Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Аналіз застосування блокчейну для підвищення безпеки інформаційних систем"

Виконав: студент (ка)
4 курсу, групи СБ-41
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Тюпа Іванна Олександрівна
підпис (прізвище та ініціали)

Керівник Козак Р. О.
підпис (прізвище та ініціали)
Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. 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 кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Тюпі Іванні Олександрівні
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз застосування блокчейну для підвищення безпеки інформаційних систем.

Керівник роботи Козак Руслан Орестович, к.т.н., доцент., кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «15» 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 26.06.2024

3. Вихідні дані до роботи Документи та звіти; Статистичні дані; Аналіз випадків;

4. Зміст роботи (перелік питань, які потрібно розробити)
Розкрити суть блокчейн-технології.
Проаналізувати ефективність та доцільність впровадження блокчейну.
Виявити переваги та недоліки цієї технології.
Безпека життєдіяльності, основи охорони праці.
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета, задачі кваліфікаційної роботи. Основні принципи та елементи блокчейну. Децентралізація. Ланцюг блоків. Криптографігча безпека. Смарт-контракти. Використання блокчейн-технології в різних галузях. Застосування блокчейн-технологій світовими компаніями.Аналіз переваг, ризиків та недоліків. Порівняння традиційними (централізованими) системами. Приклад 1. Застовування блокчейн для проведення виборів. Приклад 2. Застосування блокчейн для опрацювання великих даних. Приклад 3. Застосування блокчейн для безпечного зберігання даних. Порівняльний аналіз. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко Сергій Юрійович., к.т.н, доцент, кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01 – 30.01	Виконано
2.	Підбір джерел для аналізу блокчейн-технології	01.02 – 05.02	Виконано
3.	Опрацювання джерел в галузі дослідження	06.02 – 20.02	Виконано
4.	Проведення аналізу методів застосування блокчейну в інформаційних системах	22.02 – 12.03	Виконано
5.	Оцінка переваг, недоліків та ризиків блокчейн-технології	15.03-25.03	Виконано
6.	Етап порівняння та виявлення ефективності на противагу інших методів захисту	25.02 – 10.04	Виконано
7.	Оформлення розділу «Огляд блокчейн-технології»	10.02 – 05.03	Виконано
8.	Оформлення розділу «Аналіз ефективності блокчейну в різних галузях »	26.03 – 04.05	Виконано
9.	Оформлення розділу «Дослідження, класифікація та приклади реалізації блокчейн-технології для покращення безпеки»	12.04-20.04	Виконано
10.	Виконання завдання до розділу «Безпека життєдіяльності, основи охорони праці»	25.04 – 10.05	Виконано
11.	Оформлення кваліфікаційної роботи	23.05 – 08.06	Виконано
12.	Нормоконтроль	10.06 – 16.06	Виконано
13.	Перевірка на плагіат	15.06 – 18.06	Виконано
14.	Попередній захист кваліфікаційної роботи	18.06 – 21.06	Виконано
15.	Захист кваліфікаційної роботи	26.06.2024	

Студент _____ Тюпа І. О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козак Р. О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз застосування блокчейну для підвищення безпеки інформаційних систем // Кваліфікаційна робота ОР «Бакалавр» // Тюпа Іванна Олександрівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2024 // С. 58, рис. – 29, табл. – 5 , кресл. – - , додат. – -.

КЛЮЧОВІ СЛОВА: Блокчейн-технології; Децентралізація; Смарт-контракт; Розподілений реєстр; Криптографічна безпека.

Кваліфікаційна робота присвячена дослідженню та аналізу застосування блокчейну для підвищення безпеки інформаційних систем.

Роозглянуто нові підходи до забезпечення цілісності, конфіденційності та доступності інформації. Зокрема до них і відноситься блокчейн-технології, адже вони включають в себе такі принципи роботи як децентралізацію, розподілений реєстр, криптографічну безпеку та смарт-контракти. Які в свою чергу мають значні переваги при порівнянні з іншими методами забезпечення безпеки, проте варто звернути увагу також і на свої недоліки котрі можуть бути критичними для компаній/установ при виборі кваліфікованої системи захисту інформації.

Кваліфікаційна робота також може бути використана в навчанні. Адже описані елементи блокчейну, можуть бути корисними при пошуку найвигіднішого захисту безпеки інформації в різних сферах життя, таких як фінанси, медицина, громадянські права. Може слугувати прикладом для студентів, які вивчають безпеку інформаційних систем та прагнуть самостійного розвитку в даній сфері, адже в галузі використання блокчейну є досить багато цікавих напрямків які вимагають оптимізації.

ABSTRACT

Analysis of blockchain application for enhancing the security of information systems// Thesis of educational level "Bachelor"// Tiupa Ivanna Olexandrivna // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2024 // P. 58, fig. - 29, tab. - 5, chair. - , added. – -.

KEYWORDS: Blockchain technology; Decentralization; Smart contract; Distributed ledger; Cryptographic security.

The qualification work is devoted to the study and analysis of the use of blockchain to improve the security of information systems.

The new approaches to ensuring the integrity, confidentiality and availability of information have been considered. They include blockchain technologies, because they include such principles of operation as decentralization, distributed ledger, cryptographic security and smart contracts. These, in turn, have significant advantages compared to other security methods, but it is also worth paying attention to their disadvantages, which can be critical for companies/institutions when choosing a qualified information security system.

The qualification work can also be used in education. After all, the described elements of the blockchain can be useful in finding the most profitable information security protection in various areas of life, such as finance, medicine, and civil rights. It can serve as an example for students studying information systems security and seeking independent development in this area, because there are many interesting areas that require optimization in the field of blockchain use.

ЗМІСТ

ВСТУП 7
1. ОГЛЯД БЛОКЧЕЙН-ТЕХНОЛОГІЇ 8
1.1 Децентралізація 9
1.2 Ланцюг блоків 10
1.3 Криптографічна безпека 11
1.4 Математичні методи, які лежать в основі блокчейн 12
2. АНАЛІЗ ЕФЕКТИВНОСТІ БЛОКЧЕЙНУ В РІЗНИХ ГАЛУЗЯХ 16
2.1 Смарт-контракти 16
2.2 Використання блокчейн-технології в різних галузях 16
2.3 Застосування блокчейн-технологій у діяльності світових компаній 19
2.4 Аналіз переваг, ризиків та недоліків у використанні 22
2.5 Порівняння з традиційними (централізованими) системами 23
3. ДОСЛІДЖЕННЯ, КЛАСИФІКАЦІЯ ТА ПРИКЛАДИ РЕАЛІЗАЦІЇ БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ ПОКРАЩЕННЯ БЕЗПЕКИ 29
3.1 Приклад реалізації застосунку для проведення виборів 29
3.2 Досліждення розробки інформаційної системи з використанням технології блокчейн для опрацювання великих даних 37
3.3 Безпечне розподілене хмарне зберігання на основі технології блокчейн та смарт-контрактів 41
3.4 Порівняльний аналіз застосувань блокчейн-технологій в різних галузях 46
4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ 49
4.1 Розподіл підприємств, установ та організацій за ступенем ризику їхньої господарської діяльності щодо забезпечення безпеки та захисту населення і територій від НС 49
4.2 Штучне освітлення 52
ВИСНОВКИ 56
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 57

ВСТУП

Тема «Аналіз застосування блокчейну для підвищення безпеки інформаційних систем» була вибрана виходячі з огляду актуальних методів захисту і безпеки інформації. Адже вимагаючи від організацій та установ постійного удосконалення своїх заходів безпеки, технологія блокчейн виходить на передовий план як потенційний засіб для забезпечення цілісності, конфіденційності та доступності інформації.

Метою роботи є дослідження застосування блокчейн-технологій для вирішення задач кібербезпеки в інформаційних системах.

Завдання які потрібно виконати поділяються на більш теоретичні а саме, розкрити суть блокчейн-технології та проаналізувати ефективність, доцільність впровадження блокчейну. А також виявлення переваг та недоліків цієї технології на практичних прикладах.

Технологію блокчейн вперше дослідили автори G.W. Piters, E. Panayi, M. Swan, M. Iansiti, K. Lakhani. Вони показали, як блокчейн застосовується на фінансовому ринку, розглянули його перспективи, переваги та недоліки. Завдяки цьому іноземні компанії змогли швидко і ефективно впровадити блокчейн у свою діяльність. Водночас, на українському ринку криптовалюти не стали настільки популярними, і впровадження цих технологій для підприємств залишається повільним та складним процесом[6].

Робота є важливою у контексті швидкого розвитку цифрових технологій та постійної загрози кібератак. Вона спрямована на вивчення та вдосконалення підходів до забезпечення безпеки інформації.

1. ОГЛЯД БЛОКЧЕЙН-ТЕХНОЛОГІЇ

Кілька років тому криптовалюти були на піку свого розвитку, їх використання було поширене у всіх сферах життя. Ця валюта підтвердила гіпотезу про те, що світ може існувати завдяки безготівковим розрахункам і що криптовалюти стануть популярними в майбутньому. Його створення мало ще один позитивний вплив на світову економіку: відкриття технології блокчейн.

Блокчейн це розподілена і захищена від підробок база даних, яка складається з послідовних блоків інформації (див. рисунок 1.1).

Рисунок 1.1 – Приклад блокчейн-технології

Кожен блок містить запис транзакцій і хеш попереднього блоку, що забезпечує зв'язок між ними. Після додавання блоку до блокчейну його не можна змінити без зміни всіх наступних блоків, що робить дані захищеними від фальсифікації. А також всі учасники мають доступ до одного і того ж набору даних, що забезпечує прозорість транзакцій і усуває можливість шахрайства. Завдяки цьому ланцюг блоків є незмінним і прозорим. Через відсутність посередників у транзакціях, допомагає зменшити витрати і їх час проведення [14].

Атака на блокчейн буде вимагати контролю над більшістю вузлів мережі, що є практично неможливим у великих мережах [13].

Вперше створена Сатоші Накамото, анонімним розробником або групою розробників, така розподілена база даних стала основою для першої криптовалюти, біткоїну, для якого у 2008 році і була розроблена технологія блокчейн [2]. Це особливий журнал усіх транзакцій, який дозволяє вирішити проблему подвійних витрат без використання центрального сервера чи організації. Традиційні блокчейн-системи, такі як Bitcoin, мають обмежену швидкість транзакцій. Однак нові розробки, такі як блокчейн другого і третього поколінь (наприклад, Ethereum 2.0 та інші), працюють над покращенням масштабованості та швидкості [2].

1.1 Децентралізація

Децентралізація - це перехід від централізованої системи, де влада та контроль зосереджені у центральній точці, до системи, де вони розподіляються між багатьма учасниками чи вузлами[1]. В контексті блокчейну, децентралізація означає, що база даних зберігається на кожному вузлі мережі, а не централізована на одному сервері. Це забезпечує більшу стійкість до атак та надійність системи.

Упровадження децентралізації у сфері блокчейну дозволяє покращити безпеку, прозорість та автономію системи. А також надає учасникам мережі бути більш незалежними та захищеними від зовнішніх втручань. Однак варто звернути увагу на винекнення більших витрат на утримання мережі та виконання операцій.

До переваг децентралізації, особливо у контексті сфери блокчейну можна виділити вже описану стійкість мережі - якщо деякі вузли в мережі вийдуть з ладу або будуть атаковані, інші вузли продовжать працювати. Кращу безпеку даних через розподіл інформації між багатьма вузлами мережі та використання криптографічних методів шифрування. Уникненя посередників, таких як банки, знижує витрати та скорочує час проведення транзакцій [6]. З чого випливає

покращення управління власними аткивами та даними, які не залежні від організацій чи урядів.

Виходячі з цієї інформації, децентралізація сприяє покращенню безпеки, прозорості та незалежності системи, роблячи її більш стійкою до зовнішніх втручань.

1.2 Ланцюг блоків

Кожна нова група записів, яка називається блоком, пов'язана з записами попереднього блоку, створюючи «ланцюжок» згрупованих записів про транзакції, який і є «ланцюжком блоків» (див. рисунок 1.2) [6].

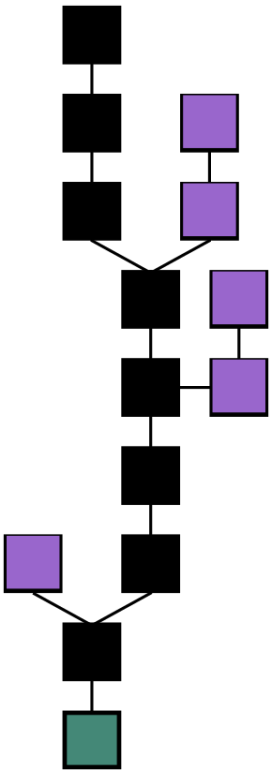

Рисунок 1.2 – Послідовність блоків

Блоки виникають в процесі, коли обчислюється алгоритмічне рішення складної в плані задачі. Таким чином, блокчейн функціонує як однорангова система розподілу.

На основі блокчейну, зокрема, для криптовалютних та грошових транзакцій, кожен користувач-платник переказує одну або більше одиниць криптовалюти одержувачу наступним чином: одержувач підписує хеш попередньої транзакції в ланцюжку разом з публічним ключем одержувача і додає результат в кінець поточного блоку, що дозволяє підтвердити транзакцію одержувачу. Кожен блок містить певний обсяг даних, таких як транзакції, текстові повідомлення або інші відомості, а також хеш-посилання на попередній блок у ланцюзі що забезпечує послідовність та незмінність [11].

Ланцюг блоків використовується для забезпечення надійного збереження даних, проведення транзакцій та реєстрації подій у різних галузях, таких як фінанси, логістика, лікарська справа, громадський сектор та багато інших.

Саме він робить процеси більш автоматизованими та безпечними для всіх учасників.

1.3 Криптографічна безпека

Криптографія має давні коріння, шифр Цезаря, вперше використаний у Римській імперії, полягав у зсуві кожної букви у тексті на певну кількість позицій у алфавіті. Це був один з перших відомих методів шифрування.

Під час світових війн, криптографія грала важливу роль у захисті військових та дипломатичних таємниць, тому було розроблено кілька складних криптографічних систем, які вплинули на перебіг війни. Дві найвідоміші з них - німецька Енігма та британська Колос.

Криптографічна безпека стала невід'ємною частиною сучасного світу, забезпечуючи захист конфіденційності та безпеки в інформаційному середовищі.

Хешування котре було описано вище, забезпечує блокчейну швидку перевірку автентичності даних, оскільки будь-які зміни в даних будуть відразу помітні через зміну хешу.

Підписи та автентифікація: Криптографія з відкритим ключем використовується для генерування цифрових підписів, які забезпечують

автентичність транзакцій [17]. Приватний ключ використовується для підпису транзакцій, а публічний ключ - для перевірки підпису [12].

Контроль доступу: Гаманці користувачів і адреси в блокчейні управляються за допомогою публічних і приватних ключів. Тільки власник приватного ключа може ініціювати транзакції з певної адреси [6].

Криптографічні методи використовуються в смарт-контрактах, котрі будуть описуватись більш детально в наступному розіді цієї роботи.

1.4 Математичні методи, які лежать в основі блокчейн

Еліптичні криві, ECDSA і ключі – це математичні методи які лежать в основі блокчейну. Один з алгоритмів криптографії які є частиною блокчейну – це алгоритм цифрового підпису на еліптичних кривих (ECDSA) використовує еліптичні криві та кінцеві поля для створення підписів даних. Він розроблений так, щоб третя сторона могла перевірити справжність підпису і виключити можливість його підробки. Підпис і перевірка в ECDSA включають різні процедури, що складаються з кількох арифметичних операцій [13].

Еліптичні криві є важливим математичним інструментом у сучасній криптографії. Вони забезпечують високий рівень безпеки при менших розмірах ключів і обчислювальних витратах, що робить їх ідеальними для використання в блокчейн-технологіях та інших криптографічних системах [13].

Алгебраїчно кожна еліптична крива може бути записана як рівняння: $y^2 = x^3 + ax + b$. У мережі криптовалюти Bitcoin використовуються коефіцієнти $a = 0$ і $b = 7$. На рисунку 1.3 показано графік цієї функції.

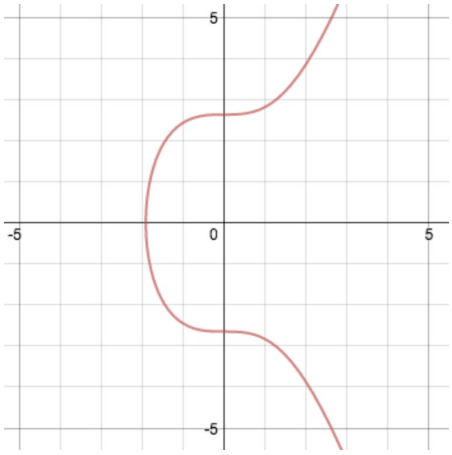

Рисунок 1.3 – Еліптична крива в Bitcoin

Сумою двох точок на даній кривій P + Q називають точкою R, яка є відображенням точки -R відносно осі X. Точка -R утворюється продовженням прямої, що проходить через точки P і Q, до її перетину з кривою (див. рисунок 1.4) [13].

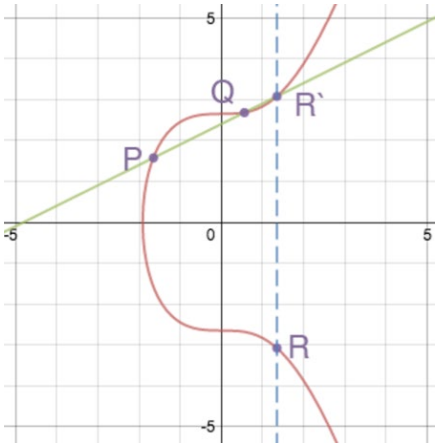

Рисунок 1.4 – Еліптична крива в Bitcoin

При проведенні прямої через дві точки з координатами P (a, b) і Q (a, -b), ця пряма буде паралельна осі ординат. У такому випадку не буде третьої точки перетину з кривою. Для вирішення цієї проблеми вводиться точка на нескінченності (point of infinity), яка позначається як O. Тому, при відсутності перетину рівняння буде мати має вигляд: P + Q = O. Якщо потрібно подвоїти точку, наклавши її саму на себе, то проводиться дотична до цієї точки. Точка перетину дотичної з кривою відображається симетрично щодо осі X (див. рисунок 1.5).

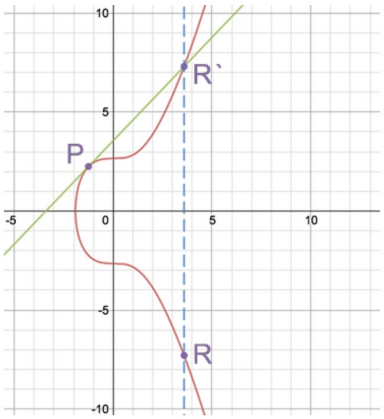

Рисунок 1.5 – Еліптична крива в Bitcoin

Ці дві операції застосовуються для скалярного множення, яке визначається як R = aP, де R виходить шляхом додавання точки P самій до себе кілька разів. Наприклад:

R = 7P

R = P + 6P

R = P + 2 (3P)

R = P + 2 (P + 2P)

Тут наведено обчислення 7P, яке представляє собою спрощене скалярне множення за допомогою комбінаційних операцій в яких додаються та подвоюються точки[13].

Кінцеве поле в розумінні еліптичної криптографії можна представити як обмежений набір додатніх чисел, у межах якого виконується кожне обчислення. Обчислення відкритого ключа здійснюється за допомогою операцій подвоєння і додавання точок. Це нескладне завдання, яке персональний комп'ютер або смартфон може виконати за мілісекунди. Проте обернене завдання (отримання секретного ключа з відкритого) є проблемою дискретного логарифмування, яка зараз вважається обчислювально складною. Найкращі відомі алгоритми для її розв’язання, такі як алгоритм Полларда, мають експоненційну складність. Для secp256k1, щоб вирішити цю задачу, потрібно виконати близько 2^256 операцій, що займе більше часу, ніж існує Всесвіт, навіть на потужному комп'ютері. Тому перехід від закритого ключа до відкритого ключа за задумом є односпрямованим.

Відкритий ключ зазвичай представлений у вигляді шістнадцяткового рядка. В нестисненому вигляді він містить два 256-розрядних числа, які представляють координати x і y точки на еліптичній кривій, з'єднані в один довгий рядок. За допомогою симетрії еліптичної кривої можна створити стиснений відкритий ключ, в якому зберігається тільки значення x і інформація про положення точки на кривій. З такої часткової інформації можна відновити обидва значення координат.

2. АНАЛІЗ ЕФЕКТИВНОСТІ БЛОКЧЕЙНУ В РІЗНИХ ГАЛУЗЯХ

2.1 Смарт-контракти

Блокчейн можна використовувати для реєстрації прав власності на певні активи. По-перше, питання безпеки при збереженні всіх даних в цьому випадку є дуже важливим, тому що в разі втрати довести своє право власності на певний об'єкт практично неможливо, або процес відновлення займе багато часу. Крім того, як згадувалося раніше, блокчейн забезпечує незмінність усіх записів, тому злочинці, які хочуть заволодіти чужим майном шахрайським шляхом, не зможуть цього зробити. Крім того, у разі атаки на один із вузлів продуктивність мережі та вміст не постраждають. Концепцію смарт-контрактів запропонував Нік Сабо в 1994 році. Однак насправді смарт-контракти стали реальністю лише з появою блокчейн-платформи Ethereum у 2015 році, яка надає інструменти для написання та виконання смарт-контрактів.

Смарт-контракти – це новітній спосіб укладання угод між людьми або установами. Умови договору, їх перевірка та результати записуються в коді контракту. Основною перевагою є те, що не потрібні треті особи для контролю виконання умов договору. Вони інтегруються в блокчейн, завдяки чому користуються всіма перевагами цієї технології. Використання смарт-контрактів може бути дуже різноманітним, і вони допомагають значно знизити витрати на нотаріальні послуги, послуги посередників і юристів.

2.2 Використання блокчейн-технології в різних галузях

Блокчейн технологія має широкий спектр застосувань завдяки своїм властивостям децентралізації, прозорості та криптографічної безпеки.

Найбільш відомий приклад – криптовалюти, такі як Bitcoin і Ethereum, які функціонують на основі блокчейн-технології[16]. Bitcoin працює на децентралізованій мережі, де кожен вузол (комп'ютер) у мережі підтримує копію блокчейну. Транзакції проходять через цю мережу без центрального контролю,

а це означає, що жодна особа чи організація не контролює біткоїн. Користувачі здійснюють транзакції, які включають перекази Bitcoin з одного гаманця до іншого. Транзакції підписуються цифровими підписами, що забезпечує їх автентичність. А самі користувачі ідентифікуються за своїми гаманцями (адресами), що дозволяє залишатися анонімними, хоча всі транзакції є видимими і знаходяться в публічному реєстрі. Bitcoin часто використовується як цифровий актив для зберігання вартості, подібно до золота. А також використовується для здійснення міжнародних платежів без участі посередників. Багато людей інвестують в Bitcoin з метою отримання прибутку. Адже він став першою криптовалютою яка успішно функціонує і зрозстає починаючи з 2009 року, завдяки блокчейн технолої котра є ключовим елементом, що забезпечує функціонування, та безпеку.

Блокчейн технологія має значний потенціал для міжнародних грошових переказів. У той час як звичайні методи мають високі комісії та тривалий час обробки, транзакції в блокчейні зазвичай несуть менші витрати, оскільки вони мінімізують або усувають посередників. Час обробки знижується з декількох днів до декількох хвилин[14]. Та дозволяє надсилати кошти в будь-яку точку світу, не залежно від місця розташування, навіть в регіони з обмеженим доступом до банківських послуг. Visa та Mastercard є двома провідними світовими компаніями з обробки платежів. У той же час вони важливі у впровадженні криптовалют, технології блокчейну, працюючи над створенням блокчейну Mastercard та інтеграції блокчейну Visa.

Блокчейн може допомогти відстежувати рух товарів від виробника до кінцевого споживача. Кожен етап: виробництво, транспортування, зберігання, доставку. Це особливо важливо для товарів, що потребують особливих умов зберігання або транспортування, таких як медикаменти або продукти харчування.

Торгівля цифровими колекційними предметами та мистецтвом у формі NFT (невзаємозамінних токенів), що дає можливість художникам та творцям продавати свої роботи (див. рисунок 2.1).

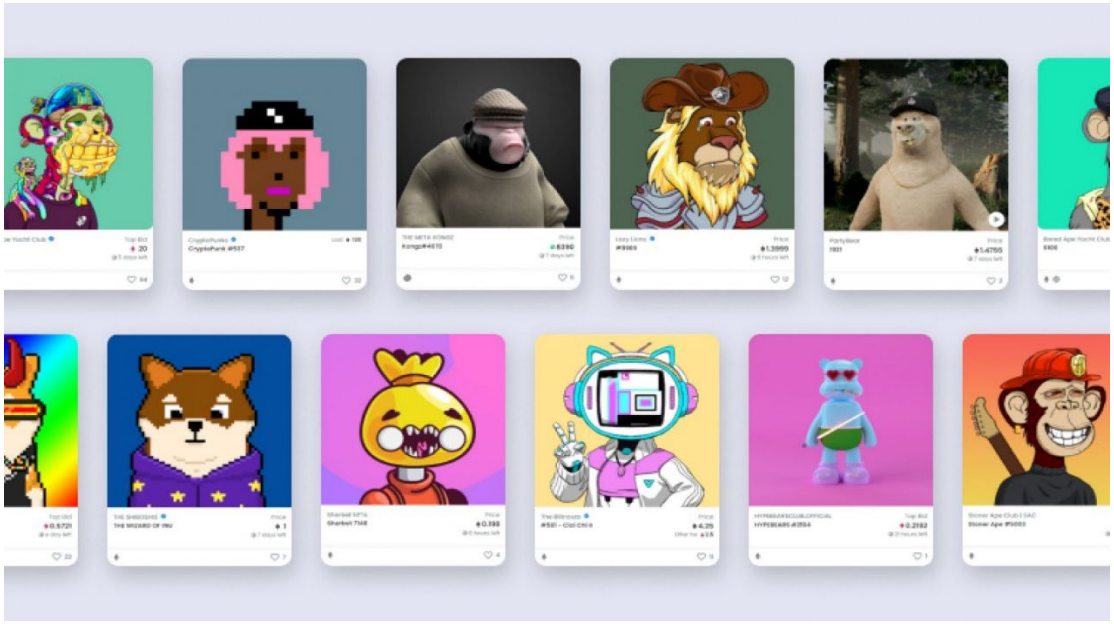

Рисунок 2.1 – Приклад NFT токенів

Перевірка дипломів та сертифікатів також можлива за допомогою блокчейну її ідея полягає в тому, щоб зберігати інформацію про дипломи та сертифікати, такі як назва установи, отримана кваліфікація, дата видачі, яка записується в блокчейн як транзакція. В подальшому та інформація підписується за допомогою криптографічних методів, що забезпечує її цілісність та автентичність. І кожен, хто має бажання та необхідний ключ доступу, може перевірити дані про диплом або сертифікат. Це може зробити роботодавець, університети чи інша зацікавлена сторона. Кожен запис в блокчейні має унікальний ідентифікатор, завдяки якому можна перевірити його автентичність та відстежити всі зміни [1]. Якщо змінити дані, наприклад, додати проходження нових курсів або отримання додаткових сертифікатів, інформацію можна оновити в блокчейні, завдяки цьому забезпечується актуальність даних.

Блокчейн полегшити процес купівлі-продажу, знижуючи витрати на посередників і прискорюючи укладання угод. Також, може відігравати важливу роль в управлінні правами власності завдяки смарт-контрактам через автоматизацію та захист прав власності. Усі дані про нерухомість (такі як власність, обтяження, права, дозволи тощо) будуть збережені у блокчейні, що забезпечує їх прозорість і доступність, а також незмінність даних, що ускладнює можливість маніпулювання і фальсифікації документів.

Здобув шикокого використання також і на фондових ринках, зокрема серед американських компаній. Існує ймовірність, що в майбутньому це може дозволити уникнути необхідності у клірингових організацій, що спростило б роботу бірж та позитивно вплинуло на прибутковість акцій. Це через можливість зменшення витрат і зміцнення позицій компаній на ринку [14].

2.3 Застосування блокчейн-технологій у діяльності світових компаній

Порівняємо прибутковість компаній, які використовують технологію блокчейн, та які не використовують дану технологію. Для цього використаємо дані про діяльність дев'яти найбільших компаній на американському фондовому ринку і проаналізуємо їхню середню дохідність за останні п'ять років для вивчення динаміки розвитку. Перші 4 компанії активно використовують блокчейн а саме:

- Amazon - відома рітейл-компанія продає товари масового виробництва через Інтернет. Amazon була однією з перших компаній на світовому ринку, яка впровадила блокчейн, вона не тільки використовує цю технологію для власних потреб, але й надає свої розробки для впровадження блокчейну на інших підприємствах.
- Facebook (Meta) – компанія, володіє одними з найбільших соціальних мереж і користується популярністю у світі, використовує блокчейн для захисту даних своїх користувачів та впровадження реклами.
- Oracle – американська компанія, розробляє програмне забезпечення використовуючи алгоритми блокчейну, що збільшує конкурентні переваги продукту.
- Згадувана Visa – найбільша в світі платіжна система. Картки компанії приймають приблизно у 150 країнах світу. Блокчейн в данному випадку допомагає суттєво зменшити кількість кіберзлочинів щоб захистити рахунки клієнтів.

Згадувані компанії почали використовувати блокчейн-технологію від 2017 року і, статистично, починаючи з цього року їхній дохід поступово зростав (див. таблицю 2.1). Перейдемо до компаній котрі на данний момент не використовують, або тільки починають намагатись впроваджувати блокчейн-технології, до них відносяться:

– NIKE – американський бренд, яка виробляє спортивне взуття, одяг та екіпірування.
– Walt Disney – провідна світова розважальна корпорація, вартістю 187,84 мільярда доларів США.
– Netflix – великий і популярний сервіс підписки для перегляду серіалів та фільмів онлайн.
– McDonald’s – американська корпорація, відома мережею ресторанів швидкого харчування, чиї прибутки залежать від світової економіки.

Таблиця 2.1 – Середньорічний дохід компаній, млрд доларів США

Назва	2019	2020	2021	2022	2023
Amazon	280.52	386.06	469.82	513.98	574.79
Facebook	70.69	85.96	117.92	116.6	134.9
Oracle	39.1	39.5	40.5	42.4	50.0
Adobe	11.1	12.87	15.79	17.61	19.41
Visa	22.98	21.85	24.11	29.31	32.65
NIKE	39.12	37.40	44.54	46.71	51.22
Netflix	20.16	25.00	29.70	31.62	33.72
McDonald’s	21.36	19.21	23.22	23.18	25.49
Walt Disney	69.61	65.39	67.42	82.72	88.90

Використання блокчейн-технологій безпосередньо впливає на прибуток компаній, оскільки знижує витрати на обслуговування баз даних та їх підтримку, що в свою чергу підвищує прибуток. Проаналізуємо зв’язок між прибутком компаній та використанням технологій (див. рисунок 2.2). Як ми бачимо компанія «Amazon», прибуток якої серед вибраних компаній є найбільшим,

швидко мобілізувала власні ресурси для використання алгоритмів блокчейн задля розроблення власних технологій, що нині приносить їй значні прибутки. Наступні йдуть компанії Facebook, Oracle, Visa - їхні доходи поступово зростають і якщо коливаються протягом року то прибуток досить швидко починає знову підніматись, так як сталось з Facebook у період 2022-2023 років.

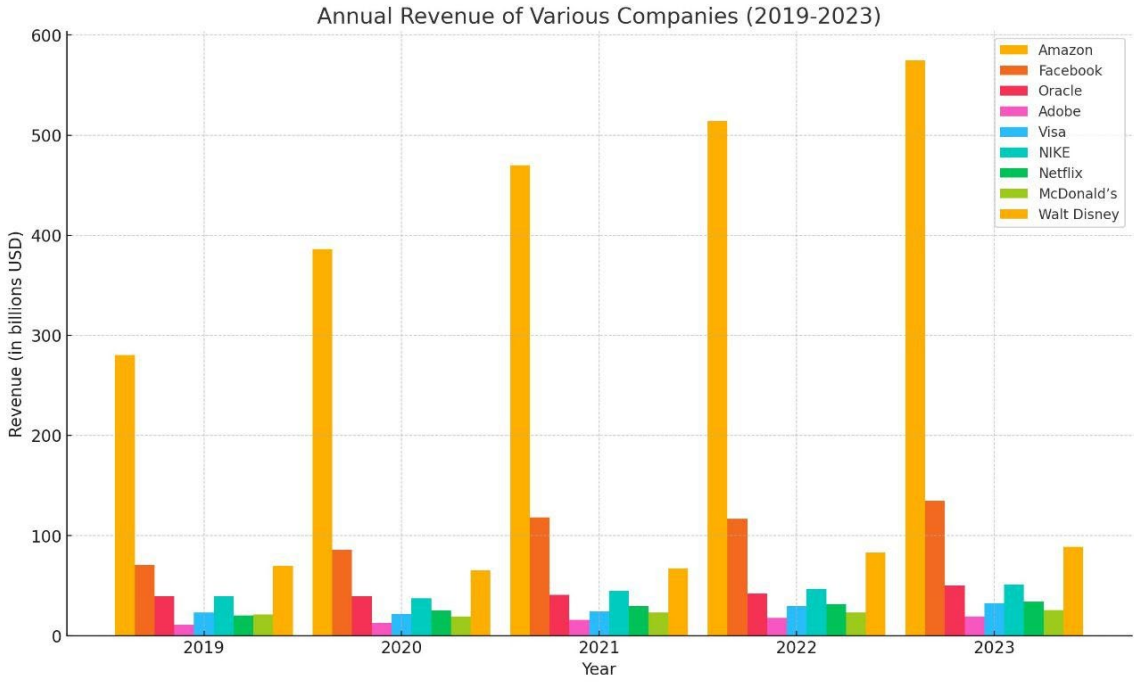

Рисунок 2.2 – Середньорічний дохід компаній, млрд доларів США

Прямих даних про використання блокчейну Nike менше, хоча варто зазначити що компанія отримала патент на «CryptoKicks», який використовує блокчейн для слідкування автентичності та походження кросівок, що також може включати систему винагород у формі цифрових активів.

Інші компанії зі списку, такі як Adobe, Netflix, McDonald's, та Walt Disney, наразі не повідомляють про застосування блокчейн-технологій у своїй основній діяльності. Хоча ці компанії конкурентоспроможні і стабільно тримаються на ринку, відсутність новітніх технологій обмежує їхні можливості для підвищення прибутків. Однак, великі корпорації постійно досліджують нові технології, тому не варто виключати що в найближчий час і вони будуть використовувати блокчейн, для різноманітних потенційних застосувань, що можуть включати захист цифрових прав, ланцюги поставок, фінансові послуги та багато іншого.

2.4 Аналіз переваг, ризиків та недоліків у використанні

Недоліки блокчейну включають відсутність єдиних правил для його використання, що знижує довіру користувачів. Також блокчейн споживає багато енергії, що є проблемою для малих компаній. Хоча з часом витрати окупаються, початкові етапи використання дуже дорогі [11]. Ось кілька проблем, які заважають широкому впровадженню блокчейну:

Блокчейн може знизити витрати користувачів на комісії за транзакції, але ця технологія не є дешевою. Наприклад, система "підтвердження роботи," яка використовується для перевірки транзакцій біткойнів, споживає значну кількість обчислювальних ресурсів[2].

Чинні правила в США забороняють користувачам онлайн-бірж, наприклад тих, що побудовані на блокчейні, зберігати повну анонімність, онлайн-платформи зобов’язані отримувати інформацію про своїх клієнтів, коли вони відкривають рахунок, перевіряти особу кожного клієнта та підтверджувати, що клієнт не фігурує в жодному списку записів, які є відомими або підозрюваними як терористичні організації [11].

Попри широке використання нових технологій, основними проблемами для звичайних інтернет-користувачів залишаються недостатня обізнаність і недовіра до технології. Блокчейн впроваджується не тільки в економіці, але й в інших сферах. Як і будь-яка технологія, він не є на 100% досконалим, тому може стати ціллю атак, про які користувачі повинні знати.

Технологія блокчейн забезпечує безпеку та надійність кількома способами. Для початку як вже відомо, нові блоки завжди додаються послідовно і хронологічно до ланцюжка. Додавши блок, його важко редагувати, оскільки кожен блок містить унікальний хеш та хеш попереднього блоку. Хеш-коди генеруються математичною функцією, яка втілює цифрову інформацію в унікальний рядок цифр і літер. Змінюючи дані, змінюється і хеш-код [3].

Наприклад, якщо хакери намагаються змінити вашу транзакцію на Amazon, щоб здійснити подвійну оплату, змінивши суму транзакції, це призведе до зміни хеш-коду цього блоку. Наступний блок в ланцюжку все ще буде містити

старий хеш, і хакеру доведеться оновити цей блок і всі наступні. Перерахунок всіх цих хеш-значень потребує значних енерговитрат. Отже, коли блок додано до блокчейну, його важко змінити і неможливо видалити. Якби хакер хотів здійснити атаку, йому довелося б розв'язати складні задачі, а це в свою чергу перевищило б витрати на атаку порівняно з вигодою.

Основна мета блокчейну полягає в забезпеченні можливості запису та поширення цифрової інформації без можливості її редагування.

Коли мова йде про друковані гроші, їх використання регулюється та контролюється банком або урядом. Однак Bitcoin не контролюється жодною організацією. Транзакції в Bitcoin перевіряються мережею комп'ютерів[6].

Для проведення транзакцій в мережі Bitcoin учасники використовують програму, яку називають "гаманцем". Кожен гаманець має два унікальних криптографічних ключі: відкритий і закритий. Відкритий ключ використовується для отримання і відправки транзакцій, а також є цифровим підписом користувача. Навіть якщо користувач отримує платіж на свій відкритий ключ, він не зможе вилучити його без закритого ключа. Відкритий ключ є скороченою версією закритого ключа, створеною за допомогою складного математичного алгоритму[18]. Завдяки складності цього алгоритму практично неможливо створити закритий ключ з відкритого. Через це блокчейн вважається безпечним.

Головною перевагою і причиною популярності блокчейну є відмовостійкість, захист даних від пошкоджень і злочинних дій. Ось чому технологія все більше привертає увагу в галузях, де ці параметри мають особливе значення.

2.5 Порівняння з традиційними (централізованими) системами

Для оцінки ефективності технології блокчейн порівняно з традиційними системами пропонується використовувати математичну модель, що ґрунтується на логістичних функціях[13]. Ця модель дозволяє досліджувати вплив збільшення кількості блоків у блокчейні на точність системи у запобіганні та

протидії загрозам безпеки. Оцінка точності блокчейн-системи здійснюється за формулою 2.1.

$$A_{BC} = A_{base} + \frac{L}{1 + e^{-k(B - x_0)}}, \tag{2.1}$$

де:

- ABC - визначає точність системи блокчейну,
- Abase - встановлена як базова точність системи на рівні 80% для цього дослідження,
- L - максимальне збільшення точності, встановлене на рівні 20%,
- B - кількість блоків у блокчейні,
- k - коефіцієнт приросту, що визначає швидкість зростання функції,
- x0 - точка, з якої починається стрімке зростання функції.

У традиційній системі точність буде вважатись сталою і не залежити від кількості блоків або інших зовнішніх факторів (див. формулу2.2).

$$A_T = A_{base}, \tag{2.2}$$

де: AT - є точністю традиційної системи.

У таблиці 2.2 показано, як точність системи блокчейн зростає з кожним наступним блоком [13]. Ця таблиця наочно ілюструє поступове підвищення точності, що розпочинається з базового рівня для одного блоку. Швидкість цього зростання ніколи не буде перевищувати 100%, що відповідає реалістичній моделі підвищення точності в системі блокчейн. В той же час точність традиційних систем залишається стабільною на рівні 80%.

Таблиця 2.2 – Порівняння точності блокчейн-системи в залежності від кількості блоків.

Кількість блоків	Точність блокчейну (Модифікована Логістична)	Точність традиційної системи
1	0.819	0.80
2	0.824	0.80
3	0.830	0.80
4	0.836	0.80
5	0.845	0.80
6	0.854	0.80
7	0.864	0.80
8	0.876	0.80
9	0.888	0.80
10	0.900	0.80

Для докладнішого розгляду цих результатів зроблено графік (див. рисунок 2.3) [13], який наочно демонструє, як точність блокчейн-системи зростає з кожним новим блоком, у той час як точність традиційних систем залишається без змін. Цей графік відображає важливість технології блокчейн у забезпеченні безпеки, підкреслюючи її здатність покращувати ефективність в міру розширення мережі.

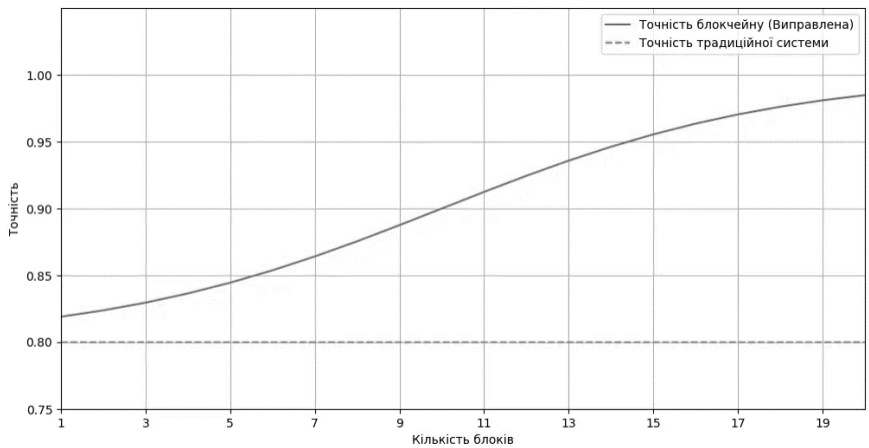

Рисунок 2.3 – Порівняння точності традиційної системи та блокчейну в залежності від кількості блоків

На основі цього методу порівняння видно, що зі збільшенням кількості блоків блокчейн стає продуктивним у захисті даних, особливо в тих сферах, де надійність та безпека є критичними аспектами.

Для глибшого розуміння впливу технології блокчейн необхідно також розглянути, як вона впливає на швидкість обробки даних. Збільшення кількості блоків у ланцюжку блокчейн, час обробки транзакцій та запитів збільшується. Це відображає той факт, що з ростом мережі блокчейн збільшується час, необхідний для виконання операцій. Математична модель для такого порівняння може бути виражена у вигляді (див. формулу 2.3):

$$S_{BC} = \frac{S_{base}}{1 + a \times (\mathrm{B} - 1)}, \tag{2.3}$$

де:

- SBS - швидкість обробки запитів у системі блокчейн,
- Sbase - базова швидкість обробки запитів,
- B - кількість блоків у блокчейні,
- a - коефіцієнт, що визначає, як збільшення кількості блоків впливає на зниження швидкості обробки.

Початкова швидкість обробки запитів (SBS) визначається як базова (Sbase). З кожним наступним блоком у блокчейні швидкість обробки зменшується, причому ступінь цього зниження контролюється коефіцієнтом (a).

У контексті традиційних систем швидкість обробки запитів залишається сталим значенням і не залежить від кількості блоків або інших зовнішніх факторів(див. формулу 2.4).

$$S_T = S_{base}. \tag{2.4}$$

Отже, ця модель дозволяє порівняти, як змінюється швидкість обробки запитів в системі блокчейн зі зростанням кількості блоків, у порівнянні з постійною швидкістю обробки в традиційній системі [13].

Для аналізу швидкості обробки запитів в системі блокчейн залежно від кількості блоків припускається, що базова швидкість обробки в традиційній системі складає 100 запитів на секунду і залишається постійною в будь-яких умовах. У системі блокчейн ця швидкість зменшується зі зростанням кількості блоків, оскільки кожен додатковий блок вимагає більше часу для обробки. Результати аналізу представлені в таблиці (див. таблицю 2.3) [13].

Таблиця 2.3 – Порівняння швидкості обробки запитів блокчейн-системи в залежності від кількості блоків

Кількість блоків	Швидкість блокчейну (запитів/сек)	Швидкість традиційної системи (запитів/сек)
1	100.00	100
2	95.24	100
3	90.91	100
4	86.96	100
5	83.33	100
6	80.00	100
7	76.92	100
8	74.07	100
9	71.43	100
10	68.97	100

Візуальна демонстрація даних на графіку (див. рисунок 2.4) показує, як швидкість обробки запитів у системі блокчейн знижується з кожним новим блоком.

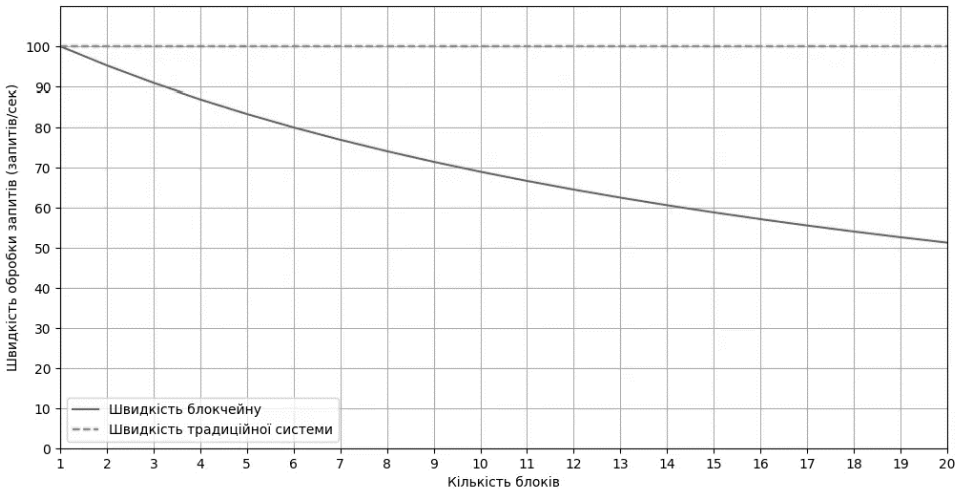

Рисунок 2.4 – Швидкість обробки запитів блокчейн-системи в порівнянні з традиційною системою

Порівняння доводить, що блокчейн може забезпечити вищий рівень безпеки і надійності порівняно з традиційними системами, але при цьому виникають обмеження у швидкості обробки транзакцій і запитів.

Ці результати допомагають краще розуміти переваги і недоліки технології блокчейн. З одного боку, вона зміцнює безпеку та надійність даних. З іншого боку, є можливість зниження швидкості обробки даних яка важлива для застосувань, де висока швидкість є ключовим фактором успіху.

Отже, вибір між блокчейном і традиційними системами має бути обґрунтованим аналізом конкретних вимог застосування і значущості різних аспектів, таких як безпека, швидкість і надійність.

3. ДОСЛІДЖЕННЯ, КЛАСИФІКАЦІЯ ТА ПРИКЛАДИ РЕАЛІЗАЦІЇ БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ ПОКРАЩЕННЯ БЕЗПЕКИ

3.1 Приклад реалізації застосунку для проведення виборів

Варто зазначти що розробку цього застосунку було взято з відкритих джерел та використано згідно усіх правил що до авторських прав, а саме буде доступне посилання на роботу автора.

Суть застосунку полягає в написанні смарт-контракту мовою програмування Solidity (див. рисунок 3.1) , вона запозичила багато функцій з інших мов програмування і нагадує JavaScript [11].

```
pragma solidity >=0.4.22 <0.8.0;

contract Voting {
    struct Candidate {
        uint id;
        string name;
        string surname;
        string patronymic;
        string description;
        string dateOfBirth;
        uint votesNumber;
    }
    mapping(address => uint) public voters;
    mapping(uint => Candidate) public candidates;
    uint public candidatesNumber;

    function addCandidate(string memory _name, string memory _surname,
        string memory _patronymic, string memory _description, string memory _dateOfBirth) private{
        ++candidatesNumber;
        candidates[candidatesNumber] = Candidate(candidatesNumber, _name, _surname, _patronymic, _description, _dateOfBirth, 0);
    }

    function vote (uint _candidateId) public {
        require(voters[msg.sender]==0);
        require(_candidateId > 0 && _candidateId <= candidatesNumber);
        voters[msg.sender] = _candidateId;
        candidates[_candidateId].votesNumber++;
    }

    constructor() public {
        addCandidate("Петро","Порошенко","Олексійович","Голова партії \"Європейська Солідарність\"","1958-09-26");
        addCandidate("Володимир","Зеленський","Олександрович","Голова партії \"Слуга Народу\"","1978-01-25");
        addCandidate("Юлія","Тимошенко","Володимирівна","Голова партії \"БЮТ\"","1960-11-27");
    }
}
```

Рисунок 3.1 – Смарт контракт для виборів

Тіло контракту визначається за допомогою ключового слова «contract», за яким йде його назва. Це схоже на оголошення класу в об'єктно-орієнтованому програмуванні. [11]. Тип кандидата описується за допомогою структури, яка

містить поля для ідентифікатора, імені, прізвища, по-батькові, дати народження, опису та кількості голосів. Для збереження кандидатів і голосів виборців використовується структура «mapping», яка є хеш-таблицею. У Solidity відсутня можливість безпосередньо отримати кількість елементів у хеш-таблиці, тому для ведення обліку кандидатів потрібно використовувати додатковий лічильник. Для додавання нового кандидата до хеш-таблиці створюється окрема функція, яка приймає всі необхідні поля та створює відповідний елемент у таблиці. Цей метод є приватним і може викликатись тільки всередині контракту, наприклад, у конструкторі при ініціалізації контракту.

Функція для віддання голосу приймає ідентифікатор обраного кандидата і за допомогою require перевіряє правильність параметра та перевіряє, чи вже голосував виборець раніше.

Адреса виборця додається до списку тих, хто вже проголосував при умові що всі перевірки успішні, а голос зараховується до загальної кількості. Таким чином завершується створення контракту. Важливо розробити тести та переконатися у правильній роботі контракту, оскільки після його додавання до блокчейну змінити контракт буде неможливо.

Наступним кроком йде перевірка роботи і розгортання контракту, щоб це зробити використовується truffle ide, його можна завантажити за допомогою менеджеру пакетів – npm [11]. Також потрібно встановити додатки: Ganache, MetaMask. Завдяки ним ми можемо бачити інформацію про локальну блокчейн-систему яка була утворена (див. рисунок 3.2), та підключатись до локальної мережі блокчейну із баузеру (див. рисунок 3.3). Після установки всіх необхідних додатків і налаштування власної Ethereum-блокчейн мережі для тестування і роботи програми, в ній був запущений контракт. Завдяки цьому контракту ми можемо брати участь у голосуванні [11].

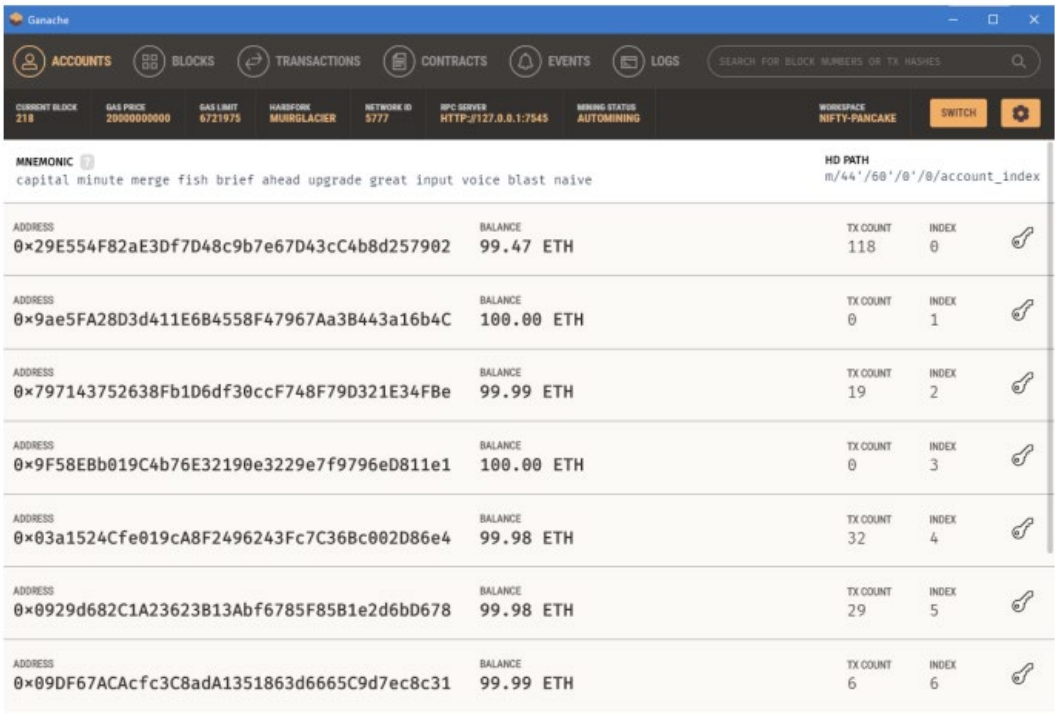

Рисунок 3.2 – Додаток Ganache

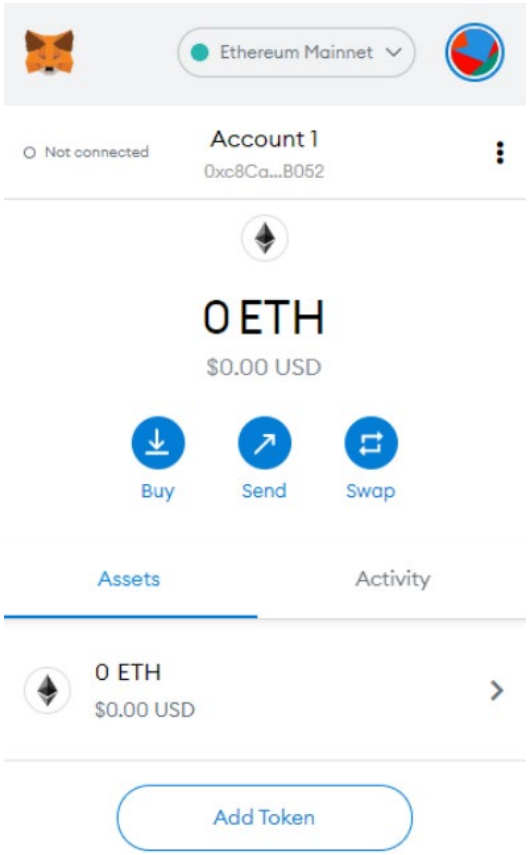

Рисунок 3.3 – Додаток Metamask

Для взаємодії користувача з мережею було розроблено простий вебзастосунок. Створений html заготовки базових сторінок, додано та

підключено стилі, шрифти, зображення, JavaScript-файли, конфігурація серверу, встановлення залежності. Особливістю застосунку є код, що забезпечує взаємодію з блокчейном та контрактом. Для цього використовується бібліотека web3.js. На нашій HTML-сторінці підключаємо файл з об’єктом App, що містить дані про провайдера, контракти, акаунт та голос користувача.

```
App = {
    web3Provider: null,
    contracts: {},
    account: '0x0',
    userVote: 0,

    init: function() {
        return App.initWeb3();
    },

    initWeb3: function() {
        App.web3Provider = new Web3.providers.HttpProvider('http://localhost:7545');
        web3 = new Web3(App.web3Provider);
        return App.initContract();
    },

    initContract: function() {

        $.getJSON("Voting.json", function(election) {
            App.contracts.Voting = TruffleContract(election);
            App.contracts.Voting.setProvider(App.web3Provider);
            return App.render();
        });
    },
```

Рисунок 3.4 – Використання web3

При завантаженні сторінки викликається функція ініціалізації об’єкту App (див. рисунок 3.4). яка налаштовує провайдера з адресою локального блокчейну, завантажує дані контракту і будує інтерфейс користувача на основі цих даних. Завдяки web3.js застосунок отримує доступ до даних контракту (див. риснок 3.5), та може ініціювати транзакції (див. рисунок 3.6) [11].

```
await App.contracts.Voting.deployed().then( fn: function(instance) {
    contractInstance = instance;
    return contractInstance.candidatesNumber();
```

Рисунок 3.5 – Отримання екземпляру контранкту

```
App.contracts.Voting.deployed().then( fn: function(instance) {
    return instance.vote(candidateId, { from: App.account });
});
```

Рисунок 3.6 – Взаємодія з контрактом

Для взаємодії з блокчейном через браузер використовується MetaMask. За замовчуванням MetaMask використовує головну мережу Ethereum, тому треба підключитися до нашої локальної мережі, створивши нове підключення в MetaMask та вказавши адресу мережі (див. рисунок 3.7).

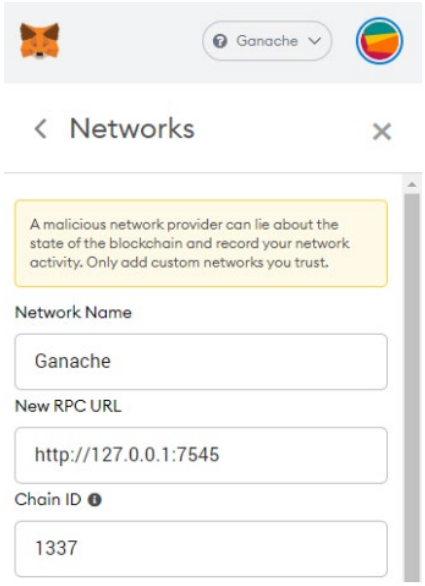

Рисунок 3.7 – Підключення до локального блокчейну

Після підключення можна обрати акаунти з нашого блокчейну і бачити їх баланс. MetaMask надає глобальні API для веб-сайтів, що дозволяють отримувати інформацію про акаунти користувача і доступ до блокчейну. Таким чином, наш застосунок отримує доступ до обраного акаунту в MetaMask (див. рисунок 3.8).

```
web3.eth.getCoinbase(async function(err, account) {
    localStorage.setItem("accounts",web3.eth.accounts.length.toString());
        const accounts = await ethereum.request({ method: 'eth_requestAccounts' });
        const account = accounts[0];
        App.account = account;
        $('#content').show();
        $("#accountAddress").html("Ваш ідентифікатор: " + account);
});
```

Рисунок 3.8 – Отримання даних про акаунт користувача

Після завершення всіх потрібних налаштувань локальний блокчейн запущено, а контракт розміщено, отже взаємодія користувача з мережею через браузер вважається налаштованою.

Щоб використати застосунок потрібно запустити веб-сервер та перейти на відповідну сторінку в браузері. Користувача зустріне вікно з кнопкою "Увійти", яку потрібно натиснути після вибору акаунту в MetaMask (див. рисунок 3.9) [11].

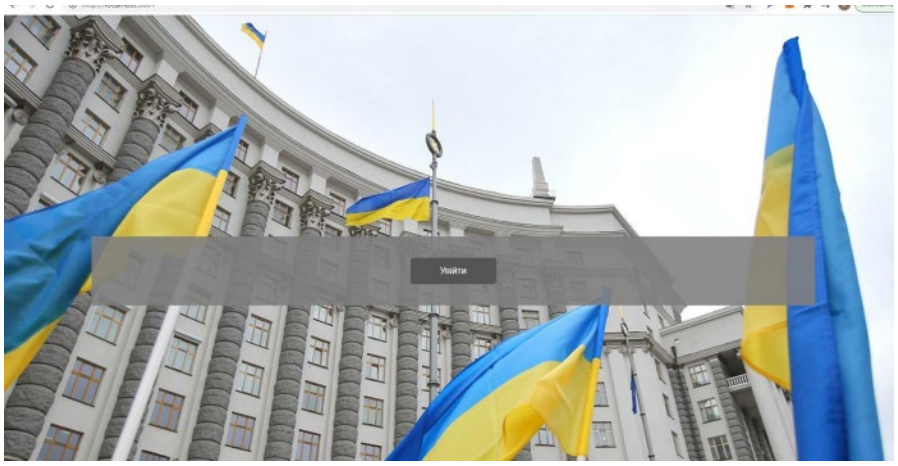

Рисунок 3.9 – Вітальна сторінка застосунку

Не увійшовши в акаунт, не можна продовжити. Цей процес імітує ідентифікацію та аутентифікацію. Після входу користувач зможе перейти на сторінку з виборчим бюлетенем, що містить опис кандидатів і місце для мітки. Користувачі, чиї акаунти не зареєстровані у локальному блокчейні, не зможуть проголосувати, але зможуть переглянути бюлетень та результати голосування (див. рисунок 3.10) [11].

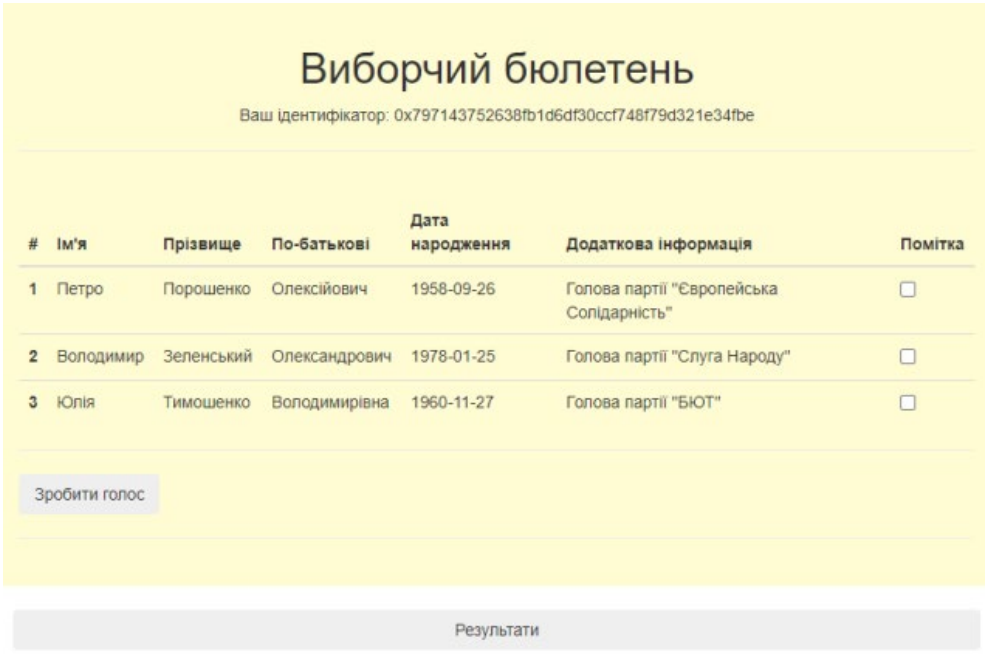

Рисунок 3.10 – Виборчий бюлетень

Інші користувачі можуть обрати кандидата, поставивши позначку, та натиснути кнопку для підтвердження голосування. При умові що користувач вже голосував, йому надсилається повідомлення де можна побачити свій голос(див. рисунок 3.11).

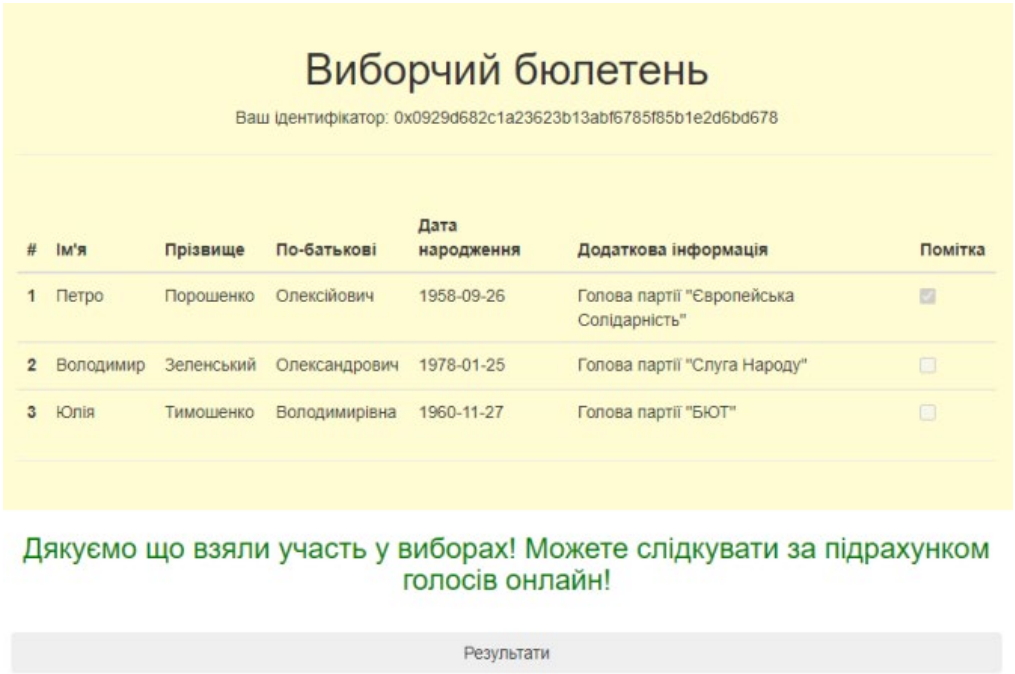

Рисунок 3.11 – Сторінка особи, що взяла участь у виборах

Щоб переглянути поточну явку користувач може натиснути кнопку «Результати», і побачити (середню кількість голосів), кількість голосів за кожного кандидата, а також діаграму на якій видно відсотковий розподіл голосів. (див. рисунок 3.12).

Ім'я	Прізвище	По-батькові	Кількість голосів
Петро	Порошенко	Олексійович	3
Володимир	Зеленський	Олександрович	2
Юлія	Тимошенко	Володимирівна	1

Рисунок 3.12 – Поточний результат

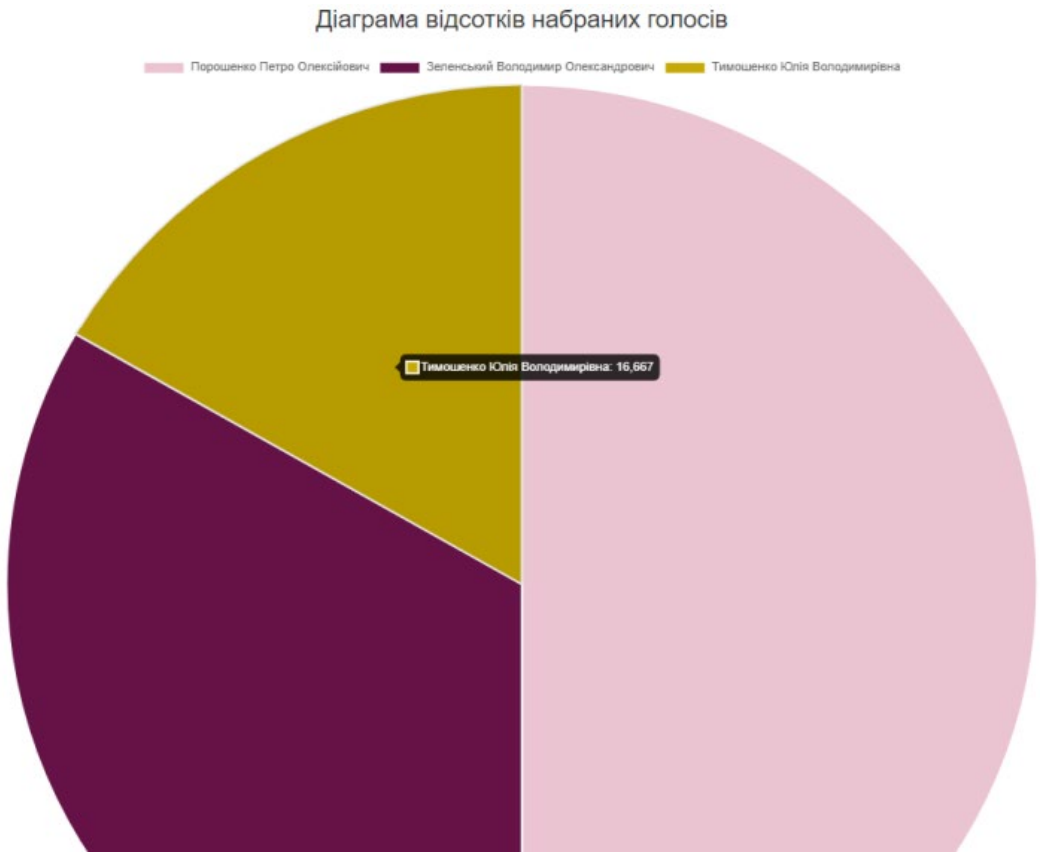

Рисунок 3.12 – (Продовження)

Змінючи акаунт або виходячі з MetaMask користувач буде перенаправлений на сторінку вітання, що імітує зміну виборця. В результаті був

розроблений смарт-контракт, запущена тестова мережа на локальній машині, досліджено взаємодію блокчейну з клієнтською частиною застосунків та створено веб-застосунок[11].

3.2 Досліждення розробки інформаційної системи з використанням технології блокчейн для опрацювання великих даних

Великі дані в блокчейні – це великі обсяги послідовних даних, які клієнти надсилають до мережі через анонсера. Кожен блок (Block) складається з заголовка (BlockHead), що гарантує цілісність даних (Data). BlockHead включає хеш попереднього блоку (PreviousBlockHash) і хеш даних цього блоку (DataHash). Moment – значення, що визначається випадковою перевіркою. Формула Zero(Hash(PreviousBlockHash || DataHash || Timestamp || Moment)) ≥ Difficulty визначає складність хешування, Zero(▪) – це функція, яка повертає кількість послідовних нулів зліва у вхідному рядку в байтах. Difficulty – це ціле число, яке визначає, скільки послідовних нулів має бути на початку результату хешування.

Наприклад, Difficulty=3 означає, що перші три байти вихідного хешу повинні бути нулями. Timestamp – це час створення поточного блоку. Data::= включає Metadata, яке є кортежем дескриптора для BData, і BData, що є обов'язковим кортежем з даними[15]. Приклад запису для представлення неструктурованих даних наведено в таблиці 3.1 [13].

Оскільки дані майже не змінюються, вони можуть ефективно зберігатися і читатися через блокчейн. info_hash представляє унікальний хеш торрент-роздачі, що формується з даних, перетворених у словник і зашифрованих за допомогою хешу SHA-1. Процес запису включає кілька кроків:

Етап 1: Дані структуруються і автоматично очищаються від дублікатів.

Етап 2: Дані групуються за змістом та обсягом, перетворюються в шістнадцятковий формат і створюється сире транзакційне значення.

Етап 3: Перевіряється наявність записів в блокчейні. Якщо запис вже існує, створюється мітка вказівника на його місце.

Етап 4: Дані записуються в блокчейн за допомогою функцій перетворення в транзакційне значення.

Метод запису включає такі етапи:

1. Центральний вузол записує BData у локальне сховище і регулярно упаковує їх у заголовкові блоки кожен період P.
2. BData записується як BData1, BData2, ..., BDatan протягом періоду P. Заголовковий блок формується з BData1, BData2, ..., BDatan, кожний з яких включає метадані-META, модифіковані дані BNEW та адресу доступу до BLOCATION.
3. Обчислюється DataHash як хеш (BData1 || BData2 || ... || BDatan), використовуючи SHA-1, SHA-256 або MD5.
4. Заголовок записується як BHEAD з PreviousHash, BHASH, LinkofDATA, Timestamp, BINDEX та Signature.

Таблиця 3.1 – Типи даних, які отримує анонсер з клієнта

Параметр	Опис
info_ip	IP адреса у форматі ip2long.
info_port	Інформація про порт клієнта.
info_peer	Інформація про піра.
info_md5	Унікальний хеш ключа, IP, порту в форматі md5.
info_sha1	Унікальний хеш ключа, IP, порту в форматі sha1.
info_upload	Інформація про обсяг розданих даних, у байтах.
info_download	Інформація про обсяг завантажених даних, у байтах.
info_left	Обсяг даних, що залишилося завантажити, у байтах.
info_update	Мітка часу останньої активності піра.
info_expire	Мітка часу зі зміщенням на 1 годину.
info_ipv46	Інформація про IP у звичайному форматі.

PreviousHash забезпечує цілісність попереднього блоку, гарантуючи, що його дані не були змінені. BHASH вказує на те, що дані BDATA залишилися незмінними. LinkofDATA визначає місцезнаходження конкретних даних BDATA, а Timestamp є відміткою часу, що вказує на момент створення блоку. BINDEX служить глобальним індексом, що містить ключові слова, номер об'єкта та номер моделі. Signature генерується центральним вузлом приватного блокчейну і підтверджує автентичність блоку за допомогою закритого ключа [13].

Показ як система працює в умовах великої навантаженості є відмінним прикладом ефективності цієї технології. Впровадження її у великих проектах дозволяє значно знизити навантаження на сервери, особливо у порівнянні з традиційними реляційними базами даних типу MySQL. Наприклад, на торрент-анонсері з мільйонами записів система на основі блокчейну оптимізує обробку великої кількості запитів. Використання класичних реляційних баз даних, таких як MySQL, часто супроводжується проблемами обробки даних при високих навантаженнях, що призводить до затримок і черг у вибірці або додаванні даних і внаслідок — до збільшення навантаження на сервер. Для вирішення цих проблем було розроблено систему та обробник даних на основі блокчейну.

Схема роботи цієї системи при великій кількості запитів показана на рисунку 3.13, а результати зменшення навантаження на сервери представлені на рисунку 3.15.

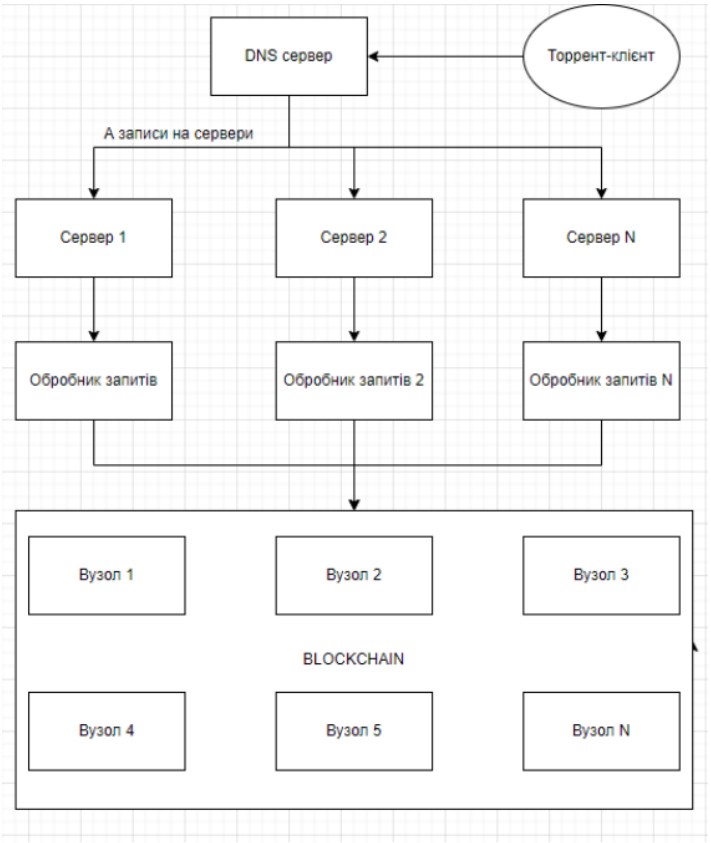

Рисунок 3.13 – Схема роботи системи

Рисунок 3.14 – Навантаження на сервер, до введення в експуатацію

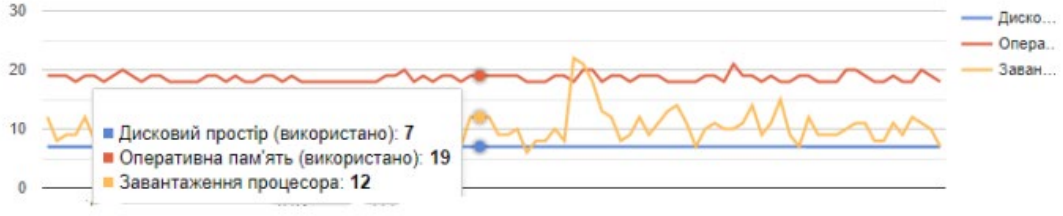

Рисунок 3.15 – Навантаження на сервер, після введення в експлуатацію

Розроблена система може бути використана як інструмент для оптимізації обробки статичних даних, таких як логи для статистики. У якості ідентифікатора виступає адреса (відкритий ключ), а транзакції представлені хешованими мета-

даними. Зменшення кількості запитів майже удвічі обумовлене зниженням навантаження на процесор сервера в такій схемі, що дозволяє уникнути проблем з keep-timeout і знижує ризик втрати даних. Розроблена модель "Великі дані в блокчейні" і її реалізація дозволяють зберігати обсяги даних, недосяжні для певних реляційних баз даних, наприклад MySQL, навіть на потужних серверах.

3.3 Безпечне розподілене хмарне зберігання на основі технології блокчейн та смарт-контрактів

Розподілене хмарне зберігання в данному випадку використовує Ethereum блокчейн, та смарт-контракти для взаємодії між користувачами і системою таким чином: Користувач повинен згенервати свою пару публічних-приватних RSA ключів і завантажити їх разом з унікальним ім'ям користувача[12], [8]. На рисунку 3.16 зображено процес створення та зберігання RSA-ключів. Створюються два файли типу «.pem», один з яких містить приватний ключ («private.pem»), а інший - відкритий ключ («public.pem») [8]. Потім користувач вибирає папку призначення на своїй локальній машині, в якій ці файли будуть зберігатися. На цьому першому етапі користувач ще не взаємодіє з блокчейном.

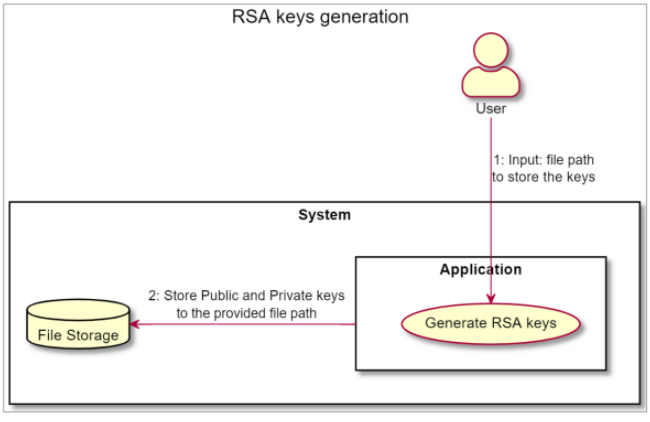

Рисунок 3.16 – Генерація RSA ключів

Згодом користувач може використовувати функціонал смарт-контракту для завантаження, сертифікованим способом, своєї особистої інформацію в блокчейн, яка буде публічною і доступною для всіх користувачів. Цей контракт

буде використовуватися будь-ким хто захоче відправити файли цьому користувачеві. Це передбачає процес реєстрації користувача, показаний на рисунку 3.17.

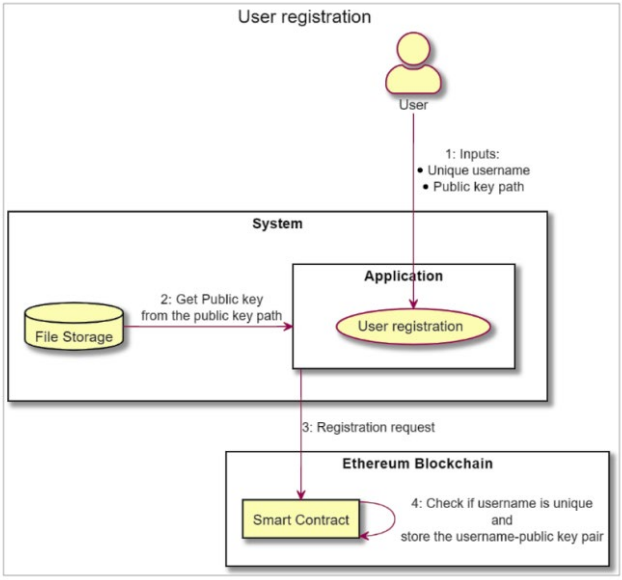

Рисунок 3.17 – Блок-схема реєстрації користувача

Кожен користувач вводить у контракт наступну інформацію:

– Ім'я користувача за його/її вибором.
– Відкритий ключ, згенерований на попередньому кроці (тобто файл «public.pem», створений за допомогою існуючих інструментів генерації ключів RSA або сертифікованих методів, (якщо інформація, що зберігається, є критично важливою).

Процес виконується повністю в рамках блокчейну, з тієї точки зору, що навіть контроль здійснюється під час виконання смарт-контракту[9]. Одне і те ж ім'я користувача не може бути введено двічі (див. рисунок 3.17).

Процес завантаження файлів (див. рисунок 3.18) [4], та обмін файлами здійснюється наступним чином. Користувач розгортає цей функціонал, щоб надати доступ до файлу з потрібним іменем користувача у безпечний спосіб за допомогою RSA-шифрування[5]. Припустимо, що користувач «A» хоче надати спільний доступ до файлу користувачеві «B». Користувач «A» вибирає потрібний файл. Потім, використовуючи смарт-контракт система запитує відкритий ключ користувача «B», щоб зашифрувати файл і переконатися, що тільки користувач «B» може розшифрувати його за допомогою смарт-контракту.

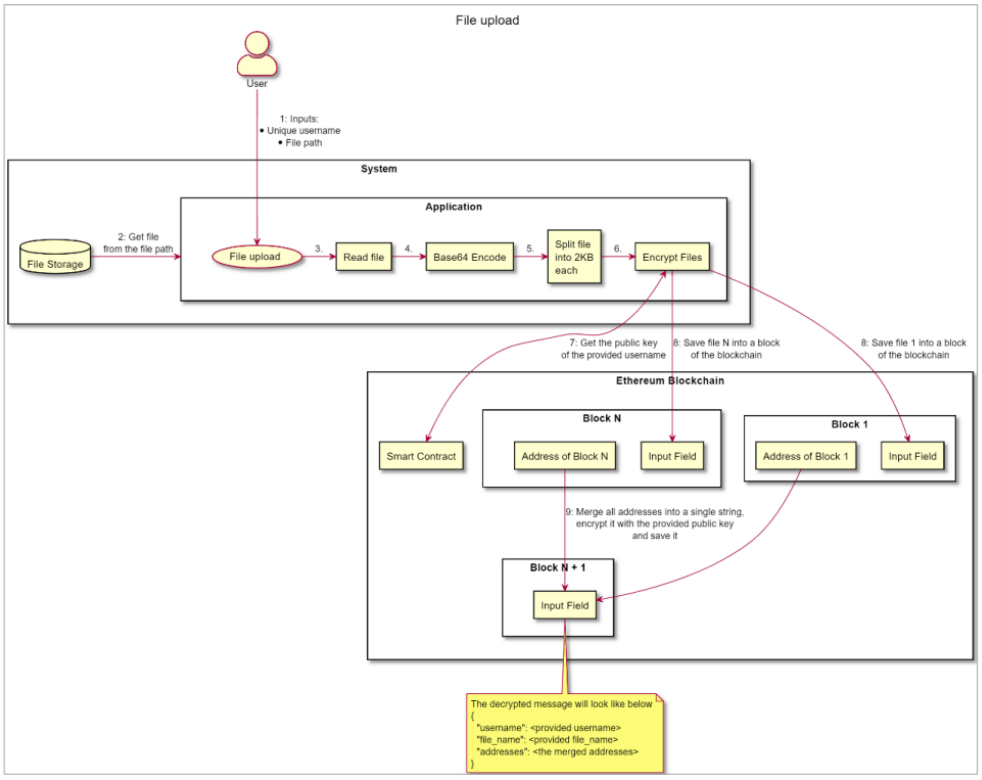

Рисунок 3.18 – Блок-схема завантаження файлу

Програма зчитує файл і кодує його, використовуючи представлення Base64. Таке кодування дозволяє надсилати будь-який файл будь-якого можливого формату, наприклад, «.txt», «.png» або «.pdf». Файл розбивається на менші частини, оскільки він зберігається в полі введення блоку в блокчейні Ethereum і простір, доступний в цьому полі, обмежений[10]. Потім кожна частина файлу шифрується за допомогою RSA з використанням публічного ключа одержувача публічним ключем одержувача, який став відомим завдяки функціоналу смарт-контрактів. Нарешті, адреса блоку , в якому зберігається кожна частина файлу. Зібравши всі адреси блоків, в яких зберігалися розділені частини, додаток створює об'єкт, який містить ім'я користувача, ім'я файлу та всі адреси блоків, в яких зберігаються фрагменти файлу[7]. Нарешті, він шифрує цей об'єкт тим самим ключем і зберігає його у новому блоці.

Опишемо сценарій процесу завантаження файлу (див. рисунок 3.19). Користувач «B» запускає процес завантаження через смарт-контракт і обирає файл, який він/вона хоче завантажити. Система надає обраний файл у

зашифрованому вигляді, і лише після завершення завантаження автоматично починається процес розшифрування за допомогою наданого приватного ключа.

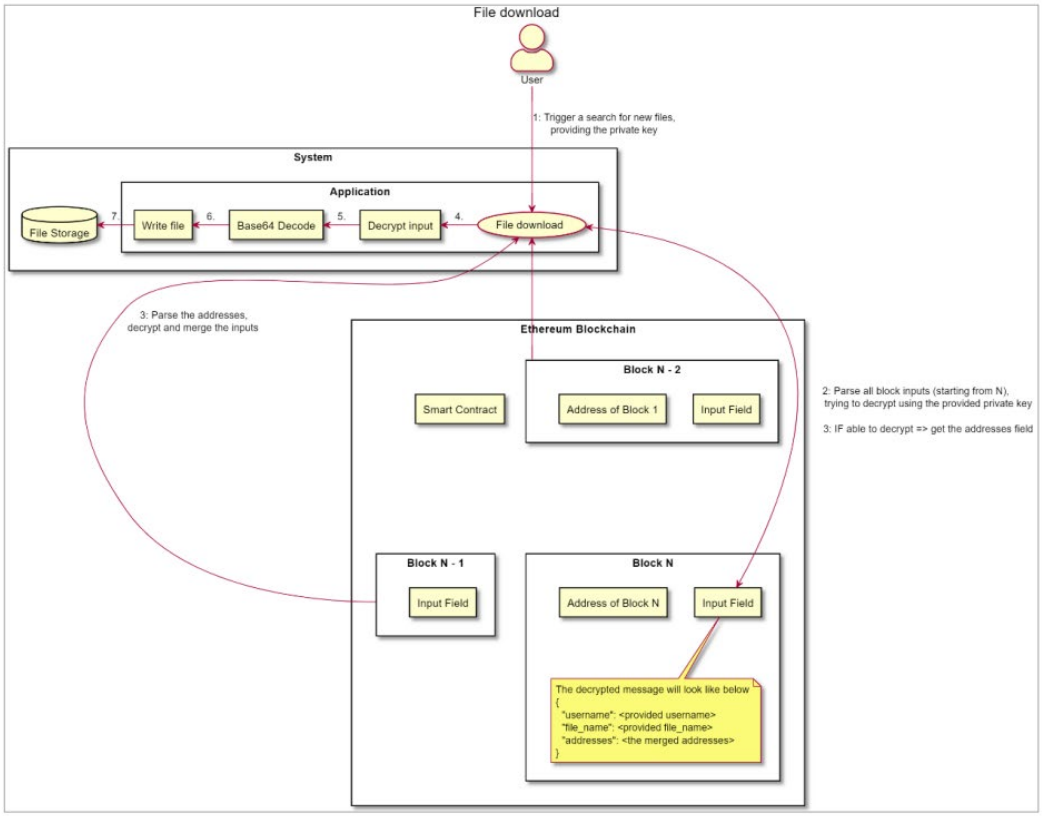

Рисунок 3.19 – Блок-схема завантаження файлу

Загалом, оскільки запропонована система спирається на структуру блокчейну, вона успадковує його робочі характеристики. Функція завантаження, зокрема, призначена для пошуку в структурі блокчейну у відповідь на інформаційний запит[12]. Таким чином, операція пошуку вимагає часу, пропорційного загальному розміру структури. Більш конкретно, алгоритм пошуку починається з останнього блоку і рухається до першого блоку в структурі блокчейну, і, таким чином, пошук може бути виконаний за кілька операцій доступу до блоків, що дорівнює, в найгіршому випадку, кількості блоків у блокчейні. Однак, пошук в блокчейні можна легко розпаралелити, оскільки можна залучити кілька вузлів, які володіють поточним блокчейном володіння поточною структурою блокчейну і призначити їм окремі, суміжні підланцюги, в межах яких вони можуть паралельно шукати потрібну інформацію. Крім того, шифрування даних (для завантажених фрагментів

файлів) на основі RSA є досить повільним і стає нездійсненним для дуже довгих файлів. Зокрема, нижче наведено кілька прикладів пілотного тестування на Docker-контейнері:

- Створення ключа: 00:00,68;
- Реєстрація: 00:04,96;
- Шифрування та завантаження файлу 4.0K: 00:08,80;
- Розшифрування та завантаження файлів (через 32 блоки):
- Розбір блокчейну для перевірки доступних завантажень: 00:02,26;
- Фактичне завантаження: 00:00,60;

Давайте подивимося, як на наведені вище результати впливає довжина блокчейну. Таким чином, ми залишимо процес майнінгу, щоб він відбувався на 1-2 хвилини,а нова ова довжина Blockchain становитиме 97 (~3 рази більше, ніж при попередньому тестуванні).

- Створення ключа: 00:00,66;
- Реєстрація: 00:05,68;
- Шифрування та завантаження файлу 4.0K: 00:07,85;
- Розшифрування та завантаження файлів (32 блоки) від того ж користувача, що і на попередньому кроці:
- Розбір блокчейну для перевірки доступних завантажень: 00:03,03;
- Фактичне завантаження: 00:00,81.

Крок «Розбір блокчейну» є тим, на який найбільше впливає довжина блокчейну. Це очікувано, оскільки синтаксичний аналіз працює, запитуючи блокчейн від останнього до першого блоку. Таким чином, якщо дані користувача зберігалися в старому блоці а довжина ланцюжка велика, то цей крок займе набагато більше часу в порівнянні з іншими кроками.

Система була протестована на віртуальній машині на основі образу Ubuntu 20.04. Були встановлені необхідні інструменти, було розгорнуто блокчейн-сервер, налаштувавши значення складності генерації нового блоку на відносно низьке значення для тестування. Додатки UI і CLI були протестовані з обмеженим обсягом даних і двома користувачами. Один з них виступав у ролі відправника, а інший у ролі одержувача спільного секрету. Секрет являв собою

простий «.txt» файл, що містить ключ доступу до бази даних з привілеями root. Оскільки обсяг даних був обмежений, весь процес (включаючи завантаження, вивантаження, а також шифрування/розшифрування) був завершений протягом приблизно 3 хвилин.

Ця система це ще один прикладний домен блокчейну (Ethereum) який може використовуватися як безпечне однорангове сховище даних у хмарі, а також для спільного використання в хмарі, для обміну файлами та перевірки автентичності файлів.

3.4 Порівняльний аналіз застосувань блокчейн-технологій в різних галузях

В контексті застусунку, варто зазначити, що дані оброблялись доволі швидко, що майже ніяк не впливало на енергозатратність через їх мінімалізацію, а використання смарт-контракту досить доцільне і покращює безпеку. Тому «Застосунок для проведення виборів» - доречний приклад якісного впровадження блокчень-технології.

На рахунок «Розробки інформаційної системи з використанням технології блокчейн для опрацювання великих даних», оскільки блокчейн використовувався для запису постійних даних, а тимчасові були записані в MySQL, варто зазначти що це допомогло оптимізувати зменшення навантаження на сервери, де показник навантаження після введеня в експуатацію знизився майже удвічі. З чого можна зробити висновок що завдяки блокчейн швидкість обробки великих даних зросла. І при цьому витрати енергії стали ще меншими, оскільки навіть на потужних серверах реляційних баз даних, такі як MySQL, буде доволі проблематичним здійснення таких операцій. Це ще один переконливий приклад успішного впровадження технології блокчейн.

І останній «Безпечне розподілене хмарне зберігання», якщо в вище описаних прикладах блокчейн показав себе з доволі екфективної сторони, то в даному випадку навпаки. Оскільки алгоритм пошуку починається з останнього блоку і рухається до першого то час на його виконання збільшується, це можна змінити якщо розпаралелити залучивши кілька вузлів, котрі будуть паралельно

шукати потрбну інформацію, проте саме шифрування даних на основі RSA є повільним і нездійсненним для довгих файлів. Цей приклад доводить що для кожного випадку потріно обирати свій метод.

Для ліпшого порівняння сформуємо таблицю 3.2, в котрій будуть описуватись такі параметри як «Швидкість», «Безпека», «Енергозатратність», та проаналізуємо.

Таблиця 3.2 – Опис параметрів під час застосування блокчейн

Назва проєкту	Швидкість	Безпека	Енергозатратність
Застосунок для проведення виборів	Висока	Середня	Низька-середня
РІСВТБ для опрацювання великих даних	Середня	Середня	Середня
Безпечне розподілене хмарне зберігання	Низька-середня	Висока	Низька-середня

В таблиці 3.2 ми бачило позначки які оцінюють параметри у вигляді шкали переходу з результатів «середній-високий».

Таблиця 3.3 – Параметри зі шкалою даних

Швидкість	Безпека	Енергозатратність
Висока: 148-230 (запитів/сек)	Висока: 0.2%-0.5% (ймов/втрч)	Висока: 6.10-7.67гВт/транзц
Середня: 55-147(запитів/сек)	Середня: 0.5%-0.20%(ймов/втрч)	Середня: 5.05-6.10гВт/транзц
Низька-середня: 10-54(запитів/сек)	Низька-середня: 0.20%-0.30%(ймов/втрч)	Низька-середня: 4.53-5.05гВт/транзц

Шкала була розроблена виходячі з математичних досліджень (див. таблицю 3.3) [12], [13]. В ній записані дані щодо швидкості обробки записів на секунду, ймовірність втручання в систему, та споживання електроенергії (гігават на одну транзакцію).

В цілому якщо говорити про швидкість то все буде залежати від кількості блоків, і пропорційно чим більше блоків тим більша безпека, з чого випливає і більша енергозатрантість.

4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Розподіл підприємств, установ та організацій за ступенем ризику їхньої господарської діяльності щодо забезпечення безпеки та захисту населення і територій від НС

Відповідно до Постанови Кабінету Міністрів України «Про затвердження критеріїв розподілу суб’єктів господарювання за ступенем ризику від провадження господарської діяльності для безпеки життя і здоров’я населення, навколишнього природного середовища та періодичності здійснення заходів державного нагляду (контролю)», критерії розподілу суб’єктів господарювання за ступенем ризику їх господарської діяльності для безпеки життя і здоров’я населення, навколишнього природного середовища (далі - критерії) встановлюються з метою оцінювання ступеня ризику від провадження господарської діяльності.

За критеріями суб’єкти господарської діяльності незалежно від форм власності розподіляються за високим, середнім та незначним ступенем ризику для безпеки життя і здоров’я населення, навколишнього природного середовища.

Критеріями оцінки ступеня ризику від впровадження господарської діяльності для безпеки життя і здоров'я населення, навколишнього природного середовища є:

1. Наявність:

- хімічних, біологічних, радіаційних, вибухо-, пожежо- та інших небезпечних речовин і матеріалів;
- загрози від потенційно небезпечних об'єктів, об'єктів підвищеної небезпеки;
- загрози від небезпечних гідрологічних (підтоплення, затоплення територій) та геологічних процесів (ґрунти, що просідають, карстоутворення, зсуви, обвали, селі, лавини, землетруси тощо);
- гідротехнічних споруд, хвостосховищ, шламонакопичувачів, накопичувачів токсичних відходів;

- будівель та споруд, що належать до аварійно небезпечних об'єктів;
- об'єктів інфраструктури життєзабезпечення населення та населених пунктів (енерго-, тепло-, газо-, водо- та інших видів постачання);
- будівель з покрівлею площею понад 1000 кв. метрів, виготовленою з використанням вантових та арочних конструкцій;

2. Чисельність людей, що за прогнозами можуть постійно або тимчасово перебувати на об'єктах та у місцях масового скупчення населення;
3. Належність підприємств до потенційно небезпечних об'єктів, об'єктів підвищеної небезпеки і таких, що мають стратегічне значення для економіки та безпеки держави.

До суб'єктів господарювання з високим ступенем ризику належать суб'єкти, у яких на праві власності, володіння чи користування перебувають:

- Об'єкти підвищеної небезпеки, потенційно небезпечні об'єкти і такі, щомають стратегічне значення для економіки та безпеки держави;
- Аварійно-рятувальні служби та формування;
- Об'єкти виробництва, зберігання, транспортування, використання, захоронення, знищення та утилізації отруйних речовин, у тому числі продуктів біотехнології та інших біологічних агентів, переліки та класи небезпеки яких визначені постановами Кабінету Міністрів України "Про затвердження Порядку одержання дозволу на виробництво, зберігання, транспортування, використання, захоронення, знищення та утилізацію отруйних речовин, у тому числі продуктів біотехнології та інших біологічних агентів" і "Про затвердження переліку особливо небезпечних хімічних речовин, виготовлення та реалізація яких підлягає ліцензуванню";
- Бази, склади, арсенали боєприпасів та військового озброєння;
- Об'єкти утилізації боєприпасів, небезпечних речовин та матеріалів;
- Радіаційно небезпечні об'єкти (крім атомних електростанцій), підприємства з виготовлення і переробки відпрацьованого ядерного палива, підприємства із захоронення радіоактивних відходів, науково-дослідні та проектні організації, що працюють з ядерними реакторами;

- Шлаконакопичувачі, накопичувачі токсичних відходів та гідротехнічні споруди;
- Об'єкти, що підлягають постійному та обов'язковому обслуговуванню державними аварійно-рятувальними службами;
- Об'єкти з масовим перебуванням людей, стадіони, ринки, рекреаційні зони, місця відпочинку населення (турбази, водні об'єкти тощо);
- Захисні споруди цивільного захисту (цивільної оборони).

До суб'єктів господарювання з середнім ступенем ризику належать суб'єкти, у яких на праві власності, володіння чи користування перебувають:

- Об'єкти, що за прогнозами можуть опинитися у зоні можливого ураження у разі виникнення надзвичайної ситуації на об'єкті підвищеної небезпеки та потенційно небезпечному об'єкті;
- Об'єкти, розташовані на територіях з небезпечними гідрологічними та геологічними процесами;
- Об'єкти, розташовані на територіях, що за прогнозами можуть опинитися у зоні можливого затоплення у разі прориву або руйнування гідроспоруди;
- Об'єкти інфраструктури життєзабезпечення населення та населених пунктів;
- Будівлі та споруди з покрівлею площею понад 1000 кв. метрів, виготовленою з використанням вантових та арочних конструкцій;
- Навчальні та дошкільні заклади, домоуправління, інші суб'єкти господарювання, що згідно з нормативно-правовими актами проводять навчання населення діям у надзвичайній ситуації;
- Проектні та експертні, інші організації, діяльність яких пов'язана із забезпеченням техногенної безпеки у сфері цивільного захисту.

До суб'єктів господарювання з незначним ступенем ризику належать суб'єкти, що не віднесені до суб'єктів господарювання з високим та середнім ступенем ризику.

4.2 Штучне освітлення

За функціональним призначенням штучне освітлення підрозділяється на такі види: робоче, аварійне, охоронне, чергове. Аварійне освітлення поділяється на освітлення безпеки і евакуаційне. Робоче освітлення створює необхідні умови для нормальної трудової діяльності людини. Аварійне освітлення включають при виході з ладу робочого освітлення. Світильники аварійного освітлення живляться від автономного джерела й повинні забезпечувати освітленість не менше 5 %% величини робочого освітлення, але не менше 2 лк на робочих поверхнях і не менше 1 лк на території підприємства. Аварійне освітлення передбачається на підприємствах, де зупинка технологічних процесів може призвести до людських жертв або значних економічних втрат. Аварійне освітлення поділяється на освітлення безпеки і евакуаційне.

Охоронне освітлення передбачається для території підприємств, а також включається в неробочий час для освітлення приміщень. З цією метою використовується частина світильників робочого або аварійного освітлення. Евакуаційне освітлення призначене для евакуації людей і матеріальних цінностей під час виникнення небезпеки. Воно передбачається у виробничих приміщеннях з кількістю працюючих більше 50 осіб, а також у приміщеннях цивільних і допоміжних будинків підприємств, якщо в них одночасно знаходиться більше 100 осіб. Така система повинна забезпечувати освітленість на підлозі основних переходів не менше, ніж 0,5 лк, а на відкритих територіях – не менше 0,2 лк. Чергове освітлення передбачається в неробочий час, де використовується частина світильників робочого освітлення.

За розміщенням джерел світла штучне освітлення підрозділяється на загальне, місцеве і комбіноване. При загальному освітленні світильники розташовують у верхній зоні приміщення. Загальне освітлення, у свою чергу, підрозділяється на рівномірне, коли світильники розташовані на однаковій відстані один від одного у верхній частині приміщення, і локальне, коли щільність розміщення світильників неоднакова й відповідає розташуванню устаткування в приміщенні. При місцевому освітленні світильники розміщують

безпосередньо над робочою поверхнею. При недостатньому рівні загального освітлення, місцева освітленість робочого місця й навколишнього простору значно відрізняються, що створює несприятливі умови праці й підвищує небезпеку травматизму. Тому на підприємствах використання тільки місцевого освітлення заборонено. Поєднання системи місцевого й загального освітлення називається комбінованим освітленням.

Нормування штучної освітленості виконують в такий спосіб. Визначають точність виконуваної зорової роботи (за найменшим розміром об'єкта розрізнення); за цією характеристикою визначають розряд і під розряд зорових робіт з урахуванням характеристик тла й контрасту об'єкта розрізнення з тлом. Сукупність цих характеристик дозволяє визначити величину нормативної освітленості ($E_н$). Алгоритм визначення нормованої штучної освітленості наведений на рисунку 4.1.

Рисунок 4.1 – Алгоритм визначення нормованої штучної освітленості

Розрахунок системи штучного освітлення зводиться до вибору системи освітлення, визначення типу й необхідної кількості світлових приладів (ламп) та світильників.

Розрахунок освітлювальної установки може бути виконаний різними способами, що базуються на трьох основних методах: світлового потоку (коефіцієнта використання світлового потоку), питомої потужності і точкового.

Метод світлового потоку (коефіцієнта використання) застосовують для розрахунку системи загального рівномірного освітлення. Він дає змогу визначити світловий потік джерел світла, необхідний для створення нормованого освітлення горизонтальної площі (S), з урахуванням прямого й відбитого потоків світла.

Необхідний світловий потік $Ф_р$ визначають за формулою 4.1:

$$Ф_р = E_н \cdot K \cdot S \cdot Z / (N \cdot \eta \cdot v), \quad (4.1)$$

де:

- $E_н$ – нормативна освітленість, лк (за ДБН В.2.5-28-2018);
- K = 1,2...2,0 – коефіцієнт запасу, що враховує запиленість приміщення (і, як наслідок – світильників) і зниження світлового потоку світлових приладів у процесі їх експлуатації;
- S – площа, що освітлюється, м^2; Z = 1,0...1,15 – коефіцієнт, що характеризує нерівномірність освітлення;
- N – прийнята кількість світильників;
- v = 0,8 – коефіцієнт затінення (для приміщень з фіксованим розташуванням працюючих);
- η – коефіцієнт використання світлового потоку світильників на розрахунковій площі.

Величину цього коефіцієнта визначають залежно від типу світильника, коефіцієнтів відбиття полу, стін, стелі й індексу приміщення (див. формулу 4.2):

$$i = A \cdot B/h(A + B), \quad (4.2)$$

де:

- A та B – розміри приміщення в плані;
- h – висота підвісу світильників над робочою поверхнею, м.

Обчислений світловий потік ($Ф_р$) світильника порівнюють із світловими потоками існуючих світлових приладів ($Ф_{факт}$) і приймають значення, найближче до розрахункової величини. При цьому допустиме відхилення $Ф_{факт}$

від $Ф_р$ повинне складати не більше (–10...+ 20 %%). У результаті цього етапу розрахунку системи освітлення здійснюють і вибір світлових приладів (ламп).

Різновидом розглянутого методу є метод питомої потужності. Його застосовують тільки для орієнтовних розрахунків при різних системах освітлення. Метод дає змогу визначити необхідну потужність лампи $Р_л$, (Вт), що буде використовуватися в системі освітлення, для створення нормованого освітлення (див. формулу 4.3).

$$P_л = r \cdot S/N, \qquad (4.3)$$

де:

- r – питома потужність прийнятої лампи, Вт/м^2. Цей параметр знаходять за спеціальними таблицями залежно від нормованої освітленості, площі приміщення, висоти підвісу, типу світильника і коефіцієнта запасу; S – площа приміщення, м^2;
- N – кількість ламп у системі освітлення.

При розрахунках систем освітлення, що утворені декількома світильниками, підраховують освітленість у необхідній точці приміщення від кожного з них, а кінцеві результати зіставляють.

ВИСНОВКИ

В першому розділі ми зрозуміли принципи роботи блокчейн-технології, ознайомились з методами які лежать в основі блокчейн.

Другий розділ був більш теоретичний, наповнений прикладами застосувань в різних сферах нашого життя, та порівнянь дохідності компаній після початку використання блокчейн технологій, що дало змогу на реальній статистиці зрозуміти доцільність впровадження цієї технології. Аналіз ризиків та недоліків також присутній у розділі, що допомагає об’єктивно оцінити ефективність блокчейн виходячи з математичної моделі яка заснована на логістичних функціях.

Реалізація досить важливий етап під час аналізу застосування блокчейн-технології, якщо порівнювати з другим розділом, то в третьому ми бачимо вже принципи роботи програм та систем і можемо на практиці бачити усі плюси, мінуси та проблеми які потрібно вирішувати при впровадженні блокчейн у систему.

В цілому варто зазначити що блокчейн-технології досить ефективні завдяки децентралізованій системі та незмінним блокам, що забезпечують безпеку та прозорість до даних. Проте незважаючи на використання у багатьох галузях все ще потребує оптимізації зі сторони швидкості та енергозатратності.

Порівнюючи блокчейн з традиційними системами не можна сказати що має унікальні переваги, але в питанні безпеки він стає доволі ефективним, і в поєднанні ліпше обробляє великі обсяги даних та має нижчі вимоги до ресурсів. Тому для кожного випадку потрібно обирати відповідний метод.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Coulouris, G. F., Dollimore, J., & Kindberg, T. (2005). Distributed systems: concepts and design. Pearson Education, New York City, United States.

2. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260. Available online: https://www.debr.io/article/21260-bitcoin-a-peer-to-peer-electronic-cash-system (accessed on January 2023).

3. Lee, D. K. C., Guo, L., & Wang, Y. (2018). Cryptocurrency: A new investment opportunity? Journal of Alternative Investments, 20(3), 16–40. doi:10.3905/jai.2018.20.3.016.

4. Yu, S. (2010). Data sharing on untrusted storage with attribute-based encryption. Ph.D. Thesis, Worcester Polytechnic Institute,Worcester, United States.

5. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. doi:10.1145/359340.359342.

6. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми Україна), 191-193. https://doi.org/10.62731/mcnd-14.06.2024.004

7. Titcomb, j. (2017). US regulator warns of 'fraud and manipulation' amid cryptocurrency craze. Daily Telegraph. Available online: http://www.telegraph.co.uk/technology/2017/12/12/us-regulator-warns-fraud manipulation-amid-cryptocurrency-craze/ (accessed on January 2023).

8. He, H., Zheng, L., Li, P., Deng, L., Huang, L., & Chen, X. (2020). An efficient attribute-based hierarchical data access control scheme in cloud computing. Human-Centric Computing and Information Sciences, 10(1), 1-19. doi:10.1186/s13673-020-00255-5.

9. Wang, S., Wang, X., & Zhang, Y. (2019). A Secure Cloud Storage Framework with Access Control Based on Blockchain. IEEE Access, 7, 112713–112725. doi:10.1109/ACCESS.2019.2929205.

10. Qin, X., Huang, Y., Yang, Z., & Li, X. (2021). A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. Journal of Systems Architecture, 112, 101854. doi:10.1016/j.sysarc.2020.101854.
11. Тимощук, В., & Стебельський, М. (2023). Шифрування даних в операційних системах. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 183-184.
12. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146. https://doi.org/10.62731/mcnd-24.05.2024.001
13. Кучковський В. В. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ БЛОКЧЕЙН ДЛЯ ОПРАЦЮВАННЯ ВЕЛИКИХ ДАНИХ : дис. … д-ра техн. наук : 122. Львів, 2022. URL: https://lpnu.ua/sites/default/files/2022/radaphd/21254/disertaciya_0.pdf
14. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170. https://doi.org/10.36074/logos-21.06.2024.034
15. Yesin, V., Karpinski, M., Yesina, M., Vilihura, V., Kozak, R., Shevchuk, R. (2023). Technique for Searching Data in a Cryptographically Protected SQL Database. Applied Sciences, 13(20), art. no. 11525, 1-21. doi: 10.3390/app132011525.
16. Kuznetsov, A., Karpinski, M., Ziubina, R., Kandiy, S., Frontoni E., Veselska, O., & Kozak, R. (2023). Generation of nonlinear substitutions by simulated annealing algorithm. Information, 14(5), art. no. 259, 1-16. doi: 10.3390/info14050259.
17. Yakymenko, I., Karpinski, M., Shevchuk, R., & Kasianchuk, M. (2024). Symmetric Encryption Algorithms in a Polynomial Residue Number System. Journal of Applied Mathematics, art. id 4894415, 1-12. doi: 10.1155/2024/4894415.
18. Kuznetsov, O., Poluyanenko, N., Frontoni, E., Kandiy, S., Karpinski, M., & Shevchuk, R. (2024). Enhancing Cryptographic Primitives through Dynamic Cost Function Optimization in Heuristic Search. Electronics, 13(10), 1-52. doi: 10.3390/electronics13101825.

19. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль: ТНТУ. 2022. 150 с.