Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження блокчейн-технологій для проведення електронного голосування у «розумних містах»

Виконав: студент VI курсу, групи СНм-61
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

_____ Титжинський А.А.
(підпис) (прізвище та ініціали)

Керівник _____ Липак Г.І.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ _____
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Титжинський Анатолій Андрійович
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження блокчейн-технологій для проведення електронного голосування у «розумних містах»

Керівник роботи Липак Галина Ігорівна доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 29 » листопада 2024 року № 4/7-1141

2. Термін подання студентом завершеної роботи 25 грудня 2024р.

3. Вихідні дані до роботи Наукові публікації про дослідження блокчейн-технологій для проведення електронного голосування у «розумних містах»

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналітичний огляд технологій та підходів до електронного голосування. Електронне голосування як ознака «розумності» міст та громад: аналіз сучасного стану. Блокчейн у контексті електронного голосування. Огляд існуючих рішень та прототипів. Можливості інтеграції аспектів блокчейн-технологій голосування у інші сервіси «розумного» міста. 2. Дослідження та вибір технологій і методів реалізації електронного голосування на основі блокчейну. Концептуальні основи блокчейн-технології для систем голосування. Вимоги до системи голосування. Вибір платформи та архітектури системи. Розробка моделі процесу голосування. 3. Практична реалізація системи голосування та аналіз ефективності. Розробка прототипу системи голосування з використанням блокчейн-технологій. Тестування системи. Аналіз результатів і перспективи впровадження. Перспективи для «розумного» Міста. 4. Охорона праці та безпека в надзвичайних ситуаціях. Показники ефективності та заходи щодо покращення умов та охорони праці. Суть та зміст управління охороною праці. Підвищення стійкості роботи об'єктів господарської діяльності у воєнний час. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Титульний слайд. Мотивація та актуальність теми. Мета та завдання дослідження. Аналітичний огляд предметної області. Методи та інструменти дослідження. Розробка прототипу системи голосування. Результати тестування системи. Перспективи впровадження. Висновки та рекомендації. Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Сенчишин В.С., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. викладач		

7. Дата видачі завдання 29 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.11.2024	*Виконано*
2.	Підбір наукових джерел про дослідження блокчейн-	29.11.2024-04.12.2024	*Виконано*
	технологій для проведення електронного голосування		
	у «розумних містах»		
3.	Опрацювання наукових публікацій та збір даних по	29.11.2024-04.12.2024	*Виконано*
	темі роботи		
4.	Виконання дослідження згідно мети кваліфікаційної	05.12.2024-09.12.2024	*Виконано*
	роботи		
5.	Оформлення розділу «аналітичний огляд технологій та	05.12.2024-09.12.2024	*Виконано*
	підходів до електронного голосування»		
6.	Оформлення розділу «дослідження та вибір технологій	05.12.2024-09.12.2024	*Виконано*
	і методів реалізації електронного голосування на		
	основі блокчейну»		
7.	Оформлення розділу «практична реалізація системи	05.12.2024-09.12.2024	*Виконано*
	голосування та аналіз ефективності»		
8.	Виконання завдання до підрозділу «Охорона праці»	02.12.2024-09.12.2024	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	02.12.2024-09.12.2024	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	10.12.2024-11.12.2024	*Виконано*
11.	Нормоконтроль	12.12.2024-13.12.2024	*Виконано*
12.	Перевірка на плагіат	16.12.2024	*Виконано*
13.	Попередній захист кваліфікаційної роботи	17.12.2024	*Виконано*
14.	Захист кваліфікаційної роботи	26.12.2024	

Студент _____ Титжинський А. А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Липак Г. І.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження блокчейн-технологій для проведення електронного голосування у «розумних містах» // Кваліфікаційна робота освітнього рівня «Магістр» // Титжинський Анатолій Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНм-61 // Тернопіль, 2024 // С. 73, рис. – 12, додат. – 3, бібліогр. – 53.

Ключові слова: блокчейн, «розумне місто», голосування, криптографія, квантовий захист

Кваліфікаційна робота присвячена розробці безпечної, прозорої та масштабованої системи електронного голосування з використанням блокчейн-технологій, адаптованої до потреб «розумних міст».

У першому розділі проаналізовано сучасні тенденції електронного голосування, його значення для «розумних міст» та можливості використання блокчейн-технологій. Розглянуто децентралізацію, прозорість, незмінність даних, а також переваги та недоліки існуючих рішень.

Другий розділ досліджує основи блокчейн-технологій, вимоги до системи голосування, зокрема безпеку та пост-квантовий захист, і моделювання процесу голосування.

У третьому розділі описано розробку прототипу системи, результати тестування та оцінку перспектив впровадження. Підтверджено безпеку, прозорість і ефективність системи, її можливу інтеграцію з іншими сервісами «розумного міста».

Об'єкт дослідження: процеси організації та захисту електронного голосування у «розумних містах». Предмет дослідження: методи впровадження блокчейн-технологій, що забезпечують прозорість і безпеку виборчого процесу.

ANNOTATION

Research on Blockchain Technologies for Electronic Voting in «Smart Cities» // The educational level «Master» qualification work // Tytzhynskyi Anatolii Andriyovych // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, SNm-61 group // Ternopil, 2024 // P. 73, fig. — 12, annexes — 3, ref. — 53.

Key words: blockchain, smart city, voting, cryptography, quantum protection

The qualification work is dedicated to the development of a secure, transparent, and scalable electronic voting system using blockchain technology, adapted to the needs of «smart cities».

The first chapter analyzes current trends in electronic voting, its significance for «smart cities», and the possibilities of using blockchain technology. Decentralization, transparency, immutability of data, as well as the advantages and disadvantages of existing solutions, are examined.

The second chapter explores the fundamentals of blockchain technology, the requirements for a voting system, including security and post-quantum protection, and the modeling of the voting process.

The third chapter describes the development of a system prototype, the results of testing, and an evaluation of implementation prospects. The security, transparency, and efficiency of the system, as well as its potential integration with other "smart city" services, are confirmed.

The object of the study: the processes of organizing and protecting electronic voting in «smart cities».

The subject of the study: methods of implementing blockchain technology that ensure the transparency and security of the voting process.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Блокчейн — розподілений реєстр даних, що забезпечує децентралізоване зберігання та захист інформації.

Хеш — результат роботи хеш-функції, яка перетворює довільний обсяг даних у фіксований рядок символів для забезпечення цілісності.

Валідатор — вузол у блокчейн-мережі, який перевіряє правильність транзакцій і додає їх до блоку.

IoT (Internet of Things) — Інтернет речей, мережа підключених пристроїв, які обмінюються даними для автоматизації процесів.

Zero-Knowledge Proof (ZKP) — криптографічний метод, що дозволяє довести істинність твердження без розкриття додаткової інформації.

WebAssembly (Wasm) — двійковий формат інструкцій для виконання програм у веббраузерах з високою продуктивністю.

ЗМІСТ

ВСТУП

Актуальність теми. Розвиток концепції «розумних міст» вимагає створення безпечних, прозорих та ефективних рішень для електронного голосування. Блокчейн-технологія пропонує інноваційний підхід до вирішення цих завдань завдяки своїй децентралізованості, незмінності даних і прозорості процесів. Традиційні системи електронного голосування стикаються з проблемами, такими як ризики фальсифікацій, втручання у виборчий процес та недостатня довіра з боку громадян. Інтеграція блокчейн-технологій у такі системи дозволяє усунути ці недоліки, забезпечуючи надійний захист даних і прозорість підрахунку голосів. Однак для успішного впровадження таких систем необхідно подолати низку викликів: забезпечення анонімності голосування, вибір оптимального алгоритму консенсусу та відповідність національним законодавствам. Дослідження та розробка блокчейн-рішень для електронного голосування є актуальним напрямом, що сприятиме підвищенню довіри до виборчих процесів і реалізації концепції «розумних міст».

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є дослідження можливостей застосування блокчейн-технологій для розробки безпечної, прозорої та масштабованої системи електронного голосування у «розумних містах». Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати стан досліджень у сфері використання блокчейн-технологій для електронного голосування;
- дослідити існуючі методи реалізації алгоритмів консенсусу в блокчейн-системах;
- проаналізувати способи забезпечення анонімності та захисту даних у блокчейн-системах голосування;
- виконати порівняння існуючих рішень для електронного голосування, що використовують блокчейн, за критеріями безпеки, прозорості та продуктивності;

- розробити прототип системи електронного голосування з використанням блокчейн-технологій, адаптований до умов «розумного міста»;
- оцінити ефективність запропонованого рішення та визначити його потенційні перспективи для впровадження.

Об’єкт дослідження. Процеси організації, проведення та захисту електронного голосування у «розумних містах» із використанням блокчейн-технологій.

Предмет дослідження. Методи впровадження блокчейн-технологій у системи електронного голосування, що забезпечують прозорість, безпеку та довіру учасників виборчого процесу.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає в отримані подальшого розвитку методу застосування блокчейн-технологій для організації електронного голосування у «розумних містах», що дозволяє забезпечити прозорість, незмінність даних та високий рівень захисту результатів голосування.

Практичне значення одержаних результатів. Виконано макетування та прототипування системи електронного голосування з використанням блокчейн-технологій, що демонструє можливість її впровадження у муніципальних і державних установах.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на XII науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2024 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додатки А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 53 найменувань та 3 додатків. Загальний обсяг кваліфікаційної роботи складає 86 сторінки, з них 73 сторінки основного тексту, який містить 12 рисунків.

1 АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ ТА ПІДХОДІВ ДО ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

1.1 Електронне голосування як ознака «розумності» міст та громад: аналіз сучасного стану

Електронне голосування, або е-голосування, є одним з найбільш сучасних методів проведення виборів, що передбачає використання цифрових технологій для голосування. До електронного голосування належать як онлайн-голосування через Інтернет, так і застосування спеціальних електронних пристроїв на виборчих дільницях. В умовах глобалізації та цифровізації електронне голосування розглядається як інструмент для збільшення активності виборців, спрощення доступу до виборів та підвищення прозорості процесу.

Стан електронного голосування у світі:

- Естонія є світовим лідером у впровадженні електронного голосування. З 2005 року естонці можуть голосувати онлайн, використовуючи свої електронні ID-картки. На кожних наступних виборах кількість онлайн-голосів зростала: у 2015 році 30,5% виборців скористалися цією можливістю [1]. Естонська система передбачає багаторівневу перевірку користувачів, щоб захистити дані виборців та знизити ризики фальсифікацій. Цей підхід дозволяє громадянам, зокрема тим, хто проживає за кордоном, брати участь у виборах із будь-якого місця.
- Франція розглядала електронне голосування як спосіб полегшити виборчий процес, проте у 2017 році відмовилася від його використання, мотивуючи це високими ризиками кібератак і можливими втручаннями у виборчий процес [2]. Це рішення засвідчує важливість забезпечення кібербезпеки та захисту від зовнішніх загроз для успішного функціонування електронного голосування.
- Німеччина у 2009 році припинила використання електронного голосування через рішення Конституційного суду, який визнав цей метод невідповідним принципу таємності виборів. Суд постановив, що електронні

системи не можуть гарантувати, що голоси збережуться та будуть пораховані точно, що викликає занепокоєння щодо прозорості і відкритості процесу [3].

- Литва у 2019 році вирішила не впроваджувати електронне голосування, посилаючись на ризики кібервтручання, особливо з боку Росії [4]. Це рішення свідчить про необхідність додаткових заходів безпеки для захисту національних інтересів та забезпечення стабільності виборчого процесу.

В Україні електронне голосування на загальнонаціональному рівні поки не впроваджене, але дискусії щодо його доцільності тривають. У 2020 році Центральна виборча комісія сформувала робочу групу для аналізу можливостей застосування цифрових технологій у виборчому процесі. Проводяться консультації щодо технічних, правових та організаційних аспектів, необхідних для впровадження е-голосування [5]. Опитування Центру Разумкова в жовтні 2024 року показало, що близько 33% українців підтримують електронне голосування, особливо серед молоді, людей з обмеженими можливостями та громадян, які проживають за кордоном [6] [7].

Варто також зазначити, що проводилися електронні опитування, зокрема через додаток «Дія». Одним із таких було опитування щодо легалізації вогнепальної зброї для цивільного населення [8]. У травні 2022 року Міністерство внутрішніх справ ініціювало це опитування, яке тривало до 1 червня 2022 року. У ньому взяли участь понад 1,7 мільйона громадян. Результати показали, що 58,75% респондентів підтримали легалізацію зброї для особистого захисту, 21,82% висловилися проти обігу зброї серед цивільного населення, а 19,43% підтримали варіант «для спеціальних потреб» [9].

Ці опитування в «Дії» сприяють вивченню громадської думки з важливих питань, але вони не є офіційними референдумами чи виборами. Вони слугують інструментом для збору думок громадян та можуть впливати на формування державної політики.

На рівні міст в Україні електронне голосування починає набувати популярності. Воно використовується для обговорення та ухвалення місцевих рішень, створення більш доступного та прозорого процесу участі в житті громад. Наприклад:

- Київ у 2022 році в рамках застосунку «Київ Цифровий» організував онлайн-голосування для зміни назв міських об’єктів, пов’язаних з Російською Федерацією. Понад 6,5 мільйонів громадян України долучилися до процесу, що свідчить про великий інтерес до цифрових інструментів участі [10].

- Більшівцівська громада Івано-Франківської області у 2023 році запровадила систему «Голос», яка дозволяє депутатам голосувати онлайн, переводить проєкти рішень у цифровий формат і веде автоматичний облік відвідуваності засідань [11]. Це сприяє підвищенню прозорості і ефективності роботи органів місцевого самоврядування, роблячи процес прийняття рішень більш відкритим для громади.

Переваги електронного голосування на місцевому рівні:

- зручність та доступність: громадяни можуть брати участь у голосуваннях без необхідності відвідувати виборчі дільниці, що особливо важливо під час пандемій або інших обмежень;

- підвищення громадської активності: цифрові платформи спрощують процес участі у прийнятті рішень, залучаючи більше громадян до місцевого самоврядування;

- прозорість та довіра: електронні системи забезпечують відкритість процесу голосування та підрахунку голосів, що підвищує довіру до результатів і легітимність прийнятих рішень.

Виклики та ризики електронного голосування:

- кібербезпека: необхідність забезпечення захисту систем від можливих атак і втручань, особливо з боку хакерів та зовнішніх загроз;

- технічні збої: можливість виникнення технічних неполадок, які можуть вплинути на результати голосування або призвести до втрати голосів;

- довіра громадян: важливо, щоб громадяни довіряли системі, а для цього необхідно забезпечити її надійність, безпеку та простоту використання.

Процес електронного голосування складається з кількох ключових етапів, які забезпечують надійність, точність та конфіденційність виборчого процесу. Ці етапи варіюються в залежності від системи та технологій, що використовуються, але загальна структура виглядає наступним чином:

- реєстрація — перший і важливий етап електронного голосування. Виборці повинні пройти процедуру підтвердження особи для отримання доступу до голосування. Це може включати використання ID-карток, біометричних даних або онлайн-платформ, де виборець підтверджує свою особу за допомогою державних документів або облікових записів. У деяких країнах використовують спеціальні цифрові ID або токени для забезпечення унікальності та достовірності реєстрації [12].
- На цьому етапі система перевіряє особу виборця, щоб переконатися, що він або вона має право голосувати та не здійснює повторне голосування. Ідентифікація може здійснюватися різними способами, включаючи біометричну ідентифікацію (відбиток пальця, розпізнавання обличчя) або двофакторну аутентифікацію (наприклад, через SMS-код чи електронний підпис). Аутентифікація забезпечує високий рівень захисту та перешкоджає несанкціонованому доступу до системи.
- Після успішної аутентифікації виборець отримує доступ до інтерфейсу голосування. Інтерфейс повинен бути зручним і зрозумілим, щоб забезпечити легкий вибір кандидатів чи варіантів відповідей. Електронна платформа має гарантувати, що голосування буде конфіденційним та анонімним, а також забезпечувати надійне зберігання результатів.
- На цьому етапі виборець робить свій вибір і підтверджує його. У блокчейн-системах голос стає зашифрованим і незмінним записом у системі. Важливо, щоб система запобігала можливості зміни або скасування голосу після його подання. У деяких платформах виборцям дозволяється перевірити правильність запису голосу, не розкриваючи змісту вибору.
- Після подання голосів вони зберігаються в системі до завершення голосування. У випадку використання блокчейну, кожен голос записується в блокчейн-мережу, де він залишається незмінним. Інші системи можуть використовувати спеціальні бази даних з високим рівнем захисту. Зберігання голосів має гарантувати цілісність і недоторканність даних.
- Підрахунок у системах електронного голосування зазвичай автоматизований, що дозволяє швидко отримати результати одразу після

закінчення голосування. Блокчейн-системи забезпечують прозорість підрахунку, оскільки всі голоси є відкритими для перевірки, але не розкривають особу виборця. Підрахунок здійснюється так, щоб зберегти анонімність і точність результатів.

- Для запобігання можливих помилок результати проходять додаткову перевірку. У деяких системах застосовують зовнішній аудит, що забезпечує незалежний контроль за дотриманням процедур. Це підвищує довіру до системи та дозволяє уникнути будь-яких непорозумінь щодо легітимності результатів.
- Завершальний етап — офіційне оголошення результатів голосування. Зазвичай це робиться через офіційні державні органи, які підтверджують коректність і легітимність результатів [13]. У електронних системах це може відбуватися практично одразу, що значно прискорює процес у порівнянні з традиційними методами.

Кожен етап електронного голосування є важливим для забезпечення чесного і прозорого виборчого процесу. Вони працюють у комплексі, щоб гарантувати безпеку, конфіденційність та доступність виборчого процесу для громадян, роблячи вибори більш ефективними та зручними.

Впровадження електронного голосування в Україні може стати важливим інструментом для підвищення активності громадян та прозорості виборчого процесу. Проте для успішного запуску електронного голосування необхідно подолати ризики, пов’язані з кібербезпекою, забезпечити надійність системи і створити законодавчі рамки для захисту прав виборців. Успішне впровадження електронного голосування також залежатиме від інформаційної роботи з громадянами, що має допомогти сформувати довіру до нових цифрових інструментів у виборчому процесі.

1.2 Блокчейн у контексті електронного голосування

Використання блокчейн-технології в електронному голосуванні пропонує інноваційний підхід до підвищення безпеки, прозорості та довіри до виборчого процесу. Блокчейн, як децентралізована та незмінна система запису даних, може

вирішити багато проблем, властивих традиційним методам голосування, таким як маніпуляції результатами та відсутність належної прозорості.

Переваги блокчейн-голосування:

- прозорість та незмінність: кожен голос записується в блокчейн у вигляді незмінного запису, що запобігає можливим спробам підробити або видалити дані. Усі транзакції в системі блокчейн можуть бути перевірені громадськістю, зберігаючи тим самим прозорість виборчого процесу та довіру до його результатів.
- Безпека: децентралізована структура блокчейну значно знижує ризик кібератак, оскільки відсутня єдина точка відмови. Кожен вузол в мережі зберігає копію всіх транзакцій, що ускладнює стороннє втручання. Додаткові рівні криптографічного захисту гарантують безпеку інформації про виборців і обмежують доступ до їхніх даних.
- Анонімність та конфіденційність: використання криптографічних методів у блокчейн-голосуванні дозволяє зберегти таємницю голосування, гарантує анонімність виборців та захищає їх особисті дані від несанкціонованого доступу. Технології, такі як Zero-Knowledge Proof (докази з нульовим розголошенням), дозволяють підтверджувати дійсність голосів без розкриття особи виборця [14].
- Незалежна перевірка: блокчейн забезпечує можливість перевірки результатів усіма учасниками процесу. Кожен учасник має доступ до запису про власний голос у системі та може самостійно переконатися у правильності підрахунку, що суттєво підвищує рівень довіри до виборів.
- Смарт-контракти: вони дозволяють автоматизувати процес голосування, наприклад, початок і завершення голосування або підрахунок голосів. Завдяки смарт-контрактам процес стає точнішим і зменшує ризик людських помилок, оскільки дії виконуються автоматично на основі заздалегідь визначених умов.
- Можливість міжнародної верифікації: блокчейн дозволяє організувати міжнародний моніторинг виборів, що особливо важливо для країн з низьким рівнем довіри до виборчого процесу. Незалежні спостерігачі можуть у реальному

часі спостерігати за голосуванням та перевіряти його прозорість, підвищуючи тим самим легітимність виборів на міжнародному рівні.

- Стійкість до збоїв: блокчейн-системи є розподіленими, що означає, що дані зберігаються на багатьох вузлах, і навіть у разі часткової відмови система залишається працездатною. Це дозволяє зберегти безперервність процесу голосування та захищає від зовнішніх атак або перебоїв у мережі.

Приклади впровадження блокчейн-голосування:

- Естонія: піонер у впровадженні електронного голосування, використовує блокчейн для забезпечення безпеки та прозорості виборчого процесу. Естонська система ID-картки дозволяє громадянам голосувати онлайн, а блокчейн захищає дані та забезпечує незмінність процесу. В 2021 році понад 40% виборців у країні скористалися можливістю електронного голосування [2].

- Швейцарія: у 2018 році кантон Женева провів експериментальні вибори з використанням блокчейн-голосування [15]. Мета проекту полягала в тому, щоб продемонструвати, як технологія може допомогти забезпечити прозорість і цілісність виборчого процесу. Випробування показали, що блокчейн-технології можуть бути інтегровані з існуючими методами голосування.

- Таїланд: у листопаді 2018 року Демократична партія Таїланду вперше застосувала блокчейн для проведення внутрішніх виборів. Більше ніж 120 000 виборців скористалися можливістю подати голос, який зберігався у блокчейн-мережі, що значно зменшило можливості для фальсифікацій і втручання [16].

Виклики та обмеження блокчейн-голосування:

- технічна складність: розробка та впровадження блокчейн-систем потребує значних ресурсів, високого рівня експертизи та інфраструктури, яка повинна бути доступна всім виборцям. Це особливо складно в умовах віддалених регіонів або країн із низьким рівнем технологічного розвитку.

- Масштабованість: блокчейн-мережі мають обмежену пропускну здатність і можуть стикатися з проблемами при обробці великої кількості транзакцій одночасно, що є викликом для масштабних національних виборів. Оптимізація мереж для зменшення витрат на транзакції та підвищення швидкості обробки голосів залишається одним із пріоритетних завдань.

- Юридичні та регуляторні питання: для широкого впровадження блокчейн-голосування необхідно адаптувати законодавство, що забезпечить юридичну силу такого виду голосування. Розробка чітких нормативних актів та міжнародних стандартів залишається актуальним завданням, оскільки відсутність правових рамок може знижувати довіру до системи.
- Енергетичні витрати: традиційні блокчейн-мережі, такі як Bitcoin та Ethereum, потребують значних обчислювальних потужностей, що збільшує витрати на енергію [17]. Високі енергетичні витрати можуть стати суттєвою перешкодою для впровадження блокчейн-голосування в країнах, що не можуть забезпечити відповідні енергетичні ресурси.

В Україні блокчейн-технологія розглядається як засіб підвищення прозорості та боротьби з корупцією в державному управлінні, включаючи виборчий процес. Експерти вважають, що впровадження блокчейну може забезпечити чесність та відкритість виборів, зменшити можливість фальсифікацій, а також підвищити участь громадян у прийнятті рішень [18]. Однак впровадження такої технології на національному рівні потребує значних інвестицій та часу для адаптації законодавства, створення технічної інфраструктури і побудови довіри з боку громадян.

Таким чином, блокчейн має значний потенціал у сфері електронного голосування, пропонуючи рішення для багатьох існуючих проблем, таких як прозорість, безпека, надійність та довіра до виборчого процесу. Водночас його інтеграція може сприяти підвищенню громадської участі у виборах завдяки зручності та інноваційності запропонованих рішень. Проте для успішного впровадження блокчейн-голосування необхідно подолати технічні, юридичні та соціальні виклики, щоб забезпечити справжню довготривалу ефективність цієї системи.

1.3 Огляд існуючих рішень та прототипів

Використання блокчейн-технології в електронному голосуванні привертає увагу дослідників та розробників, оскільки вона пропонує новий підхід до

забезпечення безпеки, прозорості та довіри у виборчому процесі. Завдяки децентралізованому підходу, блокчейн дозволяє створити середовище, де результати голосування можна перевірити, а записи неможливо змінити або видалити. Це привело до створення кількох прототипів і систем, орієнтованих на різні аспекти голосування, наприклад:

- EtherVote — це система електронного голосування, побудована на платформі Ethereum, що стала однією з перших спроб застосування блокчейну для забезпечення прозорості виборчого процесу [19]. Була розроблена групою ентузіастів блокчейну, які прагнули продемонструвати можливість використання децентралізованої системи для виборів. Її децентралізована структура дозволяє обійтися без центральних серверів, що значно знижує ризики злому. EtherVote підтримує ідентифікацію виборців за допомогою криптографії, забезпечуючи високий рівень конфіденційності голосування та цілісність результатів. Кожен голос зберігається у вигляді незмінного запису, що дозволяє перевіряти результати без можливості їх редагування чи підробки. Схему роботи даної системи зображено на рисунку 1.1.

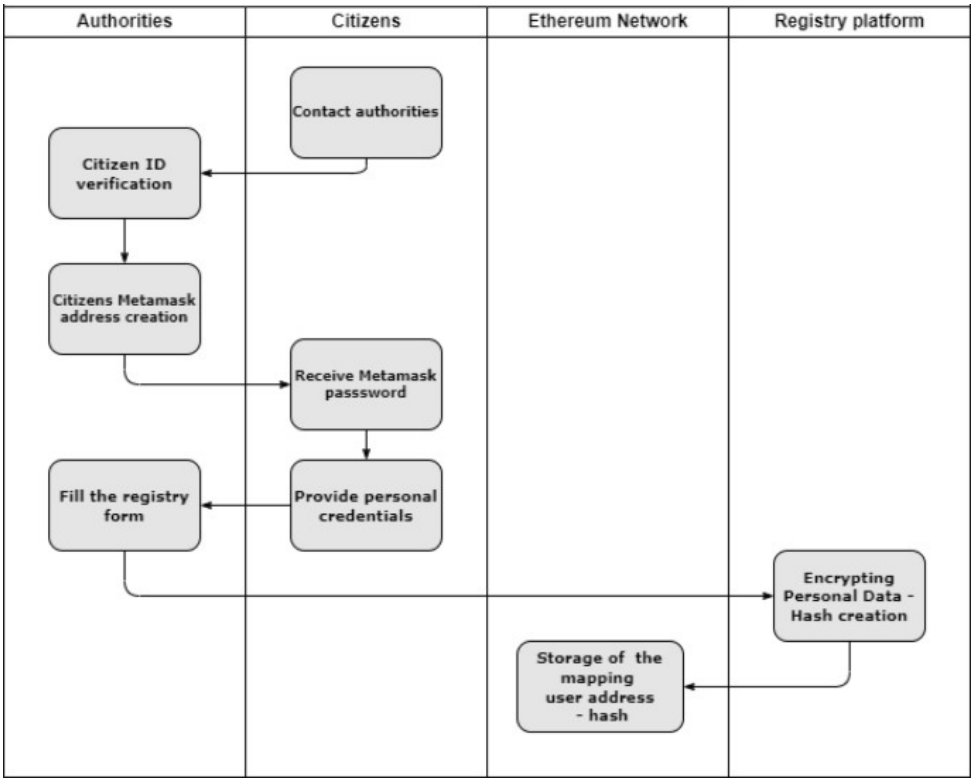

Рисунок 1.1 — Схема роботи системи електронного голосування EtherVote [20]

- BBB-Voting — це протокол голосування, розроблений з урахуванням підтримки багатоваріантного вибору (1-out-of-k). Він також базується на Ethereum, проте головний акцент зроблено на підвищенні стійкості до збоїв та зниженні витрат на транзакції. Конфіденційність голосів гарантується криптографічними методами, а універсальна можливість перевірки результатів дозволяє усім учасникам процесу самостійно переконатися у правильності підрахунку голосів. Цей протокол підходить як для виборів різного рівня, так і для опитувань та референдумів [21].
- Democracy Earth — це неприбуткова організація, яка ставить перед собою амбітну мету — децентралізувати політичну участь за допомогою блокчейн-технології. Цей проект був заснований у 2015 році Сантьяго Сіром, відомим соціальним активістом і підприємцем. Вона розробила платформу, яка базується на концепції «політичної криптовалюти» — токенів, які користувачі можуть використовувати для голосування. Ця платформа спрямована на забезпечення прозорості та запобігання цензурі, надаючи кожному виборцю контроль над своїм голосом. Democracy Earth розглядає можливість використання токенів не лише у виборах, але й у прийнятті рішень на рівні громади та організацій [22].
- Polyas — компанія, що спеціалізується на рішеннях для онлайн-голосування. Вона пропонує приватні блокчейн-мережі для забезпечення додаткової безпеки, що робить систему особливо актуальною для організацій, які потребують підвищеної конфіденційності даних. Їхні послуги охоплюють не лише електронне голосування, а й живе голосування на місці, голосування за резолюції, поправки та інші важливі рішення. Polyas фокусується на забезпеченні універсальної перевірюваності, пропонуючи інтуїтивно зрозумілий інтерфейс для користувачів і можливість підрахунку голосів у режимі реального часу. Рішення було розроблене німецькою компанією Polyas GmbH, яка спеціалізується на створенні онлайн-платформ для голосування та управління виборчим процесом. Компанія розпочала свою діяльність у 1996 році, пропонуючи різноманітні електронні рішення для виборів [23].

- Votem — це мобільна платформа для голосування на основі блокчейн-технології була заснована компанією Votem Corp, що базується в Клівленді, США. Платформа спрямована на створення зручного процесу для виборців із різними потребами, зокрема вона підтримує онлайн-реєстрацію, електронне маркування бюлетенів і голосування для людей з обмеженими можливостями. Система дозволяє користувачам голосувати з мобільних пристроїв, забезпечуючи високий рівень захисту та прозорості. Votem орієнтована на застосування в державних виборах, корпоративних голосуваннях і для різних неурядових організацій [24].

- Boulé — це система, що була розроблена стартапом у Франції, який фокусується на безпечних рішеннях для виборчого процесу. Команда Boulé поєднала блокчейн-технологію Ethereum з біометричною ідентифікацією для забезпечення найвищого рівня безпеки та прозорості виборів. Для підтвердження особи виборця використовуються власні токени та технологія розпізнавання обличчя. Завдяки цьому підходу система Boulé забезпечує високий рівень безпеки та прозорості, роблячи процес виборів практично невразливим до підробок. Вона також дозволяє перевірити результати виборів, що робить її актуальною для виборів в умовах підвищених вимог до ідентифікації виборців [25].

- Horizon State — платформа заснована в Австралії, яка пропонує стійку до змін цифрову скриньку для голосування та залучення громадян до виборчого процесу. Вона підтримує різні типи голосувань, включаючи преференційне та зважене голосування, що робить її універсальною для різних організацій. Horizon State застосовується для урядів, профспілок, політичних партій та навіть корпорацій, забезпечуючи повну прозорість і контроль над процесом голосування [26].

Застосування блокчейн-технологій у виборах має великий потенціал для підвищення довіри до процесу та забезпечення надійності результатів. Блокчейн створює можливості для децентралізації, що зменшує ризик централізованих маніпуляцій. Крім того, цей підхід сприяє прозорості — кожен голос записується у вигляді незмінного запису, який можна перевірити, але не змінити чи видалити.

Завдяки високому рівню конфіденційності, забезпеченому криптографією, блокчейн-системи можуть зберегти анонімність виборців і гарантувати, що жоден з них не зможе проголосувати двічі або змінити свій голос.

Блокчейн-технологія надає можливості для різноманітних застосувань: від місцевих виборів та корпоративних голосувань до національних референдумів. Однак для успішного впровадження потрібні значні ресурси для подолання технічних викликів, забезпечення кібербезпеки та створення нормативної бази, яка дозволить легалізувати та регулювати цей інноваційний підхід.

1.4 Можливості інтеграції аспектів блокчейн-технологій голосування у інші сервіси «розумного» міста

Інтеграція блокчейн-технологій у сервіси «розумного» міста відкриває широкі можливості для підвищення ефективності управління міськими процесами, забезпечення прозорості взаємодії громадян із міською інфраструктурою та розвитку інноваційних підходів до демократичного управління. Завдяки властивостям блокчейну, таким як децентралізація, незмінність даних і прозорість, ці технології можуть стати ключовим елементом у формуванні цифрової інфраструктури міст.

Електронне голосування є одним із прикладів використання блокчейн-технологій, яке може бути інтегроване з іншими сервісами. Зокрема, блокчейн може стати базою для платформ електронного урядування, що забезпечують доступ громадян до державних і муніципальних послуг. Завдяки таким системам можна автоматизувати подання заявок, участь у громадських обговореннях та голосування за міські ініціативи, таких як бюджети участі чи вибір локальних проєктів для реалізації [27] [28].

Ще одним перспективним напрямом є інтеграція блокчейну з системами збереження даних, зокрема історичної та культурної спадщини. Цифровізація музеїв, бібліотек і архівів у рамках «розумного» міста сприяє збереженню культурної ідентичності та надає громадянам доступ до цінної інформації. Завдяки використанню блокчейну забезпечується надійний захист даних від змін

і зловживань, а також підвищується прозорість у процесі їх використання [28] [29].

Крім того, блокчейн може бути інтегрований із системами штучного інтелекту та машинного навчання для підвищення ефективності міських сервісів. Наприклад, у процесі аналізу результатів голосування чи обробки великих обсягів даних блокчейн забезпечує прозорість і захист, а машинне навчання сприяє автоматизації процесів. Таке поєднання дозволяє створювати інноваційні сервіси, орієнтовані на потреби громадян [30] [31].

Таким чином, блокчейн-технології мають значний потенціал для інтеграції в інфраструктуру «розумного» міста. Вони забезпечують не лише прозорість і надійність, але й розширюють можливості міських сервісів, сприяючи демократизації процесів управління та підвищенню якості життя громадян.

1.5 Висновки до першого розділу

Аналіз технологій та підходів до електронного голосування продемонстрував його важливість для розвитку сучасного суспільства та інтеграції в цифрову інфраструктуру «розумних» міст. Електронне голосування виступає не лише інструментом підвищення ефективності демократичних процесів, але й механізмом, що сприяє залученню громадян до управління суспільними ресурсами.

Особливу увагу привертає використання блокчейн-технологій, які забезпечують високий рівень безпеки, прозорості та довіри до процесу голосування. Огляд існуючих рішень та прототипів свідчить про значний потенціал інтеграції таких систем у реальні умови, зокрема у великих міських агломераціях. Водночас, впровадження таких рішень вимагає врахування технічних, юридичних та соціальних аспектів.

Таким чином, електронне голосування на основі сучасних технологій, зокрема блокчейн, є перспективним напрямом, який поєднує в собі інноваційність та здатність відповідати викликам цифрової епохи.

2 ДОСЛІДЖЕННЯ ТА ВИБІР ТЕХНОЛОГІЙ І МЕТОДІВ РЕАЛІЗАЦІЇ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ БЛОКЧЕЙНУ

2.1 Концептуальні основи блокчейн-технології для систем голосування

Блокчейн – це технологія, яка базується на розподіленому реєстрі даних, організованому у вигляді послідовного ланцюга блоків. Кожен блок містить набір транзакцій, пов’язаних між собою за допомогою криптографічних хешів.

Складові блокчейну:

- дані: вміст блоку може варіюватися залежно від сфери застосування. У випадку систем голосування це можуть бути зашифровані голоси виборців або транзакції, які підтверджують факт голосування.
- Хеш блоку: унікальний криптографічний ідентифікатор, який генерується на основі даних у блоці. Зміна навіть одного байта інформації змінює хеш, роблячи підробку блоку надзвичайно складною.
- Хеш попереднього блоку: зв’язує блоки між собою в єдиний ланцюг, забезпечуючи послідовність даних і незмінність історії. Схему структури блокчейну показано на рисунку 2.1.

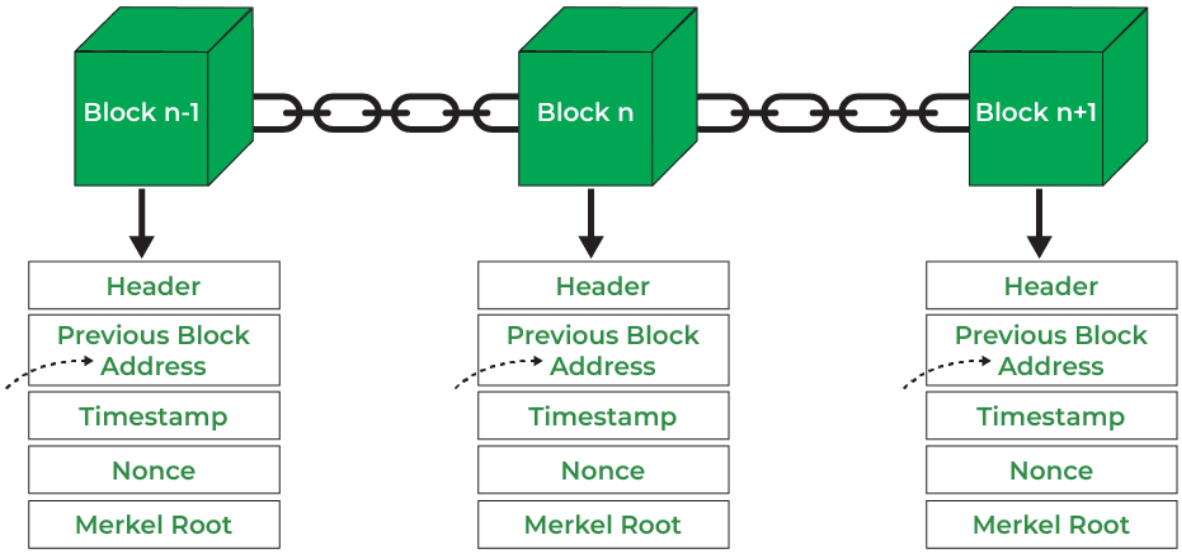

Рисунок 2.1 — Схема структури блокчейну [30]

- Мережа вузлів: блокчейн працює на основі децентралізованої мережі вузлів (нодів), які спільно підтримують функціонування системи. Кожен вузол зберігає копію всього реєстру, забезпечуючи його доступність та стійкість до збоїв.

- Алгоритми консенсусу: це механізми, які забезпечують узгодженість між вузлами щодо додавання нових блоків. Найпоширенішими алгоритмами є Proof of Work (PoW), Proof of Stake (PoS) та їх варіації. Вони гарантують, що нові дані додаються до блокчейну лише після підтвердження їхньої коректності більшістю вузлів.

- Смарт-контракти: це програмні алгоритми, які автоматизують виконання певних умов у блокчейні. У системах голосування смарт-контракти можуть бути використані для перевірки права виборця голосувати, реєстрації голосів і автоматичного підрахунку результатів. Схему взаємодії смарт-контрактів з блокчейн-сисмемою забражено на рисунку 2.2.

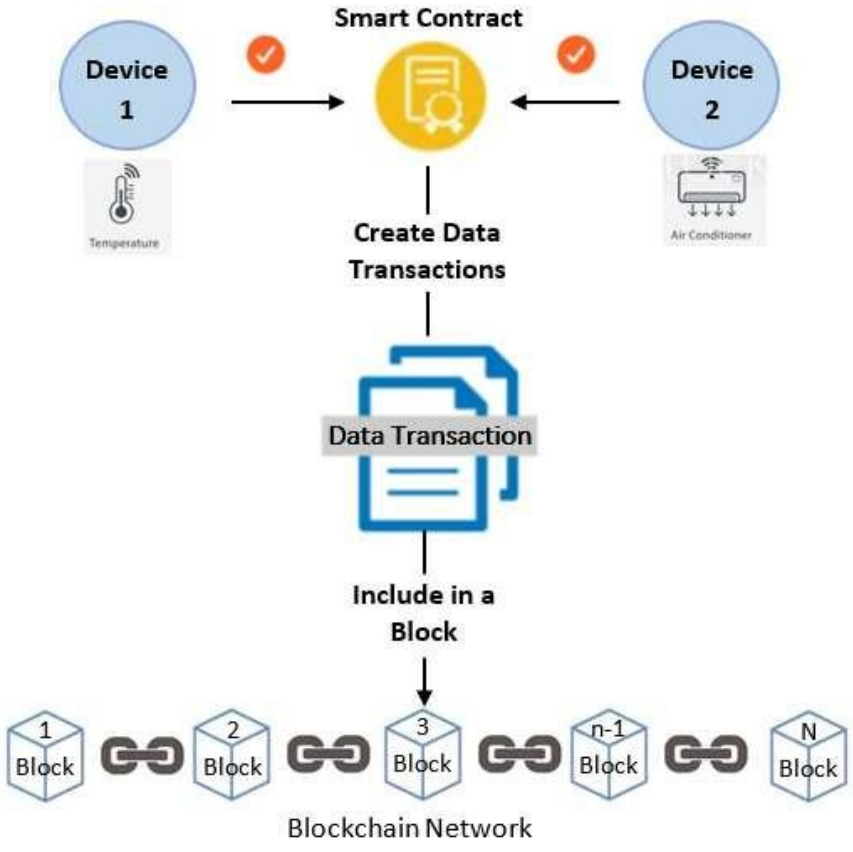

Рисунок 2.2 — Схема взаємодії смарт-контрактів з блокчейн системою [31]

Як працює блокчейн:

- реєстрація виборця: кожен виборець отримує унікальний цифровий ідентифікатор, який може бути реалізований на основі криптографічних ключів. Приватний ключ дозволяє виборцю голосувати, а публічний ключ забезпечує перевірку його голосу.
- Голосування: виборець надсилає свій голос у вигляді транзакції до мережі. Ця транзакція шифрується, щоб забезпечити анонімність, і потрапляє до пулу непідтверджених транзакцій.
- Додавання голосу до блоку: спеціальний алгоритм консенсусу підтверджує коректність транзакції, після чого голос додається до нового блоку. Усі вузли в мережі отримують оновлену копію блокчейну, забезпечуючи прозорість і синхронізацію.
- Підрахунок голосів: оскільки всі голоси зберігаються у блокчейні, система може автоматично підрахувати їх, виключивши можливість дублювання чи фальсифікації.
- Перевірка результатів: будь-який учасник виборчого процесу може перевірити результати, порівнюючи дані у блокчейні. Це дозволяє підвищити довіру до процесу голосування.

Загальний алгоритм роботи блокчейн-систем зображено на рисунку 2.3.

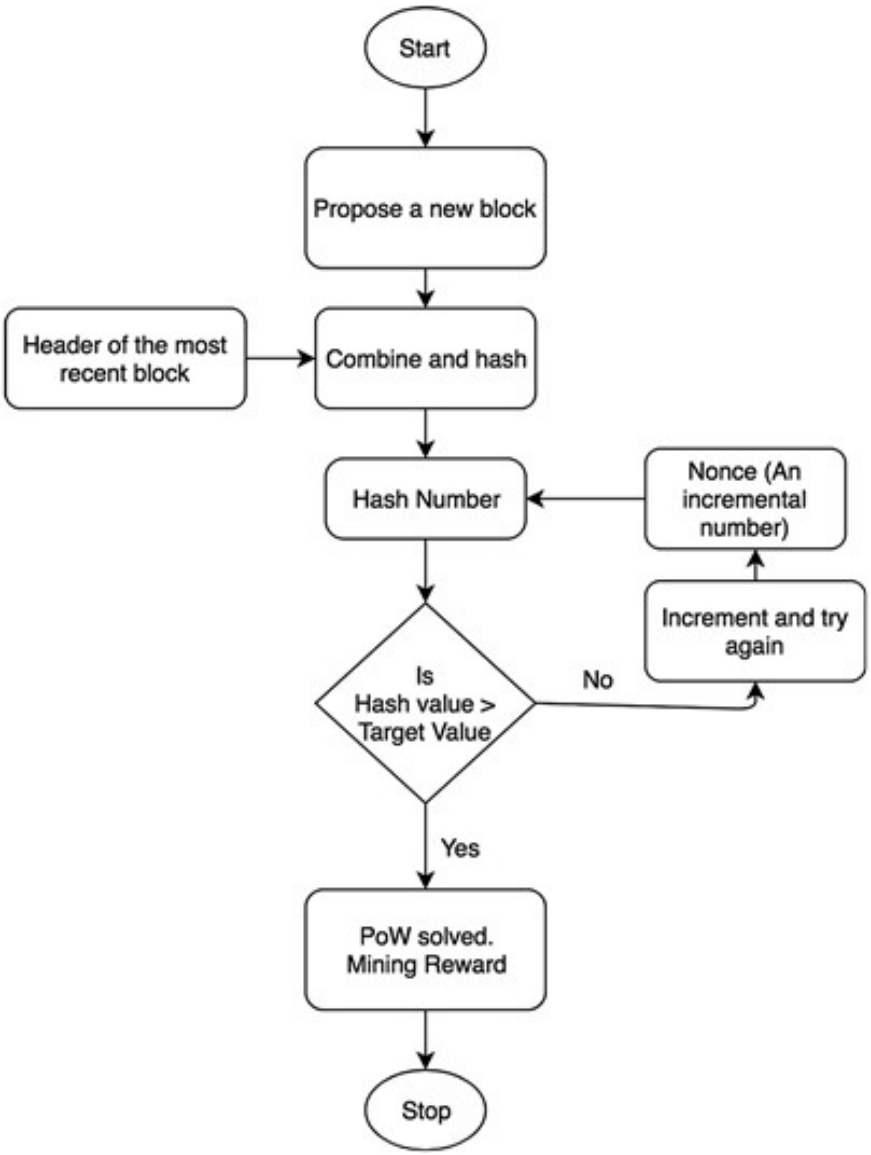

Рисунок 2.3 — Алгоритм роботи блокчейн-систем [32]

Особливості застосування у системах голосування:

- прозорість: усі дії у системі – від реєстрації виборців до підрахунку голосів – є доступними для перевірки, що мінімізує ризики маніпуляцій.
- Захист даних: блокчейн гарантує, що кожен голос є зашифрованим і недоступним для сторонніх осіб, що забезпечує конфіденційність виборців.
- Незмінність: будь-яка зміна в блокчейні фіксується, що унеможливлює видалення або зміну голосів після їх подання.
- Доступність: децентралізована мережа забезпечує безперебійну роботу системи навіть за умов технічних збоїв чи спроб атак.

Використання блокчейну у голосуванні відкриває нові горизонти для проведення виборів у «розумних містах». Ця технологія дозволяє створити

безпечне, прозоре та ефективне середовище, яке відповідає вимогам сучасного суспільства, сприяючи розвитку довіри до демократичних процесів.

2.2 Вимоги до системи голосування

Система голосування, що базується на блокчейн-технології, повинна відповідати ряду детально сформульованих вимог, які охоплюють технічні, функціональні та організаційні аспекти. Ці вимоги є ключовими для того, щоб забезпечити не лише ефективність роботи системи, але й її надійність, безпеку та зручність використання для всіх учасників процесу. Важливо, щоб кожен елемент системи був ретельно продуманим, а всі процеси – оптимізованими для виконання поставлених завдань. Особливу увагу слід приділити тому, щоб система могла функціонувати стабільно навіть у складних умовах, таких як велика кількість користувачів чи можливі зовнішні загрози.

Вимоги до такої системи є багатогранними, оскільки її основою є складна технологія, яка повинна інтегруватися в широкий спектр інфраструктурних компонентів. Технічні вимоги включають не лише високий рівень продуктивності, але й здатність системи ефективно адаптуватися до можливих змін у навантаженні. Функціональні вимоги спрямовані на забезпечення зручності користування, зокрема інтуїтивно зрозумілого інтерфейсу та простоти доступу для виборців. Організаційні вимоги гарантують відповідність системи законодавству, дотримання стандартів інформаційної безпеки та забезпечення довіри до виборчого процесу.

Зважаючи на складність і багатокомпонентність системи голосування на основі блокчейну, її проектування та впровадження потребує особливої уваги до деталей. Нижче наведено основні вимоги, які є критично важливими для розробки ефективної системи, здатної відповідати всім сучасним викликам.

Технічні вимоги:

- масштабованість: система повинна бути здатною обробляти велику кількість транзакцій одночасно, щоб забезпечити ефективну роботу під час виборів із великою кількістю учасників. Це особливо актуально для виборів у

масштабах «розумних міст», де кількість виборців може обчислюватися сотнями тисяч.

- Децентралізація: система повинна працювати на основі розподіленої мережі вузлів, щоб уникнути залежності від єдиного централізованого сервера. Це знижує ризик збоїв, атак на сервер та можливих маніпуляцій.
- Стійкість до атак: система повинна забезпечувати захист від різних типів атак, таких як DDoS-атаки, спроби модифікації даних або несанкціонованого доступу. Використання криптографічних алгоритмів і надійних протоколів консенсусу є ключовими для досягнення цієї вимоги.
- Продуктивність: час обробки кожного голосу повинен бути мінімальним, щоб забезпечити швидкий підрахунок голосів та своєчасне оновлення даних у реєстрі.

Функціональні вимоги:

- Аутентифікація виборців: система повинна забезпечувати надійну ідентифікацію виборців, використовуючи сучасні методи аутентифікації, такі як електронні підписи, біометричні дані чи цифрові сертифікати.
- Захист конфіденційності: система повинна гарантувати, що голос кожного виборця є анонімним і не може бути відслідкованим, забезпечуючи при цьому можливість перевірки результатів.
- Одноразовість голосу: кожен виборець повинен мати можливість проголосувати лише один раз, що виключає можливість дублювання голосів.
- Прозорість: система повинна забезпечувати можливість перевірки всіх етапів процесу голосування без порушення конфіденційності. Учасники повинні мати доступ до перевірки даних голосування через блокчейн.
- Автоматизація підрахунку голосів: система повинна автоматично підраховувати голоси одразу після завершення виборів, що скорочує час на оголошення результатів.
- Можливість інтеграції: система повинна підтримувати інтеграцію з іншими технологіями «розумних міст» для спрощення її впровадження та використання.

Організаційні вимоги:

- Юридична відповідність: система повинна відповідати законодавчим вимогам країни, зокрема щодо захисту даних, виборчого процесу та електронного урядування.
- Зручність використання: інтерфейс системи повинен бути інтуїтивно зрозумілим і доступним для різних груп виборців, включаючи людей з обмеженими можливостями.
- Довговічність: система повинна бути стійкою до змін технологій і підтримувати можливість оновлення та модернізації.
- Навчання користувачів: перед впровадженням системи необхідно забезпечити інформаційно-роз'яснювальну кампанію серед виборців та навчання персоналу, який буде обслуговувати систему.

Специфічні вимоги для блокчейн-технології в голосуванні:

- Алгоритм консенсусу: вибір алгоритму консенсусу має забезпечувати оптимальний баланс між продуктивністю, енергоефективністю та безпекою.
- Смарт-контракти: використання смарт-контрактів повинно забезпечувати автоматизацію процесу голосування, перевірки права виборця голосувати та підрахунку голосів.
- Доступність: система повинна працювати у реальному часі, забезпечуючи доступ до даних голосування для авторизованих користувачів.

Врахування цих вимог дозволяє створити надійну, безпечну та прозору систему голосування, яка відповідає потребам сучасних «розумних міст». Впровадження блокчейн-технології відкриває нові можливості для демократизації виборчих процесів і підвищення довіри до результатів голосування.

Розвиток квантових обчислень становить серйозну загрозу для традиційних криптографічних алгоритмів, які є основою сучасних блокчейн-систем. Квантові комп'ютери, завдяки своїй здатності до паралельних обчислень, можуть легко зламати алгоритми асиметричного шифрування, такі як RSA, ECDSA та алгоритм Еліптичних кривих, які використовуються для створення цифрових підписів і забезпечення безпеки транзакцій [33]. У зв'язку з цим, постає необхідність розробки та впровадження пост-квантових криптографічних

методів для забезпечення захисту блокчейн-систем від потенційних атак квантових комп’ютерів.

Пост-квантовий захист базується на використанні криптографічних алгоритмів, які є стійкими до атак квантових комп’ютерів. Ці алгоритми розробляються на основі математичних задач, які складно розв'язати навіть для квантових комп’ютерів. Основними підходами до пост-квантової криптографії є:

- Схеми на основі ґраток (Lattice-Based Cryptography): ці алгоритми використовують складність розв'язання задач на евклідових ґратках, таких як задача найкоротшого вектора (SVP) або найближчого вектора (CVP) [34]. Прикладом є алгоритми NTRU та Kyber.
- Кодова криптографія (Code-Based Cryptography): базується на складності розв’язання задачі декодування заздалегідь заданих кодів, наприклад, кодів Ріда-Соломона [34]. Відомим прикладом є алгоритм McEliece.
- Мультиваріантна криптографія (Multivariate Cryptography): використовує системи багатоваріантних нелінійних рівнянь, які важко зламати навіть квантовим комп'ютером [34]. Прикладом є алгоритм Rainbow.
- Криптографія на основі хеш-функцій (Hash-Based Cryptography): використовує криптографічні хеш-функції для створення цифрових підписів, які стійкі до квантових атак [34]. Прикладом є алгоритм XMSS.
- Ізогенійна криптографія (Isogeny-Based Cryptography): використовує ізогенії (морфізми між еліптичними кривими), що робить алгоритми стійкими до квантових обчислень [34]. Відомим прикладом є протокол SIKE. Ізогенійні еліптичні криві зображено на рисунку 2.4.

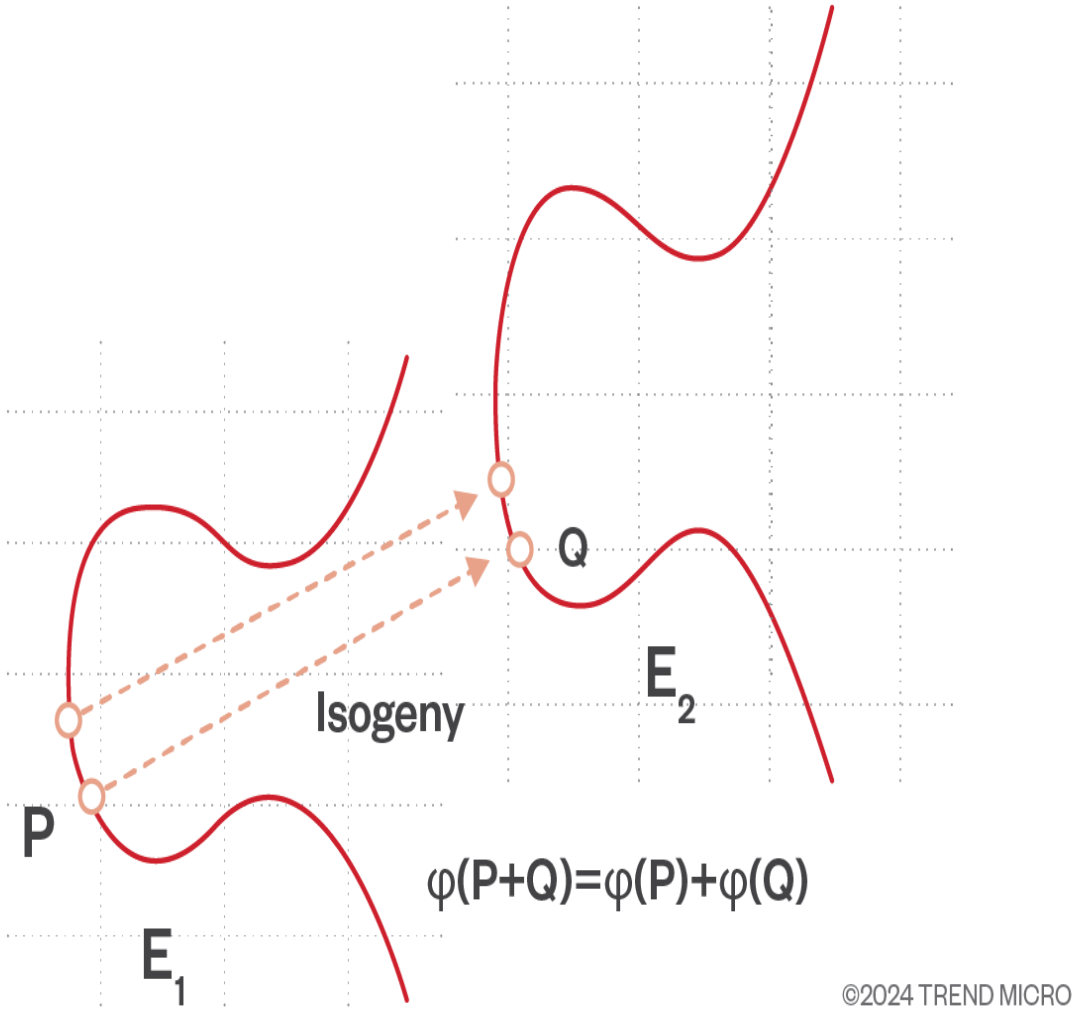

Рисунок 2.4 - Ізогенійні еліптичні криві, що використовуються для пост-квантових алгоритмів криптографії [35]

У контексті блокчейн-систем пост-квантовий захист може бути впроваджений у кількох аспектах:

- цифрові підписи: заміна існуючих алгоритмів (наприклад, ECDSA) на пост-квантові альтернативи, такі як алгоритм SPHINCS+ або XMSS, які базуються на хеш-функціях і забезпечують стійкість до квантових атак [36].
- Шифрування: інтеграція пост-квантових схем шифрування для захисту конфіденційних даних, таких як особисті ключі або транзакції.
- Протоколи консенсусу: адаптація механізмів консенсусу до пост-квантових алгоритмів, щоб забезпечити надійність підтвердження транзакцій навіть за наявності квантових комп’ютерів.

Важливо зазначити, що перехід до пост-квантової криптографії потребує ретельного тестування та оптимізації, оскільки нові алгоритми можуть бути більш вимогливими до обчислювальних ресурсів і збільшувати час виконання транзакцій. Проте інтеграція таких алгоритмів є критично необхідною для довгострокового захисту блокчейн-систем, особливо у таких чутливих сферах, як голосування.

Впровадження пост-квантового захисту забезпечить стійкість блокчейн-систем до майбутніх загроз, пов'язаних із розвитком квантових технологій, і зробить їх надійним інструментом для «розумних міст».

Інтеграція блокчейн-технологій у ці репозиторії забезпечує прозорість і надійність обміну даними. У контексті електронного голосування це може бути використано для захисту даних виборців і створення довіреного середовища для демократичних процесів. Таким чином, консолідація соціально-комунікаційних ресурсів стає важливим етапом у побудові повноцінної інфраструктури «розумного» міста.

2.3 Вибір платформи та архітектури системи

Вибір платформи та архітектури для системи голосування є одним із ключових етапів її проєктування, оскільки від цього залежить безпека, ефективність, зручність використання та вартість розробки. При виборі платформи необхідно враховувати технічні, економічні та функціональні вимоги, а також можливість подальшої адаптації та масштабування системи.

Аналіз існуючих платформ:

- Ethereum: Ethereum є однією з найпоширеніших блокчейн-платформ, яка підтримує смарт-контракти та децентралізовані додатки. Її основними перевагами є велика спільнота розробників, доступність інструментів для створення смарт-контрактів і надійність мережі. Проте високі комісії за транзакції та обмеження у швидкості обробки даних можуть стати проблемою для виборчих систем з великою кількістю учасників [37].

- Binance Smart Chain (BSC): ця платформа забезпечує низькі комісії за транзакції та високу швидкість роботи, що робить її привабливим вибором для систем голосування. Проте децентралізація мережі є меншою порівняно з іншими платформами, що може викликати питання щодо безпеки [37].

- Hyperledger Fabric: це приватна блокчейн-платформа з гнучкими налаштуваннями для різних сценаріїв використання. Її перевагами є можливість налаштування дозволів доступу, висока продуктивність і підтримка різних мов програмування для створення смарт-контрактів. Однак Hyperledger Fabric вимагає значних ресурсів для налаштування та підтримки, що може бути економічно невигідним для невеликих проєктів [39].

- Cardano: Cardano є платформою нового покоління, яка пропонує високу безпеку та низькі енергетичні витрати завдяки використанню алгоритму консенсусу Proof of Stake. Її архітектура добре підходить для створення голосувальних систем, але складність у навчанні та відсутність широкого поширення можуть стати перепоною [39].

До переваг готових платформ входять такі пункти:

- Швидкий початок роботи завдяки готовим рішенням.
- Наявність технічної підтримки та документованих інструментів.
- Перевірена надійність і безпека у великих проєктах.

До недоліків готових платформ входять такі пункти:

- Високі витрати на ліцензії та комісії за транзакції.
- Можливі обмеження у кастомізації під специфічні потреби.
- Залежність від сторонніх розробників і спільноти платформи.

Вибір архітектури має забезпечити баланс між продуктивністю, безпекою та масштабованістю системи. Для цього пропонується модульний підхід, який включає наступні компоненти:

- Модуль аутентифікації: відповідає за перевірку права виборців на участь у голосуванні, використовуючи методи аутентифікації, такі як цифрові підписи або біометрія.

- Модуль обробки голосів: приймає, шифрує та додає голоси до блокчейну. Забезпечує захист конфіденційності даних виборців.

- Модуль підрахунку голосів: автоматично підраховує результати виборів на основі даних у блокчейні. Використовує смарт-контракти для виконання цього процесу без втручання людини.
- Модуль перевірки: дозволяє учасникам виборчого процесу перевіряти коректність підрахунку голосів, зберігаючи при цьому анонімність.
- Модуль управління системою: надає адміністраторам інструменти для налаштування параметрів системи, моніторингу її роботи та усунення можливих проблем.

Після аналізу існуючих платформ можна зробити висновок, що кожна з них має свої переваги, але їх вартість і обмеження можуть ускладнити процес впровадження системи голосування. Для економії ресурсів та кращого розуміння всіх технічних аспектів, пов’язаних із реалізацією голосувальної системи, пропонується розробити власну платформу. Це дозволить уникнути витрат на ліцензування, адаптувати систему під конкретні вимоги, а також показати всі деталі її роботи.

Власна платформа надасть можливість створити кастомізоване рішення, яке враховуватиме специфіку виборчого процесу у «розумних містах», забезпечуючи необхідний рівень безпеки, прозорості та продуктивності.

2.4 Розробка моделі процесу голосування

Розробка моделі процесу голосування є важливим етапом створення ефективної та захищеної системи. Модель має охоплювати всі ключові аспекти виборчого процесу, починаючи з реєстрації виборців і закінчуючи підрахунком голосів та верифікацією результатів. Основою цієї моделі є блокчейн-технологія, яка забезпечує децентралізованість, прозорість і високий рівень захищеності.

Блокчейн-технологія відіграє центральну роль у забезпеченні прозорості процесу голосування. Завдяки децентралізованому зберіганню інформації всі дії системи можуть бути верифіковані учасниками, що виключає можливість фальсифікацій. Крім того, блокчейн дозволяє автоматизувати багато ключових

аспектів процесу, таких як підрахунок голосів і перевірка цілісності даних, що значно знижує ризики людських помилок [40].

Таким чином, розробка моделі процесу голосування не лише забезпечує структурованість і злагодженість усіх етапів виборів, але й створює фундамент для довіри до системи з боку виборців, незалежно від її масштабу чи специфіки. Модель має враховувати всі технічні, організаційні та функціональні аспекти, щоб стати надійним інструментом для проведення виборів у сучасному цифровому світі.

Модель процесу голосування включає кілька основних етапів.

- Перший етап – це реєстрація виборців. На цьому етапі кожен виборець проходить ідентифікацію, яка може базуватися на цифрових підписах, біометричних даних або використанні національного ідентифікаційного номера. Після реєстрації виборцю надається унікальний ключ, що дозволяє брати участь у голосуванні. Ця інформація фіксується в блокчейні для подальшої перевірки без зберігання персональних даних.
- Другий етап – аутентифікація виборців, яка підтверджує право користувача на участь у голосуванні. Користувач надає свій приватний ключ, який звіряється з даними, записаними у блокчейні. Після успішної аутентифікації виборець отримує доступ до виборчого бюлетеня.
- На третьому етапі відбувається сам процес голосування. Виборець робить свій вибір, який шифрується за допомогою криптографічного алгоритму для забезпечення конфіденційності. Шифрований голос передається до пулу транзакцій, де він очікує підтвердження іншими вузлами мережі. Це дозволяє зберігати анонімність виборців і захищає їхній вибір від зовнішнього втручання. Загальний алгоритм майнингу для підтвердження транзакцій і додавання нового блоку до блокчейну зображено на рисунку 2.5.

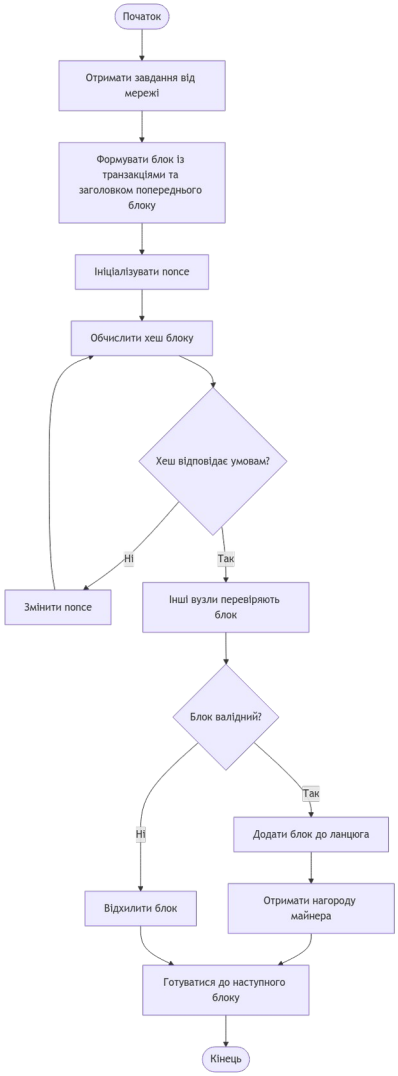

Рисунок 2.5 — Блок-схема загального алгоритму майнингу

- Четвертий етап передбачає обробку та підтвердження голосів. Усі голоси обробляються децентралізованою мережею вузлів, які підтверджують їхню коректність за допомогою алгоритму консенсусу. Після цього голос додається до нового блоку, який синхронізується між усіма вузлами мережі. Такий підхід гарантує незмінність даних і прозорість процесу.

- П'ятий етап – підрахунок голосів. Він здійснюється автоматично за допомогою смарт-контрактів, що забезпечує швидкий і точний підрахунок без участі людини. Смарт-контракти аналізують інформацію, записану у блокчейні, і визначають результати виборів. Блок-схема алгоритму цього етапу зображено на рисунку 2.6.

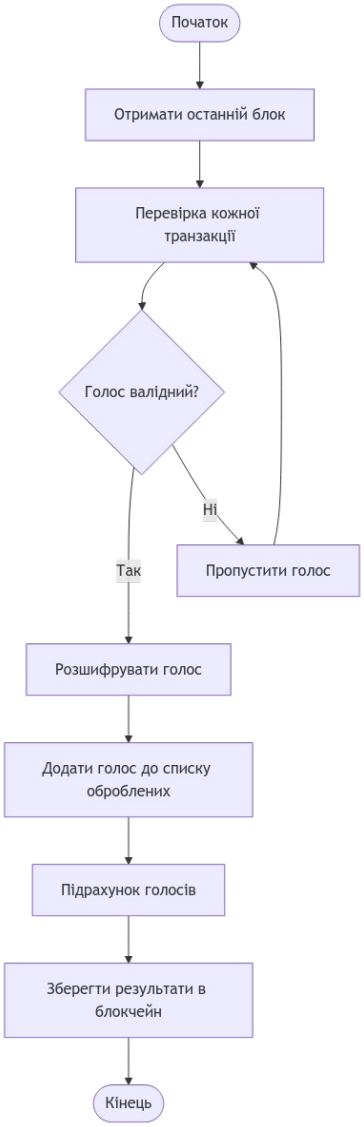

Рисунок 2.6 — Блок-схема алгоритм підрахунку голосів в блокчейн-системах голосування

- Шостий, завершальний етап – перевірка результатів. Усі учасники виборчого процесу можуть переконатися у коректності підрахунку, переглянувши дані у блокчейні. При цьому анонімність виборців зберігається, а дані про їхні голоси залишаються зашифрованими.

Модель процесу голосування базується на кількох ключових принципах. Конфіденційність забезпечується шифруванням голосів, що унеможливлює ідентифікацію виборців. Прозорість досягається за рахунок відкритого доступу до даних у блокчейні, які не можуть бути змінені без згоди більшості учасників мережі. Захищеність системи гарантується криптографічними алгоритмами та

децентралізованою структурою. Автоматизація процесу дозволяє мінімізувати людський фактор, що знижує ризик помилок і маніпуляцій.

Розроблена модель є універсальною та адаптованою для використання у «розумних містах». Вона враховує особливості сучасного виборчого процесу, забезпечує високий рівень довіри та безпеки, а також дозволяє детально показати, як працює система на всіх етапах.

2.5 Висновки до другого розділу

Дослідження та вибір технологій і методів реалізації електронного голосування на основі блокчейн дозволили визначити ключові аспекти для створення ефективної, безпечної та масштабованої системи. Концептуальні основи блокчейн-технології, такі як децентралізація, прозорість і незмінність даних, забезпечують фундамент для впровадження інноваційних рішень у виборчі процеси.

Сформульовані вимоги до системи голосування, включаючи високий рівень безпеки, пост-квантовий захист і зручність використання, визначають критично важливі параметри, які необхідно враховувати на етапі розробки. Вибір відповідної платформи та архітектури системи дозволив адаптувати технологію до сучасних викликів, таких як необхідність масштабування для великих спільнот або інтеграція з іншими сервісами «розумних» міст.

Розроблена модель процесу голосування забезпечує комплексний підхід до реалізації всіх етапів, від реєстрації виборців до підрахунку голосів, з урахуванням вимог прозорості та захищеності. Отримані результати створюють надійну основу для подальшого впровадження системи електронного голосування, здатної відповідати потребам як локальних громад, так і масштабних державних ініціатив.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ГОЛОСУВАННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ

3.1 Розробка прототипу системи голосування з використанням блокчейн-технологій

Розробка прототипу системи голосування є важливим кроком для перевірки функціональності та ефективності моделі, описаної у попередніх розділах. Прототип реалізовано за допомогою платформи .NET WebAssembly, яка дозволяє створювати високопродуктивні веб-застосунки, що працюють безпосередньо у браузері, з мінімальними вимогами до серверної інфраструктури. Це робить систему особливо перспективною для інтеграції у цифрову інфраструктуру «розумних» міст, де ключовим є забезпечення доступності та зручності використання для громадян.

Для зберігання даних використовується SQLite, що забезпечує локальне зберігання та високу швидкість доступу до даних у рамках тестового середовища. Такий підхід дозволяє адаптувати систему для використання у міських ініціативах, таких як електронні референдуми або бюджети участі, сприяючи розвитку демократичних процесів у сучасних міських спільнотах.

Прототип складається з клієнтської частини, яка працює у браузері, та локальної бази даних SQLite, що використовується для зберігання інформації про виборців, голоси та блоки. Основна логіка роботи системи реалізована на C# з використанням .NET WebAssembly.

WebAssembly (Wasm) – це сучасна технологія, яка дозволяє виконувати високопродуктивний код у веб-браузері. Вона була створена для забезпечення швидкості та ефективності, які традиційно були доступними лише у нативних застосунках. WebAssembly працює як компактний, низькорівневий байт-код, який може виконуватися у браузерах практично безпосередньо, що забезпечує значно вищу продуктивність порівняно з JavaScript. Завдяки підтримці багатьох мов програмування, таких як C#, C++, Rust, і Python, WebAssembly відкриває

можливості для розробки складних застосунків, таких як системи голосування, прямо у веб-середовищі [41].

Основною перевагою WebAssembly є його сумісність із сучасними браузерами та здатність працювати кросплатформно без додаткових плагінів. WebAssembly забезпечує безпеку, працюючи у «пісочниці», яка ізолює виконуваний код від решти системи, знижуючи ризики для безпеки. Крім того, WebAssembly підтримує інтеграцію з JavaScript, що дозволяє легко розширювати існуючі веб-застосунки без значного переписування коду. У контексті блокчейн-систем голосування WebAssembly забезпечує швидку обробку транзакцій, надійність алгоритмів шифрування та доступ до локальних баз даних, таких як SQLite, що робить цю технологію ідеальним вибором для прототипів і готових рішень. Порівняння в швидкодії WebAssembly та JavaScript у різних браузерах зображено на рисунку 3.1.

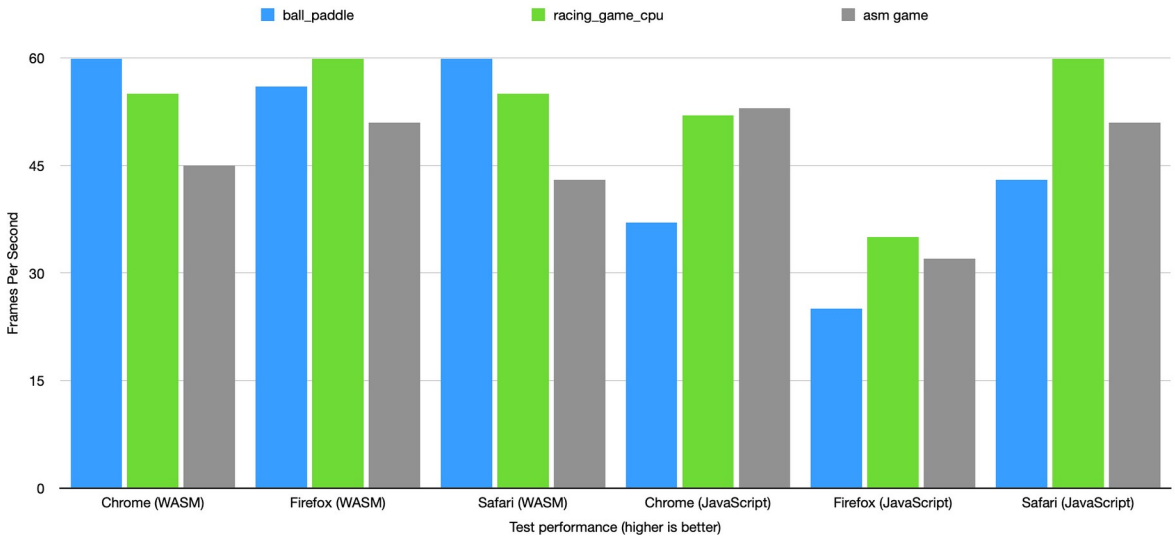

Рисунок 3.1 — Діаграма порівняння швидкодії WebAssembly та JavaScript у різних браузерах [42]

Компоненти системи:

- клієнтська частина: клієнтський застосунок є основним інтерфейсом для виборців. Він дозволяє реєструватися у системі, проходити аутентифікацію, переглядати бюлетень та подавати голоси. Уся логіка виконання запитів до бази даних та блокчейн-алгоритмів реалізована безпосередньо у клієнтській частині,

що мінімізує навантаження на сервер. Вигляд клієнтської частини зображено на рисунку 3.2.

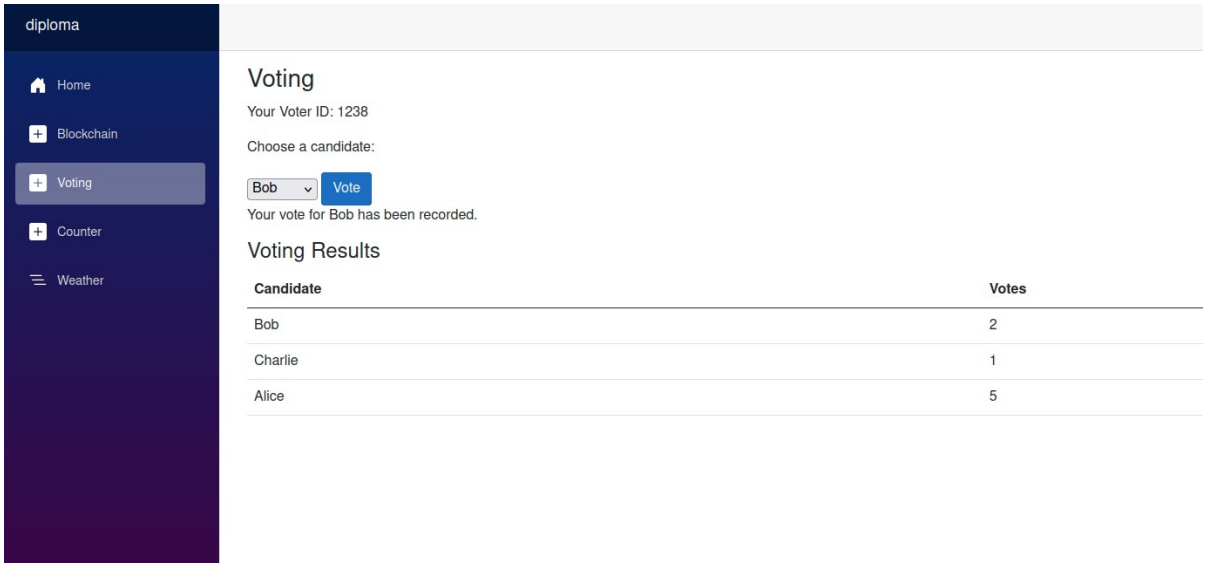

Рисунок 3.2 — Інтерфейс клієнтської частини прототипу системи голосування з використанням блокчейн-технологій

- Використання SQLite: база даних SQLite інтегрована у клієнтську частину прототипу та використовується для зберігання тимчасових даних, таких як реєстр виборців, список кандидатів та транзакції з голосами. Це забезпечує швидкий доступ до даних без необхідності постійного підключення до зовнішнього сервера.

- Реалізація блокчейну: блокчейн реалізовано у вигляді локальної структури даних, що симулює повноцінну децентралізовану мережу. Кожен блок містить такі елементи: шифрований голос виборця, хеш попереднього блоку, цифровий підпис, що підтверджує автентичність блоку, мітка часу, що фіксує момент створення блоку.

Для додавання нового блоку до ланцюга використовуються алгоритми хешування, які гарантують незмінність даних.

Також створено інтерфейс для перегляду записів блокейну, його можна побачити на рисунку 3.3.

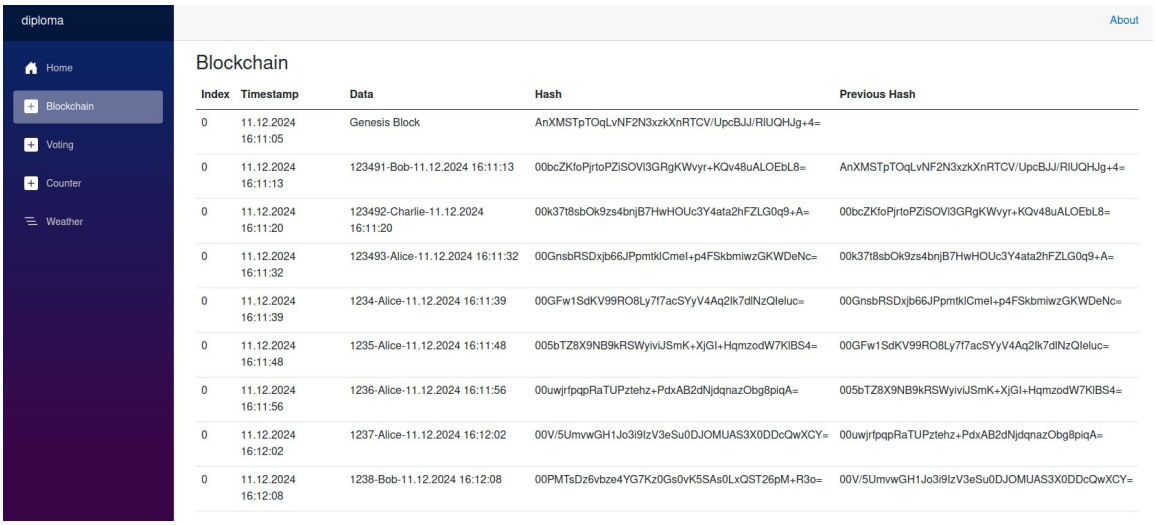

Рисунок 3.3 — Інтерфейс для виводу інформації про блоки

Застосовано алгоритм хешування SHA3-256 який є стійким до квантових обчислень побудований на Keccak-архітектурі.

Keccak-архітектура заснована на губчастій структурі, яка поділяє алгоритм на два етапи:

- поглинання (Absorbing): початкові дані (вхідне повідомлення) обробляються шляхом поділу на блоки фіксованого розміру [43].
- Видача (Squeezing): після обробки даних, генерується вихідний хеш, що має заданий розмір (256 біт для SHA3-256) [43].

Схему роботи алгоритму SHA3-256 зображено на рисунку 3.4.

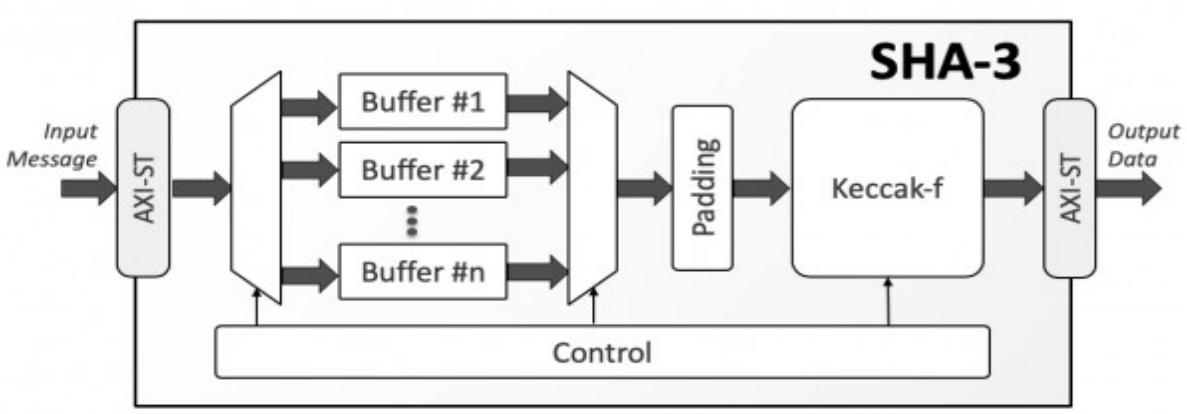

Рисунок 3.4 — Схема роботи алгоритму SHA3-256 [44]

Вхідні дані для хешування перетворюються наступним чином:

- вхідні дані (інформація про блок у блокчейні) перетворюються в бінарну форму.
- До даних додається спеціальне доповнення (padding), щоб їх довжина стала кратною блоку, який використовується Keccak.

Після доповнення дані проходять через ряд ітерацій Keccak-функції, яка виконує:

- Підстановки (Substitutions): замінює бітові групи на нові значення.
- Перестановки (Permutations): перемішує бітові блоки для кращої ентропії.
- Побітові операції XOR між вхідними даними та внутрішнім станом алгоритму.

Коли дані поглинуті, алгоритм переходить до генерації (squeezing) хешу. У разі SHA3-256 генерується 256-бітний вихід, що є унікальним представленням вхідного повідомлення.

Причинами квантової стійкості алгоритму SHA3-256 є:

- квантовий алгоритм Гровера який може зменшити обчислювальні зусилля для знаходження прообразу хеш-функції з 2^n до $2^{n/2}$, де n — розмір хешу [45].
- У SHA3-256 з розміром хешу 256 біт складність атаки становитиме 2^{128}, що є практично непосильним навіть для квантових комп'ютерів.
- Використання губчатої структури дає можливість інтегрувати додаткові параметри для адаптації до майбутніх загроз [46].
- Keccak має кращу ентропію (розподіл випадковості), що ускладнює пошук колізій навіть із використанням потужних квантових обчислень.

Для забезпечення надійності та узгодженості даних у прототипі було впроваджено консенсусний алгоритм Proof of Authority (PoA). Цей алгоритм був обраний для прототипу з огляду на його високу продуктивність та відповідність вимогам локальної тестової мережі.

Proof of Authority (PoA) – це алгоритм консенсусу, який покладається на обмежену кількість довірених вузлів (валідаторів), які підтверджують транзакції та додають нові блоки до блокчейну [47]. У даному випадку ролі валідаторів

виконують спеціально налаштовані вузли, які відповідають за перевірку голосів та додавання блоків.

Особливості реалізації PoA у прототипі:

- висока продуктивність: завдяки обмеженій кількості валідаторів, PoA забезпечує швидке підтвердження транзакцій і мінімальні затримки при додаванні блоків.
- Захищеність: у прототипі доступ до ролі валідаторів суворо обмежений, що запобігає несанкціонованому доступу до мережі.

Робота консенсусного алгоритму:

- кожен новий блок, що містить зашифрований голос, пропонується одним із валідаторів.
- Інші вузли мережі перевіряють валідність запропонованого блоку, включаючи перевірку відповідності хешу попереднього блоку та цілісності даних.
- Після успішної перевірки блок додається до блокчейну, а всі вузли синхронізують свою копію реєстру [47].

Переваги PoA для голосування:

- мінімальні затрати на обчислювальні ресурси, що знижує вимоги до обладнання.
- Висока швидкість роботи, що важливо для оперативного підрахунку голосів у масштабних виборах.
- Контрольований доступ до ролі валідаторів, який підвищує безпеку мережі.

Обмеження PoA:

- залежність від валідаторів може створювати ризики у разі компрометації довірених вузлів.
- Менш децентралізований підхід у порівнянні з PoW або PoS.

У прототипі PoA став основою для створення ефективної моделі консенсусу, яка дозволяє перевіряти концепцію роботи системи та її функціональність. Подальше розширення системи може передбачати

впровадження більш складних алгоритмів консенсусу, таких як PoS, для забезпечення кращої масштабованості та децентралізації.

База даних SQLite відіграє ключову роль у клієнтській частині прототипу системи голосування, забезпечуючи ефективне та локальне зберігання даних. SQLite – це легковагова реляційна база даних, яка ідеально підходить для застосунків, що працюють у веб-браузері, оскільки не потребує окремого серверного середовища для своєї роботи. У контексті прототипу голосувальної системи SQLite використовується для організації та управління тимчасовими даними, що є важливими для функціонування системи [48].

У межах клієнтської частини застосунку SQLite використовується як центральний інструмент для управління даними, з якими взаємодіють виборці. Коли користувач реєструється у системі, його дані одразу зберігаються у базі даних, і подальші запити на аутентифікацію виконуються локально. Аналогічно, після того як виборець подає голос, ця транзакція зберігається у базі до підтвердження через алгоритм консенсусу, після чого вона синхронізується з блокчейном.

SQLite також використовується для реалізації тестового середовища, у якому можна симулювати багатокористувацькі сценарії голосування, перевіряючи, як система реагує на велику кількість транзакцій одночасно. Це дозволяє виявляти потенційні вузькі місця у роботі застосунку до його масштабування.

Процес роботи системи:

- реєстрація виборців: виборці створюють обліковий запис, який зберігається у локальній базі даних SQLite. При цьому система генерує пари ключів (публічний та приватний), які використовуються для підпису транзакцій.
- Аутентифікація: при вході у систему виборець вводить свої дані. Після успішної перевірки йому надається доступ до функціоналу голосування. Програмний інтерфейс дозволяє легко додавати різноманітні методи аутентифікації такі як BankID, що буде корисно при широкому впровадженні системи та більшою інтеграцією в правовому полі.

- Голосування: виборець обирає свого кандидата у веб-інтерфейсі. Після цього система шифрує його вибір, додає голос до черги транзакцій та створює новий блок.
- Додавання блоку: транзакції перевіряються за допомогою алгоритму консенсусу. Після підтвердження блок додається до локального ланцюга, який синхронізується з іншими вузлами у тестовому середовищі.
- Підрахунок голосів: смарт-контракт аналізує дані з блокчейну, підраховує голоси та виводить результати виборів.

Технічні переваги прототипу:

- використання .NET WebAssembly забезпечує високу продуктивність і кросплатформність, дозволяючи запускати систему у будь-якому сучасному браузері.
- інтеграція SQLite дозволяє швидко зберігати та отримувати дані без складної конфігурації серверної частини.
- блокчейн-алгоритми реалізовані у компактній формі, що підходить для тестування концепції у невеликому середовищі.

Розроблений прототип демонструє основні принципи роботи системи голосування з використанням блокчейн-технологій. Використання .NET WebAssembly та SQLite дозволило створити легкий і функціональний клієнтський застосунок, який може бути базою для подальшого розширення системи та її адаптації для реальних умов. Цей підхід також забезпечив прозорість і деталізацію роботи кожного етапу, що є важливим для довіри до системи голосування.

3.2 Тестування системи

Тестування системи голосування є невід’ємною частиною процесу її розробки та впровадження, особливо в контексті інтеграції в інфраструктуру «розумних» міст, де важливо забезпечити безпеку, прозорість і зручність для широкого кола користувачів.

Підходи до тестування:

- функціональне тестування: перевірка відповідності основних функцій системи технічним вимогам. На цьому етапі тестуються реєстрація виборців, аутентифікація, подання голосів, обробка транзакцій у блокчейні та підрахунок результатів [49].

- Тестування зручності використання: перевірка інтерфейсу на зручність для користувачів. Залучаються тестові групи, які оцінюють легкість навігації, зрозумілість елементів управління та зручність роботи із системою [49].

- Тестування безпеки: аналіз стійкості системи до різних видів атак, включаючи: спроби несанкціонованого доступу до даних виборців, атаки типу «людина посередині» під час передачі голосів, спроби зміни транзакцій у блокчейні [50].

- Тестування продуктивності: оцінка здатності системи обробляти велику кількість одночасних транзакцій, що важливо для масштабованості. Використовуються навантажувальні тести для визначення максимального числа користувачів, які можуть працювати із системою без зниження її продуктивності [51].

- Тестування інтеграції: перевірка взаємодії між усіма компонентами системи, включаючи фронтенд, блокчейн, базу даних SQLite та смарт-контракти. Мета – забезпечити узгоджену роботу всіх модулів.

Етапи тестування:

- підготовка тестового середовища: створюється тестова мережа блокчейну з обмеженою кількістю вузлів, що імітує реальну роботу системи. У базу даних SQLite вносяться тестові дані про виборців, їхні ключі та можливі транзакції.

- Написання тестових сценаріїв: сценарії розробляються для покриття всіх можливих сценаріїв використання системи, включаючи: успішне голосування, спробу повторного голосування одним виборцем, перевірку запису транзакцій у блокчейн.

- Виконання тестів: усі тести виконуються як автоматично, так і вручну. Результати тестування фіксуються для аналізу та виправлення помилок.

- Аналіз результатів: за підсумками тестування аналізуються всі виявлені помилки, недоліки в роботі системи та можливі шляхи їх усунення.

- Перевірка виправлень: після внесення змін до коду система тестується повторно, щоб переконатися у відсутності нових помилок.

Для автоматизації тестування були написані юніт-тести. Створення тестового проєкту зображено на рисунку 3.5.

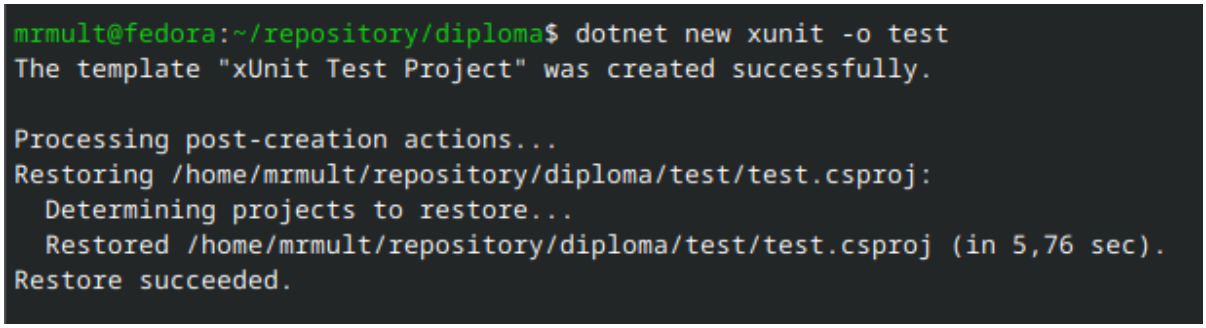

Рисунок 3.5 — Процес створення проєкту для автоматизованого тестування блокчейн-системи

Для функціонального тестування були написані наступні сценарії автоматичного тестування:

- Blockchain_CreatesGenesisBlock: перевірка, що під час створення нового блокчейну додається Genesis-блок із коректними значеннями.

- Blockchain_AddBlock_AddsBlockToChain: перевірка, що новий блок додається до ланцюга блоків із правильними даними.

- Blockchain_AddVote_AddsVoteToChain: перевірка, що голос успішно додається до блокчейну у вигляді нового блоку з правильними даними.

- Blockchain_HasVoted_ReturnsTrueIfVoterExists: перевірка, що метод `HasVoted` повертає `true`, якщо виборець із вказаним ідентифікатором вже голосував.

- Blockchain_HasVoted_ReturnsFalseIfVoterDoesNotExist: перевірка, що метод `HasVoted` повертає `false`, якщо виборець із вказаним ідентифікатором ще не голосував.

- Blockchain_GetResults_ReturnsCorrectVoteCounts: перевірка, що метод `GetResults` повертає коректні підрахунки голосів для кожного кандидата.

- Blockchain_PreventsDuplicateVotes: перевірка, що система не дозволяє одному виборцю голосувати більше одного разу, навіть якщо спроба повторного голосування здійснюється з іншим вибором.

За результатами функціонального тестування підтверджено, що система коректно обробляє реєстрацію виборців, подання голосів і підрахунок результатів. Тестування безпеки показало, що всі дані голосів зашифровані належним чином, а система стійка до спроб змінити транзакції у блокчейні.

Для тестування продуктивності системи було написано кілька юніт-тестів:

- Blockchain_Performance_AddingManyVotes: перевірка здатності системи до отримання великої кількості голосів одночасно. Згідно тестів, обробка 10000 голосів займає 4,24 секунди, без врахування спілкування між вузлами та передачею даних мережею.

- Blockchain_Performance_GetResults: перевірка швидкості системи в обрахунку переможця голосування при тисячах голосів. Згідно тестів, отримання результатів голосування на 10000 голосів займає 0,078 секунди.

Продуктивність системи відповідає очікуваним параметрам, забезпечуючи стабільну роботу для одночасної участі тисяч виборців.

Для тестування безпеки даних було написано кілька юніт-тестів, а саме:

- Blockchain_Security_DoesNotAllowTamperingWithBlocks: перевіряє, що зміна даних у блоці призводить до зміни хешу, що порушує послідовність блокчейну.

- Blockchain_Security_DetectsInvalidChain: перевіряє, чи блокчейн здатний виявити, якщо послідовність хешів порушена через зміну даних у блоці.

Результат виконання усіх тестів зображено на рисунку 3.6.

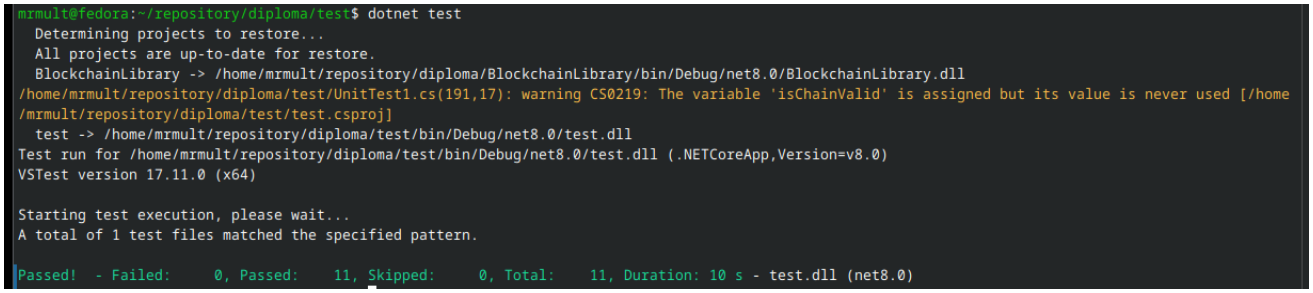

Рисунок 3.6 — Результат виконання написаних юніт-тестів

Тестування системи дозволило виявити та усунути недоліки на ранніх етапах розробки, що значно підвищило її надійність і готовність до використання у реальних умовах. Завдяки ретельним перевіркам були оцінені всі ключові аспекти роботи системи, зокрема коректність обробки даних голосування, стійкість до зовнішніх атак, продуктивність при високому навантаженні та відповідність технічним і юридичним вимогам. Проведені тестування також дозволили оптимізувати взаємодію між компонентами системи, що сприяло підвищенню її швидкодії та ефективності. Результати перевірок підтвердили, що система відповідає високим стандартам функціональності, безпеки та продуктивності, забезпечуючи надійність навіть у складних сценаріях. Це дає підстави для впевненості у здатності системи ефективно працювати у масштабах «розумних» міст, гарантуючи безпечне, прозоре та доступне електронне голосування для широкого кола користувачів.

3.3 Аналіз результатів і перспективи впровадження

Аналіз результатів розробки та тестування системи голосування демонструє її повну відповідність поставленим вимогам щодо безпеки, прозорості та ефективності. Система враховує всі критичні аспекти, зокрема захист персональних даних виборців, гарантії анонімності, відсутність можливостей для маніпуляцій чи фальсифікацій. Впроваджена технологія на основі блокчейну забезпечує не лише високий рівень захищеності даних, але й створює децентралізовану інфраструктуру, що унеможливлює несанкціоновані зміни інформації в системі. Крім того, прозорість блокчейн-технології дозволяє виборцям і незалежним спостерігачам переконатися в чесності та точності результатів, що підвищує довіру до процесу голосування. Ефективність системи проявляється також у її здатності працювати в умовах великого навантаження, забезпечуючи стабільність та оперативність навіть у масштабах національних виборів або інтеграції з іншими сервісами «розумного» міста.

Результати розробки та тестування:

- функціональність системи: усі ключові етапи процесу голосування, включаючи реєстрацію виборців, шифрування голосів, запис транзакцій у блокчейн та автоматичний підрахунок результатів, реалізовані та протестовані. Виявлені під час тестування помилки були оперативно усунені.

- Безпека: система продемонструвала високий рівень стійкості до загроз. Шифрування даних та механізми хешування забезпечують захист голосів від несанкціонованого доступу та змін. Алгоритми консенсусу підтверджують коректність транзакцій, мінімізуючи ризики маніпуляцій.

- Продуктивність: тестування показало, що система здатна обробляти великий обсяг транзакцій у режимі реального часу. Це забезпечує стабільну роботу навіть під час голосування з високою кількістю виборців.

- Зручність використання: проведене тестування із залученням користувачів підтвердило зручність інтерфейсу. Інтуїтивно зрозумілий дизайн забезпечує простоту роботи із системою, навіть для користувачів без технічних навичок.

- Стійкість до квантових загроз: впроваджені пост-квантові алгоритми шифрування підвищують захищеність системи в умовах розвитку квантових обчислень. Це забезпечує її довгострокову надійність.

Перспективи для розумного міста:

- інтеграція з міськими сервісами: Система голосування на базі блокчейну може стати частиною комплексної екосистеми «розумного» міста, інтегруючись із платформами електронного урядування, системами управління громадським транспортом або навіть із міськими системами оплати послуг. Це дозволить створити єдину мережу цифрових послуг, доступних для громадян у зручному форматі.

- Електронне урядування: Завдяки прозорості та захищеності системи, вона може бути використана для голосування в рамках міських ініціатив, таких як бюджети участі, опитування громадської думки чи вибір проєктів для реалізації. Це сприятиме залученню мешканців до управління міським середовищем.

- Міські референдуми: Швидка та зручна організація референдумів на локальному рівні дозволить громадянам приймати рішення щодо важливих

аспектів міського життя, таких як затвердження інфраструктурних проєктів чи зміни міського бюджету.

- Розумний моніторинг громадської активності: Використання даних із системи голосування в рамках аналітичних інструментів «розумного» міста дозволить муніципалітетам краще розуміти потреби мешканців, аналізувати рівень участі громадян у різних ініціативах та ефективніше планувати подальші заходи.
- Стимулювання довіри до міської інфраструктури: Завдяки прозорості голосування, мешканці отримують впевненість у чесності та ефективності рішень, що приймаються. Це підвищує рівень задоволеності міськими послугами та активніше залучає громадян до їх використання.
- Екологічна складова: Завдяки переходу на цифрове голосування зменшуються витрати на паперові бюлетені, транспортування та утилізацію, що сприяє зниженню екологічного навантаження міста.

Система голосування, адаптована для «розумного» міста, має потенціал стати універсальним інструментом, здатним ефективно функціонувати як на локальному рівні в межах окремих громад, так і на глобальному рівні для національних чи навіть міжнародних виборчих процесів. Її впровадження створює основу для прозорої та інтерактивної взаємодії між громадянами та міською адміністрацією, сприяючи розвитку демократичних процесів та підвищенню довіри до інституцій. Система не лише оптимізує виборчі процеси, але й може інтегруватися з іншими сервісами «розумного» міста, такими як електронні референдуми, консультації з громадянами чи соціальні ініціативи, що робить міське середовище більш орієнтованим на потреби мешканців.

Попри значні переваги, впровадження системи голосування на основі блокчейн-технології супроводжується низкою суттєвих викликів. До них належать високі початкові витрати на розробку і впровадження, необхідність забезпечення масштабованості для великих виборчих процесів, вирішення питань, пов’язаних із законодавчим регулюванням, а також підготовка користувачів до роботи з новою технологією. Важливо також враховувати технічні аспекти, такі як стійкість до кіберзагроз, забезпечення стабільної роботи

під час пікових навантажень та інтеграція з існуючою міською інфраструктурою. Подолання цих викликів є критичним для успішного впровадження системи та її подальшого використання в умовах «розумних» міст.

Основні виклики:

- недостатнє розуміння нової технології серед широкого загалу: У «розумних» містах, які покладаються на цифрові рішення для покращення якості життя громадян, довіра до нових технологій є ключовим фактором. Виборці часто недовіряють технологіям, які вони не розуміють, тому необхідно провести роз'яснювальну роботу, що пояснить принципи роботи блокчейн-системи, її переваги та механізми захисту. У рамках міських ініціатив можна створити інтерактивні інформаційні платформи, організувати громадські семінари та вебінари, а також розробити освітні програми для підвищення цифрової грамотності мешканців.

- Підтримка інфраструктури: У «розумних» містах інфраструктура відіграє важливу роль у забезпеченні стабільної роботи всіх сервісів, включаючи системи голосування. Хоча блокчейн-система може працювати децентралізовано, для її функціонування потрібне належне технічне обладнання, надійні мережі передачі даних та кваліфікований персонал, здатний забезпечити її роботу. Для великих міських агломерацій це передбачає створення центрів обробки даних, інтеграцію з міськими інформаційними системами та забезпечення резервних каналів зв'язку для уникнення перебоїв у роботі.

- Відповідність національним законодавствам: У «розумних» містах часто виникає потреба гармонізувати локальні ініціативи з національним та міжнародним законодавством. Інтеграція блокчейн-системи повинна враховувати юридичні норми, які регулюють виборчий процес, захист персональних даних та використання електронних технологій. Співпраця з державними органами та місцевою адміністрацією, а також розробка спеціальних нормативних актів, що забезпечать правове регулювання нової системи, є критично важливими.

- Кібербезпека та конфіденційність: У рамках «розумного» міста блокчейн-система має забезпечувати не лише прозорість, але й захист

персональних даних виборців. Впровадження сучасних стандартів кібербезпеки та постійне оновлення алгоритмів захисту сприятимуть зниженню ризиків витоку чи зловживання даними. Крім того, необхідно врахувати питання захисту інформації на рівні міських дата-центрів.

- Складність масштабування для великих міських агломерацій: Міста з великим населенням, де одночасно можуть голосувати мільйони виборців, потребують систем, здатних масштабуватися без втрати продуктивності. Для цього можуть бути розроблені локальні вузли блокчейну, що об’єднуються у глобальну мережу міста, дозволяючи розподіляти навантаження та забезпечувати безперебійність процесу.

Шляхи подолання викликів:

- навчання та громадська залученість: розробка інтерактивних мобільних додатків і порталів, які пояснюють функціонал системи голосування, сприятиме підвищенню рівня довіри мешканців до технології.
- Технічна модернізація: інвестування в міську цифрову інфраструктуру, проведення тренінгів для технічного персоналу та розвиток мережевих технологій є основою для успішного впровадження блокчейн-рішень.
- Міжнародний досвід: залучення експертів з інших «розумних» міст, які вже впроваджують подібні системи, може стати цінним джерелом знань для уникнення можливих помилок.

Інтеграція блокчейн-системи в інфраструктуру «розумного» міста є не лише технологічним викликом, а й перспективною можливістю для підвищення ефективності управління міськими процесами, оптимізації взаємодії між громадянами та міською адміністрацією і створення комфортного, безпечного та прозорого середовища. Використання блокчейн-технології дозволяє забезпечити не тільки захист даних і зменшення ризиків несанкціонованих втручань, але й посилює довіру до електронного урядування, яке стає фундаментом сучасного управління містами.

Система голосування, побудована на основі блокчейн-технології, є важливим етапом трансформації виборчих процесів, що охоплює як локальні громади, так і державний рівень. Вона створює умови для залучення більшої

кількості громадян до прийняття рішень завдяки простоті використання, високому рівню захисту даних і гарантованій прозорості результатів. Її впровадження сприятиме підвищенню ефективності управління громадськими ресурсами, зниженню витрат на організацію виборів і зменшенню людського фактора у виборчих процесах.

Крім того, така система стане важливим кроком на шляху до створення інноваційного суспільства, де технології служать не лише для вирішення технічних завдань, але й для зміцнення демократичних цінностей, забезпечуючи відкритість і доступність для всіх громадян. Інтеграція блокчейн-систем у міську інфраструктуру відкриває широкі можливості для подальшого розвитку «розумних» міст, формуючи міцний зв’язок між технологіями, громадянами та міським управлінням.

3.5 Висновки до третього розділу

Розроблений прототип системи електронного голосування продемонстрував високий рівень готовності технології до реального впровадження, поєднуючи безпеку, прозорість і продуктивність. Використання платформи .NET WebAssembly дозволило створити ефективний і легкий веб-застосунок, що мінімізує залежність від серверної інфраструктури. Це забезпечує легкість у розгортанні системи навіть у містах із обмеженими технічними ресурсами, роблячи її доступною для широкого кола користувачів. Такий підхід сприяє масштабуванню системи та її інтеграції в цифрову екосистему «розумних» міст, де важливими є доступність, швидкість обробки даних та здатність до інтеграції з іншими цифровими сервісами, наприклад, системами електронного урядування чи міського управління.

Тестування системи показало її повну відповідність заданим вимогам. Система забезпечує високий рівень захисту даних, прозорість процесу голосування та стабільність навіть за умови високого навантаження. Практичні випробування підтвердили її стійкість до зовнішніх загроз, таких як спроби несанкціонованого втручання чи кібератаки, що є критично важливим у

сучасному інформаційному середовищі. Особливо позитивно відзначено інтуїтивно зрозумілий інтерфейс, що отримав високу оцінку від тестувальників, включаючи користувачів із мінімальним технічним досвідом.

Ключовим технічним рішенням стало впровадження пост-квантового шифрування, що забезпечує довгострокову безпеку даних в умовах швидкого розвитку квантових технологій. Це інноваційне рішення гарантує, що система залишатиметься захищеною навіть у майбутньому, коли традиційні методи криптографії можуть стати вразливими. Таким чином, технологія не лише задовольняє сучасні вимоги безпеки, але й забезпечує стратегічний запас надійності на роки вперед.

Практична реалізація системи на основі блокчейн підтвердила її ефективність, адаптивність і готовність до реального впровадження. Система закладає надійну основу для інтеграції в інфраструктуру сучасних «розумних» міст, підвищуючи довіру громадян до виборчого процесу. Її використання відкриває нові можливості для автоматизації управлінських процесів, сприяючи демократизації прийняття рішень. Це рішення є значним кроком уперед у побудові цифрових сервісів, які відповідають сучасним викликам і потребам майбутнього суспільства, забезпечуючи стабільність, ефективність і інноваційність міського управління.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Показники ефективності та заходи щодо покращення умов та охорони праці

Охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів, спрямованих на збереження здоров'я, працездатності й безпеки працівників у процесі їхньої діяльності. У сучасному світі, де технології відіграють ключову роль у багатьох сферах, зокрема у «розумних містах», охорона праці виходить на новий рівень. Ефективне управління цим напрямом залежить від здатності оцінювати та підвищувати результативність впроваджених заходів, використовуючи чіткі й обґрунтовані показники ефективності.

Для забезпечення високої якості охорони праці необхідно регулярно оцінювати її стан за допомогою кількісних та якісних показників. Ці показники дозволяють не лише виявляти проблеми, але й планувати подальші дії з покращення умов роботи.

Показники ефективності охорони праці:

- рівень виробничого травматизму та професійних захворювань — зниження рівня травматизму є основним критерієм ефективності заходів з охорони праці. Аналіз включає кількість зареєстрованих випадків травматизму та їх тяжкість, а також кількість працівників, які отримали професійні захворювання.
- Часові втрати через нещасні випадки та захворювання — показник включає тривалість лікарняних листів, кількість днів простою виробництва через травматизм, що дозволяє оцінити економічні збитки.
- Відповідність умов праці нормативним вимогам — оцінюється через кількість порушень, виявлених контролюючими органами, виконання приписів та відповідність умов праці міжнародним стандартам, таким як ISO 45001.

- Економічна ефективність заходів — включає співвідношення витрат на охорону праці до економії, отриманої завдяки зниженню травматизму та втрат через простої.
- Соціальні показники — вимірюються рівнем задоволеності працівників умовами праці, зниженням плинності кадрів та покращенням психологічного клімату в колективі.
- Продуктивність праці — покращення умов праці сприяє зростанню продуктивності працівників завдяки зниженню стресу, втоми та ризиків для здоров'я.
- Рівень впровадження сучасних технологій — оцінюється часткою автоматизованих процесів, використанням новітнього обладнання та інтеграцією інформаційних систем, таких як блокчейн, для контролю за охороною праці.

Важливим аспектом є визначення та впровадження комплексних заходів, спрямованих на усунення ризиків і створення безпечних умов для працівників.

Основні заходи щодо покращення умов та охорони праці:

- встановлення сучасного обладнання — заміна застарілих технологій на сучасні, які відповідають високим стандартам безпеки, є ключовим елементом підвищення рівня охорони праці.
- Автоматизація виробничих процесів — зменшення участі людини у небезпечних операціях за рахунок автоматизації, що дозволяє мінімізувати ризики травматизму.
- Покращення санітарно-гігієнічних умов — забезпечення належного рівня освітлення, вентиляції, температурного режиму, а також чистоти робочих місць.
- Навчання працівників та інструктажі — регулярне проведення тренінгів з техніки безпеки та використання засобів індивідуального захисту. Інструктажі мають бути адаптовані до специфіки роботи кожного працівника.
- Моніторинг та оцінка ризиків — використання сучасних технологій, таких як блокчейн, для прозорого обліку даних про умови праці, результати перевірок і виконання заходів.

- Організація зон відпочинку — створення комфортних умов для відпочинку працівників сприяє покращенню їхнього психоемоційного стану та підвищенню продуктивності.
- Медичне забезпечення працівників — організація регулярних медичних оглядів та забезпечення працівників можливістю оперативного звернення до лікарів.
- Контроль за виконанням заходів — впровадження автоматизованих систем для контролю виконання заходів з охорони праці та оцінки їхньої ефективності.

У контексті «розумних міст» важливим стає використання технологій, які дозволяють досягати максимального рівня прозорості та ефективності у сфері охорони праці. Наприклад:

- системи моніторингу — виявлення небезпек у реальному часі.
- Блокчейн-технології — забезпечення захищеного обліку даних про охорону праці, що мінімізує можливість фальсифікацій.
- Інтернет речей (IoT) — контроль за станом обладнання через датчики, які передають інформацію в режимі реального часу.

Ефективне впровадження заходів з охорони праці має велике значення для організації діяльності у «розумних містах». Використання сучасних технологій та систематичний моніторинг показників ефективності дозволяють створювати безпечне та комфортне середовище для працівників, що в свою чергу сприяє підвищенню продуктивності праці, зниженню втрат і покращенню загального соціально-економічного клімату.

4.2 Суть та зміст управління охороною праці

Управління охороною праці — це комплексна діяльність, яка включає організацію, координацію, контроль та вдосконалення процесів, спрямованих на забезпечення безпечних умов праці. Головною метою є збереження життя і здоров'я працівників, а також створення безпечного середовища, яке відповідає вимогам чинного законодавства та міжнародних стандартів. У сучасних умовах,

коли технології активно впроваджуються в усі сфери діяльності, управління охороною праці стає важливим інструментом підвищення ефективності та конкурентоспроможності організацій.

Управління охороною праці базується на чітко визначених принципах, таких як пріоритет збереження життя та здоров'я працівників, системний підхід до організації безпеки, інтеграція охорони праці у всі аспекти діяльності підприємства та постійне вдосконалення. Ці принципи дозволяють адаптувати заходи до змінних умов праці та специфіки підприємства.

Суть управління охороною праці полягає у виявленні та оцінці ризиків, розробці і впровадженні заходів для їх мінімізації, а також у контролі за виконанням цих заходів. Значна увага приділяється плануванню, яке включає визначення стратегічних цілей і оперативних завдань з охорони праці, розподіл ресурсів та відповідальності.

Особливу роль відіграють навчання і підготовка працівників, що передбачають регулярні інструктажі, тренінги, лекції та використання сучасних методів, таких як симуляції або VR-технології. Ці заходи не лише підвищують обізнаність працівників, а й формують відповідальне ставлення до дотримання правил безпеки.

Управління охороною праці включає як організаційні, так і технічні аспекти. Організаційна складова передбачає створення спеціальних служб, призначення відповідальних осіб, розробку регламентів і політик. Технічна складова охоплює застосування сучасного обладнання, автоматизацію небезпечних процесів та впровадження інноваційних технологій, таких як блокчейн або IoT, для моніторингу умов праці та оцінки ефективності заходів.

Важливою складовою є санітарно-гігієнічні заходи, спрямовані на створення комфортного мікроклімату, оптимального освітлення, зниження рівня шуму та інших негативних факторів. Оцінка ризиків проводиться на основі аналізу даних, отриманих через автоматизовані системи, що дозволяє приймати обґрунтовані рішення щодо їх мінімізації.

Ефективне управління охороною праці позитивно впливає на кілька ключових аспектів. Соціальне значення полягає у збереженні здоров'я та життя

працівників, підвищенні задоволеності умовами праці та зниженні плинності кадрів. Економічне значення виражається у зниженні втрат, пов’язаних з травматизмом, витрат на компенсації та простої виробництва.

У сучасних умовах управління охороною праці стає також важливим елементом формування позитивного іміджу підприємства. Організації, які приділяють значну увагу безпеці праці, викликають більше довіри у працівників, партнерів і клієнтів, що сприяє їхньому довгостроковому успіху.

Використання інноваційних методів дозволяє зменшити ризики, підвищити продуктивність працівників і забезпечити сталий розвиток підприємства в умовах «розумних міст».

4.3 Планування заходів цивільного захисту на об’єкті у випадку надзвичайних ситуацій

Надзвичайні ситуації техногенного, природного або воєнного характеру можуть спричинити значні людські, матеріальні та екологічні втрати. Планування заходів цивільного захисту на об’єкті господарської діяльності є основною складовою забезпечення безпеки працівників, населення і збереження майна. Ефективність реагування у надзвичайних ситуаціях залежить від якості підготовки до них, що включає оцінку ризиків, створення планів дій та координацію між відповідальними службами.

Ефективне планування заходів цивільного захисту передбачає врахування широкого спектру потенційних загроз, а також адаптацію об’єкта до сучасних викликів. У першу чергу це стосується воєнних загроз, що можуть завдати значної шкоди інфраструктурі, викликати втрати серед працівників або створити загрозу вторинних уражень, таких як пожежі, обвали будівель, витоки небезпечних речовин.

Процес планування заходів цивільного захисту на об’єкті включає кілька важливих етапів:

- Оцінка ризиків та загроз — на першому етапі проводиться аналіз потенційних надзвичайних ситуацій, які можуть виникнути на об’єкті. До уваги

беруться як природні загрози (повені, землетруси), так і техногенні ризики (пожежі, витоки небезпечних речовин).

- Розробка плану дій - план дій у надзвичайних ситуаціях має охоплювати всі аспекти захисту: організацію евакуації, порядок оповіщення, надання першої допомоги та забезпечення життєзабезпечення персоналу. Він також має враховувати особливості роботи об’єкта.
- Створення резервів ресурсів — на об’єкті мають бути передбачені резерви матеріальних ресурсів, включаючи засоби індивідуального захисту, медикаменти, технічні засоби для ліквідації наслідків надзвичайних ситуацій.
- Навчання персоналу — регулярні тренування і навчання працівників забезпечують їхню готовність до реагування у випадку надзвичайної ситуації. Це може включати тренування з евакуації, роботи з засобами захисту та надання медичної допомоги.
- Моніторинг та оновлення планів — плани цивільного захисту повинні регулярно переглядатися і оновлюватися відповідно до змін у законодавстві, умов роботи або нових загроз.

У випадках загроз ракетних ударів або атак безпілотників заходи цивільного захисту мають охоплювати:

- Оперативне оповіщення — системи оповіщення мають працювати на основі даних від національних служб моніторингу, забезпечуючи попередження заздалегідь.
- Розташування критично важливих об'єктів — рекомендується розміщувати критичну інфраструктуру в підземних або укріплених приміщеннях, що дозволить мінімізувати збитки.
- Обмеження доступу до об’єкта — використання систем контролю доступу, які запобігають проникненню потенційно небезпечних осіб або пристроїв, таких як вибухівка, у межі об’єкта.
- Підготовка персоналу — працівники мають знати місця укриттів, порядок дій під час повітряної тривоги та способи реагування на вторинні загрози, наприклад, пожежі чи обвали конструкцій.

Оповіщення про надзвичайну ситуацію є ключовим елементом успішного реагування. Для цього на об’єкті встановлюються системи автоматизованого оповіщення, які забезпечують швидке інформування працівників та відвідувачів. Евакуація має бути організованою, з урахуванням безпечних шляхів виходу та зон збору.

У разі тривалих загроз важливим є забезпечення персоналу не лише укриттями, а й засобами для життєзабезпечення. Укриття повинні бути оснащені:

- запасами води, їжі та медикаментів;
- портативними системами зв’язку;
- аварійними джерелами енергії, такими як генератори або акумулятори.

План евакуації має бути адаптований до специфіки об’єкта і передбачати можливість швидкого транспортування персоналу до безпечних зон.

Для мінімізації впливу надзвичайних ситуацій використовуються засоби колективного та індивідуального захисту. Колективні засоби включають укриття, ізоляцію небезпечних ділянок та вентиляційні системи з фільтрами. Індивідуальні засоби захисту, такі як респіратори, протигази та захисний одяг, забезпечують безпеку працівників під час роботи в зонах ураження.

У разі виникнення надзвичайної ситуації важливим є налагодження ефективної взаємодії з органами місцевої влади, службами ДСНС та іншими структурами, які залучаються до ліквідації наслідків НС. Ефективний цивільний захист на об'єктах господарювання неможливий без тісної взаємодії з державними структурами. Спільні навчання, оперативний обмін інформацією та надання допомоги у разі потреби дозволяють мінімізувати ризики та зменшити наслідки надзвичайних ситуацій.

Реалії сьогодення, включаючи ракетні удари та атаки безпілотників, вимагають від об’єктів господарювання не лише планування заходів цивільного захисту, але й створення сучасних систем безпеки, здатних реагувати на нові виклики. Включення до планів специфічних заходів, таких як облаштування укриттів, впровадження систем оповіщення, підготовка персоналу та інтеграція сучасних технологій, дозволяє значно підвищити стійкість об’єкта та забезпечити збереження життя працівників. Тільки комплексний підхід до

планування і реалізації заходів цивільного захисту гарантує мінімізацію наслідків у разі надзвичайних ситуацій будь-якого характеру.

4.4 Висновки до четвертого розділу

У розділі «Показники ефективності та заходи щодо покращення умов та охорони праці» було розглянуто ключові аспекти оцінки ефективності заходів з охорони праці, а також основні напрямки їх впровадження. Зазначені аспекти є важливими для забезпечення безпеки, здоров’я та комфорту працівників, особливо в умовах розвитку «розумних міст» та сучасних викликів.

У рамках розділу були охарактеризовані основні показники ефективності, такі як рівень виробничого травматизму, відповідність умов праці нормативним вимогам, економічна ефективність заходів та соціальні аспекти, зокрема задоволеність працівників умовами роботи. Особливу увагу приділено заходам із покращення умов праці, які включають модернізацію обладнання, автоматизацію процесів, створення комфортних санітарно-гігієнічних умов та організацію навчання персоналу.

Крім того, розділ охопив питання планування заходів цивільного захисту на об’єкті у випадку надзвичайних ситуацій. У цьому контексті особливо актуальними стали питання підготовки до воєнних загроз, зокрема ракетних ударів та атак безпілотників. Було підкреслено важливість створення укриттів, забезпечення систем раннього оповіщення, організації евакуації та життєзабезпечення працівників у кризових ситуаціях.

Інтеграція сучасних технологій, таких як блокчейн, автоматизовані системи моніторингу та засоби захисту від новітніх загроз, дозволяє не лише забезпечити прозорість та контроль у сфері охорони праці, а й підвищити готовність об’єктів до надзвичайних ситуацій. Такий підхід сприяє мінімізації ризиків, збереженню життя і здоров’я працівників, а також підвищенню стійкості роботи об’єкта господарювання. Врахування цих аспектів є основою для створення безпечного, продуктивного та стійкого робочого середовища.

ВИСНОВКИ

У даній роботі було проведено всебічне дослідження блокчейн-технологій у контексті розробки системи електронного голосування для «розумних міст». Особливу увагу приділено аналізу потенціалу блокчейну для вирішення таких критичних завдань, як забезпечення прозорості виборчого процесу, запобігання фальсифікаціям та збереження конфіденційності голосів виборців. Здійснено детальний огляд існуючих рішень, що дозволило визначити як їхні ключові переваги, так і обмеження, пов’язані з продуктивністю, масштабованістю та юридичною адаптацією. На основі проведених досліджень запропоновано практичну реалізацію системи, орієнтованої на безпеку, прозорість, децентралізованість і зручність для кінцевих користувачів, що відповідає сучасним викликам і потребам цифрового суспільства.

У першому розділі було здійснено аналітичний огляд сучасного стану електронного голосування як елемента «розумного» міста. Детально розглянуто можливості застосування блокчейн-технологій у цій сфері, включаючи їх інтеграцію з іншими сервісами «розумного» міста. Проаналізовано існуючі рішення, їх сильні та слабкі сторони. Було зроблено висновок про високий потенціал блокчейну для створення безпечних, прозорих та надійних систем голосування.

У другому розділі проведено дослідження вимог до системи електронного голосування та розроблено концептуальні основи її реалізації. Було обрано відповідну платформу та архітектуру для створення системи, а також розроблено модель процесу голосування з урахуванням технічних і юридичних вимог. Особливу увагу приділено забезпеченню конфіденційності голосування, неможливості маніпуляції даними та доступності системи для широкого кола користувачів.

У третьому розділі реалізовано прототип системи голосування на основі блокчейн-технологій, який пройшов етапи тестування. Проведено аналіз ефективності системи та виявлено її потенціал для впровадження в умовах «розумних міст». Визначено основні переваги, такі як прозорість,

децентралізованість і безпека, а також виклики, пов’язані з масштабуванням, витратами на розробку та юридичною адаптацією.

У четвертому розділі висвітлено питання охорони праці, зокрема показники ефективності заходів, спрямованих на покращення умов роботи, та управління охороною праці. Особливу увагу приділено плануванню заходів безпеки в надзвичайних ситуаціях, таких як ракетні удари або атаки безпілотників, що є актуальними у сучасних реаліях. Інтеграція цих заходів у загальну структуру безпеки об’єкта сприяє захисту життя працівників та забезпеченню стабільної роботи систем.

Таким чином, у результаті дослідження було:

- Розроблено концепцію системи електронного голосування на основі блокчейну;
- Реалізовано прототип системи, що відповідає сучасним вимогам безпеки та конфіденційності;
- Визначено перспективи впровадження системи у «розумних містах», з урахуванням інтеграції з іншими сервісами.

Результати роботи можуть бути використані для подальшого вдосконалення електронних систем голосування, а також для розробки інших сервісів на основі блокчейн-технологій. Інтеграція таких рішень у «розумні міста» сприятиме підвищенню прозорості управління, забезпеченню безпеки даних та розвитку сучасної цифрової інфраструктури.

ПЕРЕЛІК ДЖЕРЕЛ

1. Е-вибори проти популістів: як інтернет-голосування в Естонії закріпило підтримку України. Eurointegration, 2023. URL: https://www.eurointegration.com.ua/articles/2023/03/6/7157412/ (дата звернення: 11.12.2024).

2. Порахувати голоси всього за 2 години замість 2 тижнів: як в Естонії організовані електронні вибори. Rubryka, 2022. URL: https://rubryka.com/article/e-elections-estonia/ (дата звернення: 11.12.2024).

3. Електронне голосування – це бомба під легітимність виборів та суцільні ризики. Uacrisis, 2022. URL: https://uacrisis.org/uk/elektronne-golosuvannya-tse-bomba-pid-legitymnist-vyboriv-ta-sutsilni-ryzyky-zvit-komitetu-vybortsiv (дата звернення: 11.12.2024).

4. Електронне голосування як елемент виборчого процесу. DSpace UzhNU, 2023. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/66098 (дата звернення: 11.12.2024).

5. Міністерство цифрової трансформації України. «Плануємо запровадити електронне голосування на виборах». 2020. URL: https://thedigital.gov.ua/news/planuemo-zaprovaditi-elektronne-golosuvannya-na-viborakh (дата звернення: 13.12.2024).

6. РБК-Україна. «Вибори через Дію підтримують третина українців». 2024 рік. URL: https://www.rbc.ua/rus/news/golosuvannya-cherez-diyu-k-ukrayintsi-stavlyatsya-1730274584.html (дата звернення: 13.12.2024).

7. Інформатор. «Голосування на виборах президента через Дію: опитування показало, що думають про це українці». 2024. URL: https://informator.ua/uk/golosuvannya-na-viborah-prezidenta-cherez-diyu-opituvannya-pokazalo-shcho-dumayut-pro-ce-ukrajinci (дата звернення: 13.12.2024).

8. Судово-юридична газета. «Як українці ставляться до виборів в «Дії», – результати опитування». 2024. URL: https://sud.ua/uk/news/ukraine/314297-yak-

ukrayintsi-stavlyatsya-do-viboriv-v-diyi-rezultati-opituvannya (дата звернення: 13.12.2024).

9. Міністерство внутрішніх справ України. «Перше опитування в Дії від МВС і одразу рекорд». 2022. URL: https://mvs.gov.ua/uk/news/perse-opituvannya-v-diyi-vid-mvs-i-odrazu-rekord (дата звернення: 13.12.2024).

10. Київ Цифровий: електронне голосування щодо перейменування міських об'єктів. 2022. URL: https://speka.media/pereimenuvannya-vulic/derusifikaciya-kiyivskix-vulic-mistyan-zaprosuyut-progolosuvati-u-zastosunku-kiyiv-cifrovii-vmdrnv (дата звернення: 13.12.2024).

11. Більшівцівська громада: впровадження системи електронного голосування «ГОЛОС». 2023. URL: https://golos.net.ua/ (дата звернення: 13.12.2024).

12. Європейська комісія. «E-voting security in Europe». 2023. URL: https://ec.europa.eu/security-and-justice/e-voting-security (дата звернення: 13.12.2024).

13. Council of Europe. «Legal and Security Standards for Electronic Voting». 2023. URL: https://www.coe.int/e-voting-standards (дата звернення: 13.12.2024).

14. Arxiv.org. «Zero-Knowledge Proofs for Blockchain Voting Systems». 2021. URL: https://arxiv.org/abs/2111.02257 (дата звернення: 13.12.2024).

15. Swissinfo. «Switzerland’s first municipal blockchain vote hailed a success». 2018 рік. URL: https://www.swissinfo.ch/eng/business/crypto-valley_-/44230928 (дата звернення: 13.12.2024).

16. Appinventiv. «Thailand To Be The First To Use Blockchain Technology for Voting». 2020. URL: https://appinventiv.com/blog/blockchain-technology-for-voting-system/ (дата звернення: 13.12.2024).

17. Ethereum Foundation. «Енергоспоживання Ethereum». 2023 рік. URL: https://ethereum.org/uk/energy-consumption/ (дата звернення: 13.12.2024).

18. PSM7. «Блокчейн у державному управлінні України як ліки від корупції». 2022 рік. URL: https://psm7.com/uk/analytics/blokchejn-u-derzhavnomu-

upravlinni-ukra%D1%97ni-yak-liki-vid-korupci%D1%97-rejderstva-i-byurokrati%D1%97-dumka-ekspertiv.html (дата звернення: 13.12.2024).

19. Arxiv.org. «A Blockchain-based Electronic Voting System: EtherVote». 2023.
URL: https://arxiv.org/abs/2307.10726 (дата звернення: 13.12.2024).

20. SpringerLink. «https://link.springer.com/chapter/10.1007/978-3-031-58053-6_14». 2024. URL: https://link.springer.com/chapter/10.1007/978-3-031-58053-6_14 (дата звернення: 13.12.2024).

21. Venugopalan S., Homoliak I., Li Z., Szalachowski P. «BBB-Voting: 1-out-of-k Blockchain-Based Boardroom Voting». 2020. URL: https://arxiv.org/abs/2010.09112 (дата звернення: 13.12.2024).

22. Democracy Earth Foundation. «Democracy Earth». 2024. URL: https://democracy.earth/ (дата звернення: 13.12.2024).

23. Polyas GmbH. «Online Voting System». 2024. URL: https://www.polyas.com/ (дата звернення: 13.12.2024).

24. Votem Corp. «Mobile Voting Platform». 2024. URL: https://votem.com/ (дата звернення: 13.12.2024).

25. Boulé. «Blockchain Voting System». 2024. URL: https://boule.one/ (дата звернення: 13.12.2024).

26. Horizon State. «Digital Voting Platform». 2024. URL: https://horizonstate.com/ (дата звернення: 13.12.2024).

27. Duda, O., Pasichnyk, V., Lypak, H., ...Matsiuk, O., Mudrokha, V. Formation of integrated repositories of social and communication data by consolidating the resources of museums, libraries and archives in smart cities projects. CEUR Workshop Proceedings, 2021, 2870, pp. 1420–1430. URL: http://ceur-ws.org/Vol-2870/paper104.pdf (дата звернення: 13.12.2024).

28. Lypak, H., Kunanets, N., Pasichnyk, V., Veretennikova, N. Digitization Project for Historical and Cultural Heritage. 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020 - Proceedings, 2020, 2, pp. 194–198, URL: https://ieeexplore.ieee.org/document/9321993 (дата звернення: 13.12.2024).

29. Lypak, H., Kunanets, N., Veretennikova, N., Matsiuk, H., Kramar, T., & Duda, O. (2023, October). An Information System Project Using Augmented Reality for a Small Local History Museum. In 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT) (pp. 1-4). IEEE. DOI: 10.1109/CSIT61576.2023.10324194
https://ieeexplore.ieee.org/abstract/document/10324194

30. Kunanets, N., Dobrovolska, V., Filippova, N., Parviz, K., Lypak, H., Duda, O., ... & Dubrovina, L. (2020, September). Designing the Repository of Documentary Cultural Heritage. In Conference on Computer Science and Information Technologies (pp. 1034-1044). Cham: Springer International Publishing. Doi: 10.1007/978-3-030-63270-0_70

31. Липак Г., Липак Т., Кунанець Н. Проєктування інформаційної системи на основі машинного навчання для збереження та класифікації артефактів документальної спадщини. Вісник Хмельницького національного університету: технічні науки. Т. 334 № 4 (2024). С. 176-182. URL: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/351 (дата звернення: 13.12.2024).

32. Ijraset. «Development Secured Blockchain Based on Agricultural Food Supply Chain in Management System». 2024. URL: https://www.ijraset.com/research-paper/development-secured-blockchain-based-on-agricultural-food-supply-chain (дата звернення: 13.12.2024).

33. ResearchGate. «A Blockchain-based Approach to Secure Cloud Connected IoT Devices». 2021. URL: https://www.researchgate.net/figure/Smart-contract-and-its-overview_fig2_350846372 (дата звернення: 13.12.2024).

34. ResearchGate. «Understanding Consensus Mechanisms in Blockchain: A Comprehensive Overview». 2023. URL: https://www.researchgate.net/figure/PoW-algorithm-flow-2-Proof-of-Stake-PoS-is-an-alternative-consensus-protocol-that-keeps_fig1_373029688 (дата звернення: 13.12.2024).

35. CyberSet. «Квантові комп'ютери: Загроза шифруванню». 2024. URL: https://cyberset.com.ua/encryption/quantum-computers-a-threat-to-encryption/ (дата звернення: 13.12.2024).

36. Sipola, T. «Applications of Post-Quantum Cryptography». *arXiv preprint arXiv:2406.13258*, 2024. URL: https://arxiv.org/abs/2406.13258 (дата звернення: 13.12.2024).

37. TrendMicro. «Post-Quantum Cryptography: Migrating to Quantum Resistant Cryptography». 2024. URL: Post-Quantum Cryptography: Migrating to Quantum Resistant Cryptography (дата звернення: 13.12.2024).

38. Synacktiv. «Quantum Readiness: Hash-Based Signatures.» 2024. URL: https://www.synacktiv.com/publications/quantum-readiness-hash-based-signatures.html (дата звернення: 13.12.2024).

39. Binance Academy. «Binance Smart Chain vs Ethereum: What's the Difference?» 2021 . URL: https://academy.binance.com/en/articles/binance-smart-chain-vs-ethereum-what-s-the-difference (дата звернення: 13.12.2024).

40. GeeksforGeeks. «Blockchain: Hyperledger vs Ethereum». 2024. URL: https://www.geeksforgeeks.org/blockchain-hyperledger-vs-ethereum/ (дата звернення: 13.12.2024).

41. Биржа.com.ua. «Огляд популярних блокчейн-платформ для створення токенів: Ethereum, Binance Smart Chain, Solana». 2024. URL: https://birzha.com.ua/osvita/tokeny/platformy-dlya-tokeniv-ethereum-binance-smart-chain-solana-ta-inshi-oglyad-populyarnyh-blokchejn-platform-dlya-stvorennya-tokeniv (дата звернення: 13.12.2024).

42. Open Election Data Initiative. «Електронне голосування та підрахунок». 2023. URL: https://openelectiondata.net/uk/guide/key-categories/electronic-voting/ (дата звернення: 13.12.2024).

43. itProger. «Роль та майбутнє WebAssembly у веб-розробці». 2024. URL: https://itproger.com/ua/news/rol-i-budushtee-webassembly-v-veb-razrabotke (дата звернення: 13.12.2024).

44. 8bitworkshop. «Emulator Performance: WebAssembly vs. JavaScript». 2021. URL: https://8bitworkshop.com/docs/posts/2021/webassembly-vs-javascript-emulator-performance.html (дата звернення: 13.12.2024).

45. Keccak Team. «The sponge and duplex constructions». 2023. URL: https://keccak.team/sponge_duplex.html (дата звернення: 13.12.2024).

46. CAST Silicon IP Cores. «SHA-3 Secure Hash Crypto Engine». 2024. URL: https://www.cast-inc.com/security/encryption-primitives/sha-3

47. EITCA. «Quantum Search and Grover's Algorithm». 2023. URL: https://uk.eitca.org/квантова-інформація/eitc-qi-qif-основи-квантової-інформації/алгоритм-квантового-пошуку-Гроверса/алгоритм-Гроверса/Алгоритм-огляду-Гроверса/скільки-ітерацій-зазвичай-потрібно-в-алгоритмі-Гроверса-і-чому-це-число-приблизно-дорівнює-квадратному-кореню-з-n/ (дата звернення: 13.12.2024).

48. NIST (National Institute of Standards and Technology). «Proposal to Update FIPS 202 and Revise SP 800-185». 2024. URL: https://csrc.nist.gov/News/2024/proposal-to-update-fips-202-and-revise-sp-800-185 (дата звернення: 13.12.2024).

49. Itstatti. «Алгоритм Proof of Authority (PoA)». 2024. URL: https://itstatti.in.ua/crypto/1068-alhorytm-proof-of-authority-poa.html (дата звернення: 13.12.2024).

50. Freehost. «Що таке SQLite?» 2024. URL: https://freehost.com.ua/ukr/faq/wiki/chto-takoe-sqlite/ (дата звернення: 13.12.2024).

51. Wezom. «Як тестувати блокчейн-додатки для автоматизації бізнес-процесів». 2024. URL: https://wezom.com.ua/ua/blog/yak-testuvati-blokcheyn-dodatki-dlya-avtomatizatsiyi-biznes-protsesiv (дата звернення: 13.12.2024).

52. QATestLab. «Testing Blockchain Technologies». 2022. URL: https://training.qatestlab.com/blog/technical-articles/testing-blockchain-technologies/ (дата звернення: 13.12.2024).

53. QATestLab Career. «Blockchain Testing: Challenges and Best Practices». 2021. URL: https://career.qatestlab.eu/ua/blog/blockchain-testing/ (дата звернення: 13.12.2024).

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18–19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 004.9
А. А. Титжинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПОРІВНЯЛЬНИЙ АНАЛІЗ КОНСЕНСУСНИХ АЛГОРИТМІВ У КОНТЕКСТІ ЇХНЬОЇ СТІЙКОСТІ ДО АТАК

UDC 004.9
A. A. Tytzhynskyi

COMPARATIVE ANALYSIS OF CONSENSUS ALGORITHMS IN THE CONTEXT OF THEIR RESISTANCE TO ATTACKS

Консенсусні алгоритми є ключовими елементами технології блокчейн, забезпечуючи узгодженість і безпеку розподіленого реєстру. Різні алгоритми мають унікальні підходи до вирішення завдань забезпечення стійкості до атак, таких як атаки 51%, сибіл-атаки та інші види порушень. Дослідження спрямоване на порівняльний аналіз таких алгоритмів, як Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) та Practical Byzantine Fault Tolerance (PBFT) [1].

Proof of Work забезпечує безпеку через складність обчислювальних задач, що ускладнює реалізацію атак. Проте висока енергозатратність та можливість централізації через пул майнінгу є серйозними недоліками. Proof of Stake покладається на підтвердження транзакцій учасниками з найбільшими ставками. Це дозволяє зменшити енергозатрати, але підвищує ризики концентрації влади у великій кількості активів [2]. У контексті DPoS пропонується модель делегованої участі, що зменшує кількість валідаторів, роблячи мережу швидшою, але створює ризики, пов'язані з довірою до делегатів. PBFT спрямований на мінімізацію впливу зловмисників у мережах, які мають до однієї третини недобросовісних вузлів. Це робить його ефективним для приватних мереж, але малопридатним для масштабованих публічних мереж [3].

Дослідження показало, що стійкість до атак значною мірою залежить від механізмів вибору валідаторів, моделі винагороди та архітектури мережі. Наприклад, PoW ефективно протистоїть сибіл-атакам, але вразливий до атак 51% через можливість централізації майнінгу. PoS має нижчу ймовірність таких атак, але ризикує через економічну нерівність. DPoS забезпечує високу швидкість транзакцій, але залежність від обраних делегатів може стати слабким місцем. PBFT демонструє високий рівень стійкості в умовах обмеженої кількості учасників, проте його ефективність падає з ростом масштабів мережі [4]. Таким чином, вибір консенсусного алгоритму має базуватися на специфіці використання блокчейн-мережі, її розмірі, рівні довіри між учасниками та потенційних ризиках. Для публічних децентралізованих мереж найбільш підходять PoW і PoS, тоді як приватні мережі можуть використовувати PBFT для досягнення високої швидкості та безпеки [5].

Подальші дослідження мають зосереджуватися на розробці гібридних моделей, які поєднують переваги різних підходів, мінімізуючи їхні недоліки. Це дозволить забезпечити більшу стійкість блокчейн-систем до атак та підвищити їхню ефективність у різних умовах використання.

Література

1. Zhebka S. V., Vlasenko V. O., Aronov A. O., Kolodiuk A. V., 2024. Solution to the dilemma of choosing a consensus algorithm in distributed systems. TIT: Telecommunications and Information Technology. No. 3, pp. 25-34. tit.dut.edu.ua.
2. Hilevskyi O. M., 2023. Comparative analysis of existing cryptocurrencies with the PoS consensus algorithm from the perspective of effective implementation reserves in terms of speed. Diploma work. Kyiv Polytechnic Institute. ela.kpi.ua.
3. Albrecht J., Andreina S., Armknecht F., Karame G., Marson G., Willingmann J., 2024. Larger-scale Nakamoto-style Blockchains Don't Necessarily Offer Better Security. ArXiv. URL: https://arxiv.org/abs/2404.09895.
5. «Analysis of consensus mechanisms in decentralized systems», 2023. A review of various consensus algorithms, including Proof of Work, Proof of Stake, Delegated Proof of Stake, and Practical Byzantine Fault Tolerance. PeerDH. peerdh.com.
6. «Performance benchmarks of consensus algorithms for decentralized oracles», 2023. Evaluation of key performance metrics of consensus algorithms such as throughput, latency, scalability, and fault tolerance, with comparisons of PoW, PoS, DPoS, and PBFT. PeerDH. peerdh.com.

Додаток Б

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18–19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 004.9
А. А. Титжинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАХИСТ БЛОКЧЕЙНУ ВІД КВАНТОВИХ ОБЧИСЛЕНЬ

UDC 004.9
A. A. Tytzhynskyi

PROTECTION OF BLOCKCHAIN FROM QUANTUM COMPUTING

Блокчейн-технологія забезпечує прозорість і захищеність даних у багатьох сферах, таких як фінанси, логістика та охорона здоров'я. Однак із розвитком квантових обчислень постає загроза для існуючих криптографічних механізмів, які є основою безпеки блокчейну. Дослідження спрямоване на аналіз методів захисту блокчейну від квантових обчислень.

Квантові комп'ютери здатні значно прискорити виконання задач, які вважаються складними для класичних комп'ютерів. Алгоритм Шора дозволяє розв'язувати задачі факторизації та обчислення дискретного логарифма за поліноміальний час, що ставить під загрозу криптографічні алгоритми, такі як RSA та ECC, які широко використовуються в блокчейні. Для вирішення цих проблем досліджуються квантово-стійкі алгоритми, що включають криптографію на основі граток, хешів, кодів та багаточленів. Ці алгоритми забезпечують новий рівень захисту від атак квантових комп'ютерів[1].

Окрім криптографічних змін, модернізація механізмів консенсусу є важливим напрямом для посилення безпеки. Існуючі механізми, такі як Proof of Work, можуть бути замінені або модифіковані із врахуванням можливостей квантових обчислень. Досліджуються альтернативи, включаючи Proof of Stake з додатковим захистом і механізми Byzantine Fault Tolerance, що дозволяють підвищити стійкість системи до квантових атак. Гібридні системи, які поєднують класичні та квантово-стійкі алгоритми, забезпечують перехідний етап до більш безпечних стандартів [2].

Було проведено дослідження впливу квантових обчислень на найбільш поширені алгоритми блокчейну, такі як SHA-256 та ECDSA. Встановлено, що квантові комп'ютери можуть значно скоротити час підбору хешів або приватних ключів, що підвищує ймовірність атак на блокчейн-мережі. Це робить актуальним розробку нових стандартів і протоколів, які враховують можливості квантових технологій [3].

Для збереження безпеки блокчейну в умовах розвитку квантових обчислень необхідно впроваджувати квантово-стійкі криптографічні методи, адаптувати існуючі протоколи та підвищувати рівень досліджень у цій сфері. Стандартизація нових криптографічних алгоритмів та їх інтеграція в існуючі блокчейн-системи є пріоритетними завданнями для забезпечення довготривалої безпеки даних. Масштабованість і швидкодія нових рішень також повинні бути враховані при розробці цих систем, щоб вони могли відповідати сучасним вимогам [4].

Таким чином, розвиток квантових обчислень вимагає переосмислення основ безпеки блокчейну. Лише активні дослідження та інноваційні підходи дозволять зберегти довіру до технологій розподіленого реєстру в умовах квантової ери.

Література

1. Procedia Computer Science. Vol. 177, pp. 183-191. ArXiv. URL: https://arxiv.org/abs/2011.03460.
2. Allende M., López León D., Cerón S., Leal A., Pareja A., Da Silva M., Pardo A., Jones D., Worrall D., Merriman B., Gilmore J., Kitchener N., Venegas-Andraca S. E., 2021. Quantum-resistance in blockchain networks. International Journal of Quantum Information. Vol. 19, No. 7, pp. 1-15. ArXiv. URL: https://arxiv.org/abs/2106.06640.
3. Gate.io Research Team, 2023. Post-Quantum Cryptography in Blockchain Security. Blockchain Technology Research Journal. No. 12, pp. 45-52. Gate.io. URL: https://www.gate.io/uk/learn/articles/post-quantum-cryptography-in-blockchain-security/1061.
4. Cryptomus Editorial Team, 2022. Quantum Computers and Cryptocurrencies: Impact and Solutions. Journal of Blockchain Applications. Vol. 8, No. 3, pp. 27-34. Cryptomus. URL: https://cryptomus.com/uk/blog/quantum-computers-and-cryptocurrencies.

Додаток В

Програмний код прототипу голосування на основі блокчейн-технологій

Файл Program.cs

```
using diploma.Components;
using BlockchainLibrary;
using Microsoft.IdentityModel.Tokens;
using System.Text;
using Microsoft.AspNetCore.Components.Authorization;
using Microsoft.EntityFrameworkCore;

var builder = WebApplication.CreateBuilder(args);

builder.Services.AddDbContext<AppDbContext>(options =>
    options.UseSqlite(builder.Configuration.GetConnectionStrin
g("DefaultConnection"),
                      b => b.MigrationsAssembly("diploma"))); // Set
migrations assembly to "diploma"

// Add services to the container.
builder.Services.AddRazorComponents()
    .AddInteractiveServerComponents();

builder.Services.AddSingleton<Blockchain>();
builder.Services.AddScoped<AuthService>();
builder.Services.AddScoped<AuthenticationStateProvider,
CustomAuthenticationStateProvider>();


builder.Services.AddHttpClient<AuthService>(client =>
{
    client.BaseAddress = new Uri("https://localhost:5266/"); //
Вкажіть адресу вашого API
});


builder.Services.AddAuthentication("Bearer")
    .AddJwtBearer("Bearer", options =>
    {
                        options.TokenValidationParameters   =   new
TokenValidationParameters
        {
            ValidateIssuer = false,
            ValidateAudience = false,
            ValidateLifetime = true,
            ValidateIssuerSigningKey = true,
                                        IssuerSigningKey   =   new
SymmetricSecurityKey(Encoding.ASCII.GetBytes("YourSuperSecretKey"))
        };
    });

builder.Services.AddAuthorization();
builder.Services.AddControllers();


var app = builder.Build();

app.UseAuthentication();
app.UseAuthorization();

// Configure the HTTP request pipeline.
if (!app.Environment.IsDevelopment())
{
    app.UseExceptionHandler("/Error",  createScopeForErrors:
true);
    // The default HSTS value is 30 days. You may want to change
this for production scenarios, see https://aka.ms/aspnetcore-hsts.
```

```
    app.UseHsts();
}

app.UseStaticFiles();
app.UseAntiforgery();

app.MapRazorComponents<App>()
    .AddInteractiveServerRenderMode();

app.MapControllers();

app.Run();
```

Файл AuthService.cs

```
using System.Net.Http.Headers;
using System.Text.Json;
using System.Text;

public class AuthService
{
    private readonly HttpClient _httpClient;
    public string Token { get; private set; }


    public AuthService(HttpClient httpClient)
    {
        var handler = new HttpClientHandler
        {
          ServerCertificateCustomValidationCallback = (message,
cert, chain, errors) => true
        };
        _httpClient = new HttpClient(handler)
        {
            BaseAddress = new Uri("https://localhost:5266/")
        };
    }

      public async Task<bool> Login(string username, string
password)
    {
        var payload = JsonSerializer.Serialize(new { Username =
username, Password = password });
        var content = new StringContent(payload, Encoding.UTF8,
"application/json");

                                        var response = await
_httpClient.PostAsync("api/auth/login", content);
        if (response.IsSuccessStatusCode)
        {
                                                var result =
JsonSerializer.Deserialize<Dictionary<string, string>>(await
response.Content.ReadAsStringAsync());
            Token = result["Token"];
          _httpClient.DefaultRequestHeaders.Authorization = new
AuthenticationHeaderValue("Bearer", Token);
            return true;
        }
        return false;
    }

     public async Task<bool> Register(string username, string
password)
    {
        var payload = JsonSerializer.Serialize(new { Username =
username, Password = password });
        var content = new StringContent(payload, Encoding.UTF8,
"application/json");

                                        var response = await
_httpClient.PostAsync("api/auth/register", content);
        return response.IsSuccessStatusCode;
```

```
        }
    }
```

Файл AppDbContext.cs

```
using Microsoft.EntityFrameworkCore;

namespace BlockchainLibrary
{
    public class AppDbContext : DbContext
    {
            public AppDbContext(DbContextOptions<AppDbContext>
options) : base(options) { }

        public DbSet<Block> Blocks { get; set; }
        public DbSet<Vote> Votes { get; set; }
    }
}
```

Файл Block.cs

```
using System.ComponentModel.DataAnnotations;
using System.Security.Cryptography;
using System.Text;

public class Block
{
    [Key]
    public int Id { get; set; }
    public DateTime Timestamp { get; set; }
    public int Index { get; set; }
    public string Data { get; set; }
    public string PreviousHash { get; set; }
    public string Hash { get; set; }
    public int Nonce { get; private set; }

   public Block(DateTime timestamp, string previousHash, string
data)
    {
        Timestamp = timestamp;
        PreviousHash = previousHash;
        Data = data;
        Hash = CalculateHash();
    }

    public string CalculateHash()
    {
        using (var sha3 = SHA3_256.Create())
        {
            string input = $"{Timestamp}-{PreviousHash}-{Data}-
{Nonce}";
            byte[] inputBytes = Encoding.UTF8.GetBytes(input);
            byte[] hashBytes = sha3.ComputeHash(inputBytes);
            return Convert.ToHexString(hashBytes);
        }
    }

    public void MineBlock(int difficulty)
    {
        string hashValidation = new string('0', difficulty);
        Nonce = 0;

        while (!Hash.StartsWith(hashValidation))
        {
            Nonce++;
            Hash = CalculateHash();
        }
```

```
            Console.WriteLine($"Block mined with hash: {Hash}");
        }
    }
```

Файл Blockchain.cs

```
    namespace BlockchainLibrary
    {
        public class Blockchain
        {
             public List<Block> Chain { get; private set; } = new
List<Block>();
            public int Difficulty { get; private set; } = 2;

            public Blockchain()
            {
                Chain.Add(CreateGenesisBlock());
            }

            private Block CreateGenesisBlock()
            {
             return new Block(DateTime.Now, null, "Genesis Block");
            }

            public Block GetLatestBlock()
            {
                return Chain.Last();
            }

            public void AddBlock(Block newBlock)
            {
                newBlock.PreviousHash = GetLatestBlock().Hash;
                newBlock.MineBlock(Difficulty);
                Chain.Add(newBlock);
            }

            public void AddVote(Vote vote)
            {
                string voteData = vote.ToString();
                                  AddBlock(new  Block(DateTime.Now,
GetLatestBlock().Hash, voteData));
            }
            public bool HasVoted(string voterId)
            {
               foreach (var block in Chain.Skip(1)) // Пропускаємо
Genesis-блок
                {
                    var data = block.Data;
                    if (!string.IsNullOrEmpty(data))
                    {
                        var voteParts = data.Split('-');
                        if (voteParts.Length >= 2)
                        {
                            var existingVoterId = voteParts[0];
                            if (existingVoterId == voterId)
                            {
                             return true; // Виборець вже голосував
                            }
                        }
                    }
                }
                return false; // Виборець ще не голосував
            }


            public Dictionary<string, int> GetResults()
            {
                var results = new Dictionary<string, int>();
               foreach (var block in Chain.Skip(1)) // Пропускаємо
Genesis-блок
                {
                    var data = block.Data;
```

```
                    if (!string.IsNullOrEmpty(data))
                    {
                        var voteParts = data.Split('-');
                        if (voteParts.Length >= 2)
                        {
                            var candidate = voteParts[1];
                            if (results.ContainsKey(candidate))
                            {
                                results[candidate]++;
                            }
                            else
                            {
                                results[candidate] = 1;
                            }
                        }
                    }
                }
                return results;
            }
        }
    }
```

Файл Vote.cs

```
using System.ComponentModel.DataAnnotations;

namespace BlockchainLibrary
{
    public class Vote
    {

        [Key]
        public int Id { get; set; }
          public string VoterId { get; set; } // Унікальний ідентифікатор виборця
        public string Candidate { get; set; } // Кандидат, за якого проголосував виборець
       public DateTime Timestamp { get; set; } // Час голосування

        public Vote(string voterId, string candidate)
        {
            VoterId = voterId;
            Candidate = candidate;
            Timestamp = DateTime.Now;
        }

        public override string ToString()
        {
            return $"{VoterId}-{Candidate}-{Timestamp}";
        }
    }
}
```

Файл Voting.razor

```
@page "/voting/{voterId}"
@rendermode InteractiveServer
@using BlockchainLibrary
@inject BlockchainLibrary.Blockchain BlockchainService

<h3>Voting</h3>

<p>Your Voter ID: @voterId</p>

<p>Choose a candidate:</p>
<select @bind="selectedCandidate">
    @foreach (var candidate in candidates)
    {
```

```
            <option value="@candidate">@candidate</option>
        }
    </select>

    <button                 class="btn                 btn-primary"
@onclick="SubmitVote">Vote</button>

    <p>@voteMessage</p>

    <h4>Voting Results</h4>
    <table class="table">
        <thead>
            <tr>
                <th>Candidate</th>
                <th>Votes</th>
            </tr>
        </thead>
        <tbody>
            @foreach (var result in results)
            {
                <tr>
                    <td>@result.Key</td>
                    <td>@result.Value</td>
                </tr>
            }
        </tbody>
    </table>


    @code {
        [Parameter]
        public string voterId { get; set; } = string.Empty;

        private string selectedCandidate;
        private string voteMessage = "";
        private Dictionary<string, int> results = new();
           private  List<string>  candidates  =  new  List<string>
{ "Alice", "Bob", "Charlie" };

        private void SubmitVote()
        {
            voteMessage = "";
                            if   (string.IsNullOrEmpty(voterId)   ||
string.IsNullOrEmpty(selectedCandidate))
            {
                voteMessage = "Please provide a valid voter ID and
select a candidate.";
                return;
            }

            if (BlockchainService.HasVoted(voterId))
            {
              voteMessage = "You have already voted. Multiple votes
are not allowed.";
                return;
            }

            var vote = new Vote(voterId, selectedCandidate);
            BlockchainService.AddVote(vote);
             voteMessage = $"Your vote for {selectedCandidate} has
been recorded.";
            UpdateResults();
        }

        private void UpdateResults()
        {
            results = BlockchainService.GetResults();
        }

        protected override void OnInitialized()
        {
            UpdateResults();
        }
    }
```