КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп'ютерних наук та кібернетики
Кафедра інтелектуальних програмних систем

Кваліфікаційна робота

на здобуття освітнього рівня бакалавра
за спеціальністю 121 Інженерія програмного забезпечення
на тему:

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СИСТЕМІ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Виконав студент 4-го курсу
Антон БАЛИКОВ _____
(підпис)

Науковий керівник:
доцент, кандидат фіз.-мат. наук
Максим ВЕРЕС _____
(підпис)

Засвідчую, що в цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Роботу розглянуто й допущено до захисту на засіданні кафедри інтелектуальних програмних систем
« 29 » травня 2023 р.,
протокол № 11
Завідувач кафедри
Олександр ПРОВОТАР _____
(підпис)

Київ – 2023

РЕФЕРАТ

Обсяг роботи 57 сторінок, 26 ілюстрацій, 3 таблиці, 18 джерел посилань, 1 додаток.

АЛГОРИТМ ГЕШУВАННЯ, АНОНІМНІСТЬ, БЛОК, БЛОКЧЕЙН, ГЕШ, ДЕЦЕНТРАЛІЗАЦІЯ, ЕЛІПТИЧНА КРИВА, КЛЮЧ, КОНСЕНСУС, КРИПТОГРАФІЯ, НЕЗМІННІСТЬ, ПРОЗОРІСТЬ, СИСТЕМА ГОЛОСУВАННЯ, ТРАНЗАКЦІЯ, ЦИФРОВИЙ ПІДПИС.

Об’єктом розроблення є технологія блокчейн у системі електронного голосування, зокрема механізм досягнення консенсусу, структури даних, які використовуються в системі та механізми перевірки даних.

Метою кваліфікаційної роботи є впровадження технології блокчейн у системі електронного голосування за рахунок створення відповідного компонента системи, який буде відповідати за логіку блокчейну.

Методи розроблення: реалізація механізму досягнення консенсусу, вузлів-валідаторів, методів верифікації даних. Інструменти розроблення: безкоштовне, вільно поширюване інтегроване середовище розробки IntelliJ IDEA 2023.1, мова програмування GoLang.

Результати роботи: розроблено компонент системи електронного голосування «Digital-Voting», який відповідає за блокчейн. Новизною роботи є використання механізму досягнення консенсусу PBFT в системі електронного голосування та досягнення анонімності користувачів.

Сферою застосування даного продукту є впровадження блокчейну в системах електронного голосування, подібних до реалізованої.

Значимість роботи полягає у демонстрації можливості та переваг використання технології блокчейн для систем електронного голосування.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

API – Application Programming Interface, прикладний програмний інтерфейс;

DPoS – Delegated Proof of Stake, делегований доказ частки;

IDE – Integrated Development Environment, інтегроване середовище розробки;

POA – Proof of Authority, доказ повноважень;

PBFT – Practical Byzantine Fault Tolerance, практична візантійська відмовостійкість;

PoS – Proof of Stake, доказ частки;

PoW – Proof of Work, доказ виконаної роботи.

ВСТУП

Оцінка сучасного стану об’єкта розробки. Системи голосування з часу їх виникнення зазнавали ряду видозмін. Цифрові системи голосування уже були впроваджені, й використовуються в багатьох країнах. Проте ці існуючі рішення не позбавлені недоліків, низького рівня довіри та небажаної централізації, коли існує єдина точка довіри та зламу системи.

Існують також рішення із застосуванням технології блокчейн, проте в усіх також є проблеми, зокрема зі швидкодією та анонімністю.

Актуальність роботи та підстави для її виконання. Було вирішено удосконалити та покращити систему, реалізовану в якості об’єкта дослідження курсової роботи.

Актуальність роботи полягає в тому, що технологія блокчейн, як демонструють поточні дослідження, вирішує поточні проблеми існуючих систем електронного голосування. Було бажання розробити компонент, який відповідає за технологію блокчейн у системі, та який буде найбільш оптимальним для специфіки системи електронного голосування.

Підставами для виконання роботи також є проходження курсів з Криптології, Блокчейну, Децентралізованих фінансів та Смарт-контрактів від компанії Distributed Lab, яка займається дослідженням та впровадженням технології блокчейн.

Мета й завдання роботи. Метою кваліфікаційної роботи є впровадження технології блокчейн у системі електронного голосування за рахунок створення відповідного компонента системи, який буде відповідати за логіку блокчейну.

Для цього було поставлено наступні завдання:

- дослідити технологію блокчейн;
- дослідити можливість та особливості використання технології блокчейн для побудови системи голосування;
- розробити технічне завдання до продукту;

– спроєктувати та розробити компонент програмного продукту «Digital-Voting», що відповідає за механізм досягнення консенсусу та логіку блокчейну, блоків і транзакцій.

Об'єкт, методи й засоби розроблення. Об’єктом розроблення є компонент системи електронного голосування, який відповідає за блокчейн, зокрема механізм досягнення консенсусу, структури даних, які використовуються в системі та механізми перевірки даних.

Аналізу та розробці програмного продукту передувало вивчення теоретичної складової алгоритмів, що використовуються системою. Також було планування архітектури системи та розробка покроково в ітераційному режимі та в команді. Було застосовано такі методи розроблення як аналіз і синтез.

В якості інструменту створення програмного засобу було обрано IntelliJ IDEA 2023.1 – інтегроване середовище розробки (IDE), яке є безкоштовним, вільно поширюваним, з відкритим вихідним кодом.

В якості мови програмування було обрано мову GoLang. Ця мова програмування надає зручний функціонал для написання системних продуктів в парадигмі об’єктно-орієнтовано програмування. Також мова пропонує зручне використання багатопоточності задля забезпечення потреб підтримки багатьох операцій одночасно. Було використано ряд бібліотек для алгоритмів гешування, роботи з великими числами та утилітарних потреб.

Можливі сфери застосування. Програмний продукт «Digital-Voting» може застосовуватися у якості основи чи прототипу для створення системи голосування на основі технології блокчейн, яка буде застосована в реальних умовах на виборах та під час голосувань.

Компонент системи, який відповідає за логіку блокчейну, може бути використаний в інших системах електронного голосування з використанням технології блокчейн.

Взаємозв’язок з іншими роботами. Було проведено ряд паралелей з іншими системами, що використовують технологію блокчейн, реалізовано схожі методи, часом дороблені чи покращені. Було досліджено існуючі рішення у сфері

електронного голосування, як більш традиційні, так і з використанням технології блокчейн.

РОЗДІЛ 1 ТЕХНОЛОГІЯ БЛОКЧЕЙН

1.1 Вступ до технології блокчейн

За визначенням IBM, американської корпорації, що виробляє програмне та апаратне забезпечення для комп’ютерів, «Блокчейн – це загальний, незмінний реєстр, який полегшує процес запису транзакцій і відстеження активів у бізнес-мережі» [1].

Блокчейн – це розподілений і децентралізований цифровий реєстр. Як база даних, блокчейн зберігає інформацію в цифровому форматі. Вперше блокчейн-протокол був згаданий Девідом Лі Чаумом у дисертації «Комп'ютерні системи, створені, підтримувані та довірені взаємно підозрілими групами» [2].

Найбільшої популярності технологія набула завдяки криптовалютним системам, таким як Bitcoin, Ethereum тощо. Інновація блокчейну полягає в тому, що він гарантує достовірність і безпеку запису даних та створює довіру без необхідності у довіреній третій стороні.

1.2 Порівняння зі звичайною базою даних

Одна з ключових відмінностей між звичайною базою даних та блокчейном полягає в тому, як структуровані дані. Тоді як традиційна база даних зберігає дані у більш звичному для нас вигляді (зазвичай у вигляді таблиць, які складаються з полів та значень цих полів), блокчейн зберігає інформацію у вигляді блоків.

Як зазначено в таблиці 1.1, основною відмінністю між звичайною базою даних та блокчейном є підхід до організації та зберігання даних. У блокчейні немає єдиної точки відмови, оскільки копія бази даних є у всіх вузлів системи. Також варто зазначити, що вносити зміни в дані, які вже у спільній базі даних неможливо, оскільки буде порушено правило протоколу.

Таблиця 1.1 – Порівняння звичайної бази даних та блокчейну за різними параметрами

	Звичайна база даних	**Блокчейн**
Централізація	Централізована	Розподілена, децентралізована
Точка відмови	Єдина	Багато
Операції взаємодії з даними	Створення, читання, зміна та видалення	Створення та читання
Прозорість	На розсуд адміністратора	Публічний блокчейн надає прозорість
Достовірність	Дані можуть бути змінені	Дані, що вже в розподіленій базі даних, є незмінними
Складність	Відносно стара технологія, легко реалізувати та підтримувати	Складніша реалізація, залежить від сфери застосування
Продуктивність	Висока	Порівняно низька у зв’язку із перевірками даних та необхідністю досягнення спільного стану бази даних
Масштабованість	Відносно легко масштабується	Складність масштабування залежить від сфери застосування, методу досягнення спільного стану бази даних та інших факторів

Вищезазначені особливості блокчейну призводять до підвищення складності системи, меншої продуктивності та проблем масштабованості. Детально можна почитати в джерелі [3].

1.3 Організація блокчейну

Блокчейн складається із ланцюга блоків, про що говорить назва цього способу організації бази даних. Блоки є абстракцією для структурованого

зберігання даних. Кожен блок у будь-якому блокчейні, як правило, складається з таких основних частин:

– заголовок блока;
– тіло блока.

У заголовку блока міститься службова інформація, яка потрібна для перевірки відповідності правилам протоколу. До такої інформації належать:

– мітка часу;
– геш-значення від попереднього блоку в базі даних;
– корінь дерева Меркла;
– інші метадані.

Зв’язність бази даних забезпечується полем «Геш-значення від попереднього блоку в базі даних». У цьому полі записане значення, отримане в результаті подання на вхід геш-функції попереднього блоку в блокчейні. Про геш-функцію детальніше йде мова в 1.7. Таким чином змінити попередній блок після додання поточного вже неможливо, оскільки тоді зміниться його геш-значення та буде порушено правила протоколу. У блокчейні кожен блок містить у цьому полі дані про попередній блок, що робить можливою перевірку правильності геш-значень аж до першого блоку в ланцюгу. Геш-значення попереднього блоку в заголовку першого блоку в блокчейні містить наперед визначені дані, оскільки цей блок не має попередника. Схематично список блоків у блокчейні можна побачити на рис. 1.1 [4].

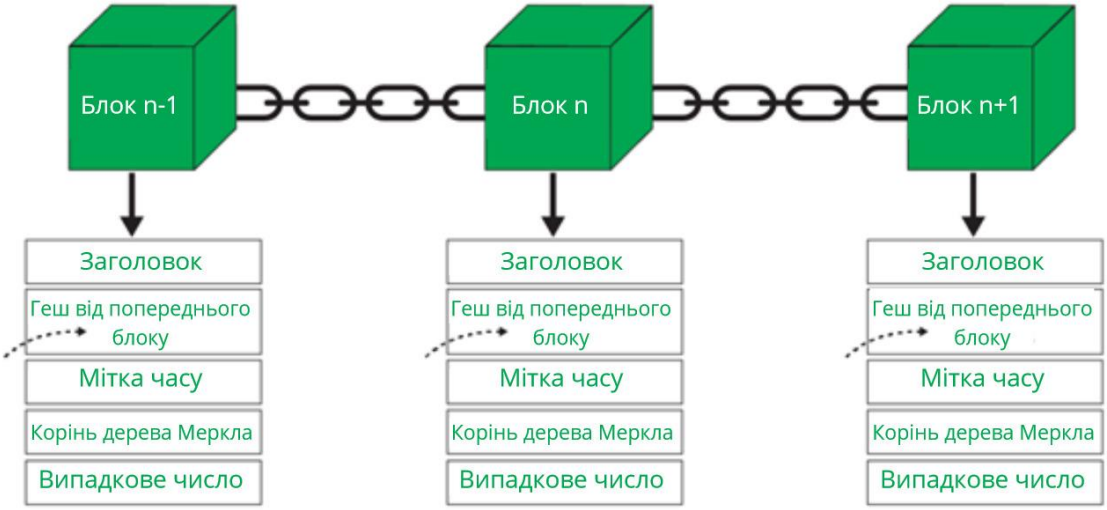

Рисунок 1.1 – Схематичне зображення блокчейну

Корінь дерева Меркла – спеціальне значення, яке визначає усі транзакції в тілі блока. Дерево Меркла – це деревоподібна структура, в якій кожен листовий вузол є гешем блоку даних, а кожен не листовий вузол – гешем конкатенації (об'єднання) даних його дочірніх вузлів. Детальніше у джерелі [5]. Це поле дозволяє переконатися в тому, що транзакції, які лежать в тілі блока, не були модифіковані.

У тілі блока містяться транзакції, або корисне навантаження. Транзакції також є абстракцією та структуризацією даних, які потрібно зберігати в блокчейні. Структура транзакцій відрізняється в залежності від сфери застосування блокчейну. Так, зокрема, для системи голосування, транзакції містять наступні поля:

– тип транзакції (з підтримуваних системою);
– випадкове значення, часто назване «сіллю» або «nonce»;
– тіло транзакції (залежить від типу);
– дані підпису.

Тип транзакції наведений для зручної класифікації транзакції та службових цілей.

Випадкове число наявне в заголовку транзакції задля забезпечення відсутності співпадінь геш-значень різних транзакцій.

У тілі транзакції лежать дані, які мають зберігатися в блокчейні. Для блокчейнів у системах криптовалют в цій частині зберігаються дані про грошові перекази, у системах голосування – деталі щодо віддання голосу чи створення голосування тощо.

Дані підпису є ключовим для усієї системи голосування полем, оскільки саме це поле відповідає за збереження даних підпису для перевірки транзакції. Цифрові підписи згадані в 1.7.

1.4 Схема роботи блокчейну

База даних блокчейн та її стан підтримуються так званими валідаторами. Валідатор блокчейну – це вузол в мережі блокчейн, який відповідає за перевірку транзакцій в мережі. Про валідаторів розповідається за посиланням в джерелі [6]. Ці вузли працюють за правилами протоколу, перевіряють транзакції, додають їх у блоки, формують блоки, в деяких реалізаціях блокчейну підписують блоки, розповсюджують блоки та досягають спільного стану загальної бази даних, тобто консенсусу, про який буде йти мова у розділі 2.

Загалом роботу блокчейну можна розділити на етапи:

- надсилання транзакцій валідаторам та перевірка цих транзакцій;
- створення блоку та його розповсюдження;
- перевірка блоку та додавання у спільну базу даних.

Цей перелік є загальним для усіх систем, які використовують технологію блокчейн, детальний опис цих етапів залежить від конкретної системи та сфери застосування.

Система, яка використовує блокчейн, складається із валідаторів, що не довіряють одне одному, але завдяки спільним правилам протоколу для всіх вони можуть і мають перевірити блоки, що були запропоновані іншими валідаторами. Перевірки варіюються від порівнянь на входження тих чи інших даних в уже

підтверджений ланцюжок блоків до складних криптографічних алгоритмів, таких як геш-функція чи алгоритми цифрового підпису. У разі проходження перевірки певним блоком, його необхідно додати у загальний блокчейн за умови виконання правила, згідно з яким валідатори вважають, що дійшли згоди стосовно наступного блоку. Це правило називається консенсусом і буде детально розглянуто у розділі 2.

1.5 Види блокчейнів

Блокчейн – загальна назва технології, а не конкретне ім'я певної реалізації. Існує велика кількість сфер застосування та різних реалізацій технології в залежності від потреб та вимог.

За рівнями дозволів у системі виділяють [7]:

– «бездозвільний» блокчейн (англ. permissionless);
– «дозвільний» блокчейн (англ. permissioned).

Бездозвільні або публічні блокчейни, доступні для всіх, хто бажає взяти участь у процесі блокчейну, який використовується для перевірки транзакцій і даних. Вони використовуються в мережі, де потрібна висока прозорість.

Бездозвільний блокчейн не має центрального органу, платформа має повністю відкритий вихідний кодом, прозорість транзакцій.

Переваги:

– кожен може брати участь, єдиною вимогою є хороше обладнання та інтернет;
– забезпечує довіру між користувачами або організаціями. високий рівень прозорості, оскільки є більшою мережею;
– ширша децентралізація доступу до більшої кількості учасників.

Недоліки:

– низька енергоефективність через велику мережу;
– менша масштабованість продуктивності;
– менша конфіденційність, оскільки багато речей є видимими.

Дозвільний блокчейн – це закрита мережа, в якій лише певній групі осіб дозволено підтверджувати транзакції або дані в даній мережі блокчейн. Використовуються в мережах, де потрібна висока конфіденційність і безпека.

Особливостями є прозорість, заснована на меті організації, відсутність центрального органу управління, розробляється приватним органом.

Переваги:

- цей тип блокчейну дозволяє значні зміни на вимогу одного органу, тобто компанії;
- високий рівень конфіденційності, оскільки для доступу до інформації про транзакції потрібен дозвіл;
- оскільки задіяно мало вузлів, підвищується продуктивність і масштабованість.

Недоліки:

- не є по-справжньому децентралізованою системою, оскільки вимагає дозволу;
- ризик корупції, оскільки залучено відносно небагато учасників;
- власник та оператор можуть будь-коли змінити правила відповідно до своїх потреб.

За масштабом виділяють такі типи блокчейну [8]:

- публічний блокчейн;
- приватний блокчейн;
- гібридний блокчейн;
- консорціумний блокчейн.

Публічні блокчейни є бездозвільними за своєю природою, дозволяють будь-кому приєднатися до них і є повністю децентралізованими. Публічні блокчейни дозволяють всім вузлам блокчейну мати рівні права на доступ до блокчейну, створення нових блоків даних і перевірку блоків даних.

Приватні блокчейни, які також можуть називатися керованими блокчейнуми – це дозвільні блокчейни, контрольовані однією організацією. У приватному блокчейні центральний орган визначає, хто може бути вузлом. Центральний орган також не обов'язково надає кожному вузлу рівні права на виконання функцій. Приватні блокчейни є лише частково децентралізованими, оскільки доступ громадськості до них обмежений.

Гібридні блокчейни – це блокчейни, які контролюються однією організацією, але з певним рівнем нагляду з боку публічного блокчейну, який необхідний для виконання певних перевірок транзакцій.

Консорціумні блокчейни – це дозволені блокчейни, якими керує група організацій, а не один суб'єкт, як у випадку з приватними блокчейнуми. Таким чином, консорціумні блокчейни є більш децентралізованими, ніж приватні блокчейни, що призводить до вищого рівня безпеки. Однак створення консорціумів може бути складним процесом, оскільки вимагає співпраці між кількома організаціями, що створює логістичні проблеми, а також потенційні антимонопольні ризики.

1.6 Прозорість

Завдяки децентралізованій природі блокчейну всі транзакції можна прозоро переглядати, маючи особистий вузол або використовуючи блокчейн-переглядачі, які дозволяють бачити будь-які транзакції в режимі реального часу. Кожен вузол має свою власну копію ланцюжка, який оновлюється в міру підтвердження та додавання нових блоків, тому він володіє всією повнотою про стан системи на момент запиту на перегляд тієї чи іншої інформації.

Варто звісно зазначити, що задля забезпечення анонімності приватних даних осіб немає серед даних транзакцій. Там знаходяться лише ідентифікатори певного виду, які можна зв’язати безпосередньо з особою лише за умови зберігання цих зв’язків у певному місці.

1.7 Криптографічні алгоритми

Блокчейн працює та задовольняє вимогам завдяки ряду криптографічних алгоритмів. Серед цих алгоритмів можна виділити два основних класи: геш-функції та алгоритми цифрового підпису.

Геш-функція – однонапрямлена функція, що приймає в якості аргументу будь-які дані, а на виході повертає рядок фіксованої довжини. Детальніше про геш-функції у джерелі [9]. Особливістю геш-функцій є те, що за мінімальної зміни вхідних даних вихідний рядок змінюється до невпізнанності. Геш-функція використовується в якості ідентифікатора даних, оскільки за однакових вхідних даних буде повернуто одне й те ж значення. В силу своє однонапрямленої природи відновити вхідні дані з вихідного рядку складно або неможливо. Співпадіння вихідних даних для різних вхідних називають «колізіями». На практиці, зокрема в технології блокчейн, використовують геш-функції, для яких колізії мінімальні.

Для підпису транзакцій, блоків та перевірки цих підписів використовуються алгоритми цифрового підпису. Ці алгоритми використовують специфічну структуру даних, яка називається «ключова пара». На вхід алгоритму для підпису передається «приватний ключ», який підписант тримає в секреті, та повідомлення, яке може бути довільним. На виході алгоритму отримується значення підпису, вигляд та зміст якого відрізняється залежно від конкретної реалізації алгоритму цифрового підпису. Для перевірки необхідно надати «публічний ключ», який відомий усім та часто передається разом із значенням підпису, повідомлення та значення підпису. На виході отримується значення «true/false», в залежності від результату перевірки правильності підпису.

Існують різні алгоритми цифрового підпису, але в блокчейнух, як правило, застосовуються алгоритми цифрового підпису на основі еліптичних кривих. Еліптична крива схематично зображена на рис. 1.2 [11]. Процес генерації ключової пари відображений на рис. 1.3 [11].

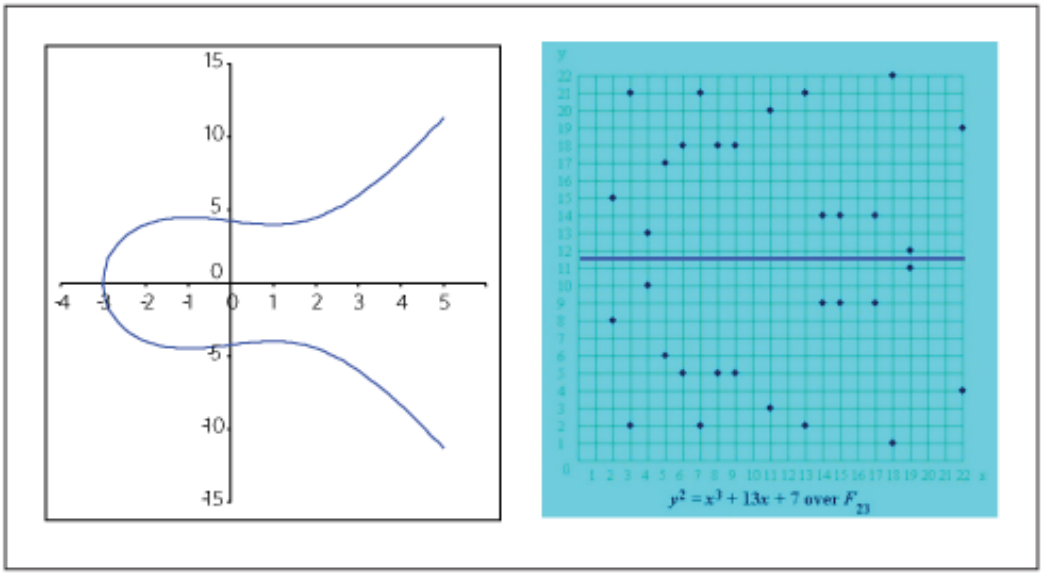

Рисунок 1.2 – Еліптичні криві третього ступеня, дійсна область (ліворуч), над простим полем (праворуч)

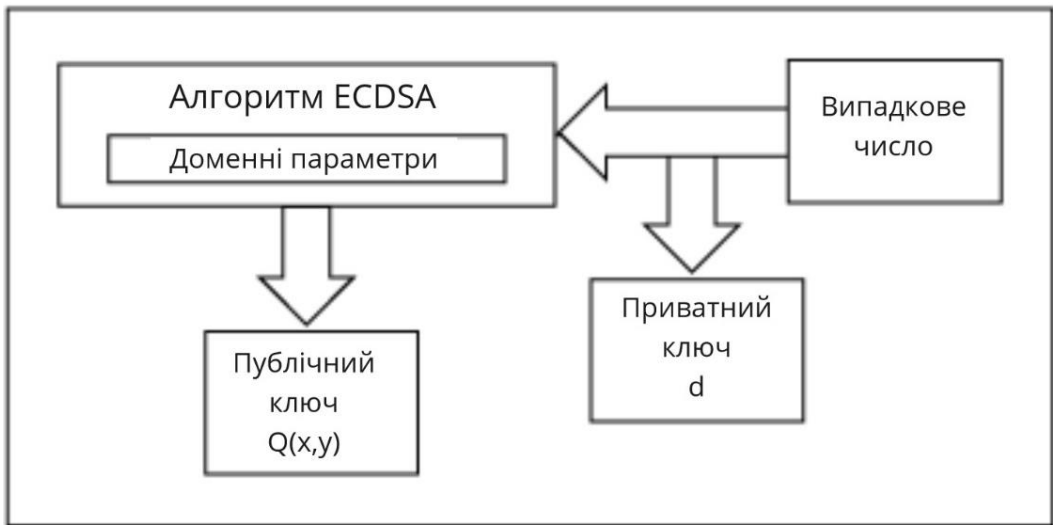

Рисунок 1.3 – Генерація ключової пари за алгоритмом ECDSA

Алгоритм цифрового підпису на основі еліптичних кривих, або ECDSA, є одним з найскладніших алгоритмів шифрування з відкритим ключем. Ключі генеруються за допомогою криптографії еліптичних кривих, які є меншими за середні ключі, що генеруються алгоритмами цифрового підпису. Криптографія еліптичних кривих – це форма криптографії з відкритим ключем, яка базується на алгебраїчній структурі еліптичних кривих над скінченними полями. Криптографія еліптичних кривих в основному використовується для створення

псевдовипадкових чисел, цифрових підписів тощо. Згідно [10], цифровий підпис – це метод автентифікації, при якому пара відкритих ключів і цифровий сертифікат використовуються як підпис для підтвердження особи одержувача або відправника інформації. ECDSA робить те ж саме, що і будь-який інший цифровий підпис, але більш ефективно. Це пов'язано з тим, що ECDSA використовує менші ключі для створення такого ж рівня безпеки, як і будь-який інший алгоритм цифрового підпису. Схема процесу обрахунку підпису зображено на рис.1.4 [11], а схема процесу перевірки підпису – на рис.1.5 [11].

Для підпису повідомлення використовується приватний або закритий ключ, який тримається в таємниці, а для перевірки – відкритий, який можна розголошувати, адже відновити з нього приватний, згідно з правилами генерації, неможливо.

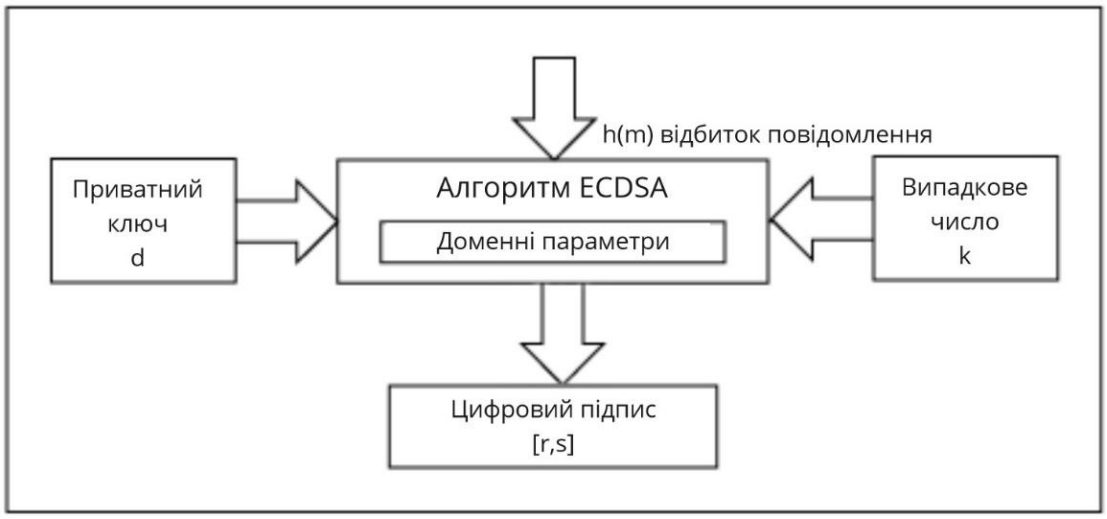

Рисунок 1.4 – Процес обрахунку підпису за алгоритмом ECDSA

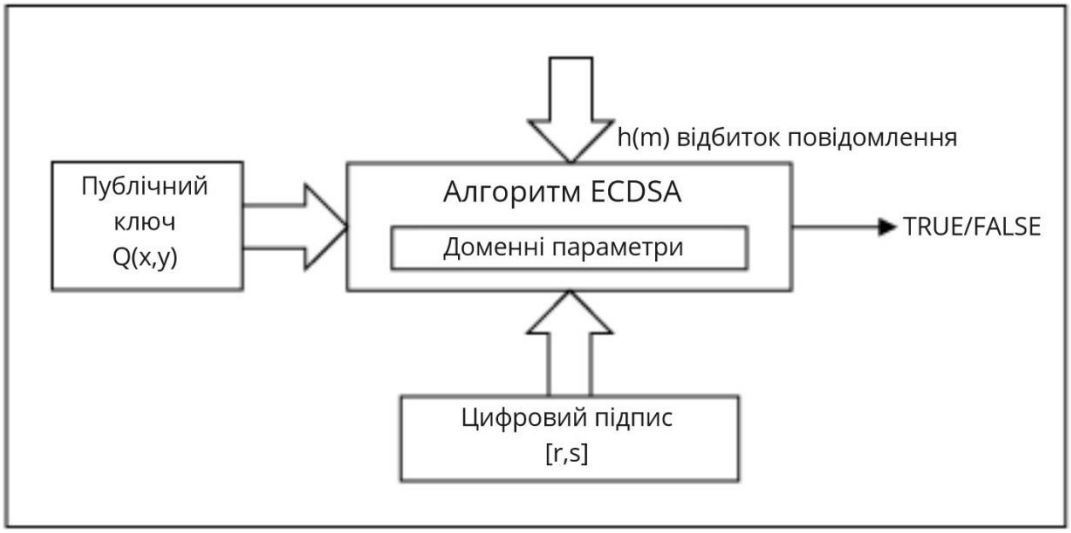

Рисунок 1.5 – Процес перевірки підпису

РОЗДІЛ 2 КОНСЕНСУС

2.1 Потреба досягнення спільного стану системи

Механізми досягнення консенсусу відіграють вирішальну роль у мережах блокчейн, дозволяючи учасникам домовитися про дійсність транзакцій та блоків і досягти консенсусу щодо стану блокчейну. Вони гарантують, що всі вузли мережі працюють разом, щоб підтримувати цілісність і безпеку блокчейну. Детально про консенсус йдеться у джерелах [12, 13].

Основною метою механізмів досягнення консенсусу в мережах блокчейн є досягнення згоди між вузлами щодо порядку і дійсності транзакцій. Завдяки встановленню консенсусу, мережі блокчейн можуть запобігати подвійним витратам, підтримувати узгодженість даних, протистояти атакам і забезпечувати взаємодію без довіри в децентралізованих середовищах.

2.2 Види механізмів досягнення консенсусу

Існує декілька основних механізмів досягнення консенсусу:

- доказ виконаної роботи (англ. Proof of Work, PoW);
- доказ частки (англ. Proof of Stake, PoS);
- делегований доказ частки (англ. Delegated Proof of Stake, DPoS);
- практична візантійська відмовостійкість (англ. practical Byzantine Fault Tolerance, PBFT);
- доказ повноважень (англ. Proof of Authority, POA).

Доказ виконаної роботи

У механізмі досягнення консенсусу PoW учасники (майнери) змагаються у вирішенні складних математичних задач для перевірки блоків і додавання їх до блокчейну. Рішення вимагає значних обчислювальних потужностей і є ресурсоємним. Основною ідеєю цього механізму досягнення консенсусу є

виконана робота та можливість інших членів системи переконатися у факті її виконання. Складне математичне завдання залежить від блоку та даних, які там є. Суть у підборі параметру, тобто випадкового числа, задля отримання геш-значення певного вигляду.

Доказ частки

PoS вибирає валідаторів блоків на основі їх частки (власності) в блокчейні. Валідатори обираються для створення і перевірки блоків на основі кількості криптовалюти, якою вони володіють, або «частки». Такий доказ є більш енергоефективним, проте він накладає значні обмеження на тих, хто може стати валідатором у системі. Цей механізм досягнення консенсусу використовується в системах, де фігурує власність, тобто якісь активи.

Делегований доказ частки

DPoS запроваджує механізм голосування, в якому зацікавлені сторони (власники токенів) обирають обмежену кількість делегатів, які відповідають за валідацію блоків від їхнього імені. Основна відмінність від PoS полягає у тому, що цей механізм досягнення консенсусу дозволяє делегувати свої повноваження голосувати за блоки іншим валідаторам.

Практична візантійська відмовостійкість

PBFT – це механізм досягнення консенсусу, розроблений для дозвільних блокчейнів, згаданих у 1.5. Він використовує модель на основі лідера, де призначений лідер пропонує блок, а інші вузли перевіряють і погоджуються на його включення в блокчейн. Цей механізм досягнення консенсусу корисний для облікових систем, на кшталт системи електронного голосування.

Доказ повноважень

PoA покладається на набір затверджених валідаторів або авторитетних вузлів, які є заздалегідь відібраними і відомими в мережі особами. Валідатори по черзі пропонують і підтверджують блоки, а консенсус досягається завдяки їхньому авторитету і репутації. PoA пропонує високу пропускну здатність, низькі обчислювальні та енергетичні вимоги і підходить для приватних і консорціумних блокчейнів, згаданих у 1.5.

2.3 Порівняння різних механізмів досягнення консенсусу

Вищезазначені у 2.2 механізми досягнення консенсусу мають свої відмінності, з яких випливають їх плюси, мінуси та сфери застосування. Порівняння наведено у таблиці 2.1, сформованої на основі інформації з статей [12, 13].

Таблиця 2.1 – Порівняння різних механізмів досягнення консенсусу

	PoW	**PoS**	**DPoS**	**PBFT**	**PoA**
Анонімність валідаторів	Є	Є	Немає	Немає	Немає
Дозвільність	Бездозвільний	Бездозвільний	Через голосування	Дозвільний	Дозвільний
Безпека	Висока	Середня	Середня	Висока	Низька
Масштабованість	Низька	Середня	Висока	Середня	Висока
Енергоефективність	Низька	Середня	Середня	Середня	Висока
Децентралізація	Повна	Повна	Часткова	Часткова	Низька
Швидкодія	Низька	Середня	Висока	Висока	Висока
Варінти використання	Публічні блокчейни, криптовалюти	Публічні блокчейни, криптовалюти	Публічні блокчейни, облікові застосунки	Бездозвільні блокчейни	Приватні, консорціумні блокчейни

У таблиці кожен механізм досягнення консенсусу оцінюється за кількома параметрами:

- анонімність валідаторів відображає чи відомі дані про валідаторів системи широкому загалу;
- дозвільність показує наскільки вільно можна додати валідатора в системі;
- безпека вказує на рівень безпеки, який забезпечує механізм досягнення консенсусу, враховуючи такі фактори, як стійкість до атак і потенційні вразливості;
- масштабованість відображає здатність механізму досягнення консенсусу обробляти великий обсяг транзакцій і підтримувати продуктивність мережі в міру її зростання;
- енергоефективність відноситься до споживання енергії, пов'язаного з механізмом досягнення консенсусу;
- децентралізація описує ступінь, до якого механізм досягнення консенсусу розподіляє повноваження щодо прийняття рішень між учасниками мережі;
- швидкість досягнення консенсусу відображає час, необхідний для досягнення консенсусу щодо транзакцій і додавання їх до блокчейну;
- варіант використання вказує на типові програми або сценарії, в яких зазвичай використовується механізм досягнення консенсусу.

РОЗДІЛ 3 ТЕХНОЛОГІЯ БЛОКЧЕЙН У КОНТЕКСТІ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

3.1 Проблеми існуючих систем голосування

Системи електронного голосування мають потенціал революціонізувати спосіб проведення виборів, забезпечуючи більшу зручність, ефективність та прозорість. Однак традиційні системи голосування та існуючі рішення для е-голосування часто стикаються з низкою проблем, які підривають довіру, безпеку та точність. Застосування технології блокчейн у системі електронного голосування обіцяє вирішити ці проблеми та підвищити цілісність і надійність процесу голосування.

Традиційні системи голосування, такі як паперові методи, страждають від різних проблем, які можуть поставити під загрозу чесність виборів. Деякі з ключових проблем включають:

- брак прозорості: паперовим системам голосування часто бракує прозорості, що ускладнює перевірку виборцями та зацікавленими сторонами точності результатів; непрозорість процесу може викликати підозри та підірвати довіру до виборчої системи;
- можливе шахрайство: традиційні методи голосування є вразливими до різних форм шахрайства, включаючи підробку бюлетенів, видачу себе за іншого виборця та помилки під час підрахунку голосів; ці вразливості можуть підірвати легітимність результатів виборів;
- обмежену доступність: фізичні виборчі дільниці та фіксовані години голосування створюють проблеми для виборців, які стикаються з географічними бар'єрами, проблемами мобільності або часовими обмеженнями; це обмежує участь і може призвести до позбавлення права голосу;

Хоча **системи електронного голосування** спрямовані на подолання деяких обмежень традиційних методів, вони також стикаються з низкою проблем:

- ризики безпеки: існуючі системи електронного голосування мають вразливі місця в системі безпеки, які можуть бути використані для маніпуляцій з голосами, порушення конфіденційності виборців або здійснення кібератак; ці ризики викликають занепокоєння щодо конфіденційності та цілісності процесу голосування;
- брак довіри: без прозорої системи, яку можна перевірити, існуючим рішенням для е-голосування важко завоювати довіру виборців та інших зацікавлених сторін; залежність від централізованих органів влади та непрозорі процеси можуть підірвати довіру до результатів виборів;
- єдина точка відмови: багато систем е-голосування покладаються на центральний орган або сервер, що робить їх вразливими до єдиної точки відмови; якщо їх скомпрометувати, вся система голосування може опинитися під загрозою, що призведе до неточних результатів або втрати даних.

3.2 Переваги застосування технології блокчейн

Технологія блокчейн пропонує кілька переваг, які можуть вирішити проблеми, пов'язані з традиційними методами голосування та існуючими системами електронного голосування.

Однією з ключових переваг технології блокчейн є її незмінність. Після того, як голос записаний у блокчейні, його стає майже неможливо змінити або маніпулювати ним без досягнення консенсусу в мережі. Ця властивість забезпечує цілісність і достовірність даних голосування, знижуючи ризик шахрайських дій.

Системи голосування на основі блокчейну також можуть вирішити проблеми, пов'язані з приватністю та конфіденційністю виборців. Використовуючи криптографічні методи, виборці можуть голосувати анонімно, захищаючи свою особистість і водночас забезпечуючи можливість перевірки своїх голосів. Ця функція захисту приватності заохочує більше людей брати участь у процесі

голосування, в тому числі тих, хто може вагатися через побоювання, що їхня особиста інформація може бути скомпрометована.

Механізми децентралізованого досягнення консенсусу, що використовуються в технології блокчейн, пропонують надійний і безпечний метод досягнення згоди щодо дійсності голосів. Залучаючи мережу вузлів до процесу досягнення консенсусу, системи голосування на основі блокчейну усувають потребу в центральному органі влади або довірених посередниках. Такий децентралізований підхід знижує ризик маніпуляцій, змови чи примусу, підвищуючи загальну довіру до виборчого процесу.

Блокчейн дозволяє здійснювати прозору перевірку та аудит процесу голосування в режимі реального часу. Кожен голос, записаний на блокчейні, видно всім учасникам, що дозволяє проводити незалежну перевірку підрахунку голосів і гарантує, що кожен голос буде точно врахований в остаточних результатах. Аудит стає простішим, оскільки вся історія голосування зберігається в блокчейні, що дозволяє виявляти та розслідувати будь-які порушення або невідповідності.

Системи голосування на основі блокчейну мають потенціал для підвищення доступності та участі у виборах. Використовуючи цифрові платформи, виборці можуть зручно голосувати з будь-якого місця, усуваючи необхідність у фізичних виборчих дільницях і фіксованих годинах голосування. Така підвищена доступність сприяє інклюзивності, дозволяючи особам, які стикаються з географічними обмеженнями, проблемами мобільності або часовими обмеженнями, реалізувати своє право голосу.

РОЗДІЛ 4 КОМПОНЕНТ РЕАЛІЗОВАНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ, ЩО ВІДПОВІДАЄ ЗА БЛОКЧЕЙН

4.1 Вимоги до системи та компонента

Для системи електронного голосування, що розробляється, було поставлено наступні вимоги:

- анонімність: користувачі системи мають могти віддати свій голос анонімно;
- відкритість: дані в системі мають зберігаються у відкритому вигляді, будь-хто може перевірити результати голосувань та переглянути дані;
- децентралізованість: у системи не має бути єдиної точки;
- масштабованість: у системі має бути можливість додавання нових валідаторів та нових типів транзакцій;
- цілісність даних: дані, які вже внесені в систему, мають бути захищені від модифікації.

Під час розроблення технічного завдання для реалізації компонента було виділено ряд вимог, специфічних для нього:

- конфіденційність: не має бути можливим виявлення персональних даних, їх отримання чи викриття на основі інформації, яка зберігається в блокчейні;
- висока швидкодія: важливою вимогою до системи є створення та додавання нових блоків періодично, навіть якщо вони будуть неповні, з метою відсутності довгого очікування користувачами підтвердження своїх транзакцій;
- незмінність: у блокчейні системи має бути неможливим виникнення альтернативних ланцюжків блоків;
- автентичність даних: дані, які містяться в блокчейні, мають бути підписані за правилами протоколу та лише тими, хто має на це право.

4.2 Вибір механізму досягнення консенсусу

Вибір відповідного механізму досягнення консенсусу має вирішальне значення для забезпечення надійності та безпеки системи електронного голосування на основі блокчейну. У компоненті реалізованої системи, що відповідає за блокчейн, було прийнято рішення обрати механізм досягнення консенсусу, найбільш схожий на «practical Byzantine Fault Tolerance», згаданий у 2.2, детальніше описано в джерелах [14, 15].

Код реалізованої системи голосування на основі технології блокчейн можна знайти за посиланням в джерелі [16].

Вибір був зроблений на основі вимог до системи. Головна ідея системи – відсутність довіри вузлів-валідаторів один до одного. Суть PBFT полягає у тому, що один валідатор створює блок та є ініціатором його розповсюдження, в той час як інші перевіряють і підтверджують або відхиляють пропозицію. Кожен валідатор збирає транзакції від під’єднаних до них користувачів системи, перевіряє їх на правильність згідно правил протоколу, додає у список перевірених транзакцій, з яких потім формуються блоки.

PBFT має ряд якісних переваг перед іншими механізмами досягнення консенсусу. PBFT є швидким, якщо блок був доданий у спільну базу даних, цей ланцюжок є незмінним, альтернативні ланцюжки не допускаються, пропонувати блоки може будь-хто, без обмежень чи потреби вирішення ресурсоємної задачі.

Проте є й ряд недоліків, на які варто звернути увагу у разі масштабування системи. Це значне сповільнення при збільшенні кількості валідаторів і необхідність реєстрації нових валідаторів у системі задля розголошення їх відкритих ключів.

В реалізованій системі валідаторам відомі адреси інших валідаторів для відправки їм блоків чи відповідей стосовно підтвердження блоків.

Кожен вузол валідатора чекає на повідомлення від інших валідаторів і в залежності від типу повідомлення, робить відповідні дії:

– у разі отримання повідомлення про необхідність перевірки запропонованого блоку валідатор перевірить заповнені поля блока та його частин, перевіривши також усі поля транзакцій, що входять до тіла цього блоку, і або поверне ствердну відповідь та дані свого підпису, про які йшла мова в 1.7, або поверне повідомлення про відхилення блоку;
– у разі отримання повідомлення про додавання підтвердженого блоку відбувається повторна його перевірка та додавання у блокчейн у разі пройденої перевірки.

Той валідатор, що пропонує новий блок, по черзі надсилає його іншим валідаторам і на основі їх відповідей або розсилає цей же блок з усіма підписами на додавання в базу даних, або формує новий, попередньо перевіривши та повернувши транзакції до списку перевірених. Рішення про підтвердження блоку приймається на основі подолання певної кількості ствердних перевірок. У реалізованій системі це певна частка від загальної кількості наявних у системі валідаторів, задається через конфігурацію.

4.3 Особливості блоків та транзакцій

У 1.3 було згадано загальну структуру блоків, притаманну більшості блокчейнів. У реалізованій системі блоки складаються з таких частин:

– заголовок;
– підписи валідаторів (англ. Witness);
– тіло.

Заголовок містить:

– мітку часу;
– геш-значення від попереднього блоку в базі даних;
– корінь дерева Меркла;
– версію блока (корисне поле, якщо зміняться правила, за якими відбувається перевірка блоків, потрібне для зворотньої сумісності).

У Witness розміщені відкриті ключі валідаторів та їх підписи, які додаються в разі ствердної перевірки ними відповідного блока.

У тілі блока містяться транзакції, які несуть корисне навантаження.

Транзакції несуть інформацію ,специфічну для системи електронного голосування. Було реалізовано обробку та логіку для таких типів транзакцій:

- транзакція реєстрації нового користувача системи;
- транзакція створення голосування;
- транзакція створення нової групи;
- транзакція віддання голосу;
- транзакція анонімного віддання голосу.

Усі типи транзакцій, крім «Анонімного віддання голосу» містять такі спільні поля:

- тип транзакції, для розрізнення між собою;
- тіло транзакції, що містить дані, притаманні конкретному типу;
- випадкове число, яке було згадано в 1.3;
- значення підпису за алгоритмом цифрового підпису на еліптичній кривій, згаданим у 1.7;
- відкритий ключ підписанта, потрібний для перевірки підпису.

Тіло транзакції містить різні дані, в залежності від типу транзакції.

У тілі транзакції реєстрації нового користувача міститься його відкритий ключ, згенерований за правилами системи, та рівень доступу, який визначається типом акаунту.

У тілі транзакції створення групи лежить ідентифікатор групи, назва групи та список відкритих ключів учасників цієї групи.

У тілі транзакції створення голосування лежить дата закінчення цього голосування, опис голосування, варіанти відповідей та список відкритих ключів або ідентифікаторів груп, учасники яких можуть брати участь у даному опитуванні.

У тілі транзакції віддання голосу лежить посилання на голосування, що є геш-значенням від транзакції створення цього голосування, та варіант відповіді, який було обрано.

Транзакція анонімного віддання голосу має дещо специфічну структуру, оскільки для її підпису використовується алгоритм кільцевого підпису, що є специфічною версією алгоритму цифрового підпису на основі еліптичних кривих.

У цій транзакції лежить тип транзакції, посилання на голосування, як і в транзакції віддання голосу, варіант відповіді, що було обрано, випадкове число, згадане у 1.3 та дані підпису.

Алгоритм кільцевого підпису надає анонімність підписанта оскільки він формується завдяки приватному ключу підписанта та кільцю відкритих ключів інших користувачів системи, які мають право брати участь в тому голосуванні, голос за яке надається. В результаті в транзакції будуть лежати дані підпису, які складаються з масиву об’єднаних вихідних масивів, які формуються в результаті підпису, та «зображення ключа» (англ. Key Image), яке формується за допомогою криптографічних перетворень приватного та відкритого ключів підписанта. Також в транзакції міститься масив відкритих ключів, які брали участь у якості кільця. Основна різниця та відмінність від звичайного алгоритму цифрового підпису на основі еліптичних кривих – це те, що немає додаткових даних як визначити, який з усіх відкритих ключів, належить підписанту. Детальніше про це можна прочитати в статті [17]. Цей тип підпису додає анонімності системі. Ймовірність вгадати який саме відкритий ключ є відкритим ключем підписанта складає $\frac{1}{n}$, де n – загальна кількість відкритих ключів, які брали участь у підписанні транзакції.

Схема формування кільцевого підпису відображена на рис. 4.1 [17].

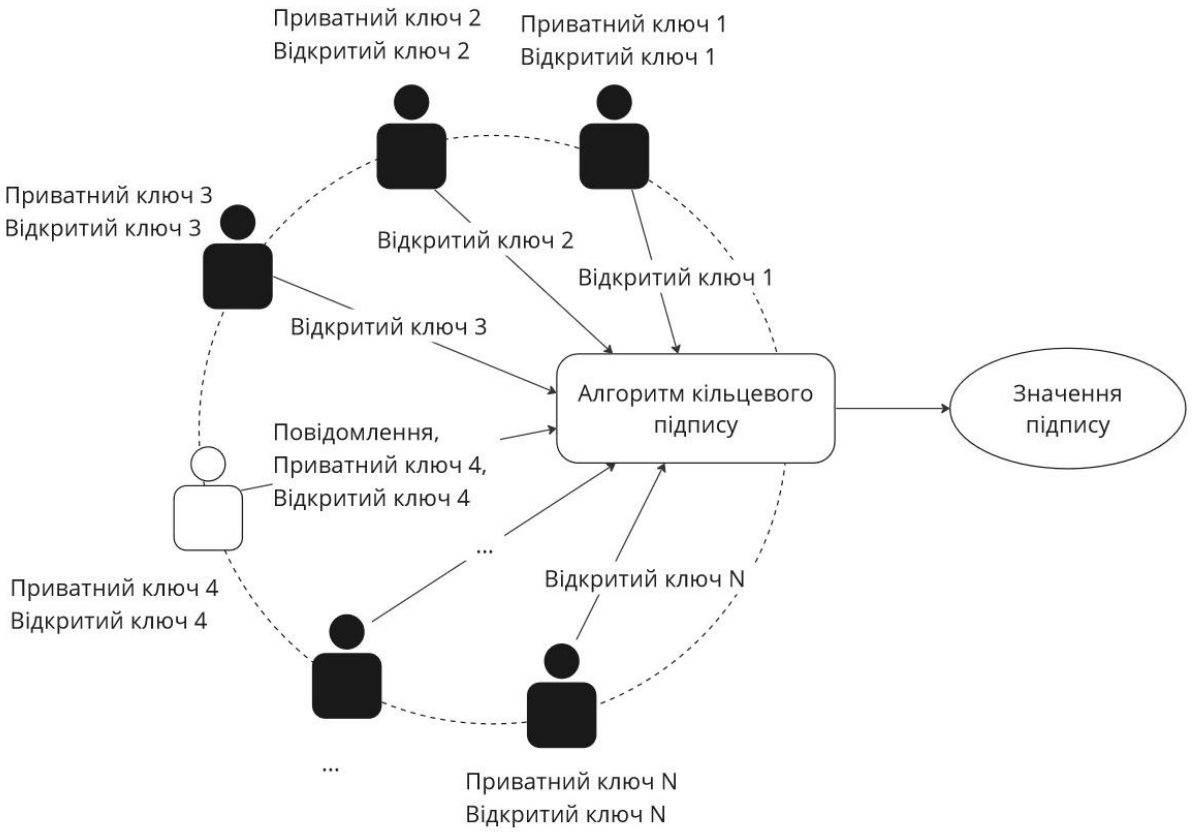

Рисунок 4.1 – Формування кільцевого підпису

Схема перевірки кільцевого підпису відображена на рис. 4.2 [17]. На схемі також відображено ймовірність вгадати який саме відкритий ключ належить підписанту.

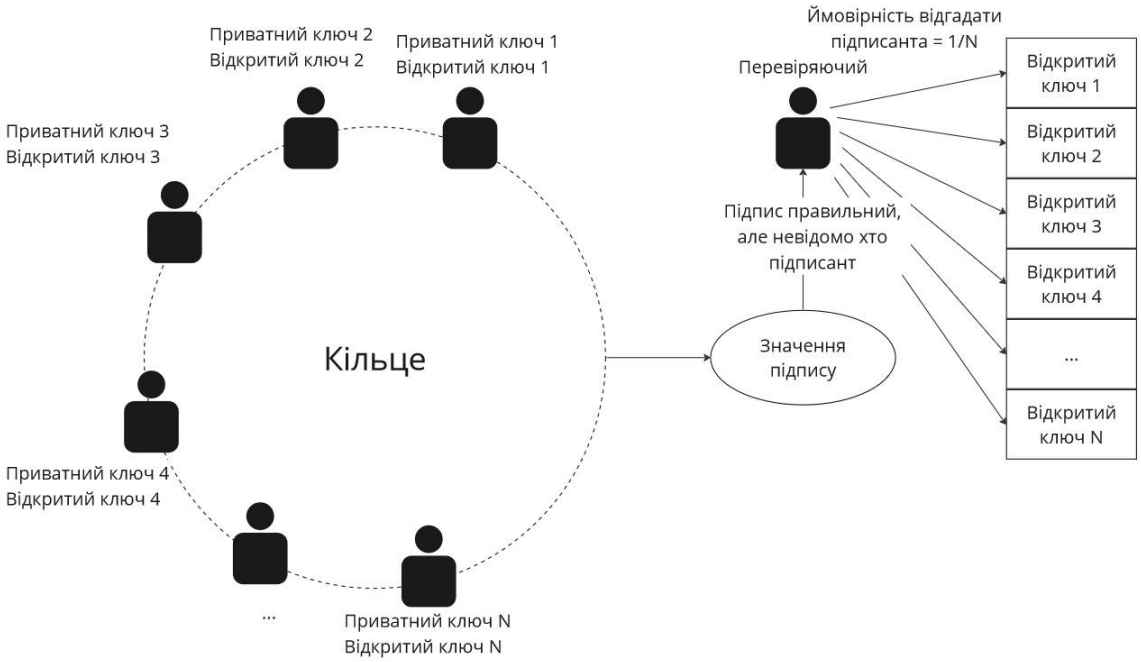

Рисунок 4.2 – Перевірка кільцевого підпису

У системі було створено інтерфейс для транзакцій та для їх тіл, тобто корисного навантаження. Єдина транзакція, яка є особливою, це транзакція анонімного віддання голосу. Як видно з концептуальної діаграми класів на рис. 4.3, під час реалізації компонента системи, що відповідає за блокчейн, було вирішено створити єдиний інтерфейс для транзакції. Це було зроблено з причин наявності однакових полів у різних транзакцій та бажання винести ці поля у загальну транзакцію. Інтерфейс потрібен для того, щоб підтримувати одночасно і транзакцію анонімного віддання голосу, яка має дещо специфічну структуру за рахунок іншого підпису. На рис. 4.3 відображено, що класи «Transaction» та «TxVoteAnonymous» реалізують інтерфейс «ITransaction».

Задля того, щоб зберігати корисне навантаження, було вирішено створити окремий інтерфейс «TxBody», як показано справа на рис. 4.3, який міститься у якості поля в транзакції. Цей інтерфейс було створено у зв’язку з різними механізмами перевірки даних транзакцій, детальніше в про які йдеться в 4.4.

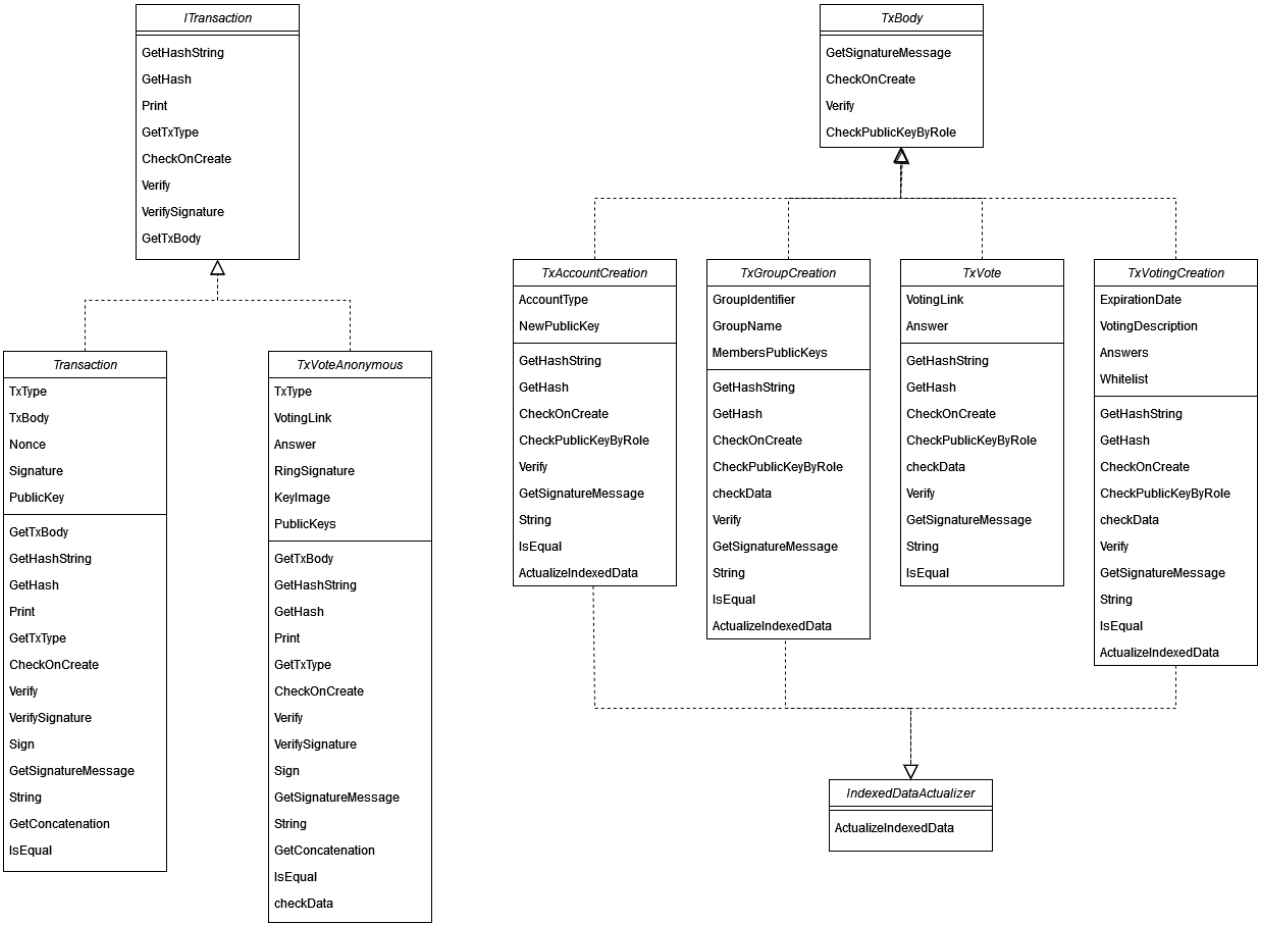

Рисунок 4.3 – Концептуальна діаграма класів для транзакцій

Як видно з рис. 4.3, кожен з типів транзакцій, крім транзакції анонімного віддання голосу, реалізують інтерфейс «TxBody». Ці транзакції мають свої поля, різні в залежності від типу, як уже було зазначено в 4.3.

Також на рис. 4.3 є ще один інтерфейс, «IndexedDataActualizer». В системі для пришвидшеного отримання актуальних даних, що містяться в блокчейні, було реалізовано ряд структур, які містять цю актуальну інформацію, зокрема, сховище відкритих ключів адміністраторів, користувачів, валідаторів та ідентифікаторів груп; індексовані сховища голосувань та груп. Ця інформація має оновлюватися після додавання блока до блокчейну, з метою автоматизації цього процесу та через відмінність даних, які потрібно актуалізувати, в залежності від типу транзакції, було вирішено створити згаданий вище інтерфейс, який реалізують транзакції реєстрації нового користувача, створення голосування та створення групи. Таким чином ці класи самі відповідають за логіку, яка необхідна для актуалізації даних, які в блокчейні містяться саме в них. Метод валідатора, який відповідає за цю

логіку, зображено на рис. А.10 додатка А. Вищезазначені інтерфейси також надають змогу додавання нових типів транзакцій у систему.

Як видно з рис. 4.3, транзакції також мають ряд інших службових функцій, потрібних для різних завдань, від виведення вмісту транзакції під час тестування системи, до отримання геш-значення від транзакції.

На рис. 4.4 зображено концептуальну діаграму класів для блока та його складових частин, які були детальніше описані в 4.3.

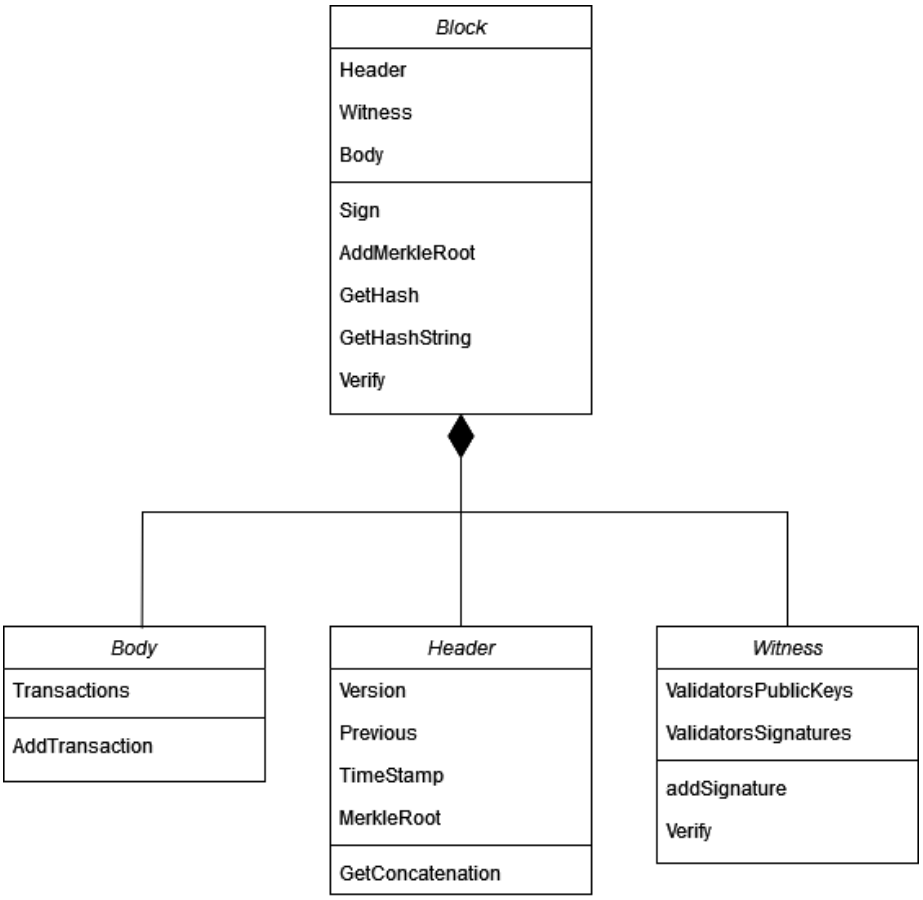

Рисунок 4.4 – Концептуальна діаграма класів для блока та його складових

Як видно з рис. 4.4, блок складається з трьох уже згаданих частин, блок є композицією своїх складових частин. Тут же зазначені ті методи, які необхідні для роботи з цими структурами, зокрема, функція для верифікації або перевірки блока, про яку детальніше йде мова в 4.4.

4.4 Перевірка або верифікація даних

Окрім досягнення консенсусу, який є зв’язуючим компонентом системи, важливу роль відіграють процеси «верифікації» або перевірки даних на різних рівнях. Верифікація є у будь-якому блокчейні, незалежно від сфери застосування чи специфіки реалізації.

Усі дані, які є в системі, зберігаються в блокчейні. Оскільки поки що ще не було зроблено швидкого алгоритму перегляду даних у блокчейні і єдиний спосіб – лінійно переглянути всі блоки з першого, щоб знайти потрібну інформацію, було вирішено зберігати корисну інформацію, яка буде неодноразово запитуватися під час верифікації, у так званих індексованих базах даних. Інформацію у них будуть актуалізувати валідатори автоматично після додавання блоку у свій блокчейн.

Такими даними є публічні ключі адміністраторів з реєстрації, адміністраторів зі створення опитувань, користувачів, валідаторів, ідентифікатори груп. Також зберігаються дані про актуальні голосування та групи (там міститься інформація, взята із тіла відповідних транзакцій).

У реалізованій системі електронного голосування можна виділити два основних рівня, на яких верифікуються дані:

– рівень транзакцій;
– рівень блоків.

На рівні транзакцій верифікація залежить від типу транзакції.

Для транзакції реєстрації нового користувача йде перевірка чи той, хто підписав транзакцію, має на це право, тобто чи є адміністратор з реєстрації з відповідним відкритим ключем.

Для транзакції створення групи перевіряється список відкритих ключів, що були додані в якості учасників цієї групи.

Для транзакції створення голосування полями для перевірки є дата закінчення голосування та список тих, хто має право голосувати, тобто чи такі

відкриті ключі користувачів вже зареєстровані або чи групи з такими ідентифікаторами вже створені.

Для транзакції віддання голосу йде перевірка чи ще можна віддавати голос за голосування з відповідним геш-значенням, і чи взагалі таке голосування існує. Також перевіряється чи має право той, хто підписав цю транзакцію, віддавати голос на відповідному голосуванні. Логіка верифікації даних для цієї транзакції зображена на рис. А.11 – А.14 додатка А.

Для транзакції анонімного віддання голосу йде перевірка чи ще можна віддавати голос за голосування з відповідним геш-значенням, чи взагалі таке голосування існує, чи мають право віддавати голос на цьому опитуванні ті, чиї відкриті ключі лежать у відповідному полі транзакції.

На рівні блоків верифікація проходить для їх частин.

У заголовку блока верифікується корінь дерева Меркла, згаданий в 1.3, який формується на основі тіла блоку та усіх транзакцій, що туди входять. У разі неспівпадіння між отриманим під час повторної побудови дерева Меркла коренем та даними, які знаходяться в заголовку блока, верифікація не пройде. Також верифікується геш-значення попереднього блоку в блокчейні, задля забезпечення умови зв’язків у блокчейні.

У Witness або частині блоку з даними підписів валідаторів йде перевірка того, що усі відкриті ключі, які фігурують у цій частині блоку, є дійсно ключами валідаторів системи і чи правильними є їх підписи.

У тілі блока верифікацію проходять усі транзакції, відповідно до вищеописаної верифікації транзакцій.

Верифікація блока на стороні валідатора, що отримав блок для верифікації, можна схематично зобразити як на рис. 4.5. Також верифікація блока зображена на рис. А.8 та А.9 додатка А.

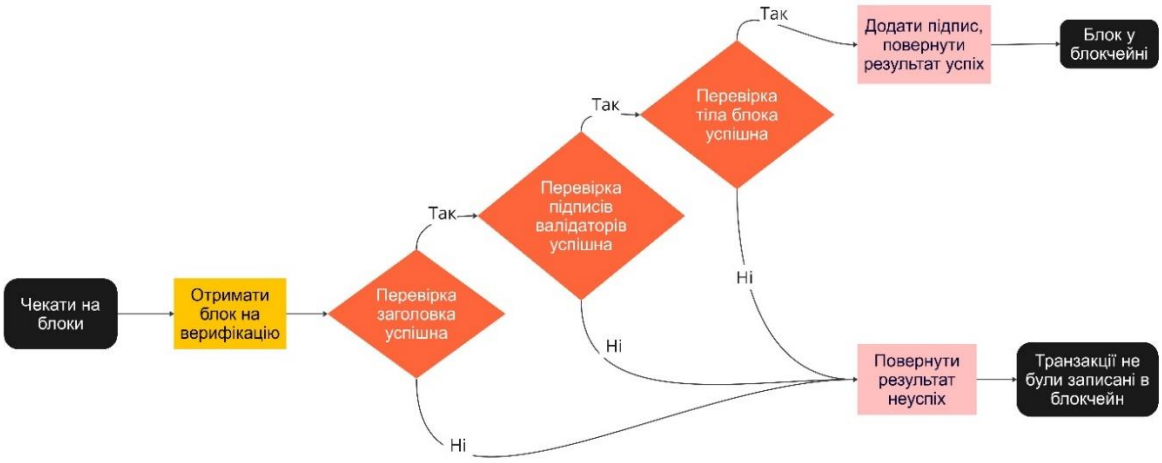

Рисунок 4.5 – Схема перевірки блока валідатором

4.5 Особливості реалізації системи

Схематично систему можна зобразити як на рис. 4.6.

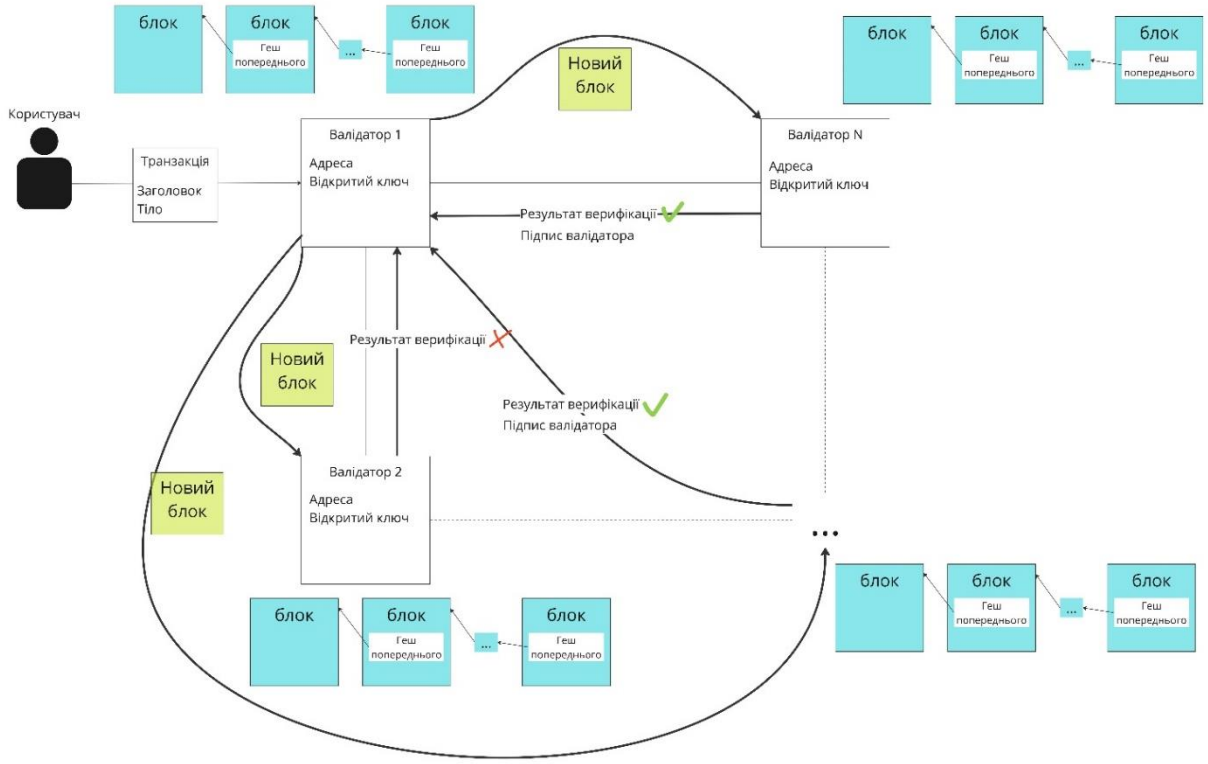

Рисунок 4.6 – Схематичне зображення системи

Як видно з рис. 4.6, в системі валідатори обмінюються новими блоками-пропозиціями та надсилаються результати перевірки. Структура валідатора зображена на рис. А.1 додатка А. Створення та надсилання нових блоків зображено на рис. А.5 додатка А. Кожен валідатор містить копію синхронізованого ланцюжка блоків. Користувачі надсилають транзакції валідаторам.

Кожен валідатор містить список перевірених, але непідтверджених (тобто не доданих у спільну базу даних) транзакцій, який називається «МемПул» (англ. MemPool), з яких і формує нові блоки. Транзакції йому надходять через запити від застосунку користувача. Додавання транзакцій до МемПулу валідатора зображено на рис. А.6 додатка А.

Схематично процес додавання нового блока на стороні пропонуючого валідатора можна зобразити як на рис. 4.7. Прийняття блока зображено на рис. А.3 додатка А, а відхилення – на рис. А.4 додатка А.

Рисунок 4.7 – Схема пропонування нового блоку для пропонуючого валідатора

У блоці може міститися до певної кількості транзакцій, щоб блоки не були необмежено великими, цей параметр задається. Також у валідаторів запускається таймер, щоб користувачі не чекали надто довго на підтвердження своїх транзакцій. Валідатори в системі генерують блоки за двох умов:

– коли вони мають транзакцій у своєму «МемПулі» не менше, ніж максимальна кількість транзакцій в одному блоці;
– коли пройшов час, заданий таймером.

Метод створення нового блока зображено на рис. А.7 додатка А. Після генерації блока він пропонується іншим валідаторам для перевірки. Перевірка блока зображена на рис. А.2, А.8 та А.9 додатка А.

Реалізована система цифрового голосування на основі технології блокчейн була розроблена з вимогою задовольнити перелікам вимог, зазначених у 3.2 та 4.1.

Незмінність даних, що були внесені в систему у вигляді корисного навантаження транзакцій, які знаходяться в тілі блоків, забезпечується тим, що як було згадано в 4.1, якщо блок було підтверджено певною кількістю валідаторів, він додається усіма валідаторами у спільну синхронізовану базу даних. Також якщо згадати порівняння зі звичайною базою даних в таблиці 1.1, зрозуміло, що з операцій доступні лише операція запису нових даних та операція читання. Зміна призведе до розриву зв’язків за геш-значенням попереднього блоку, як було описано в 1.3.

Приватність та конфіденційність забезпечуються за рахунок того, що зв’язки між відкритими ключами, що фігурують у відкритому вигляді в транзакціях та блоках, та ідентифікаційними даними, а також приватними ключами відсутні та не зберігаються системою. Це надає можливість бути певним щодо того, що ніхто крім вас, не зможе віддати голос за вас. Також варто згадати реалізований алгоритм кільцевого підпису, описаний у 4.2, завдяки якому реалізована система надає можливість проголосувати анонімно, ще сильніше збільшивши свою анонімність та приховати навіть відкритий ключ.

Децентралізований механізм досягнення консенсусу, що найбільш близький за специфікою до PBFT, згаданого та описаного у 4.1, надає змогу проводити голосування за умови, коли вузли-валідатори системи не довіряють одне одному. Синхронізація бази даних відбувається виключного за рахунок математичних операцій, перевірки уже занесеної в блокчейн інформації та алгоритму цифрового підпису на основі еліптичних кривих, згаданого в 1.7. Усі валідатори працюють за спільними правилами, а будь-яке порушення зробить ствердну відповідь після перевірки неможливою.

Система забезпечує **відкритість та прозорість**, тобто можливість перевірки й підрахунку голосів у режимі реального часу. Завдяки тому, що дані в блокчейні у відкритому вигляді, а спільна база даних синхронізована та однакова у всіх валідаторів, будь-хто може порахувати результати голосування, а знаючи свій приватний ключ, а відтак, за правилами генерації, згаданими в 1.7, і відкритий – перевірити чи враховано його голос. Така прозорість є якісною відмінністю від традиційних систем голосування, вона зменшує ризики корупції та зміни результатів на свій розсуд.

За рахунок того, що система є відкритою, а блокчейн з таким механізмом досягнення консенсусу – бездозвільним, як зазначено в таблиці 2.1, підвищується рівень **доступності**, оскільки будь-хто з доступом до Інтернету може зареєструватися та брати участь у голосуваннях.

Висока швидкодія забезпечується швидким механізмом досягнення консенсусу. За рахунок параметра періодичності створення нових блоків, який задається через конфігурацію, зменшується час очікування користувачами підтвердження своїх транзакцій.

Автентичність даних забезпечується цифровими підписами, згаданими в 1.7 та 4.3, якими підписані усі транзакції та блоки в системі та які дають змогу перевірити чи є підписант учасником системи та правильність підпису.

Цілісність даних забезпечується геш-функціями, згаданими в 1.7, які за рахунок своєї природи за найменшої зміни даних, що містяться в транзакціях або блоках, матимуть на виході зовсім інше значення та порушать правила протоколу.

Реалізований компонент може бути використаний в якості основи для систем електронного голосування, за умови додавання логіки звернення до функцій даного компонента. Компонент забезпечує механізми взаємодії з блокчейном, блоками та транзакціями, а також валідаторів між собою задля досягнення консенсусу.

4.6 Порівняння із існуючими системами голосування на базі технології блокчейн

Було досліджено ряд систем електронного голосування , які використовують технологію блокчейн. Більшість було впроваджено в основному на блокчейні з механізмом досягнення консенсусу PoS, згаданим в 2.2, на основі мережі Ethereum. Про це можна детальніше прочитати в статті [18]. Наша система пропонує відносно швидший консенсус PBFT, про який йшла мова в 4.1.

Системи, запропоновані різними групами дослідників у різний хоча час мали недоліки анонімності, швидкодії, масштабованості чи складності впровадження, проте зарекомендували себе в якості можливих та потенційно вигідних рішень для впровадження системи електронного голосування з використанням технології блокчейн.

В одній системі пропонується спосіб усунення проблемних аспектів традиційних виборів за допомогою технології блокчейн. Ця робота спрямована на створення децентралізованої методології електронного голосування замість централізованої за допомогою технології блокчейн і легкодоступного механізму голосування, який гарантує безпеку ідентифікації виборців, а також передачі та перевірки даних. Обмеженнями цієї системи є те, що відданий голос видно під час голосування, і вона не забезпечує анонімності для виборців.

Інші розробники в системі запропонували демократичний процес на основі блокчейну, заснований на мережі Ethereum. У рамках цього підходу виборча комісія створила обліковий запис в Ethereum для зберігання даних про виборців. Виборці, які не мають доступу до смартфонів чи Інтернету, можуть проголосувати у визначеному місці для голосування. Перед тим, як проголосувати, вони повинні будуть пройти процедуру біометричної верифікації. Хоча в цій системі використовується технологія блокчейн, до неї залучено багато третіх сторін. У ланцюжку записується лише поданий голос, який додається третьою стороною. У цьому випадку можлива фальсифікація голосу.

Також пропонується система електронного голосування на основі блокчейну з використанням смарт-контрактів. Смарт-контракти – це просто програми, що зберігаються на блокчейні і запускаються при виконанні заздалегідь визначених умов. Є три категорії людей, які можуть спілкуватися з програмою: «режисер», «розробник» і «виборець». Це три контракти: «Запис», «Творець» та «Голосування». Контракти «Запис» відповідають за зберігання реєстраційної інформації про виборця для перевірки автентичності. Після перевірки автентичності API переказує кошти контракту «Творець», який відповідає за створення нового контракту «Голосування». Виборчий контракт створено, і він надсилає свою адресу Контракту-засновнику для голосування.

У іншій роботі було запропоновано вдосконалену форму електронного голосування з використанням блокчейну. Цей алгоритм доказу повноти стосується розробки блоків, блокування блоків, управління інформацією та дизайну блокчейну, особливо для мережі машин для голосування. У разі формування блоку головуючий перевіряє унікальний ідентифікатор виборця та його біометричну автентифікацію. Виборець віддає свій голос, після чого машина генерує геш і надсилає дані головуючому для формування блоку. Основним недоліком цієї стратегії є те, що вона вимагає більшої безпеки, конфіденційності та прозорості, перш ніж її можна буде вважати повністю надійним методом голосування.

У роботі, яку використала компанія BroncoVote, розроблено технологію голосування на основі блокчейну для збереження анонімності виборців і підвищення прозорості при збереженні відкритого, безпечного та економічно ефективного механізму голосування. BroncoVote представляє систему голосування, що використовує блокчейн, смарт-контракти та Ethereum для адміністрування виборів та перевірки результатів виборів в університетському середовищі. У цій системі використовуються три контракти: «Реєстратор», «Творець» та «Контракт» голосування. Обмеженнями цієї системи є те, що вона має погано захищений метод реєстрації та слабку автентифікацію виборців. Також існують проблеми з дотриманням конфіденційності в цьому процесі.

Також була створена та побудована AMVchain – ефективну і масштабовану систему голосування, яка використовує блокчейн і смарт-контракти для забезпечення прозорого і децентралізованого голосування. Вони почали з вивчення недоліків і проблем існуючих систем голосування на основі блокчейну, а потім зробили огляд важливих досліджень, спрямованих на вирішення цих проблем. На основі специфікацій для надійної та ефективної системи електронного голосування. Кільцеві підписи, що зв'язуються, використовуються в процесі голосування, щоб розірвати зв'язок між виборцями та голосами і забезпечити анонімність виборців.

В одній з робіт запропоновано архітектуру цифрового голосування, яка містить смарт-контракт для вирішення таких проблем, як автентифікація, прозорість, анонімність, точність і автономність, а також цілісність і мобільність, які виникають під час використання блокчейну для голосування. На основі інформації, наданої виборцями, створюється геш, який записується в ланцюжок у їхній системі. Оскільки дані зберігаються у вигляді гешу на блокчейні, виборці отримують вигоду від масштабованості та анонімності. Смарт-контракти на блокчейні забезпечують безпеку та анонімність. Смарт-контракт звертається до майнера, щоб збільшити швидкість транзакцій. На це впливає багато змінних, в тому числі передача даних і використання енергії. Кожен блок має свій унікальний метод підрахунку голосів. Після завершення голосування можна просто підрахувати загальну кількість голосів з останнього блоку. Це скорочує час підрахунку.

В іншій роботі представлено систему електронного голосування на основі блокчейну, яка використовує специфічне шифрування «Time Lock» (шифрування з часовим блокуванням) для забезпечення цілісності, автентифікації та конфіденційності. Автентифікація здійснюється за допомогою сліпого підпису. Тільки привілейовані люди можуть приєднатися до певної політичної партії та проголосувати за неї. Завдяки тому, що технологія блокчейн є децентралізованою технологією, вона може бути використана для подолання централізованої проблеми. У цій статті шифрування з блокуванням часу використовується для

захисту виборів від фальсифікацій шляхом запобігання тому, щоб усі сторони, які беруть участь у виборах, не бачили результатів до певного, заздалегідь визначеного часу.

Зі згаданими статтями можна ознайомитися у джерелі [18].

Порівняння зі згаданими системами електронного голосування з використанням технології блокчейн можна узагальнити за допомогою табл. 4.1.

Таблиця 4.1 – Порівняння блокчейн-компонента реалізованої системи та систем зі статей

	Реалізована система	**Запропоновані системи**
Прозорість	Прозора	Часто використовується шифрування
Масштабованість	Легко масштабується, потрібно взяти до уваги швидкість перевірки блоку всіма валідаторами	Складно масштабувати через використання блокчейну Ethereum та Смарт-контрактів
Витрати	Як такої «цінності», яка б витрачалася на запис транзакції в системі немає	Потрібні цифрові гаманці з активами задля запису транзакцій
Можливість аудиту	Є репозиторій із відкритим кодом системи	Системи або теоретичні, або із закритим кодом
Швидкодія	Механізм досягнення консенсусу швидкий	Механізм досягнення консенсусу повільніший, є обмеження за рахунок особливостей блокчейну Ethereum
Безпека	Є можливість додавання перевірки даних користувача при реєстрації; варто проаналізувати ряд можливих атак та методи захисту від них	Дані шифруються; це водночас може створити потенціал цензурування системи стороною-організатором голосування

З таблиці 4.1 можна зробити висновок, що реалізована система, а саме її компонент, який відповідає за блокчейн, є кращою за багатьма параметрами, аніж запропоновані аналоги. Про те, як можна покращити систему, в 4.6.

4.7 Потенціал до розвитку системи

Реалізована система є прототипом робочої системи електронного голосування на основі технології блокчейн.

Потенційно є можливим розгортання системи для потреб різних компаній, використання системи з комерційною метою. Під час масштабування системи основними перешкодами можуть стати швидкодія обробки та додавання нових блоків. Також варто звернути увагу на безпечну передачу даних, найбільш ефективний метод зберігання блокчейну в довгострокову пам’ять, відновлення стану валідатора у разі непередбачуваних обставин, а також ефективне додавання нових валідаторів без потреби обов’язкової передачі всього блокчейну з першого блоку.

Окремим питанням є реєстрація нових користувачів. Бажаним є додавання проміжного етапу перевірки в якогось стороннього сервісу з метою ідентифікації особи в якості такої, яка має право реєструватися в системі. Таким етапом може бути запит до державного органу, який може ідентифікувати особу або база даних університету. Таким чином буде створено додатковий захист системи від безлічі неправомірно зареєстрованих користувачів з метою фальсифікації результатів голосування.

Також варто взяти до уваги обмеження на кількість транзакцій, підписаних одним і тим самим користувачем. Теоретично користувач може змінювати свій голос і остаточним буде вважатися останній, який лежить у блокчейні. Проте перевантаження системи DoS- або DDoS-атаками, мета яких – відмова в обслуговуванні, або, простими словами, перешкоджання роботі системи; є неприпустимим і варто звернути увагу на забезпечення захисту ще й від цього.

Можлива зміна структури блока, а також додавання нових типів транзакцій для розширення функціоналу системи. Індексовані дані також мають зберігатися в довгострокову пам’ять, періодично перевірятися та відновлюватися у разі потреби.

Крім вищезазначеного варто звернути увагу й на механізм перевірки даних валідатора перед його додаванням у систему та надання йому права голосувати за прийняття блоків. Така перевірка є корисною з точки зору захисту системи від нечесних вузлів, які можуть бути як вузлами зі шкідливим кодом, так і вузлами, які володіють чужим відкритим ключем.

ВИСНОВКИ

У даній роботі було розроблено продукт «Digital-Voting», а конкретно в ньому – компонент системи, що відповідає за використання технології блокчейн. Продукт задовільняє списку вимог згаданої вище системи. Можливе моделювання роботи продукту в умовах, схожих до реальних.

Особисто було розроблено механізм досягнення консенсусу, логіку блокчейну, блоків та транзакцій, їх верифікацію.

Було досліджено особливості реалізованої системи. Було зазначено, як реалізована система використовує технологію блокчейн для вирішення проблем існуючих систем електронного голосування. Було згадано особливості механізму досягнення консенсусу та реалізації механізмів перевірки даних. Окрему увагу було приділено особливостям структури та логіки таких типів даних, як транзакції та блоки, які використовуються як абстракції з метою запису даних у спільну базу даних.

В якості шляхів удосконалення системи може бути покращено методи спілкування між вузлами валідаторів та додано можливість перевірки даних людини через сторонній сервіс перед реєстрацію.

Реалізована система має високі показники швидкодії, вищі, ніж у аналогів, за рахунок швидшого механізму досягнення консенсусу. Вибраний механізм досягнення консенсусу гарантує незмінність даних та неможливість формування альтернативних ланцюжків блоків. Система є гнучкою та дешевою в реалізації, можна провести аудит, оскільки код є відкритим. Використання криптографічних алгоритмів гарантує автентичність та цілісність даних, що зберігаються в блокчейні.

Продовження розробок за цією тематикою є доцільним у зв’язку з потенціалом подальшого вдосконалення системи з метою досягнення кращих результатів за параметрами швидкодії, безпеки, прозорості, доступності та анонімності, порівняно з попередніми версіями та аналогами.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. What is blockchain technology? [Електронний ресурс] – Режим доступу до ресурсу : https://www.ibm.com/topics/blockchain
2. Лі Чаум Д. Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups : дис. докт. філос. наук / Лі Чаум Девід – Берклі, США, 1982. – 96 с. – Режим доступу до статті : https://nakamotoinstitute.org/static/docs/computer-systems-by-mutually-suspicious-groups.pdf
3. Іредейл Г. Blockchain vs Database: Understanding The Difference [Електронний ресурс] / Гвінет Іредейл. – 2021. – Режим доступу до ресурсу: https://101blockchains.com/blockchain-vs-database-the-difference/
4. Blockchain Structure [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/blockchain-structure/
5. Чамблі А. Merkle Tree [Електронний ресурс] / А. Чамблі, К. Мур, Д. Хім. – 2023. – Режим доступу до ресурсу: https://brilliant.org/wiki/merkle-tree/
6. Оренес-Лерма Л. What Is a Blockchain Validator? [Електронний ресурс] / Лінда Оренес-Лерма. – 2023. – Режим доступу до ресурсу: https://www.ledger.com/academy/what-is-a-blockchain-validator
7. Types of Blockchain [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/types-of-blockchain/
8. Вегжин К. Types of Blockchain: Public, Private, or Something in Between [Електронний ресурс] / К. Вегжин, Є. Ванг. – 2021. – Режим доступу до ресурсу: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between
9. Cryptography Hash functions [Електронний ресурс] – Режим доступу до ресурсу: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

10. What is ECDSA Encryption? How does it work? [Електронний ресурс] – Режим доступу до ресурсу: https://www.encryptionconsulting.com/education-center/what-is-ecdsa
11. The Fundamentals Of An Ecdsa Authentication System [Електронний ресурс] – Figure 1, 2, 3, 4 – Режим доступу до ресурсу : https://www.analog.com/en/technical-articles/elliptic-curve-digital-signature-algorithm-explained.html
12. Бісвас С. What Is Consensus In Blockchain? [Електронний ресурс] / Суджайні Бісвас. – 2023. – Режим доступу до ресурсу: https://cleartax.in/s/consensus-in-blockchain
13. Бехер Б. What Is a Consensus Mechanism? [Електронний ресурс] / Брук Бехер. – 2023. – Режим доступу до ресурсу: https://builtin.com/blockchain/consensus-mechanism
14. Худа П. practical Byzantine Fault Tolerance(pBFT) [Електронний ресурс] / Парікшит Худа. – 2022. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/
15. The practical Byzantine Fault Tolerance (pBFT) [Електронний ресурс] – Режим доступу до ресурсу: https://www.javatpoint.com/practical-byzantine-fault-tolerance
16. Баликов А. Digital-Voting-Team/Digital-Voting [Електронний ресурс] / А. Баликов, Р. Волчецький, Н. Саворона. – 2023. – Режим доступу до ресурсу: https://github.com/Digital-Voting-Team/Digital-Voting/tree/develop
17. Anonymous Decentralized E-Voting System [Електронний ресурс] / [О. Курбатов, К. Павло, Ш. Олексій та ін.]. – 2019. – Режим доступу до ресурсу: https://ceur-ws.org/Vol-2588/paper2.pdf
18. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system / С.Алві, М. Уддін, Л. Іслам, С. Ахамед. // Journal of King Saud University - Computer and Information Sciences. – 2022. – №34. – С. 6855–6871 – Режим доступу до статті: https://www.sciencedirect.com/science/article/pii/S1319157822002221

ДОДАТОК А

Приклади коду компонента системи електронного голосування, що відповідає за блокчейн

```
type Validator struct {
    KeyPair     *keys.KeyPair
    MemPool     *MemPool
    Node        *repository.IndexedData
    BlockSigner *signer.BlockSigner
    Blockchain  *blockchain.Blockchain

    NetworkToValidator   <-chan *blk.Block
    ValidatorToNetwork   chan<- *blk.Block
    BlockApprovalChannel <-chan *blk.Block
    BlockDenialChannel   <-chan *blk.Block
    TransactionChannel   <-chan tx.ITransaction

    TxResponseChannel    chan<- bool
    BlockResponseChannel chan<- ResponseMessage

    ValidatorKeysChannel <-chan []keys.PublicKeyBytes
}
```

Рисунок А.1 – Структура класу валідатора в системі

```go
// ValidateBlocks wait for blocks from channel and validate them
func (v *Validator) ValidateBlocks() {
    var response ResponseMessage
    for {
        newBlock := <-v.NetworkToValidator
        if v.VerifyBlock(newBlock) {
            log.Printf( format: "Successfully verified block %s", newBlock.GetHashString())
            publicKey, signature := v.SignBlock(newBlock)
            response = ResponseMessage{
                VerificationSuccess: true,
                PublicKey:           publicKey,
                Signature:           signature,
            }
        } else {
            response = ResponseMessage{
                VerificationSuccess: false,
            }
        }
        v.BlockResponseChannel <- response
    }
}
```

Рисунок А.2 – Метод валідації блока

```go
// ApproveBlock wait for transactions from channel, approve and add them to blockchain
func (v *Validator) ApproveBlock() {
    for {
        approvedBlock := <-v.BlockApprovalChannel
        if v.VerifyBlock(approvedBlock) {
            err := v.AddBlockToChain(approvedBlock)
            v.ActualizeNodeData(approvedBlock)
            if err != nil {
                log.Fatalln(err)
            }
            log.Printf( format: "Successfully added block %s", approvedBlock.GetHashString())
        }
    }
}
```

Рисунок А.3 – Метод прийняття блоків

```go
// DenyBlock wait for transactions from channel, restore transactions from it
func (v *Validator) DenyBlock() {
    for {
        deniedBlock := <-v.BlockDenialChannel
        v.RestoreMemPool(deniedBlock.Body.Transactions)
    }
}
```

Рисунок А.4 – Метод відхилення блоків

```go
func (v *Validator) CreateAndSendBlock() {
    ticker := time.NewTicker(time.Second * 5)
    for {
        select {
        case <-ticker.C:
            hash := v.Blockchain.GetLastBlockHash()
            if v.MemPool.GetTransactionsCount() > 0 {
                v.ValidatorToNetwork <- v.CreateBlock(hash)
            }
        default:
            hash := v.Blockchain.GetLastBlockHash()
            if v.MemPool.GetTransactionsCount() >= MaxTransactionsInBlock {
                v.ValidatorToNetwork <- v.CreateBlock(hash)
            }
        }
    }
}
```

Рисунок А.5 – Метод створення та надсилання блоків

```go
func (v *Validator) AddToMemPool(newTransaction tx.ITransaction) bool {
    v.Node.Mutex.Lock()
    response := newTransaction.CheckOnCreate(v.Node)
    v.Node.Mutex.Unlock()
    if response {
        response = v.MemPool.AddToMemPool(newTransaction)
    }
    return response
}
```

Рисунок А.6 – Метод додавання транзакції в МемПул валідатора

```go
func (v *Validator) CreateBlock(previousBlockHash [32]byte) *blk.Block {
    // Validator does not validate its block since it validated all transactions while adding them to MemPool

    // Takes up to MAX_TRANSACTIONS_IN_BLOCK transactions from beginning of MemPool and create block body with them
    maxNumber := MaxTransactionsInBlock
    blockBody := blk.Body{
        Transactions: v.MemPool.GetWithUpperBound(maxNumber),
    }
    // Create block header
    blockHeader := blk.Header{
        Previous:   previousBlockHash,
        TimeStamp:  uint64(time.Now().Unix()),
        MerkleRoot: merkle_tree.GetMerkleRoot(blockBody.Transactions),
    }

    // Create block itself
    newBlock := &blk.Block{
        Header: blockHeader,
        Body:   blockBody,
    }

    // Sign block
    v.SignAndUpdateBlock(newBlock)

    return newBlock
}
```

Рисунок А.7 – Метод створення нового блока

```go
func (v *Validator) VerifyBlock(block *blk.Block) bool {
    prevHashValid := block.Header.Previous == v.Blockchain.GetLastBlockHash()
    v.Node.Mutex.Lock()
    defer v.Node.Mutex.Unlock()
    return prevHashValid && block.Verify(v.Node)
}
```

Рисунок А.8 – Метод перевірки блока у валідатора

```go
func (b *Block) Verify(indexedData *repository.IndexedData) bool {
    merkleRoot := merkle_tree.GetMerkleRoot(b.Body.Transactions)

    if !b.Witness.Verify(indexedData.AccountManager, b.GetHashString()) {
        return false
    }

    for _, transaction := range b.Body.Transactions {
        if !transaction.Verify(indexedData) {
            return false
        }
    }

    return merkleRoot == b.Header.MerkleRoot
}
```

Рисунок А.9 – Метод перевірки блока у класі блока

```go
func (v *Validator) ActualizeNodeData(block *blk.Block) {
    v.Node.Mutex.Lock()
    defer v.Node.Mutex.Unlock()
    for _, transaction := range block.Body.Transactions {
        txExact, ok := transaction.GetTxBody().(IndexedDataActualizer)
        if ok {
            txExact.ActualizeIndexedData(v.Node)
        }
    }
}
```

Рисунок А.10 – Метод актуалізації даних для швидшого їх отримання з блокчейну

```go
func (tx *Transaction) Verify(indexedData *repository.IndexedData) bool {
    return tx.TxBody.Verify(indexedData, tx.PublicKey) && tx.VerifySignature()
}
```

Рисунок А.11 – Метод верифікації даних у транзакції

```go
func (tx *TxVote) Verify(indexedData *repository.IndexedData, publicKey keys.PublicKeyBytes) bool {
    return tx.checkData(indexedData) && tx.CheckPublicKeyByRole(indexedData, publicKey)
}
```

Рисунок А.12 – Метод верифікації даних у транзакції віддання голосу

```go
func (tx *TxVote) checkData(indexedData *repository.IndexedData) bool {
    indexedVoting := indexedData.VotingManager.GetVoting(tx.VotingLink)
    if indexedVoting.Hash == [32]byte{} {
        return false
    }

    if uint32(time.Now().Unix()) > indexedVoting.ExpirationDate || tx.Answer < 0 ||
        tx.Answer >= uint8(len(indexedVoting.Answers)) {
        return false
    }

    return true
}
```

Рисунок А.13 – Метод перевірки даних корисного навантаження у транзакції віддання голосу

```go
func (tx *TxVote) CheckPublicKeyByRole(indexedData *repository.IndexedData, publicKey keys.PublicKeyBytes) bool {
    if !indexedData.AccountManager.CheckPubKeyPresence(publicKey, account_manager.User) {
        return false
    }

    whiteList := indexedData.VotingManager.GetVoting(tx.VotingLink).Whitelist
    for _, identifier := range whiteList {
        if indexedData.GroupManager.IsGroupMember(identifier, publicKey) || identifier == publicKey {
            return true
        }
    }

    return false
}
```

Рисунок А.14 – Метод перевірки відкритого ключа підписанта транзакції віддання голосу