МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Мартиненко Володимир Віталійович

УДК 004.056.5:004.94

КВАЛІФІКАЦІЙНА РОБОТА

Дослідження ефективності використання технологій блокчейн для підвищення кібербезпеки

125 «Кібербезпека та захист інформації»

Подається на здобуття освітнього ступеня магістр

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи:
Веретюк Сергій Михайлович,
кандидат технічних наук, доцент

Житомир – 2024

Висновок кафедри_____

за результатами попереднього захисту:_____

Протокол засідання кафедри_____

№ ____ від «_____» _____ 20____ р.

Завідувач кафедри_____

_____ _____ _____

(науковій ступінь, вчене звання) (підпис) (прізвище, ім’я, по батькові)

«_____» _____ 20____ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____ захистив (ла)

(прізвище ,ім’я, по батькові)

кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____
за шкалою ECT8 _____
за національною шкалою _____

Секретар ЕК

_____ _____ _____

(науковій ступінь, вчене звання) (підпис) (прізвище, ім’я, по батькові)

АНОТАЦІЯ

Мартиненко В.В. Дослідження ефективності використання технологій блокчейн для підвищення кібербезпеки. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 – кібербезпека та захист інформації. – Поліський національний університет, Житомир, 2024

Дослідження присвячено розробці децентралізованої системи обробки запитів на основі технології блокчейну з метою підвищення кібербезпеки та захисту від DDoS-атак. У роботі запропоновано алгоритм, який забезпечує прозорість, масштабованість і стійкість системи до кібератак за рахунок використання смарт-контрактів, децентралізованих механізмів розподілу навантаження та захисту даних. Проведено імітаційне моделювання, розробленого. Практична цінність роботи полягає у Запропонований алгоритм дозволяє реалізувати прозорий та автоматизований процес обробки запитів у децентралізованих системах.

Ключові слова: блокчейн, кібербезпека, децентралізована система, DDoS-атака, смарт-контракти.

Робота містить 38 сторінок, 5 рисунків, 6 таблиць, 32 літературних джерел.

SUMMARY

Martynenko V.V. Research on the Effectiveness of Blockchain Technologies for Enhancing Cybersecurity.
A qualification thesis for obtaining the Master’s degree in specialty 125 – Cybersecurity and Information Protection. – Polissia National University, Zhytomyr, 2024.

This research is dedicated to the development of a decentralized request processing system based on blockchain technology to enhance cybersecurity and protect against DDoS attacks. The study proposes an algorithm that ensures

transparency, scalability, and system resilience to cyberattacks through the use of smart contracts, decentralized load-balancing mechanisms, and data protection. Simulation modeling of the developed system was conducted. The practical significance of the work lies in the proposed algorithm's ability to implement a transparent and automated request processing process in decentralized systems.

Keywords**:** blockchain, cybersecurity, decentralized system, DDoS attack, smart contracts.

Зміст

Вступ

Розвиток цифрових технологій супроводжується стрімким зростанням кількості та складності кіберзагроз, що становлять загрозу для функціонування інформаційних систем у різних галузях. Це включає атаки на державні установи, корпоративні мережі, системи Інтернету речей і персональні дані користувачів. Наслідки таких атак охоплюють фінансові втрати, втрату конфіденційності та руйнацію репутації організацій. Ці виклики зумовлюють необхідність розробки підходів до забезпечення кібербезпеки, що відповідають сучасним реаліям цифрового середовища.

Актуальність обумовлена зростаючою кількістю кібератак. Атаки, такі як DDoS, фішинг, зловмисне програмне забезпечення та витоки даних, завдають значної шкоди як бізнесу, так і державним організаціям, спричиняючи фінансові втрати та порушення конфіденційності. Тому дослідження, удосконалення та розроблення нових інструментів та методів забезпечення кібербезпеки є актуальним завданням. Удосконалено алгоритм децентралізованої обробки запитів із використанням технології блокчейн, що забезпечує стійкість до DDoS-атак шляхом економічного стимулювання та динамічного балансування навантаження.

Мета: розроблення методу розподілу запитів на основі технології блокчейн для підвищення рівня кібербезпеки об'єктів інформаційної діяльності.

Об'єкт: процеси забезпечення кібербезпеки на основі блокчейн.

Для досягнення мети дослідження, яка полягає у розробленні алгоритму децентралізованої обробки запитів в інформаційній системі на основі технології блокчейн, було поставлено такі завдання:

1. Дослідити особливості обробки запитів централізованими системами, виконати аналіз недоліків та переваг централізованих систем.
2. Дослідити механізми автоматизованого виконання умов контрактів у децентралізованих системах, а також їх переваги у порівнянні з централізованими підходами.

3. Розробити механізм, що забезпечує прозорість, безпеку та рівномірний розподіл запитів між вузлами мережі, використовуючи переваги блокчейн-технології. оцінити ефективність розробленого алгоритму в умовах високого навантаження та потенційних атак, таких як DDoS, шляхом проведення тестових сценаріїв.

4. Розробити рекомендації щодо використання блокчейну для розроблення децентралізованих систем обробки запитів.

РОЗДІЛ 1. Аналіз використання технології блокчейн для вирішень завдань кібербезпеки

1.1. Особливості технології блокчейн в кібербезпеці

Блокчейн це розподілена база даних, яка зберігає впорядкований ланцюг записів (блоків), що постійно збільшується. Кожен блок містить часову мітку, хеш попереднього блоку та дані транзакцій, організовані у вигляді хеш-дерева. Інформація про транзакції зазвичай є відкритою та не зашифрованою. Захист від фальсифікації та викривлень забезпечується тим, що хеш всього блоку включається до наступного блоку.

Технологія блокчейн пропонує розв’язання проблеми довіри між учасниками мережі, оскільки всі учасники мають доступ до повної історії транзакцій, що робить підробку або зміну даних неможливим. Це дозволяє створити систему, яка працює без потреби у третій стороні чи посереднику. [1]

Блокчейн функціонує як розподілений реєстр, у якому дані зберігаються одночасно на багатьох вузлах мережі (ноди). Кожен вузол містить повну копію всіх транзакцій, що відбуваються в системі, що мінімізує ризик централізованого контролю та забезпечує надійність і доступність даних, рисунок 1. Цей підхід запобігає втраті або модифікації інформації у разі виходу з ладу окремих вузлів чи спроб зловмисного втручання. Така архітектура знижує залежність від єдиної точки збою (single point of failure) і робить систему стійкою до зовнішніх атак.

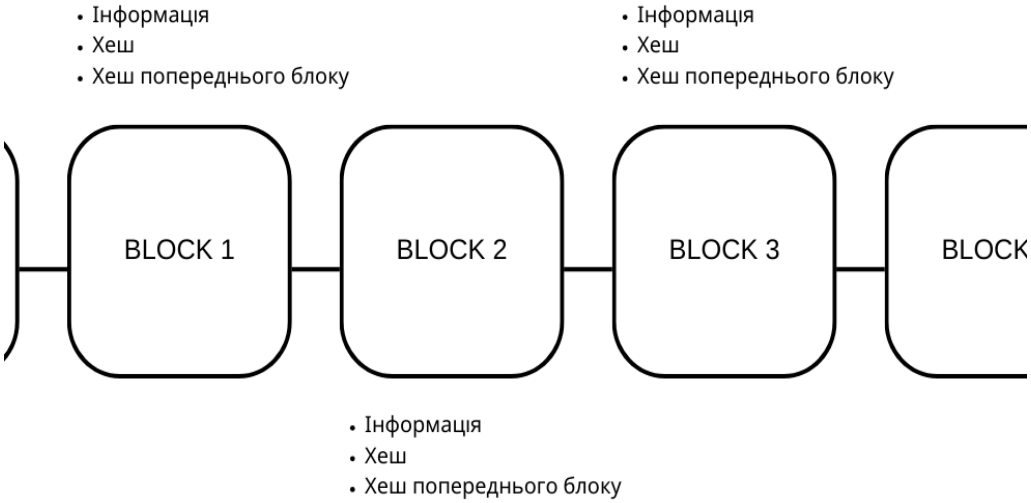

Рисунок 1. Блоки блокчейну

Технологія блокчейн забезпечує високий рівень прозорості, оскільки кожен учасник мережі має доступ до історії всіх транзакцій і може самостійно перевіряти їхню легітимність. У більшості публічних блокчейнів (наприклад, Bitcoin чи Ethereum) усі записи є відкритими для перегляду будь-яким користувачем, що підвищує рівень довіри до системи.

Прозорість також ускладнює реалізацію шахрайських схем, оскільки всі транзакції доступні для аудиту в режимі реального часу. Однак у приватних блокчейнах прозорість може бути обмеженою, що дозволяє контролювати доступ до інформації залежно від рівня авторизації.

Одна з ключових характеристик блокчейну полягає в незмінності записів. Після того як транзакція внесена до блоку та підтверджена мережею, вона стає незворотною й не може бути змінена або видалена. Це досягається завдяки криптографічному хешуванню даних і механізму консенсусу між вузлами. Будь-яка спроба модифікувати вже існуючі записи порушить цілісність блоків і буде відразу виявлена іншими учасниками мережі. Незмінність забезпечує високий рівень безпеки даних та є важливим фактором для ведення цифрових реєстрів, обліку фінансових операцій та інших критичних процесів, де важливо запобігти маніпуляціям з інформацією. [2]

Централізовані та децентралізовані системи відрізняються архітектурою, управлінням даними та рівнем безпеки. Розуміння цих відмінностей є важливим для оцінки того, як блокчейн може покращити існуючі рішення в галузі кібербезпеки, див таблиця 1.1

Таблиця 1.1 - Порівняння централізованих систем з децентралізованими

Критерій	Централізовані системи	Децентралізовані системи (блокчейн)
Архітектура та управління	Єдиний центральний сервер або кілька серверів контролюють систему.	Відсутній центральний керуючий орган; дані зберігаються на багатьох вузлах.
Безпека та надійність	Єдина точка збою (single point of failure), що	Стійкість до збоїв і атак завдяки розподіленому

	підвищує ризик збоїв.	зберіганню даних.
Контроль і довіра	Користувачі повинні довіряти центральному органу або адміністратору.	Довіра розподіляється серед учасників, прозорість записів забезпечує самоперевірку.
Продуктивність	Вища продуктивність завдяки централізованому ухваленню рішень.	Менша швидкість через потребу у досягненні консенсусу між вузлами.
Масштабованість	Проблеми масштабування при великому навантаженні на центральний сервер.	Легке масштабування за рахунок додавання нових вузлів.
Вразливість до атак	Вразливі до DDoS-атак та внутрішніх зловживань.	Стійкість до зовнішніх атак, зокрема до маніпуляцій даними.
Використання в кібербезпеці	Використовуються для зберігання конфіденційних даних та контролю доступу.	Корисні для аутентифікації, захисту інфраструктури та управління ідентичностями.

Таким чином, основна перевага децентралізованих систем, таких як блокчейн, полягає у підвищенні надійності та стійкості до атак за рахунок усунення єдиної точки збою та прозорості даних. Водночас централізовані системи можуть забезпечувати вищу продуктивність і зручність управління, але потребують додаткових заходів для мінімізації ризиків, пов’язаних із залежністю від центрального елемента. На основі порівняння можна зробити висновок, що основна перевага децентралізованих систем полягає у підвищенні надійності, прозорості та стійкості до атак. Використання блокчейн-технологій, зокрема смарт-контрактів, відкриває нові перспективи для забезпечення кібербезпеки, усуваючи недоліки централізованих рішень.[3]

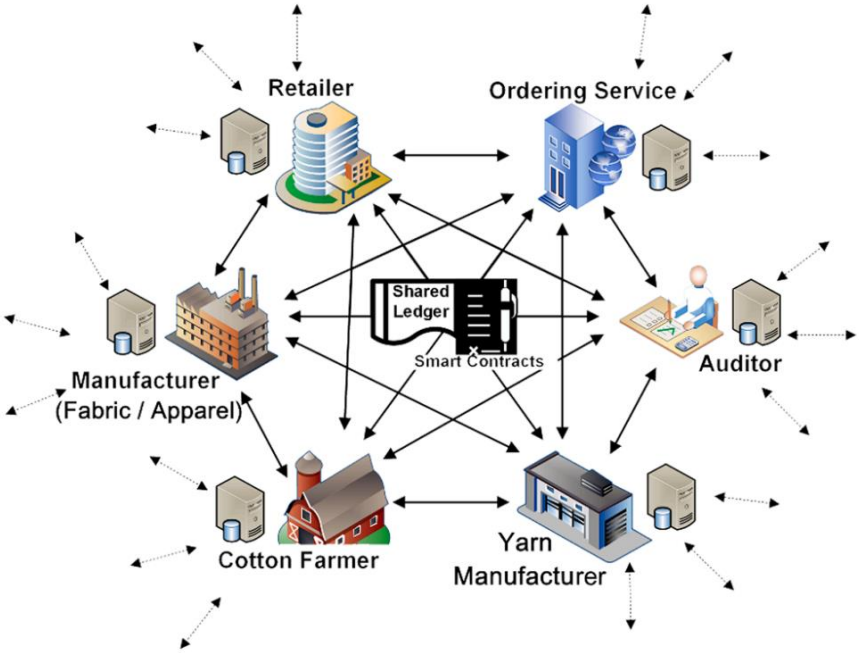

Рисунок 1.2 Децентралізована мережа для обміну інформації на основі блокчейну [4]

Смарт-контракти (англ. *smart contracts*) — це комп’ютерні протоколи, які автоматизують, забезпечують та виконують договірні угоди між сторонами без посередників. Вони функціонують на основі децентралізованих блокчейн-систем, які забезпечують прозорість, безпеку та незмінність даних.

Централізовані системи обробки запитів мають низку вразливостей, які можуть виникнути під час DDoS-атак. Використання смарт-контрактів може допомогти пом'якшити ці ризики. У таблиці 1.2 наведено основні вразливості, приклади та поясненням, як смарт-контракти можуть сприяти їхньому усуненню.

Таблиця 1.2 Використання смарт-контрактів для пом'якшення ризиків DDOS атак

Вразливість	**Опис**	**Приклад**	**Пом'якшення ризиків за допомогою смарт-контрактів**
Єдина точка відмови	Централізовані системи мають один сервер або вузол, відмова якого	DDoS-атака на центральний сервер призводить до його	Смарт-контракти працюють на децентралізованих блокчейн-платформах, що усуває єдину точку відмови. Якщо окремі вузли зазнають

	призводить до недоступності всього сервісу.	перевантаження.	атаки, інші продовжують обробляти запитти, забезпечуючи безперервність. [5]
Обмежена пропускна здатність	Централізовані системи мають фіксовану пропускну здатність, що обмежує кількість запитів, які можуть бути оброблені одночасно.	Велика кількість запитів під час DDoS-атаки перевищує можливості системи, спричиняючи відмову в обслуговуванні.	Смарт-контракти можуть бути розгорнуті на масштабованих блокчейн-мережах, які адаптуються до збільшення навантаження, розподіляючи обробку запитів між всіма вузлами. [5]
Відсутність прозорості в обробці запитів	Користувачі не мають можливості перевірити, як обробляються їхні запити, що може призвести до недовіри.	Користувачу не відомо, чи був його запит оброблений, чи відхилений під час перевантаження системи.	Смарт-контракти забезпечують прозорість обробки запитів, оскільки всі транзакції записуються в блокчейн і можуть бути перевірені. Це підвищує довіру користувачів до системи. [6]
Вразливість до маніпуляцій даними	Централізовані системи можуть бути піддані несанкціонованим змінам даних, що знижує їхню надійність.	Зловмисник отримує доступ до центральної бази даних і змінює інформацію на свою користь.	Смарт-контракти працюють на блокчейні, де дані захищені криптографічними методами, що унеможливлює їхню зміну без консенсусу мережі. Це забезпечує цілісність інформації. [6]
Складність масштабування	Збільшення потужностей централізованої системи вимагає	Необхідність придбання додаткових серверів та налаштування	Блокчейн-мережі, на яких працюють смарт-контракти, зазвичай мають вбудовані механізми масштабування, що дозволяє швидко

	значних ресурсів і часу.	інфраструктури для обробки більшої кількості запитів.	адаптуватися до зростання навантаження без значних витрат. [7]
Вразливість до атак на рівні додатків	Централізовані системи мають вразливості в програмному забезпеченні, які зловмисники використовують для проведення атак.	Атака SQL-ін'єкція через вразливість у веб-додатку призводить до витоку даних.	Смарт-контракти проходять ретельний аудит коду перед розгортанням, що знижує ймовірність наявності вразливостей. Крім того, їхній код є прозорим і доступним для перевірки. [8]

Технологія блокчейн є інноваційним рішенням, яке змінює підходи до забезпечення кібербезпеки. Її основні характеристики, такі як децентралізація, незмінність даних, прозорість транзакцій, забезпечують ефективний захист інформації та мінімізують ризики кіберзагроз. Завжди є потреби в нових механізмах захисту даних, блокчейн демонструє високу стійкість до маніпуляцій та атак, що робить його перспективним інструментом для кібербезпеки.

Актуальність дослідження підкреслюється і зростаючою популярністю смарт-контрактів, які спрощують та автоматизують виконання транзакцій, а також використанням децентралізованих систем у забезпеченні цифрової безпеки. Використання блокчейну дозволяє створити високонадійні системи без центрального контролю, що стає особливо важливим у сучасних умовах підвищених вимог до прозорості та захищеності інформації.

1.2 Застосування технології блокчейн в кібербезпеці

Блокчейн дозволяє реалізувати децентралізоване управління ідентифікацією, захист даних, автоматизацію транзакцій через смарт-контракти, а також протидію DDoS-атакам.

Блокчейн сприяє децентралізації через свої фундаментальні принципи функціонування, які усувають необхідність у центральному органі управління. Це досягається за рахунок розподілу відповідальності та контролю між учасниками мережі.

Технологія блокчейн функціонує як розподілений реєстр, де всі учасники мають копію даних. Це забезпечує прозорість і усуває ризик залежності від одного сервера. Наприклад, у криптовалютах, таких як Bitcoin чи Ethereum, транзакції записуються у всіх вузлах мережі, що робить їх доступними для перевірки кожним учасником.

Процес узгодження дійсності транзакцій здійснюється через консенсусні механізми, такі як Proof of Work (PoW) або Proof of Stake (PoS). Ці механізми дозволяють мережі досягати спільної згоди без втручання посередників. Наприклад, у Bitcoin використовується PoW, який забезпечує високу безпеку системи, тоді як Ethereum перейшов на PoS, щоб підвищити ефективність і масштабованість.[9]

Третя важлива характеристика — незмінність даних. Інформація, що записується у блокчейн, зберігається у вигляді блоків, кожен з яких містить хеш попереднього блоку. Це створює ланцюг, який надзвичайно складно змінити. Ця властивість забезпечує автентичність даних та їх цілісність, що корисно, наприклад, для захисту важливих документів або аудиту фінансових записів.

Четвертий аспект — відсутність центрального контролю. Учасники мережі мають рівні права щодо доступу до даних і ухвалення рішень. Це усуває ризик монополізації управління, що є важливим у системах децентралізованої ідентифікації.

Окрім цього, блокчейн дозволяє створювати децентралізовані додатки (DApps), які працюють на основі смарт-контрактів. Такі програми автоматично

виконують закладені у них умови, забезпечуючи прозорість і безпеку. DApps застосовуються у фінансових системах та децентралізованих організаціях.[10]

Таким чином, блокчейн забезпечує децентралізацію через розподіл даних, спільне ухвалення рішень, забезпечення цілісності інформації та автоматизацію процесів. Це створює нові можливості для підвищення безпеки, прозорості та довіри у різних галузях.

1.3 Синтез критеріїв для оцінювання ефективності блокчейну в кібербезпеці

Оцінювання ефективності блокчейну в забезпеченні кібербезпеки дозволяє комплексно оцінити, наскільки ефективно блокчейн може сприяти вирішенню завдань у сфері кібербезпеки. Вони охоплюють технічну, організаційну та регуляторну складові, забезпечуючи інтегрований підхід до оцінювання.

Таблиця 1.3 Критерії оцінки ефективності блокчейну в кібербезпеці

Категорія	**Критерій**	**Опис**	**Показник**
Захист даних	Незмінність даних	Гарантія незмінності записів у блокчейні.	Відсутність виявлених змін у записах.
	Шифрування	Використання криптографії для захисту даних.	Використання алгоритмів (наприклад, AES-256) і довжина ключа.[11]
Захищеність від атак	Захист від DDoS-атак	Стійкість до атак, спрямованих на виведення системи з ладу.	Час простою системи під час атак.
	Стійкість до підробки транзакцій	Захист даних від несанкціонованих змін.	Частота виявлення спроб підробки.

Конфіденційність	Анонімність транзакцій	Захист приватності користувачів.	Використання технологій анонімності (наприклад, zk-SNARK[12]).
	Контроль доступу	Обмеження доступу до даних неавторизованим особам.	Кількість випадків несанкціонованого доступу.
Резервування та відновлення	Відмовостійкість	Здатність системи працювати навіть у разі виходу з ладу окремих вузлів.	Відсоток доступності системи.
	Механізми резервного копіювання	Збереження та відновлення даних у разі компрометації.	Час, необхідний для відновлення даних.
Інтеграція кіберзахисту	Автоматичне реагування	Реалізація автоматизованих механізмів захисту від загроз.	Середній час реагування на кіберзагрози.
	Перевірка смарт-контрактів	Перевірка коду на наявність вразливостей.	Кількість виявлених і усунутих вразливостей.

Децентралізація	Розподіл вузлів	Географічний та організаційний розподіл вузлів у мережі.	Кількість вузлів і їхній розподіл.
	Стійкість до відмови	Запобігання захопленню контролю більшістю вузлів.	Частка вузлів, необхідна для компрометації системи.
Аудит і верифікація	Прозорість записів	Можливість безпечної перевірки даних.	Кількість успішно завершених аудитів.
Регуляторна відповідність	Відповідність стандартам	Дотримання нормативних вимог у сфері кібербезпеки.	Кількість сертифікацій чи виявлених невідповідностей.

Для оцінки ефективності блокчейну в кібербезпеці за допомогою п’ятибальної системи можна використовувати такі оцінки:

- 1 бал —(Very Low): критерій не відповідає вимогам або має серйозні недоліки, які суттєво знижують ефективність.
- 2 бали — (Low): критерій працює, але має значні обмеження або вразливості.
- 3 бали — (Medium): критерій задовільно працює, але має певні недоліки, які можуть вплинути на ефективність.
- 4 бали — (High): критерій відповідає більшості вимог і працює на високому рівні без суттєвих недоліків.

- 5 балів — (Very High): критерій працює на найвищому рівні без значних недоліків, забезпечує високу ефективність у забезпеченні кібербезпеки.

При оцінці конкретного блокчейн-рішення можна підсумувати бали по кожному критерію та отримати загальну оцінку ефективності блокчейну в контексті кібербезпеки.

Висновки до першого розділу

Технологія блокчейн має значний потенціал для покращення рівня безпеки в сфері кібербезпеки завдяки своїм характеристикам, таким як децентралізація, незмінність даних і прозорість. Блокчейн може істотно підвищити захист даних, знижуючи ризики централізованих атак, зокрема, відмовостійкість і захист від DDoS-атак, а також гарантувати цілісність і анонімність транзакцій. Важливо зазначити, що блокчейн має і деякі недоліки, зокрема, меншу швидкість обробки транзакцій порівняно з централізованими системами через потребу в досягненні консенсусу серед учасників мережі. Водночас, через свої переваги в забезпеченні прозорості і неможливості змінювати історичні дані, блокчейн залишається надійним інструментом для захисту даних і контролю доступу.

Запропонована п’ятибальна система оцінювання ефективності блокчейн-рішень дозволяє комплексно оцінити ключові характеристики рішення на основі технлогії, такі як захист даних, конфіденційність, захист від атак, децентралізація, та відповідність вимогам. Підсумкова оцінка за кожним критерієм дозволяє точно визначити рівень ефективності конкретного блокчейн-рішення в забезпеченні кібербезпеки та прийняти обґрунтовані рішення щодо його впровадження в різні сфери.

2 РОЗДІЛ. Розроблення алгоритму децентралізованої обробки запитів в інформаційній системі на основі технології блокчейн

2.1 Концепція смарт-контракт

Смарт-контракти на блокчейні характеризуються тим, що процес виконання умов контракту, включно з реалізацією зобов'язань та відповідним переказом цінностей (наприклад, платежів), відбувається автоматизовано та децентралізовано. На відміну від традиційних централізованих моделей, де операції здійснюються через постачальника, його банк або третю довірену сторону (серверна архітектура, Web 2.0), у випадку блокчейну виконання забезпечується за допомогою децентралізованої мережі (peer-to-peer, Web 3.0). [13]

Принцип роботи смарт-контракту представлений на рис. 2.1 і поділяється на три основні етапи:

Етап 1: створення смарт-контракту здійснюється за участю кількох користувачів, після чого його функціональність кодується у програмний код. Далі система смарт-контракту передає його в блокчейн-мережу, причому учасники підтверджують контракт шляхом підпису своїми приватними ключами.

Етап 2: смарт-контракт розповсюджується на всі вузли блокчейн-мережі через P2P-зв’язок. У цьому процесі вузол верифікації виконує збереження та пакетування контракту. Після перевірки контракту та досягнення консенсусу він остаточно записується у блокчейн. Основна мета верифікації - перевірити відповідність підпису приватного ключа учасників їхнім аккаунтам.

Етап 3: смарт-контракт періодично перевіряє стан автомата і виконує транзакцію, коли виконуються задані умови активації. У випадку, якщо всі транзакції, зазначені в контракті, завершені, відповідні дані блокчейну будуть збережені. Якщо ні - виконання продовжуватиметься до повного завершення. [14]

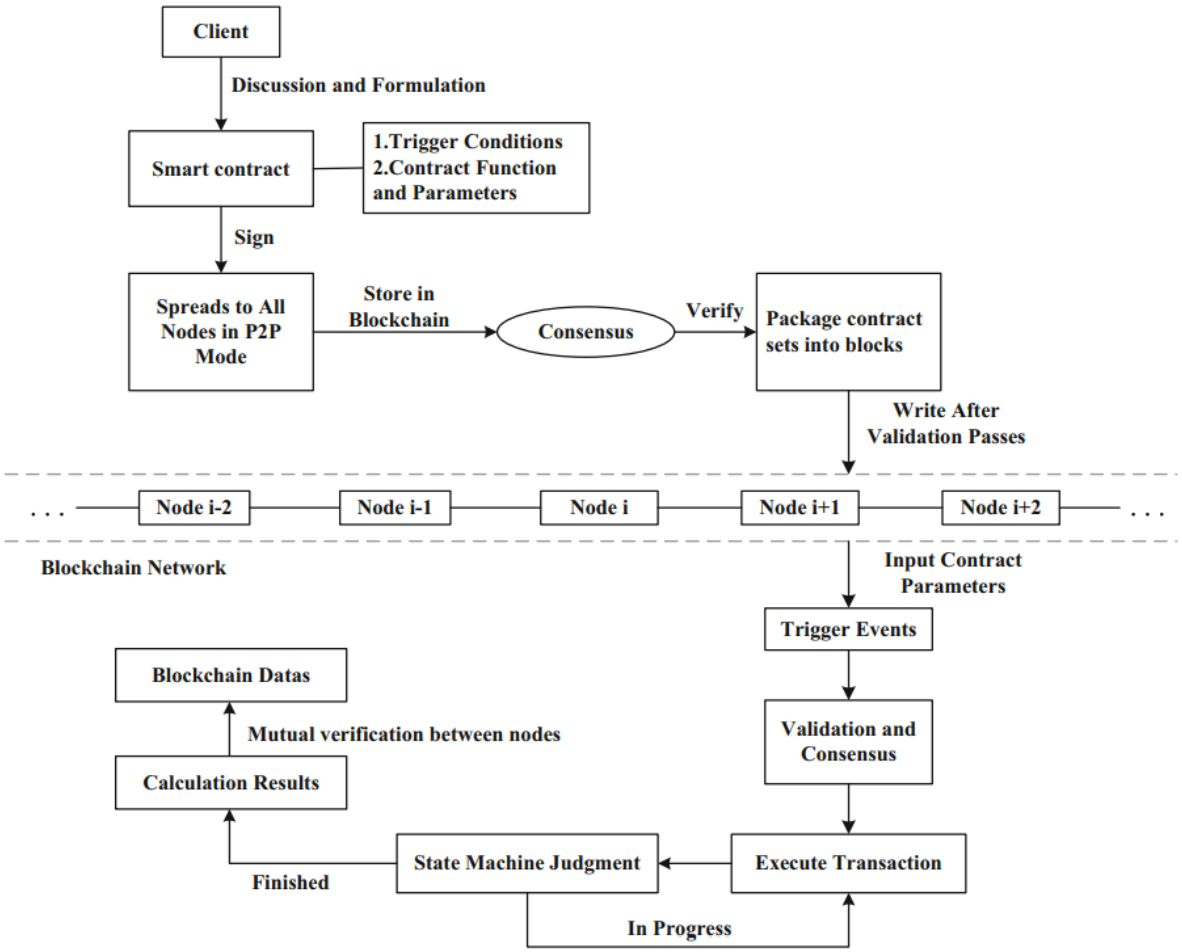

Рисунок 2.1 Принцип роботи смарт-контракту [15]

Смарт-контракти можуть управляти транзакційною діяльністю агентів, надавати їм авторизацію та нагляд, а також ефективно інтегрувати розрізнені індивідуальні інтереси з мінімальними витратами. [16]

2.2 Загальний алгоритм децентралізованої обробки запитів на технології блокчейн

Децентралізована обробка запитів у блокчейн-мережах базується на використанні механізмів розподіленого зберігання даних та алгоритмів консенсусу, що дозволяє вузлам мережі взаємодіяти без довіри до окремих учасників. Захист від DDoS-атак за допомогою блокчейну застосовують кілька підходів, зокрема децентралізовані мережі, смарт-контракти [17]. В роботі розглянуто застосування підходу смарт-контрактів на технології блокчейн для організації децентралізованої системи обробки запитів користувачів. В таблиці 2.1. наведено основні кроки алгоритму захисту через реалізацію децентралізованої обробки запитів.

Таблиця 2.1 Алгоритм захисту через реалізацію децентралізованої обробки запитів [17]

Крок	Опис
Створення пулу вузлів	Пул вузлів, які відповідатимуть за обробку запитів. Запити від клієнтів будуть динамічно спрямовуватись до різних вузлів, що дозволяє рівномірно розподілити навантаження.
Розподіл даних між вузлами	Розподілення даних між різними вузлами в блокчейн-мережі так, щоб жоден вузол не зберігав усю інформацію одночасно. Це зменшує ризик концентрації трафіку на одному вузлі.
Розподіл запитів за схемою Load Balancing (балансування навантаження)[18]	Реалізовано на основі різних стратегій балансування, наприклад: ● Round Robin (рівномірне розподілення запитів по черзі) ● Least Connections (спрямування до вузла з найменшою кількістю активних з'єднань) ● Random Selection (випадковий вибір вузла). [19]
Моніторинг стану вузлів	Кожен вузол у мережі блоку регулярно повідомляє про свій стан (наприклад, кількість активних з'єднань, час відгуку) в систему моніторингу. Це дозволяє швидко виявляти вузли, які перевантажені або мають збої.
Автоматичне переключення трафіку	Якщо певний вузол виявляє перевантаження або аномальну активність, система автоматично перенаправляє частину трафіку на інші вузли, які менш завантажені.
Використання реплікації даних	Збереження дублікатів критичних даних на кількох вузлах. У разі збою одного вузла інші можуть продовжувати обробку запитів, що забезпечує безперервність сервісу та підвищує стійкість до DDoS-атак.
Аналіз вхідного трафіку та виявлення аномалій	Система моніторингу регулярно аналізує трафік для виявлення аномалій (наприклад, різке зростання кількості запитів від однієї IP-адреси чи географічного регіону). Якщо виявляється підозрілий трафік, можна заблокувати такі запити або обмежити їх кількість.
Реакція на атаку	Якщо виявлено DDoS-атаку, система знижує навантаження, тимчасово відключаючи або

	зменшуючи пріоритет вузлів, які зазнають найвищого навантаження, і збільшує пріоритет для інших вузлів. Це дозволяє системі функціонувати навіть під час атак.
Логування та аналіз подій	Усі події логуються для подальшого аналізу. Це допомагає визначити слабкі місця та вдосконалювати захист у майбутньому.
Адаптація та оптимізація конфігурації мережі	На основі зібраних даних і аналізу атак мережа може автоматично змінювати конфігурацію розподілу трафіку та обмежень, щоб підвищити стійкість до потенційних майбутніх атак.

Розроблений алгоритм захисту від DDoS-атак із використанням блокчейну надає можливість реалізувати децентралізовану обробку запитів. Політику обмеження доступу можливо реалізувати за різними сценаріями (кількість, частота, час надходження запиту). Дозволені запити записуються в блокчейн, що забезпечує прозору і незмінну історію доступів - це суттєво спрощує аудит, оскільки вся інформація про доступ залишається доступною і незмінною. Алгоритм контролює кількість запитів, які надходять від кожного клієнта за певний проміжок часу. Завдяки цьому він блокує зловмисні дії клієнтів, які надсилають надмірну кількість запитів, тим самим знижуючи навантаження на систему.

2.3 Опис класів

Клас - це шаблон або структура, яка визначає властивості та методи, що належать об'єктам цього класу. Клас використовується як основа для створення об'єктів, що є конкретними реалізаціями цього шаблону.[20]

В алгоритмі використовується 4 класи , а саме: Block, Blockchain, Node, LoadBalancer, опис та їх роль розписано в таблиці 2.2

Таблиця 2.2 Опис класів

Клас	Опис	Приклад використання	Роль у системі

Block	Зберігає індекс, час створення, дані, хеш попереднього блоку та обчислений хеш поточного блоку.	block = Block(index=1, timestamp="2024-10-30 12:00:00", data="Client request A", previous_hash="0") print(block.hash)	Забезпечує зберігання інформації про запити та зв’язок між блоками в ланцюзі.
Block chain	Створює генезис-блок і додає нові блоки до ланцюга. Містить метод verify_request для перевірки відповідності запитів клієнта політикам.	blockchain = Blockchain() blockchain.add_block(data= "Client request B") is_valid = blockchain.verify_request(client_id="12345", max_limit=5) print("Request valid:", is_valid)	Керує блоками, зберігає історію запитів і перевіряє дотримання лімітів клієнтами.
Node	Моделює вузол мережі, що обробляє запити клієнтів із врахуванням затримки для симуляції реальних умов роботи.	node = Node(node_id=1) response = node.process_request("Client request C") print(response)	Реалізує вузол, який безпосередньо обробляє запити клієнтів.
Load Balancer	Виконує балансування запитів між вузлами за алгоритмом Round Robin. Перед пересиланням перевіряє ліміти клієнтів через блокчейн.	load_balancer = LoadBalancer(nodes=[Node(1), Node(2), Node(3)], blockchain=blockchain) load_balancer.dispatch_request(client_id="12345", data="Request D")	Забезпечує ефективний розподіл запитів між вузлами та дотримання правил роботи клієнтів.

Загальна архітектура:

- Block забезпечує збереження даних у блокчейні.
- Blockchain керує блоками та перевіряє валідність запитів.
- Node моделює окремі вузли, які обробляють запити.
- LoadBalancer оптимізує розподіл запитів між вузлами та взаємодіє з блокчейном.

Ці класи разом створюють систему децентралізованої обробки запитів на основі технології блокчейн.

Висновки до другого розділу

У цьому розділі було розроблено алгоритм децентралізованої обробки запитів в інформаційній системі на основі технології блокчейн, що ґрунтується на концепціях смарт-контрактів та децентралізованих мереж. Алгоритм побудовано на принципах розподіленого зберігання даних та консенсусу. Було запропоновано ефективні механізми розподілу навантаження та захисту від атак, таких як DDoS. Балансування запитів здійснюється за допомогою спеціалізованих методів, що забезпечують стабільність системи та рівномірний розподіл трафіку. Кожен клас відіграє важливу роль у створенні інтегрованої системи для децентралізованої обробки запитів, що підвищує ефективність та безпеку інформаційної системи.

3 РОЗДІЛ. Реалізація децентралізованої системи обробки запитів на основі блокчейн

3.1 Синтез децентралізованої системи обробки запитів на основі смарт-контрактів

У контексті децентралізованих систем обробки запитів, заснованих на смарт-контрактах, протидія DDoS потребує інтеграції кількох механізмів на рівні технічної та IT інфраструктури, блокчейну та смарт-контрактів. Протидія DDoS у блокчейн-системах базується на природних перевагах децентралізованої архітектури (див. розділ 1, розподіл даних, відсутність єдиної точки відмови) та доповнюється спеціальними техніками для оптимізації роботи мережі.

До основних принципів захисту можна віднести:

Економічний бар'єр для атакувальників: блокчейн працює за економічною моделлю, яка змушує користувачів сплачувати транзакційні збори (Gas) за виконання операцій. Для DDoS-атаки потрібно згенерувати тисячі або мільйони запитів, що в децентралізованій системі стає дорогим через необхідність сплачувати комісію за кожну транзакцію. Для підвищення ефективності захисту можна встановити динамічну вартість Gas залежно від навантаження, а також використовувати рішення L2 для відсіювання дрібних транзакцій, перенаправляючи їх на більш дешеві мережі. *Обмеження запитів*: обмеження кількості запитів із певної IP-адреси або гаманця користувача. У блокчейн-мережах безпосередньо немає IP-адрес, але можна впровадити ліміт запитів через адресу гаманця або унікальний ідентифікатор. Реалізація полягає у створенні окремого смарт-контракту для обліку запитів від кожного користувача (наприклад, дозволяється обробка лише 10 запитів за певний проміжок часу).

Децентралізовані рішення для розподілу навантаження такі як Sharding (Розподіл транзакцій між різними "шардами" блокчейну, кожен із яких обробляє свою частину даних. Це дозволяє уникнути перевантаження однієї ланки мережі, або Layer 2 (L2) Solutions (системи, як-от Optimistic Rollups або ZK-Rollups, дозволяють обробляти більшість транзакцій поза основним ланцюгом, знижуючи ризик перевантаження.)[21] [22]

Реалізація захисту на рівні смарт-контрактів передбачає використання таких механізмів:

Fee Mechanism (Динамічні збори) - впровадження змінної плати за використання смарт-контракту в залежності від навантаження, наприклад, під час атаки: підвищуються збори за транзакції для зниження кількості спам-запитів, поза атакою: збори залишаються низькими для підтримки доступності. Крім того популярним інструментом є *встановлення лімітів запитів від користувачів*, тобто кожен користувач має визначений максимум запитів за проміжок часу (для реалізації використовують time-based throttling або token bucket algorithm- користувачі отримують "токени", які витрачаються на кожен запит. Поповнення токенів відбувається через певний інтервал часу). Серед додаткових інструментів можна навести підхід *обмеження розміру запитів*, що на практиці реалізовано через перевірку розміру вхідних даних (великі запити можуть викликати переповнення пам’яті, що спричиняє відмову в обслуговуванні. Додатково встановлюють обмеження на розмір параметрів функції або загальний обсяг обчислень (Gas Limit).[23]

Перспективним є підхід на основі використання *оракулів* (спеціальний сервіс або механізм, який забезпечує зв'язок між блокчейн-системою (наприклад, смарт-контрактами) та зовнішнім світом. Він надає блокчейну доступ до зовнішніх даних, які недоступні у внутрішньому середовищі блокчейну (наприклад, біржові курси, результати спортивних подій, погодні дані тощо). Децентралізовані системи можуть використовувати оракули, наприклад, Chainlink, для перевірки запитів перед їх обробкою. Логіка роботи оракула наступна: оракул аналізує запити, щоб відсіяти підозрілі або надмірно часті, в подальшому смарт-контракт виконує запит тільки за наявністю підтвердження від оракула.[24]

Алгоритм роботи оракула:

1. Користувач відправляє запит до смарт-контракту.
2. Смарт-контракт передає запит до оракула для перевірки.
3. Оракул повертає підтвердження або відхилення запиту.

Таким чином загальна архітектура децентралізованої системи складатиметься з таких компонентів:

1. Розподілена інфраструктура вузлів (Nodes):

○ Кожен вузол у мережі є рівноправним і виконує обробку транзакцій або запитів.

○ Завдяки розподіленості мережі атака на один вузол або групу вузлів не порушує роботу всієї системи.

○ Учасники мережі виконують функції перевірки (validation) та зберігання даних.

2. Мережа на основі блокчейну:

○ Усі дії, включаючи запити та обробку транзакцій, записуються у розподілений реєстр (ledger).

○ Це дозволяє прозоро відстежувати активність, зокрема спроби перевантажити систему.

3. Механізм економічного стимулювання (Tokenomics):

○ Запити до системи потребують оплати у вигляді токенів або комісій. Це створює фінансовий бар’єр для зловмисників.

○ Чесні вузли отримують винагороду за обробку запитів, а перевантаження стає економічно недоцільним.

4. Масштабування на рівні другого шару (Layer 2):

○ Обробка дрібних транзакцій переноситься на шар 2 (наприклад, Rollups або Sidechains).

○ Основний блокчейн фокусується лише на перевірці та записі ключових даних, що мінімізує ймовірність перевантаження.

5. Децентралізовані захисні протоколи:

○ Rate Limiting: Обмеження кількості запитів від одного вузла або гаманця у певний проміжок часу.

○ Кворум перевірки: Запити перевіряються консенсусом декількох вузлів перед виконанням.

6. Оракули для перевірки даних:

- Оракули (наприклад, Chainlink) підтверджують, чи є запит легітимним, перед його виконанням.

3.2 Імітаційне моделювання: перевірка децентралізованої системи обробки запитів на стійкість проти DDOS атак

Метою імітаційного моделювання є оцінка ефективності розробленого механізму захисту децентралізованої системи обробки запитів під час DDoS-атаки. Основні завдання включають:

1. Виявлення зловмисної активності.
2. Перевірка стійкості системи до перевантаження.
3. Аналіз впливу атаки на легітимних користувачів.

Основні параметри моделі:

1. Система обробки запитів: Децентралізована система, де кожен клієнт надсилає запити, які обробляються вузлами мережі (кількість вузлів обрано 5)
2. Типи клієнтів:
   - Легітимні клієнти (№1, 3–50) надсилають помірну кількість запитів, що відповідає встановленим правилам.
   - Зловмисник (клієнт №2) генерує аномально велику кількість запитів для перевантаження системи.
3. Види запитів:
   - Прийняті запити (accepted): Легітимні запити, які успішно обробляються системою.
   - Відхилені запити (denied): Запити, які перевищують встановлені ліміти або ідентифіковані як підозрілі.
4. Обмеження системи:
   - Rate Limiting: Обмеження кількості запитів від одного клієнта за певний проміжок часу.
   - Вартість обробки запитів (економічний бар'єр): Для зловмисників вартість надмірної активності зростає.

- Аномалії активності: Моніторинг активності клієнтів для виявлення потенційних атак.

Сценарій моделювання

1. Початкові умови:

- У системі одночасно працюють 50 клієнтів.
- Більшість клієнтів надсилають нормальну кількість запитів (в межах ліміту).
- Клієнт №2 (зловмисник) ініціює велику кількість запитів (більше 400), щоб перевантажити систему.

2. Процес моделювання:

- Кожен клієнт надсилає запити в систему.
- Система аналізує запити й застосовує механізми обмежень:
  - Перевірка на ліміти (Rate Limiting).
  - Визначення аномальної активності на основі обсягу запитів.
- Легітимні запити обробляються успішно, а надмірні або підозрілі запити відхиляються.

3. Результати моделювання:

- Система приймає легітимні запити від звичайних клієнтів.
- Більшість запитів від клієнта №2 (зловмисника) відхиляються.
- Система продовжує обслуговувати інших клієнтів без значних збоїв.

Алгоритми, використані в моделюванні:

1. Rate Limiting:

Запроваджено обмеження на кількість запитів, які може відправити клієнт за певний проміжок часу: Threshold-based control: Запити від клієнта блокуються, якщо перевищується встановлений поріг (наприклад, 20 запитів за хвилину).

2. Виявлення аномалій:

Порівняння активності кожного клієнта з середнім рівнем активності системи. Клієнти, що генерують аномально велику кількість запитів, маркуються як потенційно шкідливі.

3. Економічний механізм (опціонально):

Підвищення вартості обробки запитів у періоди підвищеного навантаження, щоб зробити атаку економічно невигідною.

Результати моделювання для різних сценаріїв (кількість клієнтів, кількість запитів) представлено на рис. 3.1 та рис. 3.2

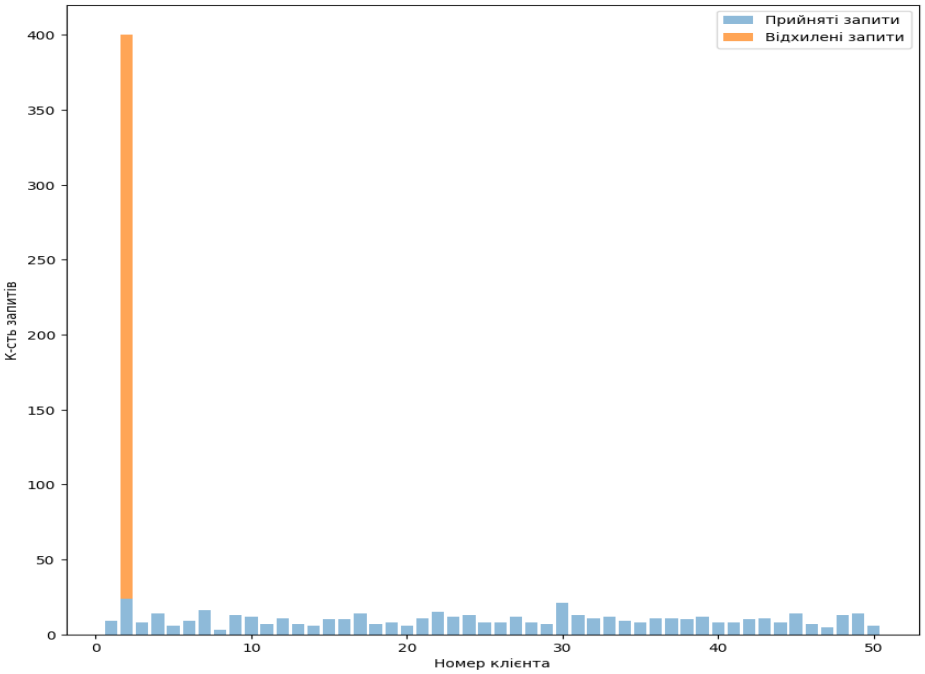

Рисунок 3.1 Результати імітаційного моделювання (50 клієнтів, 500 запитів)

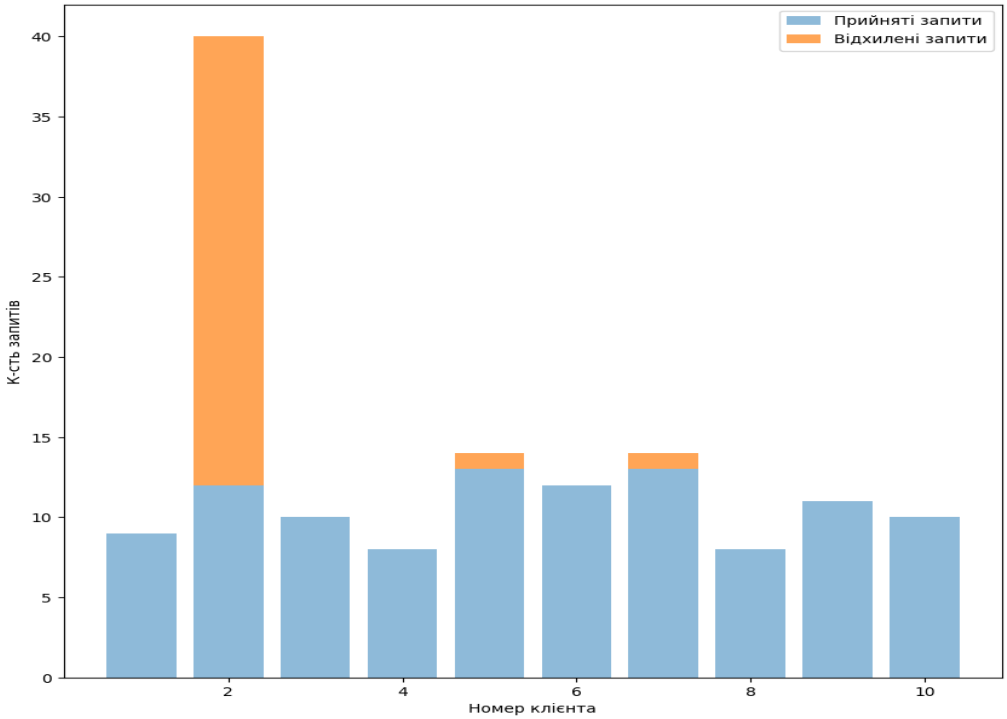

Рисунок 3.2 - Результати імітаційного моделювання (10 клієнтів, 100 запитів)

Аналіз атаки клієнтом №2: клієнт №2 (зловмисник) надіслав аномально велику кількість запитів (понад 400), що значно перевищує активність інших клієнтів. Кількість відхилені запити (помаранчевий стовпець) для клієнта №2 значно переважають, що свідчить про спрацьовування механізмів захисту системи. Отже, система успішно виявила аномальну активність з боку клієнта №2 та відхилила більшість його запитів. Це свідчить про ефективну роботу протоколів протидії DDoS, таких як Rate Limiting (обмеження кількості запитів) та фільтрація на основі аномального навантаження.

Легітимні клієнти (№1, 3–50) мають відносно низький рівень активності: кількість прийнятих запитів (блакитні стовпці) є стабільною та приблизно однаковою. А відсутність відхилених запитів для більшості клієнтів вказує на те, що їх активність визнана легітимною системою.

Таким чином система забезпечила стабільний доступ для чесних користувачів, не обмежуючи їх роботу навіть під час атаки.

3.3 Синтез практичних рекомендацій щодо використання блокчейну для розроблення децентралізованих систем обробки запитів

Проведений аналіз та результати імітаційного моделювання надають можливість синтезувати набір практичних рекомендацій (табл. 3.1)

Таблиця 3.1 – Практичні рекомендації на основі моделювання

Етап/модуль	Рекомендація
Архітектура системи	1. Вибір платформи: використання блокчейн-платформ із високою пропускною здатністю та низькими комісіями (layer-2 рішення, solana, polkadot).[25]
	2. Гібридна архітектура: поєднання обробки на блокчейні з off-chain рішеннями для складних обчислень, а також збереження даних у децентралізованих файлових системах (ipfs, filecoin).[26], [27]

	3. Layer-2 інтеграція: запровадження рішень другого рівня (rollups, sidechains) для масштабування мережі та розподілу навантаження.
	4. Шардінг: розподіл обробки запитів між сегментами блокчейну для мінімізації перевантажень.
Смарт-контракти	1. Rate limiting: обмеження кількості запитів від користувача чи вузла за певний часовий проміжок.
	2. Оптимізація gas-витрат: використання ефективних структур даних і скорочення складних обчислень на блокчейні.
	3. Динамічне коригування вартості: підвищення вартості обробки запитів під час пікового навантаження.
	4. Фільтрація запитів: перевірка легітимності запитів перед їх обробкою на рівні смарт-контракту.
Захист від ddos-атак	1. Економічний бар'єр: впровадження комісій або застав (bonding) для запобігання економічній вигоді від атак.
	2. Rate limiting та throttling: обмеження частоти запитів для контролю надмірної активності.
	3. Виявлення аномалій: аналіз активності вузлів і користувачів для ідентифікації підозрілих патернів запитів.
	4. blacklisting: автоматичне блокування адрес чи вузлів із перевищенням встановлених лімітів.
Перевірка даних	1. Децентралізовані оракули: залучення оракулів для підтвердження легітимності даних і запобігання шахрайству.[28]
	2. Фільтрація на вузлах: перевірка даних на рівні вузлів перед передачею до смарт-контрактів.

Масштабування	1. layer-2 рішення: використання rollups (optimistic або zk) для обробки запитів поза основним ланцюгом і мінімізації навантаження.[29]
	2. Балансування навантаження: розподіл запитів між вузлами мережі для уникнення перевантажень окремих сегментів.[30]
Моніторинг та виявлення	1. Аналіз активності: моніторинг кількості запитів і активності вузлів для виявлення аномалій у реальному часі.
	2. Логи та аудит: збереження логів запитів для подальшого аналізу активності та ідентифікації потенційних атак.
	3. Автоматичне блокування: реакція на підозрілу активність із тимчасовим блокуванням адрес чи ір.
Стабільність системи	1. Децентралізація вузлів: розподіл інфраструктури обробки запитів для усунення єдиної точки відмови.
	2. Географічний розподіл вузлів: розміщення вузлів у різних регіонах для покращення стійкості до атак.
	3. Автоматичне відновлення: запровадження механізмів швидкого відновлення вузлів після збоїв.
Користувацький інтерфейс	1. Зручність користування: розроблення інтерфейсу для відправлення запитів і відстеження статусу.
	2. Валідація на клієнтському рівні: перевірка правильності даних до надсилання для зниження кількості помилкових запитів.
	3. Інформування про блокування: повідомлення користувачів про причини блокування чи відхилення запитів.
Тестування та аудит	1. Навантажувальне тестування: перевірка системи на стійкість до пікових навантажень.

	2. Безпековий аудит: проведення перевірки смарт-контрактів для виявлення вразливостей.
	3. Стрес-тестування: імітація ddos-атак для оцінки ефективності захисних механізмів.

Висновки до третього розділу

Запропоновано децентралізовану система обробки запитів, яка базується на використанні смарт-контрактів для зменшення навантаження на основну мережу.

Реалізовано ефективні механізми захисту від DDoS-атак, зокрема динамічне коригування вартості запитів, обмеження частоти запитів (Rate Limiting).

Проведено імітаційне моделювання, результати якого продемонстрували, що система здатна успішно відхиляти більшість атакуючих запитів без значного впливу на роботу легітимних користувачів.

Впроваджені механізми моніторингу та автоматичного розподілу трафіку забезпечують стабільну роботу мережі навіть за умов високого навантаження.

Розроблено практичні рекомендації щодо проектування та організації децентралізованої системи обробки запитів.

Висновки

У роботі розроблено алгоритм децентралізованої обробки запитів на основі блокчейну, який підвищує стійкість систем до кібератак, зокрема DDoS.

Аналіз сучасних підходів до використання блокчейну в кібербезпеці дозволив сформувати архітектуру системи, яка поєднує децентралізацію, масштабованість і прозорість.

Запропонований алгоритм забезпечує балансування навантаження між вузлами мережі, прозорість обробки запитів та зменшення залежності від централізованих вузлів.

Імітаційне моделювання підтвердило ефективність запропонованої системи в умовах реальних загроз та надмірного навантаження.

Практичне впровадження запропонованих механізмів може значно підвищити рівень кібербезпеки інформаційних систем, зменшити витрати на інфраструктуру та забезпечити високу доступність даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & information systems engineering*, *59*, 183-187.
2. Смірнов, І. С. РЕГУЛЮВАННЯ КОНФІДЕНЦІЙНОСТІ У ЕПОХУ БЛОКЧЕЙНУ: ПРАВОВІ АСПЕКТИ ТА ПЕРСПЕКТИВИ PRIVACY REGULATION IN THE ERA OF BLOCKCHAIN: LEGAL ASPECTS AND PERSPECTIVES.
4. Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers & industrial engineering*, *154*, 107130.
5. Чи можна зламати блокчейн, веб-сайт: https://psm7.com/uk/articles/mozhno-li-vzlomat-blokchejn.html дата звернення: 13 листопада 2024 року.
6. Безпечніший Ethereum, веб-сайт: https://ethereum.org/uk/roadmap/security/ дата звернення: 14 листопада 2024 року.
7. Wang, X., He, J., Xie, Z., Zhao, G., & Cheung, S. C. (2019). ContractGuard: Defend ethereum smart contracts with embedded intrusion detection. *IEEE Transactions on Services Computing*, *13*(2), 314-328.
8. Загальні вразливості в смарт-контрактах та як їх пом'якшити, веб-сайт: https://peerdh.com/uk/blogs/programming-insights/common-vulnerabilities-in-smart-contracts-and-how-to-mitigate-them дата звернення: 15 листопада 2024 року.
9. Kiayias, A., & Zindros, D. (2020). Proof-of-work sidechains. In *Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23* (pp. 21-34). Springer International Publishing
10. Brummer, C. (2022). Disclosure, dapps and DeFi. *Stan. J. Blockchain L. & Pol'y*, *5*, 137.
11. Lanjewar, R., & Pande, G. (2015). Implementation of AES-256 Bit: A Review. *Inventi Rapid: Information Security*.
12. Petkus, M. (2019). Why and how zk-snark works. *arXiv preprint arXiv:1906.07221*.
13. De Graaf, T. J. (2019). From old to new: From internet to smart contracts and from people to smart contracts. *Computer law & security review*, *35*(5), 105322.
14. Lin, S. Y., Zhang, L., Li, J., Ji, L. L., & Sun, Y. (2022). A survey of application research based on blockchain smart contract. *Wireless Networks*, *28*(2), 635-690.
15. Lin, S. Y., Zhang, L., Li, J., Ji, L. L., & Sun, Y. (2022). A survey of application research based on blockchain smart contract. *Wireless Networks*, *28*(2), 635-690

16. Gereffi, G., & Fernandez-Stark, K. (2018). Global value chain analysis: A primer. In Global value chains and development: Redefining the contours of 21st century capitalism (p. 305).
17. Joshi P. et al. Blockchain technology for sustainable development: a systematic literature review, Journal of Global Operations and Strategic Sourcing. 2023. Vol. 16. No. 3. P. 683–717.
18. Shafiq, D. A., Jhanjhi, N. Z., & Abdullah, A. (2022). Load balancing techniques in cloud computing environment: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 3910-3933.
19. Kaur, S., Kumar, K., Singh, J., & Ghumman, N. S. (2015, March). Round-robin based load balancing in Software Defined Networking. In *2015 2nd international conference on computing for sustainable global development (INDIACom)* (pp. 2136-2139). IEEE.
20. Класи, веб-сайт: https://docs.python.org/uk/3/tutorial/classes.html дата звернення: 17 листопада 2024 року.
21. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 17-30).
22. Motepalli, S., Freitas, L., & Livshits, B. (2023). Sok: Decentralized sequencers for rollups. *arXiv preprint arXiv:2310.03616*.
23. Chung, H., & Shi, E. (2023). Foundations of transaction fee mechanism design. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)* (pp. 3856-3899). Society for Industrial and Applied Mathematics.
24. Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., ... & Zhang, F. (2021). Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. *Chainlink Labs*, *1*, 1-136.
25. Blocks, G. B. (2021). An Introduction to Solana. *no. December*.
26. Steichen, M., Fiz, B., Norvill, R., Shbair, W., & State, R. (2018, July). Blockchain-based, decentralized access control for IPFS. In *2018 Ieee international conference on internet of things (iThings) and ieee green computing and communications (GreenCom) and ieee cyber, physical and social computing (CPSCom) and ieee smart data (SmartData)* (pp. 1499-1506). IEEE.
27. Bauer, D. P. (2022). Filecoin. In Getting Started with Ethereum: A Step-by-Step Guide to Becoming a Blockchain Developer (pp. 97-101). Berkeley, CA: Apress.

28. Віровець, Д. В., & Обушний, С. М. (2021). ОРАКУЛ ЯК ІНСТРУМЕНТ ПОСТАЧАННЯ ДАНИХ ДЛЯ ДЕЦЕНТРАЛІЗОВАНИХ АВТОНОМНИХ ОРГАНІЗАЦІЙ.
29. Li, J. (2023). On the security of optimistic blockchain mechanisms. *Available at SSRN 4499357*.
30. Sharma, S., Singh, S., & Sharma, M. (2008). Performance analysis of load balancing algorithms. *International Journal of Civil and Environmental Engineering*, *2*(2), 367-370.