

АНОТАЦІЯ

ЗМІСТ

Вступ	7
1 Теоретичні основи та аналіз сучасних підходів до організації електронних голосувань	8
1.1 Основи блокчейн-технології	8
1.2 Методи досягнення консенсусу у розподілених системах	9
1.3 Огляд та аналіз існуючих рішень для організації голосувань	11
1.4 Інноваційні підходи у технологіях електронного голосування	12
1.5 Висновки до розділу	13
2 Постановка завдання розробки системи та обґрунтування вибору технологій	14
2.1 Мета та завдання розробки	14
2.2 Обґрунтування вибору технологій та методів	14
2.3 Специфікація вимог	16
2.3.1 Призначення, мета	16
2.3.2 Загальний опис	16
2.3.3 Характеристики системи	17
2.3.4 Вимоги зовнішніх інтерфейсів	18
2.3.5 Інші нефункційні вимоги	18
2.4 Висновки до розділу	19
3 <Проектний розділ>	20
3.1	20
3.2 Висновки до розділу	20

4	<Розділ програмної реалізації та тестування>	21
4.1	21
4.2	Висновки до розділу	21
5	<Розділ з економіки>	22
5.1	22
5.2	Висновки до розділу	22
	Висновки	23
	Список літератури	23
A	<Назва додатку>	26

ВСТУП

У сучасному світі цифрові технології відіграють ключову роль у забезпеченні прозорості та довіри в різних сферах суспільного життя. Однією з таких сфер є електронне голосування, яке дедалі частіше використовується як альтернатива традиційним методам голосування. Однак існуючі централізовані системи голосування стикаються з низкою проблем, таких як ризик шахрайства, можливість маніпуляцій та складність забезпечення прозорості процесу.

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 цієї роботи є дослідження та розробка системи для проведення голосувань та опитувань, яка відповідатиме вимогам прозорості, безпеки та достовірності результатів. Буде розроблено архітектуру системи голосування, яка відповідає вимогам безпеки, надійності та ефективності.

Об'єктом дослідження є процес організації електронного голосування. Предметом дослідження виступають технологічні підходи та методи побудови систем голосування, що забезпечують надійність і прозорість результатів.

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, що виключають необхідність довіри до єдиного централізованого органу. Головною особливістю блокчейну є його здатність забезпечувати незмінність і прозорість даних завдяки криптографічним методам і структурі ланцюжка блоків.

Структура блокчейну складається з послідовності блоків, кожен з яких містить запис про транзакції, хеш попереднього блоку та тимчасову позначку [1]. Зміна даних у будь-якому блоці призведе до порушення цілісності всього ланцюжка, що робить блокчейн надзвичайно стійким до маніпуляцій. Усі дані в мережі блокчейн розподілені між учасниками, кожен із яких має копію всього ланцюжка.

Однією з ключових переваг блокчейну є прозорість. Усі транзакції, які здійснюються в системі, доступні для перегляду кожному учаснику мережі. Це дозволяє перевіряти достовірність даних без необхідності довіри до централізованого органу або адміністратора.

Ще однією важливою властивістю блокчейну є незмінність даних. Після того як транзакція додана до ланцюжка, вона не може бути змінена або видалена без згоди більшості учасників мережі. Це забезпечує високий рівень надійності та захищеності від фальсифікацій.

Децентралізація є ще однією перевагою блокчейну. Відсутність єдиного центру управління означає, що система не залежить від конкретного адміністратора чи серверу. Це значно знижує ризик зловживань або помилок, пов'язаних із людським фактором.

Блокчейн знаходить застосування в багатьох галузях, включаючи фінанси, ло-

гістику, охорону здоров'я та управління ланцюгами поставок. У контексті електронного голосування блокчейн 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 своїм властивостям блокчейн стає ключовою технологією для створення сучасних цифрових систем, які потребують високого рівня довіри, безпеки та надійності.

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, низькі витрати та захищеність, що впливає на вибір найбільш відповідного алгоритму для створення ефективної системи.

1.3. 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	Не обмежена	Обмежена
Енергоспоживання	Низьке	Залежить від реалізації
Швидкість	Висока	Залежить від реалізації

1.4. 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.

1.5. 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

Для розробки системи обрано блокчейн як технологічну основу, що забезпечує децентралізацію, прозорість і незмінність даних. Серед доступних блокчейн-платформ основними критеріями вибору були висока пропускна здатність, низькі затримки, низькі транзакційні витрати та доступність інструментів для розробників. Цим вимогам найбільше відповідає платформа Solana, яка демонструє високу продуктивність завдяки інноваційному механізму консенсусу Proof of History. Ця платформа забезпечує стабільну роботу навіть за великого навантаження, що є критично важливим для системи голосування з потенційно великою кількістю одночасних користувачів.

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 його популярністю та зручністю для користувачів Solana. Phantom дозволяє легко здійснювати транзакції, а також надає можливість користувачам безпечно зберігати свої ключі та взаємодіяти з блокчейн-додатками.

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

2.3.1. Призначення, мета

Призначенням застосування 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.

2.3.2. Загальний опис

2.3.2.1. 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.

2.3.2.2. 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 голоси за обрані варіанти та переглядає результати. Учасник має доступ лише до голосування та результатів, без можливості управління голосуванням.

2.3.2.3. Середовище функціонування

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

2.3.3. Характеристики системи

2.3.3.1. 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 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.

2.3.3.2. 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.

2.3.3.3. 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. Натискає 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.

2.3.4. Вимоги зовнішніх інтерфейсів

2.3.4.1. 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.

2.3.5. Інші нефункційні вимоги

2.3.5.1. Вимоги продуктивності

- Час підтвердження голосу не повинен перевищувати 3 секунд.
- Час відображення результатів голосування не повинен перевищувати 5 се-

кунд.

- Система має підтримувати одночасну участь до 1000 користувачів без значного зниження продуктивності.

2.3.5.2. 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.

2.3.5.3. Атрибути якості програмного продукту

- Код повинен бути модульним і читабельним, щоб спростувати 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.

Вибір блокчейн-платформи був здійснений з урахуванням потреб прозорості, незмінності даних і продуктивності системи. Платформа Solana була обрана завдяки її високій пропускній здатності, низькій латентності та підтримці мови програмування Rust, що дозволяє створювати ефективні та безпечні рішення.

РОЗДІЛ 3. <ПРОЄКТНИЙ РОЗДІЛ>

3.1.

3.2. Висновки до розділу

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.

ДОДАТОК А. <НАЗВА ДОДАТКУ>