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:

РОЗРОБКА ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ГОЛОСУВАННЯ НА БАЗІ ТЕХНОЛОГІЇ BLOCKCHAIN

Виконав студент 4-го курсу
Назарій САВОРОНА _____
(підпис)

Науковий керівник:
кандидат фіз.-мат. наук
Костянтин ЖЕРЕБ _____
(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 46 сторінок, 11 ілюстрацій, 15 джерел посилань.

АНОНІМНІСТЬ, АРХІТЕКТУРА СИСТЕМИ, BLOCKCHAIN, ВАЛІДАТОР, ВЕБКЛІЄНТ, ДЕЦЕНТРАЛІЗАЦІЯ, КІЛЬЦЕВИЙ ПІДПИС, КЛЮЧОВА ПАРА, КОНСЕНСУС, СИСТЕМА ГОЛОСУВАННЯ, ТРАНЗАКЦІЯ.

Метою роботи є розробка децентралізованої системи опитування на базі технології Blockchain, яка забезпечує прозорість, безпеку, анонімність та незмінність даних опитувань.

Об'єктом дослідження в контексті розробки є система голосування на основі Blockchain з використанням консенсусу PBFT.

Під час розробки системи опитування на базі технології Blockchain були використані наступні методи та інструменти: Agile-підхід для гнучкого керування процесом розробки, мова програмування Golang для створення бекенду, фреймворк Vue.js 3 для розробки фронтенду, інтегроване середовище розробки IntelliJ IDEA 2022.1 Ultimate для зручного написання коду, інструмент Postman для тестування та взаємодії з API, GitHub Copilot для підтримки автоматичного заповнення коду. Для управління проєктом та організації робочих процесів використовувався інструмент Jira.

Результати роботи включають створення прототипу системи електронного голосування на базі Blockchain, аналіз систем-аналогів та проведення тестування розробленої системи. Новизна полягає в застосуванні сучасних інструментів та технологій, що дозволяють провести незалежне опитування з порівняно малими затратами, забезпечуючи прозорість, безпеку та надійність даних опитувань.

Розроблена система опитування може бути впроваджена в різних сферах, включаючи громадські організації, компанії, державні установи та освітні заклади. Її модульна структура дозволяє легко адаптувати систему до потреб користувачів та розширювати її функціональність.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

API – Application Programming Interface, прикладний програмний інтерфейс;

ECDSA – Elliptic Curve Digital Signature Algorithm, алгоритм цифрового підпису на еліптичній кривій;

ID – identification, офіційна картка або документ з вашим ім'ям та іншою інформацією, яку ви використовуєте для підтвердження вашої особи;

IDE – Integrated Design Environment, інтегроване середовище розробки;

PBFT – Practical Byzantine Fault Tolerance, практична візантійська відмовостійкість;

PK – public key, публічний ключ;

SK – secret key, приватний ключ.

ВСТУП

Сучасний стан об'єкта дослідження або розробки. На сьогоднішній день в галузі систем опитування активно досліджуються та розробляються рішення, що спрямовані на покращення прозорості, безпеки та анонімності опитувань. Дослідження в галузі Blockchain технологій також набувають значного розвитку, забезпечуючи незмінність та надійність даних. Проте, існують виклики, пов'язані з швидкістю, масштабованістю та вартістю реалізації таких систем.

Актуальність роботи та підстави для її виконання. З урахуванням актуальності систем опитування, особливо в контексті демократичних процесів, розробка децентралізованої системи опитування на базі Blockchain є важливою. Потреба у прозорості, безпеці та анонімності вимагає нових підходів до розробки таких систем, які забезпечують надійність та довіру в опитувальних процесах. Потенціал застосування Blockchain технологій у системах опитування варто вивчати та реалізовувати.

Мета й завдання роботи. Метою цієї роботи є розробка децентралізованої системи опитування на базі Blockchain, що забезпечує прозорість, безпеку та анонімність опитувань.

Задля досягнення цієї мети були поставлені наступні завдання:

– проаналізувати підходи до децентралізації, що використовуються в різних системах та дослідити їх переваги та недоліки;

– дослідити технологію Blockchain, вивчити її принципи роботи, особливості та потенційні використання в системах опитування;

– систематизувати існуючий досвід у галузі електронного голосування та на його основі спроєктувати систему, що забезпечує безпеку, приватність та надійність голосування;

– реалізувати програмні компоненти, які будуть слугувати для забезпечення функцій валідаторів системи та їхньої комунікації між собою;

– розробити вебдодаток, за допомогою якого користувачі зможуть взаємодіяти з системою та реалізовувати функції, які стануть основними при використанні даної системи електронного голосування.

Ці завдання дозволили пройти шлях від аналізу до реалізації системи електронного голосування, використовуючи сучасні технології та методи децентралізації, забезпечуючи прозорість, безпеку та анонімність у процесі голосування.

Результатом роботи є реалізація програмних компонентів для валідаторів системи та вебдодатку, що дозволяють користувачам ефективно взаємодіяти з системою та реалізовувати необхідні функції, спрямовані на забезпечення надійного та анонімного електронного голосування.

Об'єкт і методи дослідження або розроблення. Об'єктом дослідження є децентралізована система опитування на базі Blockchain. Для досягнення мети роботи використовувалися методи аналізу існуючих систем, проєктування та розробки системи, а також тестування та оцінка результатів.

Можливі сфери застосування. Розроблена система опитування може бути застосована у різних галузях, де прозорість, безпека та анонімність опитувань є важливими. Наприклад, в політичних виборах, корпоративних рішеннях, громадських дослідженнях та інших сферах, де важлива збір та аналіз даних опитувань.

Взаємозв'язок з іншими роботами. Ця робота була результатом командної співпраці, в якій кожен член команди вносив свій внесок у розробку системи.

Обов'язки автора полягали у розробці архітектури системи та визначенні способів взаємодії між її компонентами. Це включало визначення основних модулів системи, встановлення протоколів комунікації та визначення способів обміну даними між цими компонентами. Робота була спрямована на створення добре структурованої та ефективно працюючої системи, яка забезпечує безперебійну взаємодію між її складовими частинами.

Впровадження Blockchain в систему було здійснено одним з учасників команди, що вимагало розуміння відповідних принципів та технологій, а також вміння інтегрувати його з існуючою системою опитування. Інший член команди відповідав за реалізацію та інтеграцію цифрових підписів, що вимагало знання

криптографічних принципів та вміння забезпечити безпеку та автентичність підписів у системі опитування.

У результаті спільної роботи команди, була створена система опитування, яка поєднує в собі елементи Blockchain та цифрових підписів, і забезпечує прозорість, безпеку та надійність опитувань.

Апробація роботи та публікації з теми роботи. Результати попередніх досліджень та розробок були оприлюднені в [1], коли був реалізований прототип системи за допомогою мови програмування Java.

РОЗДІЛ 1 ОГЛЯД ІСНУЮЧИХ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

1.1 Загальний опис систем електронного голосування

Системи електронного голосування – це комплекси програмних та апаратних засобів, які використовуються для організації та проведення голосування за допомогою електронних засобів. Вони можуть використовуватися для різних типів голосування, включаючи вибори на різних рівнях, голосування на корпоративних зборах, опитування громадської думки тощо [2].

Системи електронного голосування зазвичай мають декілька ключових складових, включаючи модулі для створення та управління бюлетенями, проведення голосування, підрахунку голосів та аудиту. Безпека є важливим аспектом систем електронного голосування, оскільки вони мають захищати приватність голосування і забезпечувати неможливість фальсифікації результатів.

Останнім часом набуває популярності використання технології Blockchain в системах електронного голосування. Blockchain може допомогти забезпечити прозорість та незмінність результатів голосування, водночас забезпечуючи приватність голосів [3].

1.2 Аналіз конкретних систем електронного голосування

Для повноцінного аналізу систем електронного голосування, варто розглянути кілька популярних систем, що існують на сьогоднішній день.

1.2.1 Google Forms

Google Forms – це інструмент, що надає можливість створювати опитування та анкети онлайн. Особливості системи Google Forms включають:

– легкість використання: система пропонує інтуїтивно зрозумілий інтерфейс, який дозволяє користувачам швидко створювати опитування без необхідності в програмуванні чи складних налаштуваннях;

– змога обрати різні види запитань дозволяє створювати різноманітні та деталізовані опитування;

– Google Forms надає можливість легко розповсюджувати створені опитування шляхом надсилання посилань або вбудовування у вебсторінки, користувачі можуть заповнювати опитування з будь-якого пристрою з Інтернет-підключенням;

– система автоматично збирає та упорядковує дані, що надходять від учасників опитування: можна використовувати інструменти Google Sheets для подальшого аналізу та обробки отриманих відповідей.

Наведена система має наступні недоліки:

– відсутність спеціалізації: Google Forms є універсальним інструментом для створення форм, а не спеціалізованою системою для проведення голосувань, це може призводити до обмежень в функціональності та безпеці при голосуванні;

– відсутність вбудованих механізмів криптографії та цифрових підписів може створювати ризик фальсифікації результатів голосування;

– обмежена гнучкість: Google Forms має обмежені можливості налаштування типів запитань, правил голосування та обробки результатів, відповідно до потреб конкретного проєкту;

– система зберігає дані голосувань на своїх серверах, що може порушувати приватність та норми захисту персональних даних.

1.2.2 Helios Voting

Helios Voting – це система електронного голосування, що базується на технології криптографічних протоколів [4]. Особливості системи Helios Voting включають:

– захист приватності: Helios Voting застосовує протоколи криптографічного голосування, що забезпечують анонімність голосів та захист особистої інформації виборців;

– перевірка голосів: Система дозволяє виборцям перевірити, що їх голоси були правильно зараховані та не піддалися фальсифікації;

– Helios Voting надає можливість налаштовувати типи голосування та вимоги до голосування, що робить систему гнучкою та адаптивною до різних сценаріїв голосування;

– система забезпечує можливість голосувати віддалено, через Інтернет, що полегшує процес голосування та робить його доступним для широкого кола виборців.

Недоліками системи Helios Voting є:

– складність використання: має складний інтерфейс та вимагає високого рівня технічної експертизи для належного використання, що може створювати бар'єри для широкої аудиторії та знижувати доступність системи;

– Helios Voting має обмежену масштабованість і може стикатися з труднощами при обробці великого обсягу голосів або проведенні масштабних голосувань;

– система має обмежені можливості для налаштування додаткових параметрів голосування та обробки результатів, це може обмежувати гнучкість та специфічні потреби користувачів.

1.2.3 Estonian i-Voting

Естонія є однією з країн, яка широко впровадила електронне голосування. Їх система i-Voting дозволяє громадянам голосувати через Інтернет за використанням їх електронного ID. Система захищає голоси за допомогою криптографії і дозволяє громадянам змінити свій голос протягом певного періоду часу [5].

Основні особливості цієї системи включають:

– голоси громадян захищені за допомогою криптографії та цифрових підписів, що гарантує їхню автентичність та недоступність для змін;

– є можливість змінити свій голос протягом певного періоду часу, що дає їм більшу гнучкість та можливість перегляду свого вибору;

– використання електронної системи дозволяє ефективно проводити голосування та підраховувати голоси без затрат на друку бюлетенів та організацію виборчих дільниць.

Недоліками системи i-Voting є:

– залежність від електронного ID: для використання системи необхідно мати електронний ID, що може бути обмеженням для тих, хто не має доступу до такого ідентифікатора або не має технічних навичок для його отримання;

– як будь-яка електронна система, i-Voting піддається ризику кібератак та вторгнень, що може підривати надійність та конфіденційність голосів;

– хоча система i-Voting забезпечує шифрування та захист голосів, вона все ж може бути наразі недостатньо анонімною, оскільки інформація про голосування пов'язана з електронним ID голосуючого;

– використання системи можливе лише для тих, хто має доступ до Інтернету та інфраструктури електронного голосування, що обмежує її доступність для окремих регіонів або соціальних груп.

1.2.4 Voatz

Voatz – це система електронного голосування, яка дозволяє громадянам голосувати за допомогою мобільних пристроїв. Особливості системи Voatz включають:

– громадяни можуть голосувати з будь-якого місця та в будь-який час за допомогою мобільного додатку Voatz, що робить процес голосування більш зручним та доступним;

– система використовує шифрування та ідентифікацію на основі біометричних даних для забезпечення безпеки голосів та захисту від шахрайства;

– Voatz має механізми для перевірки та верифікації особи голосуючого, забезпечуючи високий рівень достовірності голосів;

– система Voatz забезпечує можливість перевірити та прослідкувати голоси виборців, забезпечуючи прозорість та відстежуваність процесу голосування.

Недоліки Voatz:

– система доступна лише для певних регіонів або організацій, що обмежує її використання глобально;

– голосування за допомогою Voatz вимагає наявності сумісного мобільного пристрою та встановлення спеціального додатку, що може бути обмеженням для тих, хто не має доступу до таких пристроїв або не має навичок використання мобільних додатків;

– як і будь-яка електронна система, Voatz піддається ризику кібератак та вторгнень;

– відсутність відкритого коду та можливості перевірки системи незалежними сторонами може порушувати прозорість та довіру;

– звітність щодо того, як точно забезпечується анонімність голосування в систем, залишається неоднозначною, що може викликати сумніви щодо конфіденційності голосів;

– Voatz використовує сторонню компанію для верифікації ідентичності голосуючих, що створює певну залежність від довіри до цієї компанії та її процесів;

– система може вимагати значних витрат на розгортання та підтримку, що може бути фінансово вимогливим для організацій з обмеженими ресурсами;

– відсутність можливості повторної перевірки голосів у системі Voatz може створювати проблеми при виявленні та виправленні помилок або недоліків у процесі голосування: після того, як голос був зареєстрований або підрахований, немає можливості повторно перевірити чи переглянути цей голос.

Voatz забезпечує безпеку і прозорість голосування, але її використання біометричних даних може викликати питання щодо приватності [6]. При розробці таких системи доцільно зосередиться на забезпеченні безпеки і прозорості, водночас намагаючись захистити приватність користувачів.

1.3 Проблеми існуючих систем електронного голосування

Хоча системи електронного голосування пропонують численні переваги, вони також стикаються з рядом проблем та викликів:

– найбільш очевидною проблемою є безпека: хакерські атаки, крадіжка даних та інші кіберзлочини можуть знищити довіру до електронного голосування і змінити результати виборів [7];

– забезпечення анонімності голосів є складною задачею в цифровому середовищі, криптографія може допомогти, та вона не завжди може гарантувати абсолютну приватність;

– системи електронного голосування можуть страждати від технічних проблем, які можуть перешкоджати виборцям голосувати або навіть впливати на результати виборів;

– у районах з обмеженим доступом до Інтернету або там, де люди можуть не мати необхідних технологій, електронне голосування може бути проблематично провести;

– у системах, що дозволяють змінювати голоси, існує ризик неправильного використання цієї функції, це може призвести до ситуацій, коли виборці змушені змінювати свій голос під тиском.

Ці проблеми можуть бути вирішені різними способами, включаючи вдосконалення криптографічних методів, поліпшення інфраструктури та проведення освітніх кампаній для громадян.

РОЗДІЛ 2 РОЗГЛЯД ТЕХНОЛОГІЇ BLOCKCHAIN ТА ПОВ'ЯЗАНИХ ЗАСОБІВ В СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

2.1 Опис технології Blockchain

Технологія Blockchain, або блокчейн, представляє собою вид децентралізованої бази даних, яка зберігає дані у вигляді послідовності «блоків». Кожен блок містить інформацію про транзакції, які відбулися за певний період часу, а також криптографічний хеш попереднього блоку в ланцюзі, що забезпечує цілісність і незмінність даних (див. рис. 1).

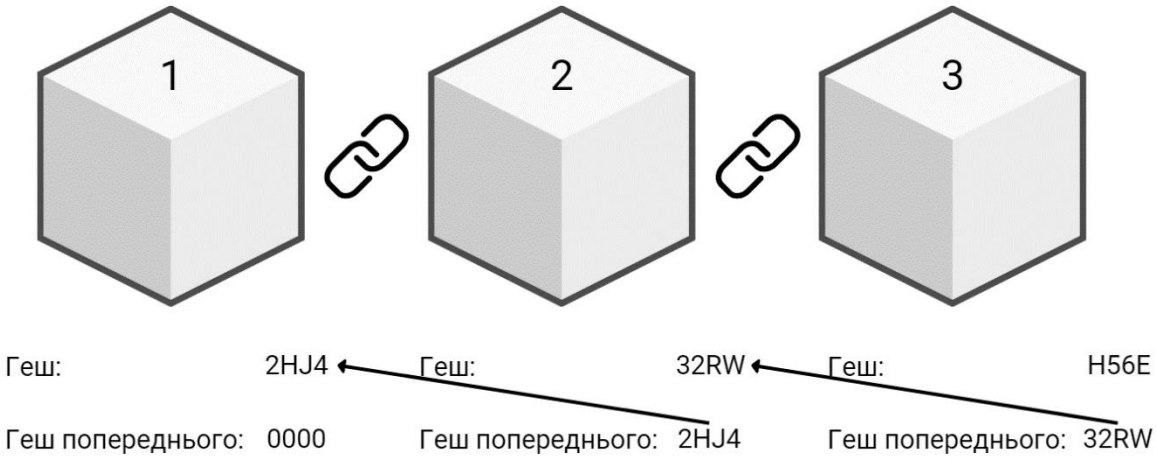

Рисунок 1 – Зв'язки блоків у Blockchain [8]

Основні характеристики технології Blockchain включають:

– децентралізація, що передбачає відсутність центральної точки контролю, це робить систему більш стійкою до атак, всі учасники мережі (вузли) мають однакову копію всього Blockchain;

– всі транзакції зберігаються без шифрування, у відкритому вигляді, для перегляду всіма учасниками мережі, що підвищує прозорість;

– однією з ключових особливостей Blockchain є неможливість змінювати вже записані дані, це забезпечує високий рівень довіри до записаних даних;

– використання криптографії дозволяє забезпечити конфіденційність транзакцій, захист від маніпуляцій і неправомірного доступу до даних.

Blockchain знайшов велику кількість застосувань, починаючи від криптовалют, як Bitcoin, і закінчуючи більш широкими застосуваннями, такими як управління постачаннями, вибори і багато інших [9].

2.2 Переваги використання Blockchain

Технологія Blockchain може бути використана в системах електронного голосування для підвищення прозорості, надійності та безпеки процесу. Використання Blockchain у системах електронного голосування може мати наступні переваги:

– як вже було описано, Blockchain забезпечує незмінність транзакцій, що означає, що однією з головних переваг є забезпечення неможливості зміни, видалення або маніпуляції з голосами після їх подання;

– всі дані про голосування, включаючи інформацію про кожен окремий голос, можуть бути відкрито доступні для перевірки, зберігаючи при цьому конфіденційність виборців;

– Blockchain використовує криптографічні методи для забезпечення безпеки даних, що робить систему стійкою до хакерських атак;

– Blockchain – це децентралізована технологія, що позбавляє необхідності в одному централізованому органі, який контролює голосування;

– Blockchain може автоматизувати та прискорити процес підрахунку голосів, значно знижуючи ризик помилок;

– виборці можуть відслідковувати свій голос в системі, щоб переконатися, що їх голос був правильно зараховано. [10]

Однак, слід зауважити, що хоча технологія Blockchain має багато переваг, її використання в системах електронного голосування все ще є предметом дискусій та досліджень через ряд потенційних викликів, зокрема питання анонімності, масштабування та енергоефективності.

2.3 Поняття ключів

Криптографічний ключ – це цифрова послідовність певної довжини, створена за певними правилами, з використанням генераторів випадкових чисел та розрахована за допомогою спеціального алгоритму.

Криптографічний ключ є основною складовою криптографічних операцій. Безпека більшості криптографічних схем в загальному випадку залежить від захищеності ключів.

Приватний ключ (private key) є натуральним числом константної довжини, яке сформовано за допомоги таких генераторів. Публічний ключ (public key) отримується з приватного шляхом математичних перетворень.

Суттєвим є той факт, що для криптографічних алгоритмів, які вважаються досить надійними, зворотній процес, тобто отримання приватного ключа з публічного, на практиці неможливий [9, с. 107-108].

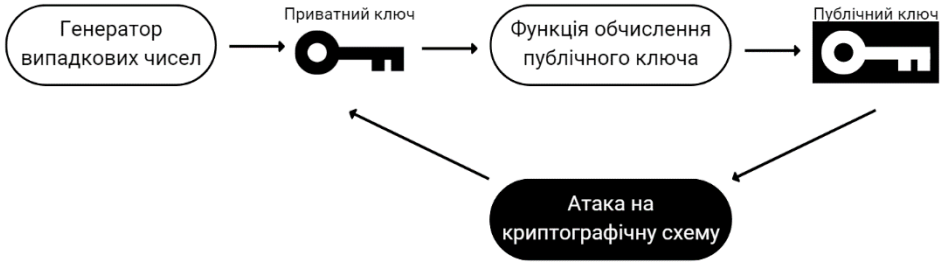

Рисунок 2 – Генерація публічних та приватних ключів
[9, с. 108]

2.4 Кільцевий підпис

Кільцевий підпис відіграє одну з головних ролей у системі цифрового голосування. Спершу розберемось із самим поняттям електронного підпису.

Завдання по забезпеченню перевірки автентичності авторства найчастіше вирішується за допомогою цифрового підпису. Дамо спрощене пояснення.

Цифровий підпис – це аналог рукописного підпису, який забезпечує дві властивості: можливість перевірки автентичності та цілісності документа, що захищає його від модифікації та підміни [9, с. 107].

Кільцеві підписи використовуються для забезпечення анонімності користувачів серед певного набору інших членів групи (кільця). Для створення такого підпису користувач використовує публічні ключі інших користувачів і свою пару ключів. Перевіряючи підпис, перевіряючий може переконатися, що його обчислив один із учасників кільця, але невідомо, ким саме.

Уявіть групу з N користувачів, як на рисунку 3. Кожен користувач має свою власну пару ключів — приватний і публічний ключ (sk, PK). Секретні ключі відомі тільки їх власникам, публічні ключі – всім учасникам системи.

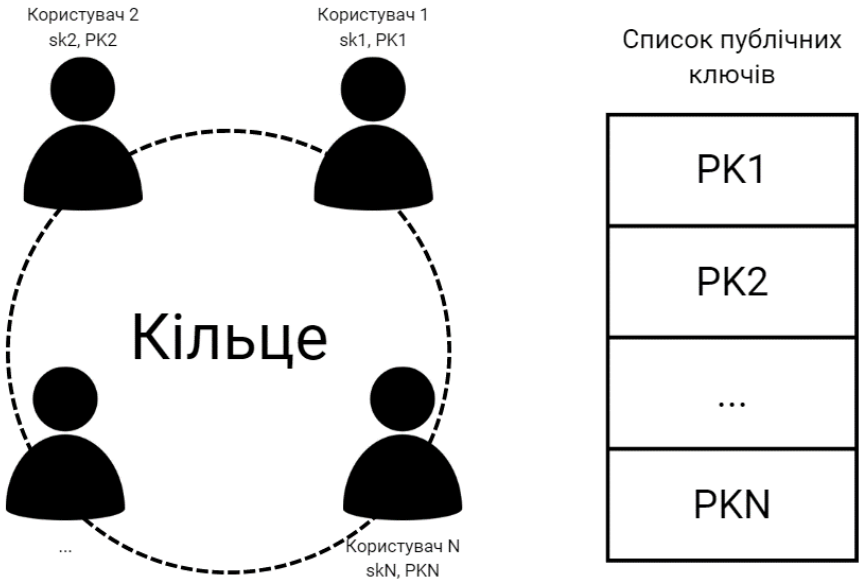

Рисунок 3 – Процес формування кільця [11, с. 7]

Для того, щоб сформувати підпис від імені групи, користувачу необхідно ввести публічні ключі всіх учасників кільця (включаючи свій власний) на вхід алгоритму та використовувати свій приватний ключ як секрет. Нагадаємо, що публічні ключі кожного з учасників є загальнодоступними. На рисунку 4 показано, як генерується кільцевий підпис користувачем під номером 2.

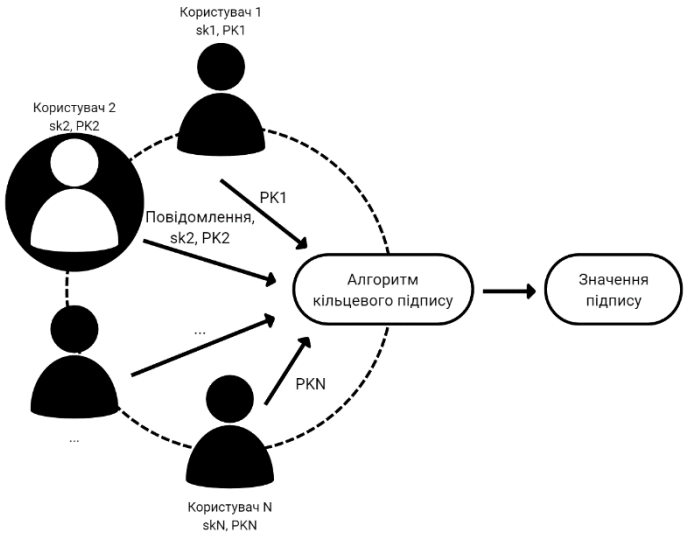

Рисунок 4 – Процес формування підпису [11, с. 8]

Коли верифікатор перевіряє значення підпису, він може переконатися, що підпис був створений одним із членів групи, але невідомо ким саме. Тільки з імовірністю 1/N він може визначити, що підпис розрахований конкретним учасником кільця (рисунок 5). Варто зазначити, що користувач може бути розкритий лише у разі змови всіх інших членів групи [11, с. 7-9].

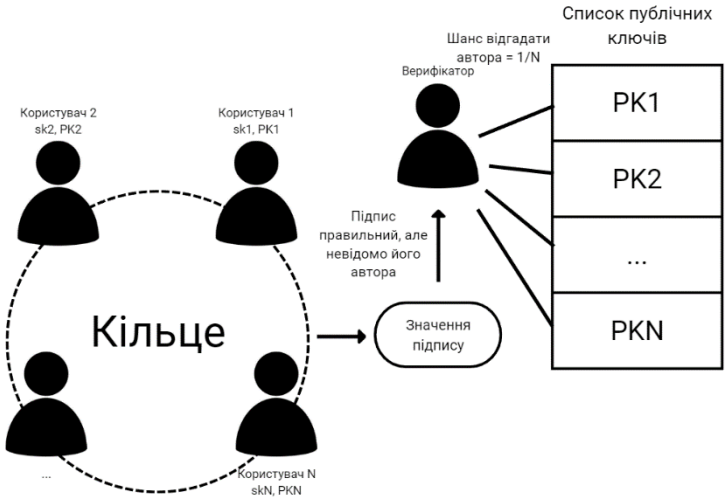

Рисунок 5 – Процес верифікації кільцевого підпису [11, с. 8]

РОЗДІЛ 3 ПРОЄКТУВАННЯ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ BLOCKCHAIN

3.1 Визначення функціональних вимог до системи

При проєктуванні системи електронного голосування на основі Blockchain необхідно визначити декілька ключових функціональних вимог:

– всі голоси мають бути публічно доступними для перегляду, але без можливості визначити, як голосував конкретний виборець;

– після того, як голос було віддано, він може бути змінений. Це повинно реалізовуватися шляхом додавання нових даних та врахування даного моменту при підрахунку голосів;

– система має запобігти можливості голосування одного й того ж виборця більше одного разу;

– ідентичність виборця має залишатися анонімною, захищеною від відстеження [10];

– система має бути доступною для виборців незалежно від їх географічного розташування. Вони мають мати змогу віддати свій голос за допомогою різних пристроїв, включаючи мобільні телефони, планшети та комп'ютери;

– інтерфейс користувача має бути інтуїтивно зрозумілим, щоб виборці могли легко голосувати без технічних складнощів.

Описані функціональні вимоги до системи електронного голосування на основі Blockchain сприятимуть проведенню прозорого і справедливого опитування. Забезпечення публічного доступу до голосів без ідентифікації конкретних виборців дозволить громадськості перевіряти результати голосування і підтверджувати їх достовірність. Врахування принципів Blockchain щодо незмінності відданих голосів запобігатиме будь-якій можливості зміни або видалення результатів голосування.

3.2 Структурна схема системи

Створення структурної схеми системи є важливим етапом під час проєктування будь-якої системи. Схема допомагає зрозуміти, як система буде функціонувати в цілому, як взаємодіють її різні компоненти, та які процеси відбуваються під час її роботи.

Схема розробленої системи електронного голосування на основі Blockchain включає наступні компоненти і елементи.

Вузли-валідатори. Ці вузли є основними учасниками системи та виконують завдання підтвердження й перевірки транзакцій, які є голосами в системі. Кожен вузол-валідатор має свою копію Blockchain та бере участь у процесі формування нових блоків.

Модуль обробки голосування є важливою складовою валідатора, який аналізує систему електронного голосування та на базі наявних даних надає результати. Він відповідає за перевірку валідності голосів, здійснює перевірку правильності формату та змісту даних, що надходять від виборців.

Модуль обробки голосування також відіграє ключову роль у реєстрації голосів у Blockchain. Він забезпечує, щоб голоси, які успішно пройшли перевірку, були додані до ланцюжка блоків системи голосування. Це гарантує, що голоси стають незмінними та недоступними для зміни після їхнього віддання.

Завдяки модулю обробки голосування забезпечується цілісність процесу голосування, оскільки він контролює критичні етапи обробки голосів та перевірку їхньої правильності. Він грає важливу роль у гарантуванні довіри до системи електронного голосування, надаючи об'єктивні та надійні результати опитування.

Вузол, що знає про всі активні вузли (вузол-з’єднувач). Цей вузол виконує роль посередника і забезпечує зв'язність між різними вузлами-валідаторами в системі. Він підтримує актуальну інформацію про активні вузли та допомагає у встановленні комунікації між ними.

Blockchain – це розподілена база даних, що зберігає усю інформацію про голосування. Кожен блок містить транзакції, що представляють голоси в системі.

Blockchain забезпечує недоступність даних, а також незмінність та недублювання голосів.

Виборці є користувачами системи, які мають можливість голосувати через вебінтерфейс. Вони можуть автентифікуватися та надавати свої голоси шляхом взаємодії з системою.

Вебінтерфейс користувача надає зручний інтерфейс для взаємодії виборців з системою. Він дозволяє користувачам реєструватися, автентифікуватися та надавати свої голоси. Спершу він під’єднується до вузла-з’єднувача, після чого отримує дані вузла, з яким відбудеться подальша взаємодія.

Консенсус на основі PBFT (Practical Byzantine Fault Tolerance, практична візантійська відмовостійкість) [12] працює шляхом взаємодії вузлів і прийняття спільного рішення щодо включення нового блоку до Blockchain. Вузли комунікують між собою, обмінюючись підписаними повідомленнями, що дозволяє перевірити легітимність і цілісність даних. Кожен вузол може запитувати інші вузли для підтвердження чи відмови в додаванні блоку.

На рисунку 6 можна ознайомитися зі схематичним представленням згаданих компонентів.

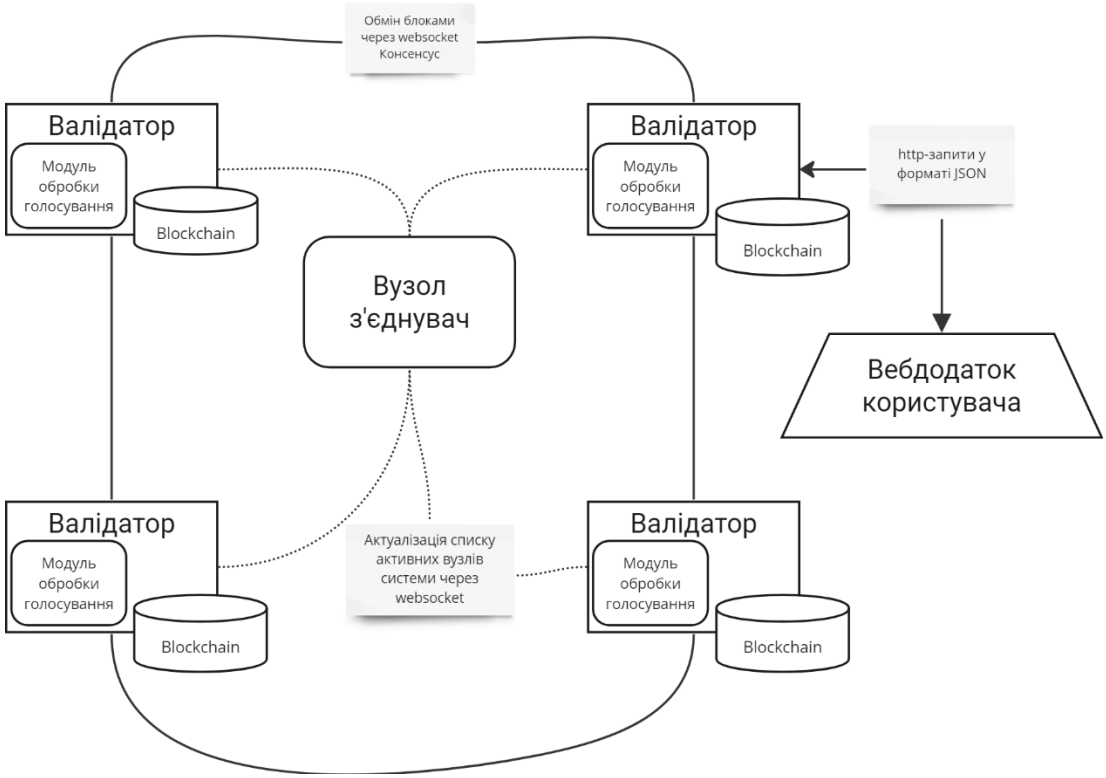

Рисунок 6 – Загальний вигляд системи

Розроблена система електронного голосування на основі Blockchain використовує цей комплексний набір компонентів та елементів для забезпечення безпеки, надійності та анонімності голосування. Використання Blockchain в системі сприяє забезпеченню незмінності та автентичності голосів, що робить її надійною та безпечною для проведення електронних голосувань.

3.3 Процеси в системі

Процеси, що відбуваються в системі, включають наступне:

– реєстрація користувача: адміністратор системи має можливість реєструвати нових користувачів. Під час реєстрації користувача, адміністратор створює транзакцію реєстрації, яка містить публічний ключ користувача. Після підтвердження транзакції, користувач отримує свій обліковий запис;

– адміністратор може створювати нові опитування, заповнюючи форму з питаннями, відповідями та тривалістю голосування. Транзакція створення голосування публікується, і інші користувачі можуть голосувати;

– користувачі мають можливість переглядати доступні опитування та вибирати варіанти відповідей. Після заповнення форми голосування, користувач створює транзакцію голосу, яка підтверджує його голос. Ця транзакція публікується і додається до Blockchain;

– після завершення голосування, система виконує підрахунок голосів для конкретного опитування. Шляхом запиту до вузла, який містить відповідні транзакції, здійснюється перегляд всіх транзакцій-голосів та підрахунок кількості голосів за кожен варіант відповіді. Результати голосування виводяться у зручному форматі для користувачів;

– користувачі можуть перевірити правильність врахування свого голосу шляхом перевірки статусу своїх транзакцій. Коли користувач запускає додаток, він періодично перевіряє статус своїх транзакцій і отримує повідомлення про їх підтвердження. У разі виявлення нових транзакцій для заданого публічного ключа, вони завантажуються і зберігаються в додатку користувача;

– транзакції, які були підтверджені вузлами-валідаторами, додаються до нового блоку. Після підписання всіма валідаторами, блок розповсюджується та вставляється в Blockchain;

– додавання нового вузла в систему: новий валідатор повинен довести своє право на перевірку транзакцій та сповістити про це інших учасників системи, а також синхронізувати локальний Blockchain з іншими вузлами.

Кожен процес повинен забезпечувати безпеку, цілісність та анонімність голосування, що є основними характеристиками системи.

РОЗДІЛ 4 РОЗРОБКА СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ BLOCKCHAIN

4.1 Вибір технологій та інструментів для розробки

Розглянемо ключові технології та інструменти, які були обрані для розробки прототипу системи електронного голосування. Основною метою було вибрати потужні та ефективні засоби, які відповідають поставленим вимогам до системи та забезпечують надійність та швидкість її функціонування.

Для розробки були вибрані наступні технології та інструменти:

– Golang. Мова програмування Golang була обрана для розробки бекенду системи. Вона відома своєю високою продуктивністю, здатністю легко впроваджувати паралельні процеси за допомогою горутин (goroutines) [13] і ефективним управлінням пам'яттю. Має потужну стандартну бібліотеку і спільноту, яка активно розробляє та підтримує нові пакети, Golang є відмінним вибором для розробки бекенду системи електронного голосування.

– Vue.js 3. Для побудови користувацького інтерфейсу був використаний фреймворк Vue.js 3. Він є прогресивним фреймворком, який надає легкий і гнучкий підхід до розробки динамічних вебінтерфейсів. Він дозволяє зручно створювати компоненти і взаємодіяти з ними, що робить його ідеальним вибором для розробки фронтенду системи.

– Docker. Для контейнеризації та розгортання додатків була використана платформа Docker. Docker дозволяє упаковувати додатки та їх залежності в контейнери, що дозволяє просто та надійно розгортати додатки на різних машинах. Це спрощує процес розгортання та забезпечує узгодженість середовища.

– Railway. Для безшовного розгортання додатків була використана платформа Railway. Вона підтримує Docker і дозволяє легко розгортати контейнеризовані додатки. Railway надає зручні інструменти для розгортання та керування додатками, спрощуючи процес розгортання та підтримки.

– IntelliJ IDEA Ultimate є потужним та інноваційним інтегрованим середовищем розробки, призначеним для професійної розробки програмного забезпечення.

Однією з ключових особливостей IntelliJ IDEA Ultimate є його потужний редактор коду. Він надає розширену підсвічування синтаксису, автоматичне завершення коду, рефакторинг, аналіз коду та багато інших функцій, що сприяють швидкому та продуктивному написанню коду.

– Postman – це популярний інструмент для тестування та розробки API. Він надає зручне інтерфейс для взаємодії з різними типами API, включаючи HTTP та WebSocket протоколи. Postman дозволяє розробникам легко створювати, надсилати та отримувати HTTP запити, а також аналізувати та відлагоджувати (debug) їх.

Щодо роботи з HTTP, Postman надає можливість створювати запити різних типів, таких як GET, POST, PUT, DELETE, PATCH тощо. Він дозволяє налаштовувати різні параметри запиту, такі як заголовки, параметри шляху (query parameters), тіло запиту (request body) та автентифікацію. Postman також дозволяє переглядати та аналізувати відповіді сервера, включаючи заголовки відповіді, тіло відповіді (response body) та код статусу.

Окрім роботи з HTTP, Postman також підтримує розробку та тестування WebSocket-протоколів. WebSocket – це протокол для двосторонньої комунікації між клієнтом та сервером. Postman дозволяє створювати WebSocket підключення, відправляти та отримувати повідомлення через WebSocket. Він підтримує режими текстових та бінарних повідомлень, а також можливість відслідковувати та аналізувати обмін повідомленнями між клієнтом та сервером.

Для організації ефективної роботи, команда розробки застосовувала наступні методології та інструменти:

– agile-розробка – це підхід до розробки програмного забезпечення, який базується на ітераційному підході, а також активній співпраці в команді. Цей підхід дозволяє розробникам працювати більш гнучко і ефективно, швидко реагувати на змінні вимоги та максимально задовольняти потреби клієнта.

Працюючи з цим підходом, члени команди змогли більш ефективно співпрацювати та розподіляти завдання між учасниками. Кожен мав свої відповідальності та цілі, і постійно звітував про прогрес, щоб впевнитися, що кожен розумів свою роль та має ресурси, необхідні для виконання завдань. Також, завдяки коротким спринтам в один тиждень, було можливим швидке виявлення та вирішення проблем, що допомагало зберегти час та підтримувати високу якість роботи.

– Jira – це популярна система управління проєктами, яка широко використовується для планування, відстеження та керування задачами в Agile-командах. В процесі розробки активно застосовувалась Jira для опису та організації усіх задач і спринтів (sprints, короткий часовий інтервал для виконання командою поставлених задач).

У Jira створювали елементи роботи, такі як задачі, історії користувачів та помилки. Кожна задача мала своє найменування, опис, пріоритет, термін виконання та відповідального виконавця. Також було використано різні поля, такі як коментарі, вкладення та мітки, щоб додатково описати та уточнити кожну задачу.

Для організації роботи в спринтах були створені відповідні спринт-дошки у Jira. На цих дошках розміщувалися задачі з поточним станом виконання. Це давало зручну візуалізацію прогресу роботи та дозволяло всій команді бачити, які завдання знаходяться у різних стадіях реалізації.

– Git та GitHub використовували для керування версіями програмного забезпечення та спільної роботи над проєктами.

Репозиторії було згруповано за допомогою організацій в GitHub, що дозволило краще керувати правами доступу, налаштуваннями та спільною роботою над проєктом.

– GitHub Copilot – це інтелектуальний помічник для програмістів, розроблений спільною командою GitHub та OpenAI. Він базується на технології штучного інтелекту, зокрема на моделі GPT-3, і надає підказки та автодоповнення коду прямо у вашому редакторі програмного забезпечення.

GitHub Copilot може автоматично доповнювати код, пропонуючи розумні підказки на основі змісту написаного коду та контексту. Він може генерувати шаблони функцій, класів, методів, умовних виразів та багато іншого. Це допомагає прискорити виконання рутинних завдань.

Вибір цих технологій та інструментів забезпечив потужний інструментарій для розробки та розгортання системи.

4.2 Реалізація окремих модулів системи

4.2.1 Вузловий з'єднувач (Node Connector)

Вузловий з'єднувач є важливим компонентом пропонованої системи. Його основне призначення полягає в тому, щоб забезпечити зв'язність між різними вузлами системи. Цей компонент відповідає за отримання та збереження інформації про активні вузли та їх статус.

API вузлового з'єднувача складається з двох основних запитів:

– запит GET /nodes: Цей запит використовується для отримання списку «живих» вузлів системи. При виконанні цього запиту, вузловий з'єднувач повертає актуальний список вузлів, які вважаються активними. Ця інформація є важливою для розповсюдження повідомлень та спілкування між вузлами системи.

– запит POST /nodes: Цей запит використовується для повідомлення про появу нового вузла. Коли новий вузол приєднується до системи, він надсилає цей запит до вузлового з'єднувача, щоб повідомити про свою присутність. Після отримання запиту, вузловий з'єднувач додає новий вузол до списку активних вузлів та починає розповсюджувати цю інформацію іншим вузлам системи.

Для підтримки актуальності списку активних вузлів, вузловий з'єднувач постійно перевіряє наявність зв'язку з вузлами за допомогою WebSockets. Вони дозволяють здійснювати двосторонню зв'язок між вузловим з'єднувачем та іншими вузлами системи, що дозволяє швидко оновлювати список активних вузлів.

Список активних вузлів зберігається в оперативній пам'яті та файловій системі. Це забезпечує швидкий доступ до інформації та його збереження між

запусками системи. Крім того, періодично список активних вузлів надсилається іншим вузлам для забезпечення актуальності та синхронізації.

Цільові вузли, зареєстровані та відомі вузловим з'єднувачем, використовуються не тільки валідаторами системи, але й вебклієнтами, які є кінцевими користувачами системи електронного голосування. Вебклієнти залежать від вузлового з'єднувача для отримання актуального списку активних вузлів, що дозволяє їм взаємодіяти з системою.

При виконанні дій, таких як віддання голосу чи перегляд результатів голосування, вебклієнти використовують інформацію про активні вузли, яку надає вузловий з'єднувач.

Отже, вузловий з'єднувач є важливим посередником між валідаторами та вебклієнтами, забезпечуючи актуальну інформацію про активні вузли системи. Це сприяє ефективній та безперебійній взаємодії кінцевих користувачів з системою електронного голосування.

4.2.2 Валідатор

Валідатор є одним з ключових компонентів системи електронного голосування, і він відіграє важливу роль у багатьох процесах. Основні функції валідатора включають прийом, валідацію та створення блоків, поширення їх по мережі, а також перевірку та прийняття блоків від інших валідаторів.

У першу чергу, валідатор приймає транзакції, що надходять до системи. Він перевіряє ці транзакції на валідність, залежно від її типу: створення голосування, реєстрація, тощо – згідно з встановленими правилами та перевіряє підписи користувачів для підтвердження їх автентичності. Якщо транзакції валідні, валідатор підготовлює їх для включення до нового блоку.

Після валідації транзакцій, валідатор має здатність створювати нові блоки. Він групує валідні транзакції разом з додатковою інформацією, такою як попередній хеш блоку та мітка часу, і формує новий блок для включення в ланцюжок блоків. Цей процес відбувається з врахуванням правил консенсусу, які забезпечують правильну послідовність та цілісність Blockchain.

Такі параметри як максимальна кількість транзакцій в блоці, максимальний час формування блоку та частка валідаторів, які повинні підтвердити блок, щоб його додали до Blockchain задаються конфігураційним файлом. Він зберігається локально у кожного валідатора.

Після створення блоків, валідатор відправляє їх по мережі до інших валідаторів та вузлів системи. Це дозволяє іншим учасникам мережі отримувати актуальну інформацію про нові блоки та оновлювати свої копії Blockchain.

Однак, важливо відзначити, що валідатор не тільки створює та поширює блоки, але й бере участь у процесі прийняття рішень щодо додавання нових блоків до системи.

Реалізована консенсусна модель найбільш близька до практичної візантійської відмовостійкості. Вона забезпечує безпеку та надійність мережі у випадку, коли деякі валідатори можуть виявити неправильну поведінку або намагатися спотворити дані.

Є кілька відмінностей із згаданим підходом. Наразі не обирається той, хто буде створювати блок, це може зробити кожен з вузлів. Голосування за додавання нового блоку відбувається послідовно, а не оголошується одночасно усім вузлам.

В силу обраної моделі, мінімальна кількість валідаторів для стабільної роботи системи залежить від порогового значення (частки валідаторів) для підтвердження блоку. Ця кількість повинна гарантувати неможливість цензурування системи одним валідатором.

У поточній реалізації, коли валідатор створює новий блок, він самостійно проводить опитування кожного з інших валідаторів щодо підтримки даного блоку. Оскільки вони зберігають копію Blockchain, вони мають змогу незалежно перевірити валідність блока. Валідатор-автор надсилає запити до інших валідаторів, щоб зібрати достатню кількість голосів-підтримки. Якщо необхідна кількість голосів набрана, валідатор-автор надсилає блок з усіма підписами валідаторів для додавання до їхніх баз даних (див. рис. 7).

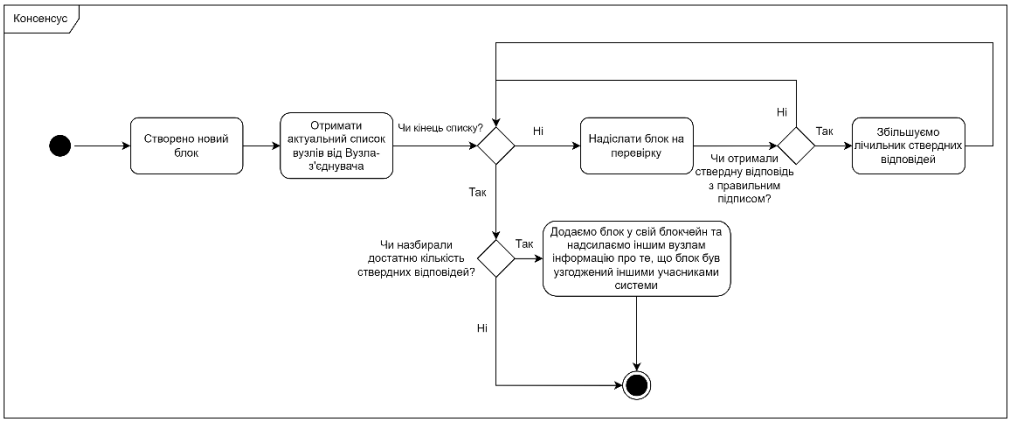

Рисунок 7 – Діаграма активностей для консенсусу

Цей підхід забезпечує розподілену прийняття рішень та забезпечує, що новий блок буде включений до Blockchain тільки після отримання підтримки від достатньої кількості валідаторів. Таким чином, система гарантує, що додавання нових блоків до Blockchain відбувається з урахуванням важливості консенсусу та підтримки від багатьох учасників.

Використання опитування та підписів валідаторів забезпечує надійність та цілісність процесу додавання блоків, зменшуючи ризик спотворення даних або неправильного прийняття рішень.

4.2.3 Вебклієнт

Для реалізації вебклієнта системи електронного голосування було використано декілька технологій для розробки. Основною платформою для фронтенду був Vue.js, який надав потужний інструментарій для створення інтерактивного та естетичного користувацького інтерфейсу (див. рис. 8). Для

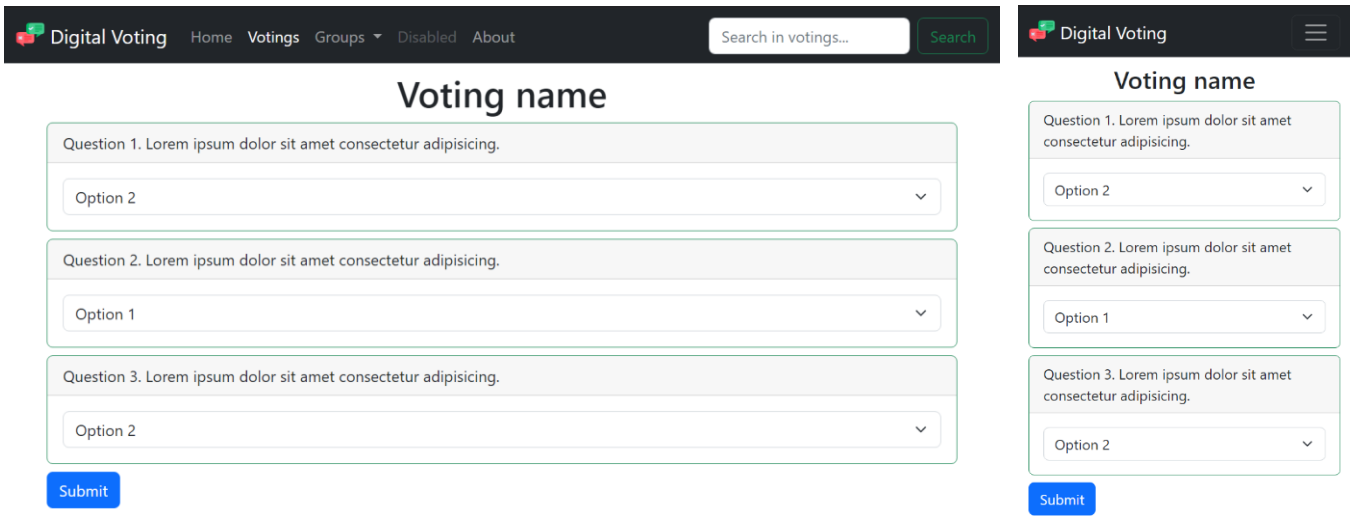

Рисунок 8 – Вигляд інтерфейсу користувача на екранах з різною роздільною здатністю

забезпечення швидкості та гнучкості дизайну, було використано бібліотеку Bootstrap v5, яка надає готові компоненти та стилізацію.

На бекенді було використано мову програмування Golang, яка має багато переваг для обробки логіки, пов'язаної з криптографією та валідацією. Завдяки використанню пакетів валідатора, було можливо забезпечити безпеку та точність обробки транзакцій та блоків у системі електронного голосування.

Один з основних переваг використання Golang полягає у підтримці модулів (go modules), що дозволяють легко перевикористовувати пакети та робити залежності від віддалених репозиторіїв. Вони пришвидшують розробку та підтримку системи.

Використаний підхід також забезпечує високий рівень безпеки приватного ключа користувача. Усі операції, пов'язані з ключами, виконуються локально на пристрої користувача, що дозволяє уникнути передачі приватних даних по мережі. Це забезпечує додаткову захист від можливих атак.

Приватний ключ користувача зберігається у файловій системі пристрою в зашифрованому вигляді.

Такий підхід з використанням Golang у бекенді системи електронного голосування дозволяє забезпечити ефективну обробку та безпеку операцій,

знижуючи навантаження на пристрої користувача та підвищуючи загальну безпеку системи.

4.3 Інтеграція модулів в єдину систему

В системі електронного голосування на основі Blockchain існує необхідність взаємодії між різними компонентами для забезпечення правильної роботи системи. Два основних модуля, які взаємодіють між собою, це вузловий з'єднувач (node connector) і валідатори (validators).

Як було зазначено, вузловий з'єднувач відповідає за збір та обмін інформацією про вузли системи. Він слугує для реєстрації нових вузлів та підтримки актуального списку активних вузлів. Адреса, за якою він проводить спілкування загальновідома, тому він є своєрідним «центром зустрічі» валідаторів.

Розгортання проводили з допомогою частково безкоштовного сервісу Railway [14]. Після реєстрації на платформі Railway та створення проєкту для системи, було створено новий сервіс, який було названо «node-connector» (див. рис. 9).

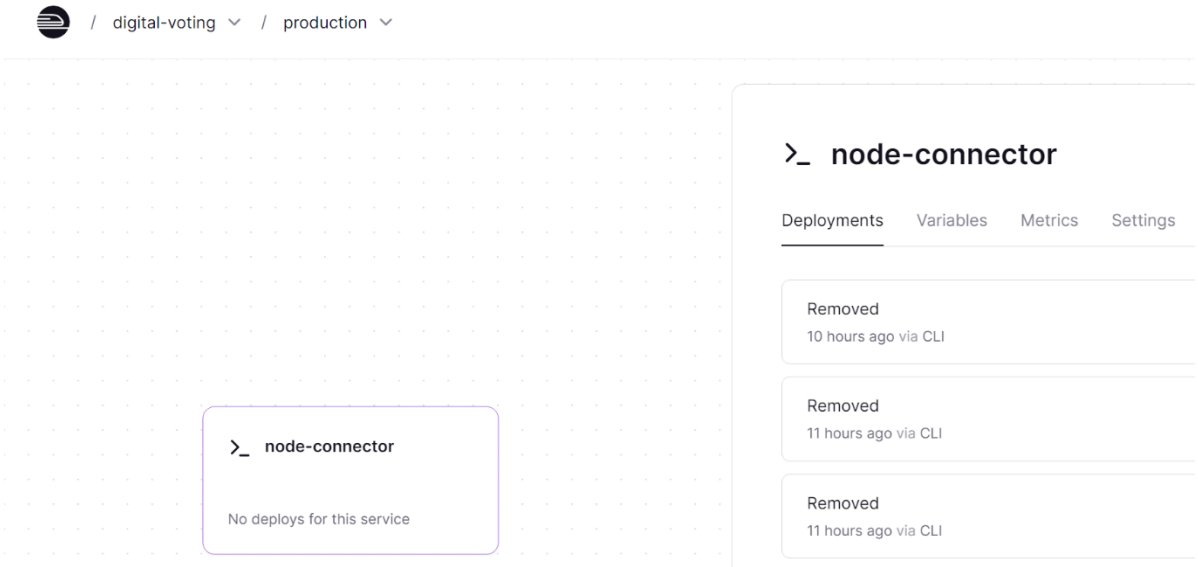

Рисунок 9 – Створений сервіс у вебінтерфейсі Railway

Для створення контейнера для вузлового з'єднувача було використано Docker, в конфігураційному файлі якого було вказано налаштування середовища для правильної роботи вузлового з'єднувача.

Після цього перейшли до налаштування сервісу на платформі Railway. В рамках конфігурації сервісу було задано необхідні змінні середовища та порти, які використовує вузловий з'єднувач для комунікації з іншими модулями системи. Дуже важливо вказати правильний порт у змінних середовища сервісу для коректної роботи сервісу (див. рис. 10).

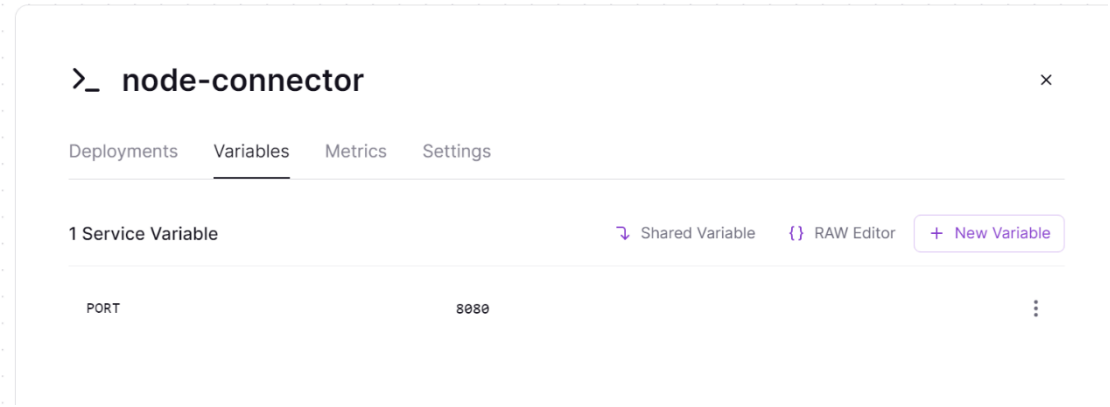

Рисунок 10 – Змінні сервісу із заданим портом

Після успішного розгортання вузлового з'єднувача на платформі Railway, було отримано публічну URL, за допомогою якої інші модулі системи можуть зв'язуватися з вузловим з'єднувачем для обміну даними та взаємодії. Її кожен з валідаторів та клієнтів кінцевих користувачів буде використовувати, в наведеному підході, в параметрах середовища (див. рис. 11), для взаємодії із системою.

```
ENV PORT 8081

ENV NODE_CONNECTOR_URL node-connector-production.up.railway.app

ENV NODE_URL validator-1-production.up.railway.app
```

Рисунок 11 – Налаштування змінних оточення для валідатора у Dockerfile

У свою чергу, валідатори можна також розгортати на як платформі Railway, так і локально.

Варто почати з опису розгортання валідатора на платформі Railway. Після створення проєкту для системи було створено новий сервіс для валідатора, «validator-service».

Для створення контейнера для валідатора було застосовано Docker. У конфігураційному файлі Dockerfile було задано необхідні залежності та налаштування середовища для правильної роботи валідатора. Серед них публічна адреса валідатора, яку потім буде передано до вузлового з’єднувача та адреса, за якою можна з’єднатись з валідатором.

В налаштуваннях сервісу на платформі Railway було проведено аналогічні операції, що й у вузловому з’єднувачі. Сервіс автоматично почав процес збирання Docker image та почав виконання програми.

Тепер щодо розгортання валідатора локально. Це можна зробити як з допомогою Dockerfile, так і шляхом запуску програми. Головне забезпечити скрипт необхідними параметрами середовища.

Для розгортання вебклієнта, який включає фронтенд та бекенд, було використано Docker Compose. Цей інструмент дозволяє зручно налаштувати та запустити обидві частини додатку у віртуальному середовищі. Під час конфігурації, було приділено особливу увагу налаштуванню правильних портів для забезпечення коректної комунікації між компонентами.

Крім того, важливим кроком було вказання публічної адреси вузлового з'єднувача, яка використовується для подальшої взаємодії з системою. Ця інформація була включена до конфігурації вебклієнта, щоб забезпечити правильне з'єднання та обмін даними з вузловим з'єднувачем.

З використанням Docker Compose можна легко управляти різними компонентами вебклієнта, забезпечуючи їх сумісність та взаємодію в єдиній системі. Це зробило процес розгортання більш зручним та ефективним, дозволяючи швидко налаштувати та запустити вебклієнт з необхідними

налаштуваннями та з'єднаннями для безперебійної роботи з системою електронного голосування.

РОЗДІЛ 5 ТЕСТУВАННЯ ТА ОЦІНКА РЕЗУЛЬТАТІВ РОЗРОБЛЕНОЇ СИСТЕМИ

5.1 Розробка тестових сценаріїв

Для тестування та оцінки результатів розробленої децентралізованої системи опитування на базі Blockchain технології, необхідно розробити декілька тестових сценаріїв. Це допоможе переконатися в коректності роботи системи та її ефективності.

5.1.1 Реєстрація адміністратора з реєстрації

Для реєстрації користувача з правами адміністратора необхідно виконати наступні кроки:

а) при створенні системи, в genesis block[1] створюється аккаунт першого адміністратора;
б) кандидат на посаду адміністратора відкриває систему;
в) кандидат вибирає опцію «Реєстрація»;
г) кандидат генерує ключову пару (публічний та приватний ключі) та відмічає, що бажає отримати права адміністратора;
д) кандидат надсилає свої дані для реєстрації;
е) у додатку адміністратора з реєстрації з’являється запит на реєстрацію нового адміністратора;
ж) адміністратор розглядає запит та приймає рішення;
з) якщо адміністратор погоджується з реєстрацією нового адміністратора, він створює транзакцію реєстрації в Blockchain;
и) якщо адміністратор відхиляє запит, процес реєстрації завершується;
к) система підтверджує транзакцію та створює аккаунт нового адміністратора;
л) система повертає підтвердження про успішну реєстрацію.

[1] Блок, який додається як перший блок ланцюга.

Очікуваний результат: дані нового адміністратора успішно збережено в Blockchain, новий адміністратор зареєстрований в системі.

5.1.2 Реєстрація користувача

Послідовність кроків для реєстрації користувача як учасника голосування в системі:

а) користувач відкриває систему;
б) користувач вибирає опцію «Реєстрація»;
в) користувач генерує ключову пару;
г) користувач надсилає запит на реєстрацію валідатору, до якого він під’єднаний;
д) адміністратор системи отримує запит після підключення до системи;
е) адміністратор створює транзакцію реєстрації користувача в Blockchain;
ж) система підтверджує транзакцію, таким чином користувач цим публічним ключем може брати участь в опитуваннях.

Очікуваний результат: дані користувача та його публічний ключ успішно збережено в Blockchain, користувач зареєстрований в системі з правами учасника.

5.1.3 Створення опитування

Перелік кроків для створення нового опитування адміністратором системи електронного голосування на основі Blockchain:

а) адміністратор системи входить в систему;
б) вибирає опцію «Створити нове опитування»;
в) вводить деталі опитування: назву, опис, питання, варіанти відповідей та вказує перелік публічних ключів, що мають право голосу;
г) зберігає опитування;
д) система створює новий блок в Blockchain з даними опитування;
е) система повертає підтвердження про успішне створення опитування.

Очікуваний результат: опитування успішно створено та збережено в Blockchain.

5.1.4 Здійснення голосування користувачем

У системі користувачі мають можливість брати участь у доступних опитуваннях та надавати свої відповіді. Цей процес має свою послідовність кроків:

а) користувач входить в систему;

б) користувач вибирає доступне опитування;

в) користувач відповідає на питання опитування;

г) користувач надсилає свої відповіді у вигляді підписаної транзакції;

д) система створює новий блок в Blockchain, який включає цю транзакцію.

Очікуваний результат: поточна відповідь користувача успішно збережено в Blockchain.

Користувач може змінити свій голос до кінця проведення голосування. Буде враховано останній підтверджений вибір, що було збережено в системі.

5.1.5 Перегляд результатів голосування

Після закінчення голосування користувачі мають можливість переглянути його результати. Для того необхідно виконати такі кроки:

а) користувач входить в систему;

б) користувач вибирає опцію «Перегляд результатів голосування»;

в) система аналізує блоки в Blockchain, що містять результати вибраного голосування;

г) система відображає результати голосування: кількість голосів за кожен варіант відповіді;

За бажанням, користувач може самостійно оглянути кожну транзакцію в Blockchain, що стосується цього голосування;

Для зручності, система також надає спрощений вигляд результатів голосування, де відображено лише загальну кількість голосів за кожен варіант відповіді.

Очікуваний результат: результати голосування відображаються коректно, відповідаючи даним, збереженим в Blockchain. Цей сценарій може виконати будь-

який користувач системи. Користувач має можливість переглянути деталі кожної транзакції або скористатися спрощеним виглядом результатів для зручності.

5.2 Проведення тестування

У процесі тестування було виконано кожен з розроблених тестових сценаріїв, результати були зібрані та проаналізовані.

Сценарії, що стосуються реєстрації адміністратора, реєстрації користувача, створення опитування, здійснення голосування користувачем та перегляду результатів голосування, були успішно виконані. Система відповідала на кожен з цих сценаріїв відповідно до очікувань, що свідчить про її надійність та ефективність.

Результати підтверджують, що розроблена система є надійною та ефективною. Це свідчить про готовність системи до впровадження в реальних умовах.

5.3 Аналіз ефективності системи

В цьому підрозділі зосередимося на ключових аспектах роботи системи.

Відповідність вимогам. Розроблена система була розроблена з урахуванням вимог до децентралізованих систем. Вона забезпечує безпеку, прозорість та незалежність від третіх сторін, що є ключовими вимогами до таких систем.

Зручність роботи з користувацьким інтерфейсом. Незважаючи на складність технологій, що використовуються «під капотом», було розроблено інтуїтивний користувацький інтерфейс, що спрощує роботу з системою та забезпечує низький поріг входження для користувача. Інтерфейс адаптивний, що дозволяє користуватися системою як на настільному ПК, так і з допомогою смартфона.

Вартість розгортання та підтримки. Ціна буде залежати від кількості валідаторів та довжини Blockchain. Вона базується на відкритих технологіях, що знижує вартість її впровадження та експлуатації.

Що стосується безпеки, система використовує PBFT консенсус з використанням ECDSA для цифрових підписів і безпечної еліптичної кривої

ed25519. Вона створена так, щоб мінімізувати потенційні атаки і підвищити безпеку системи.

Розглянемо інші аспекти забезпечення справедливого голосування. Ось як імплементована система запобігає деяким потенційним атакам:

а) Атака 51% вимагає від зловмисника контроль над більшістю вузлів, що є вкрай неправдоподібним в пропонованій системі, оскільки вона базується на децентралізованому розподілі вузлів.

Більше того, у розробленій системі використовується консенсусний алгоритм PBFT, який забезпечує надійність та стійкість до зловмисних атак. Цей алгоритм гарантує, що рішення приймається тільки за участю дозволених та надійних вузлів. Зловмиснику буде вкрай складно здійснити атаку, контролюючи більшість вузлів, оскільки система має механізми виявлення та запобігання неправомірним діям (див. 4.2.2).

б) Атака на приватні ключі. Кожен користувач системи має свій унікальний приватний ключ, який використовується для підпису голосу. Ці ключі зберігаються локально на пристрої користувача (див. 4.2.3), що забезпечує безпеку їх використання і унеможливлює доступ ззовні.

в) Атака на вузли системи. Система має розподілену архітектуру, що означає, що втрата чи компрометування окремого вузла не призводить до втрати функціональності системи. Інші вузли можуть продовжувати свою роботу і підтримувати безперебійну роботу мережі (відповідно до 4.2.2).

г) Несанкціоноване використання. Система має вбудовані механізми перевірки та автентифікації користувачів, що дозволяє уникнути злочинного використання системи. Кожен голос пов'язаний з унікальним ідентифікатором користувача, що дозволяє відстежувати та перевіряти легітимність голосу[1].

[1] У запропонованій системі, кожен голос пов'язаний з унікальним ідентифікатором користувача, але цей ідентифікатор не прямо пов'язаний з особистою інформацією користувача. Це означає, що хоча можливо відстежувати та перевіряти легітимність голосу, але неможливо визначити, хто конкретно віддав цей голос.

д) Атака підміни клієнта. Через те, що система базується на криптографічних перетвореннях, зловмиснику буде важко підібрати такі дані, щоб вони проходили перевірку та шкодили системі так чи інакше.

е) Man-in-the-middle. Оскільки користувач виконує маніпуляції з приватними даними локально та передає лише результат перетворення, а криптографічні алгоритми гарантують безпеку, то дані можна передавати навіть у відкритому вигляді без ризику викриття секретів (приватного ключа).

ж) Несправжні голосування. Як описано у пункті 5.1.3, створювати голосування може лише адміністратор. Крім того, під час створення в системі відбудуться перевірки внесених даних.

Маючи на увазі ці заходи, робимо акцент на надійності та безпеці створеної системи голосування. Проте, зрозуміло, що жодна система не є абсолютно непроникною, і необхідно постійно працювати над її покращеннями.

5.4 Перспективи системи

Заплановано проведення спеціального тестування для моніторингу реакції системи та використання ресурсів під час високої навантаженості. Воно передбачає генерацію великої кількості запитів до системи в короткий час (наприклад 1000 запитів на секунду). Тестування дозволить зібрати дані про час відповіді системи, використання ресурсів та виявлені помилки. На основі цього будуть зроблені зміни та оптимізації, щоб забезпечити надійну та ефективну роботу системи навіть при інтенсивному використанні.

Вважаю, що продовження розробки та досліджень у галузі цифрової системи голосування є надзвичайно доцільним. Україна має великий потенціал для впровадження цифрових інновацій, особливо в контексті організації прозорих та безпечних голосувань. Можливість інтеграції системи з проєктом Дія та іншими державними програмами дозволить зробити ще один крок у напрямку цифровізації громадянської участі та забезпечення демократичного процесу голосування.

Розвиток електронних систем голосування, постійне вдосконалення алгоритмів безпеки та прозорості, а також партнерство з науковими інститутами та організаціями дозволять побудувати сучасну та інноваційну систему, яка буде гордістю України. Вона допоможе забезпечити гідне майбутнє українцям, дозволяючи їм активно брати участь у прийнятті рішень та формуванні політичної волі.

Досягнення у галузі цифровізації голосування покладають основу для створення прозорої, демократичної та сильної України. Це є викликом, який кожен з нас повинен прийняти з ентузіазмом та патріотизмом, і разом, злиті в одну сильну команду, зможемо побудувати майбутнє, про яке мріємо.

ВИСНОВКИ

На основі проведених досліджень, можна стверджувати, що розроблена система голосування на основі Blockchain з використанням консенсусу PBFT виявилася ефективною та надійною. З кодом можна ознайомитися в репозиторіях GitHub [15].

Традиційні системи голосування стикаються з проблемами, такими як маніпуляція голосами, відсутність прозорості, проблеми з доступом, високі витрати та ризик помилок при підрахунку.

Розроблена система голосування на основі Blockchain з використанням консенсусу PBFT ефективно вирішує ці проблеми. Вона забезпечує безпеку та прозорість голосування, гарантує надійність прийняття рішень та унеможливлює підробку голосів.

Система також розв'язує проблему доступності, дозволяючи голосувати з будь-якого місця. Використання Blockchain та розподіленого консенсусу забезпечує фіксацію кожного голосу та його безпечне зберігання.

Розроблена система може бути впроваджена на практиці в різних сферах, включаючи місцеві вибори або корпоративне голосування. Вона може бути також використана в інших сферах, де потрібна прозорість та надійність голосування.

В процесі розробки цієї системи було створено ряд модулів, які виконують різні ролі в контексті валідації та процесу голосування.

Імплементована система має велике значення в контексті дослідження того, як побудовані подібні системи. В процесі імплементації команда стикнулася з рядом викликів, які потрібно було адресувати як у виборі технологій, так і підборі алгоритмів, які варто застосувати.

Робота відкриває нові можливості для наукових досліджень в області Blockchain та систем електронного голосування, а також вносить вклад в технічне вдосконалення технологій електронного голосування. З соціально-економічного боку, система може сприяти ефективності голосування, забезпечуючи прозорість та заощаджуючи ресурси.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Suprun O. Decentralized electronic voting system based on blockchain technology / O. Suprun, N. Savorona // Міжнародна наукова-технічна конференція «Інтелектуальні технології лінгвістичного аналізу»: Тези доповідей. / O. Suprun, N. Savorona. – Київ: НАУ, 2022. – С. 39.
2. Buchsbaum T. M. E-Voting: International Developments and Lessons Learnt [Електронний ресурс] / Thomas Buchsbaum // Citeseer – Режим доступу до ресурсу: https://tinyurl.com/37fxpkhf.
3. Jafar U. Blockchain for Electronic Voting System—Review and Open Research Challenges [Електронний ресурс] / U. Jafar, M. J. Ab Aziz, Z. Shukur. – 2021. – Режим доступу до ресурсу: https://doi.org/10.3390/s21175874.
4. Adida B. Helios: Web-based Open-Audit Voting [Електронний ресурс] / Ben Adida – Режим доступу до ресурсу: https://tinyurl.com/2edssk9v.
5. Security Analysis of the Estonian Internet Voting System [Електронний ресурс] / [D. Springall, T. Finkenauer, Z. Durumeric та ін.] – Режим доступу до ресурсу: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf.
6. Specter M. A. The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections [Електронний ресурс] / M. A. Specter, J. Koppel, D. Weitzner – Режим доступу до ресурсу: https://tinyurl.com/28xa5eyb.
7. Securing the Vote: Protecting American Democracy / [L. C. BOLLINGER, M. A. McROBBIE, D. BALTIMORE та ін.]. – Washington, DC: The National Academies Press, 2018. – 180 с. – (National Academies of Sciences).
8. Zsigmond J. Creating a Blockchain from Scratch [Електронний ресурс] / Joao Zsigmond // Level Up Coding. – 2020. – Режим доступу до ресурсу: https://levelup.gitconnected.com/creating-a-blockchain-from-scratch-9a7b123e1f3e.

9. Кравченко П. Блокчейн і децентралізовані системи : навч. посібник [для студ. закладів вищ. освіти] : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків: ПРОМАРТ, 2019. – 452 с.
10. Blockchain and decentralized systems : in three volumes. V.3 / P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina. – Kharkiv, 2020. – 298 с.
11. Anonymous Decentralized E-Voting System / [O. Kurbatov, P. Kravchenko, O. Shapoval та ін.] // International Workshop on Conflict Management in Global Information Networks / [O. Kurbatov, P. Kravchenko, O. Shapoval та ін.]. – Lviv, 2019. – С. 12–22.
12. Wang G. SoK: Understanding BFT Consensus in the Age of Blockchains [Електронний ресурс] / Gang Wang. – 2021. – Режим доступу до ресурсу: https://eprint.iacr.org/2021/911.pdf.
13. Cox-Buday K. Concurrency in Go / Katherine Cox-Buday. – Sebastopol, CA: O'Reilly Media, Inc., 2017. – 236 с.
14. Railway documentation [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://docs.railway.app/.
15. Balykov A. O. Репозиторії з кодом описаної системи [Електронний ресурс] / A. O. Balykov, R. V. Volchetskyi, N. V. Savorona. – 2023. – Режим доступу до ресурсу: https://github.com/orgs/Digital-Voting-Team/repositories.