцева точка. Кластери Solana – це різні мережі, на яких розгортаються та функціонують програми Solana. Дизайн сторінки структурований, з використанням таблиці для зручного представлення інформації про кластери.

На рисунку А.6 представлено інтерфейс, що відображає інформацію про облі-

ковий запис користувача. У верхній частині сторінки розташовані основні функції, пов'язані з управлінням обліковим записом, такі як отримання та передача криптовалюти. Нижче знаходиться інформація про історію транзакцій. Список транзакцій дозволяє користувачам відстежувати всі операції, здійснені з їхнім обліковим записом. Деталі кожної транзакції, такі як хеш, час, статус, можна переглянути на сторонньому сервісі (наприклад, Solana Explorer), що забезпечує прозорість та можливість перевірки операцій. Дизайн сторінки функціональний, з чітким розділенням інформації на блоки.

Таким чином, представлені візуалізації ключових екранів клієнтської частини застосунку демонструють інтуїтивно зрозумілий та функціональний дизайн. Кожен інтерфейс спроєктовано з урахуванням потреб користувачів на різних етапах роботи із системою голосування: від створення опитування та участі в ньому до перегляду результатів та управління власним обліковим записом і вибором кластерів Solana. Простота навігації, чітке представлення інформації та логічне розташування елементів керування сприяють зручній та ефективній взаємодії користувача з застосунком.

### 3.4. Проєктування смарт контракту

Смарт контракт являє собою самовиконуваний код, що зберігається в блокчейні та автоматично виконує умови, прописані в ньому. У контексті цього застосунку, смарт контракт відповідає за створення опитувань, реєстрацію голосів та забезпечення чесності процесу голосування. Інструкція в смарт контракті – це дія, яку користувач може ініціювати для взаємодії з контрактом. Кожна інструкція виконує певну функцію, наприклад, створення нового опитування або подача голосу. Транзакція – це підписане повідомлення, яке користувач надсилає в мережу блокчейн для виконання певної інструкції смарт контракту. Транзакція включає в себе дані інструкції та підпис користувача, що підтверджує його автентичність.

У блокчейні Solana для зберігання даних використовується акаунти. Існують два основних типи акаунтів: акаунти, що належать системній програмі, які ви-

користовуються для базових операцій, таких як переказ коштів або виділення місця для даних, та акаунти, що належать програмам, які використовуються для зберігання стану смарт контрактів та пов'язаних з ними даних.

Для функціонування смарт контракту застосунку для проведення голосувань необхідні наступні акаунти:

- Акаунт підписувача – це акаунт користувача, який ініціює транзакцію. Він потрібен для оплати комісій за транзакції та підписання інструкцій.
- Акаунт опитування – зберігає інформацію про конкретне опитування, включаючи його назву, опис, час завершення, список кандидатів та кількість голосів за кожного кандидата. Оскільки кожне опитування є унікальним, для кожного нового опитування створюється окремий акаунт опитування.
- Акаунт виборця – відіграє ключову роль у запобіганні повторному голосуванню. Коли користувач вперше голосує в певному опитуванні, для нього створюється унікальний акаунт виборця, пов'язаний як з самим опитуванням, так і з публічним ключем користувача. Коли той самий користувач спробує проголосувати в цьому ж опитуванні вдруге, смарт контракт перевірить, чи існує акаунт виборця, пов'язаний з його публічним ключем та цим опитуванням. Якщо такий акаунт вже існує, це означає, що користувач вже віддав свій голос, і транзакція на голосування буде відхилена.

Архітектурно, смарт контракт розроблений таким чином, щоб забезпечити чітке розділення між логікою створення опитування та логікою голосування. Взаємодія з блокчейном відбувається через надсилання підписаних транзакцій. Клієнт створює транзакцію, яка містить необхідну інструкцію та дані, підписує її своїм приватним ключем і надсилає в мережу Solana. Мережа верифікує підпис та виконує інструкцію смарт контракту, оновлюючи стан відповідних акаунтів.

Для створення опитування клієнт ініціює транзакцію, яка викликає інструкцію у смарт контракті. У цій транзакції клієнт передає назву опитування, його опис, час завершення та список кандидатів. Смарт контракт перевіряє ці дані на валідність та створює новий акаунт опитування, зберігаючи в ньому передану ін-

формацію. Адреса цього акаунта опитування детерміновано генерується на основі назви опитування, що дозволяє унікально ідентифікувати кожне опитування.

Для голосування клієнт ініціює транзакцію, яка викликає інструкцію vote у смарт контракті. У цій транзакції клієнт передає назву опитування та ім'я кандидата, за якого він хоче проголосувати. Смарт контракт перевіряє, чи існує опитування з такою назвою, чи не закінчився час голосування, чи існує кандидат з вказаним ім'ям, і чи не голосував вже даний користувач у цьому опитуванні (перевіряючи наявність відповідного акаунта виборця). Якщо всі перевірки проходять успішно, смарт контракт збільшує лічильник голосів для обраного кандидата в акаунті опитування та створює або оновлює акаунт виборця, фіксуючи факт голосування цього користувача в даному опитуванні.

Смарт контракт, у свою чергу, зберігає в блокчейні стан опитувань (назва, опис, час завершення, кандидати, кількість голосів) та інформацію про те, хто і в якому опитуванні вже проголосував. Усі ці дані є публічними та незмінними після запису в блокчейн, що забезпечує прозорість та чесність процесу голосування.

Схематично роботу смарт контракту зображено на діаграмі послідовності на рисунку 3.3,

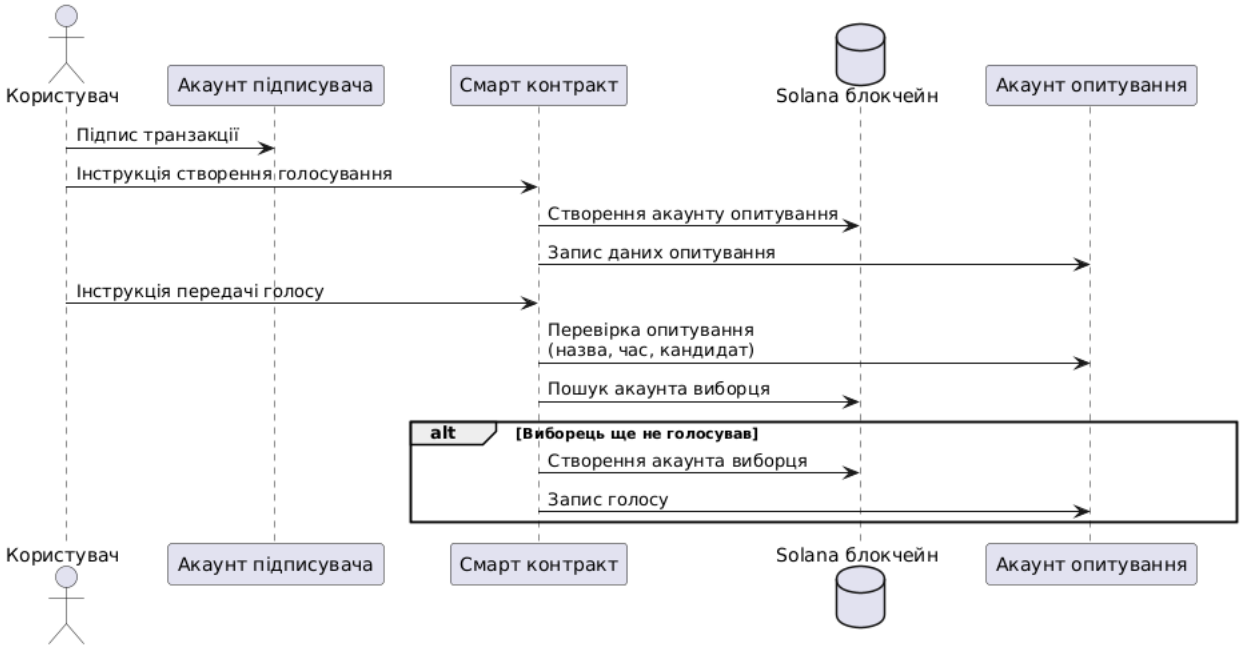


Рис. 3.3 Діаграма послідовності

### 3.5. 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 Software Development Kit (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 PoH у комбінації з Tower Byzantine Fault Tolerance (BFT) - гібридний механізм, що забезпечує високу пропускну здатність транзакцій без зниження безпеки. PoH синхронізує події у часовій шкалі за допомогою криптографічних часових міток, що унеможливлює атаки типу "подвійного витрачання"навіть при високих навантаженнях на мережу. Ця властивість дозволяє системі підтримувати мілісекундні затримки обробки та мільйонні обсяги транзакцій на годину.

### 3.6. 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 частина 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 проєктування 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. 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 З ЕКОНОМІКИ>

## 5.1.

## 5.2. Висновки до розділу

# ВИСНОВКИ

## СПИСОК ЛІТЕРАТУРИ

[1] Blockchain structure. URL: https://www.researchgate.net/publication/369352496/figure/fig1/AS:11431281414772432@1746017302739/Blockchain-structure.tif

(дата звернення 13.05.2025)

[2] Awosika E. What Is Blockchain Voting?. URL: https://second-pocket-shoot-73.hashnode.dev/what-is-blockchain-voting

(дата звернення 22.01.2025)

[3] 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)

[4] 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)

[5] 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.

[6] Victor S. Proof of history: what is it good for? URL: https://www.shoup.net/papers/poh.pdf

(дата звернення 22.01.2025)

[7] Security and technology. *Voatz*. URL: https://voatz.com/security-and-technology/

(дата звернення 22.01.2025)

[8] Specter M. A., Koppel J., Weitzner D. The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. *MIT*. URL: https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

(дата звернення 13.05.2025)

[9] 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)

[10] 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.

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

(дата звернення 18.03.2025)

# ДОДАТОК А. ПРИКЛАД ІНТЕРФЕЙСУ КОРИСТУВАЧА

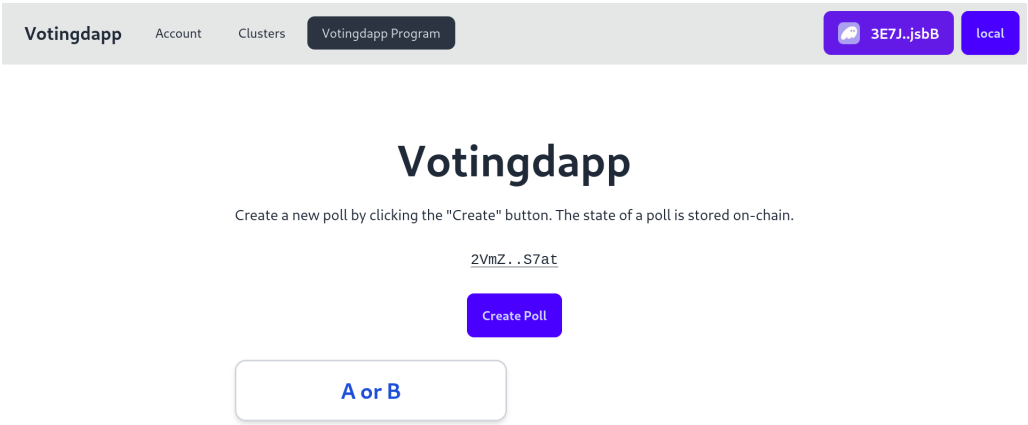


Рис. А.1 Перегляд списку голосувань

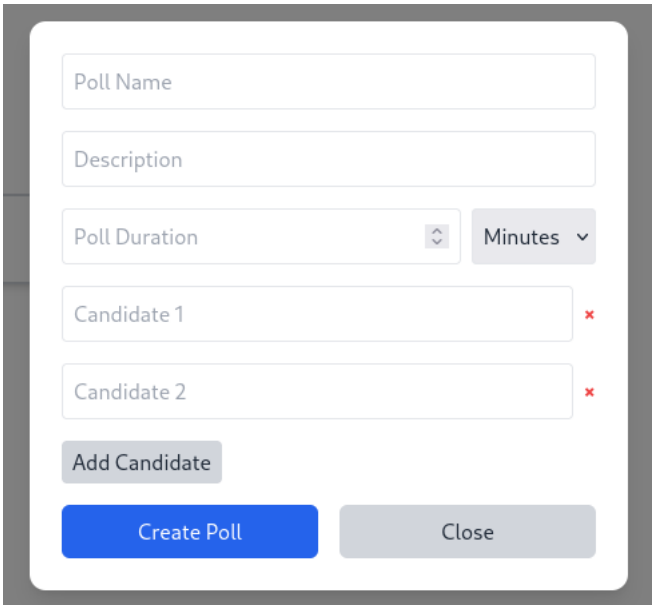


Рис. А.2 Форма для створення голосування

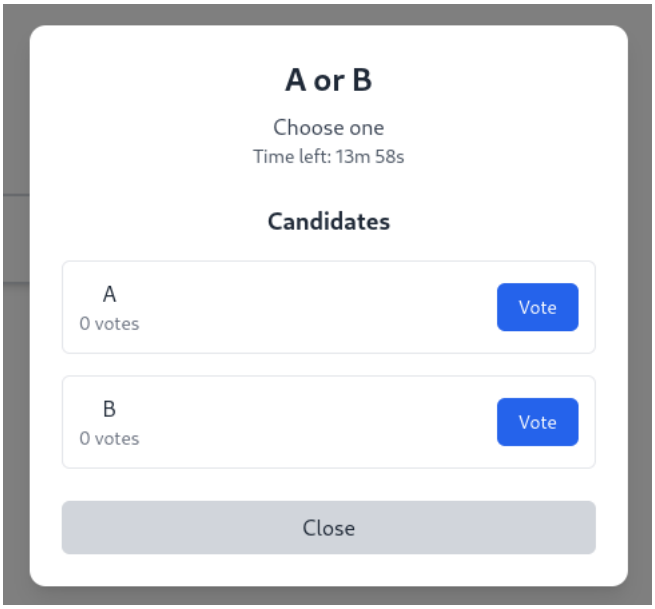


Рис. А.3 Форма для подачі голосу

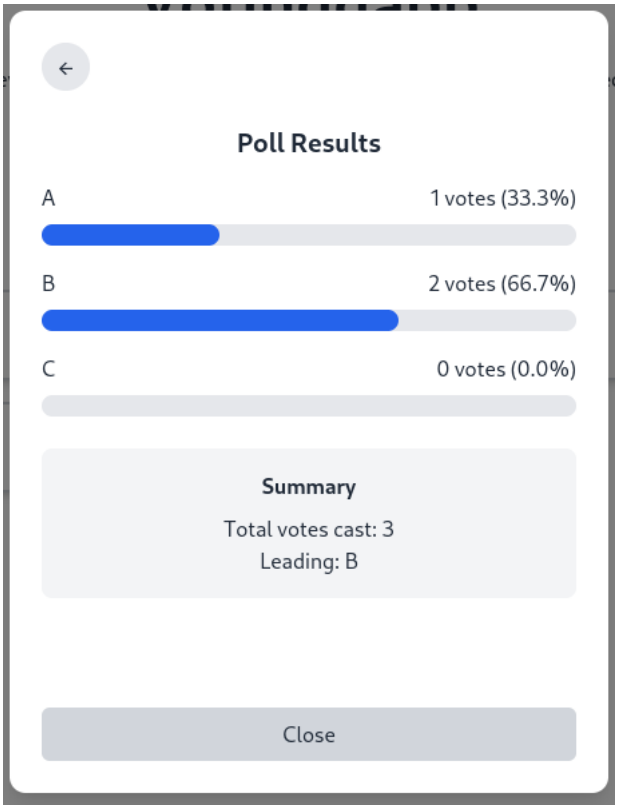


Рис. А.4 Перегляд результатів голосування

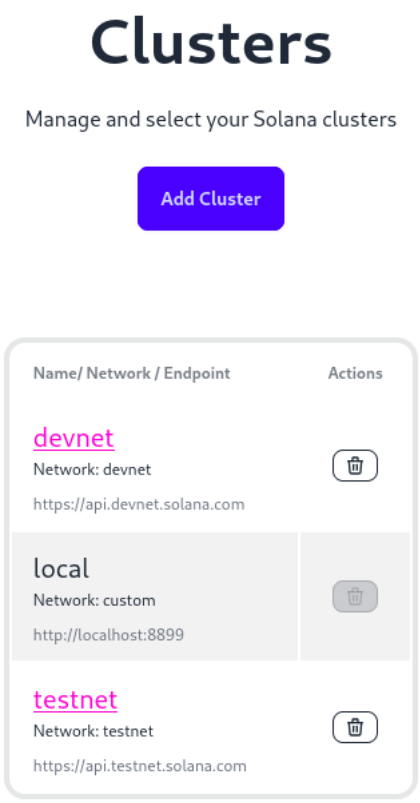


Рис. А.5 Сторінка зі списком кластерів мережі

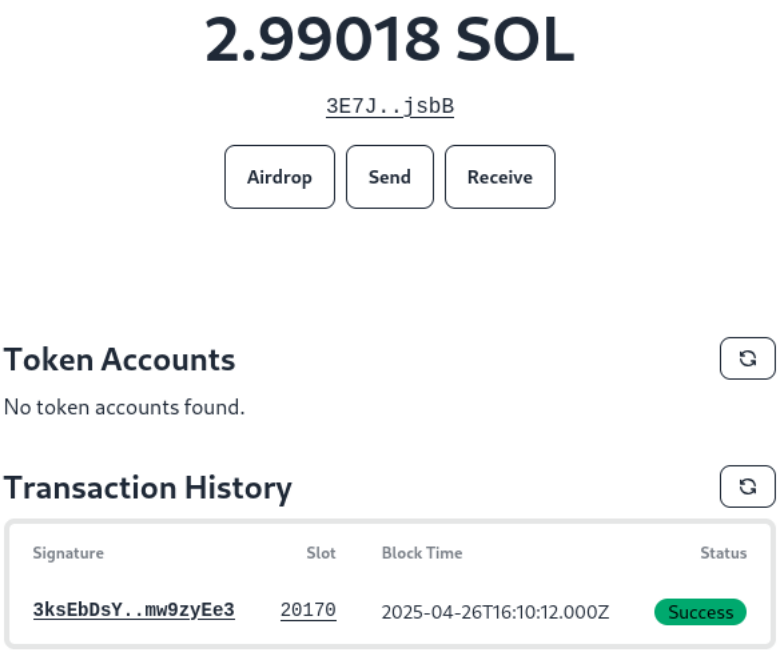


Рис. А.6 Відображення інформації про баланс акаунту та історії транзакцій