УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ДНІПРОВСЬКИЙ МЕТАЛУРГІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ДНІПРОВСЬКИЙ МЕТАЛУРГІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

СИТНИК РОМАН СЕРГІЙОВИЧ

УДК: 004.4:004.738.5:004.056

ДИСЕРТАЦІЯ

МОДЕЛІ І МЕТОДИ ОРГАНІЗАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ У РЕЄСТРАХ ІНФОРМАЦІЙНИХ СИСТЕМ

12 – Інформаційні технології
122 – Комп'ютерні науки

Подається на здобуття наукового ступеня **доктора філософії**

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

Р.С. Ситник

Науковий керівник **Гнатушенко Вікторія Володимирівна,**
доктор технічних наук, професор.

Дніпро – 2025

АНОТАЦІЯ

Ситник Р.С. **Моделі і методи організації та забезпечення цілісності даних у реєстрах інформаційних систем**. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки». – Український державний університет науки і технологій. – Дніпро, 2025.

Актуальність дослідження. В умовах стрімкого розвитку Industry 4.0 та цифровізації логістичних процесів виникає гостра необхідність вирішення критичних проблем безпеки даних у сучасних інформаційних системах.

Традиційні централізовані архітектури логістичних інформаційних систем демонструють суттєві обмеження при роботі з глобальними ланцюжками постачання, включаючи відсутність ефективних механізмів верифікації даних, недостатню прозорість, вразливість до кібератак та складність забезпечення цілісності інформації.

Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатку. Повний обсяг дисертації – 139 сторінок; список використаних джерел зі 68 найменувань, 2 додатків. Робота проілюстрована 12 рисунками та містить 5 таблиць.

Метою роботи є підвищення рівня безпеки та ефективності управління даними у логістичних інформаційних системах шляхом розробки методу забезпечення достовірності та цілісності на основі технології блокчейн.

Наукова новизна одержаних результатів

- Вперше розроблено нову модель оцінки загроз безпеці в логістичних інформаційних системах, яка враховує специфіку блокчейн-

архітектури та базується на комплексному аналізі вразливостей, що дозволило розширити можливості виявлення потенційних атак та підвищити точність оцінки ризиків в умовах розподіленої обробки даних.

- Вперше запропоновано оригінальний метод забезпечення достовірності даних, що ґрунтується на удосконалених деревах Меркла та інтелектуальних смарт-контрактах, який дозволив суттєво підвищити рівень захищеності системи, автоматизувати процеси верифікації та забезпечити незмінність даних у ланцюжку постачання.
- Отримав подальший розвиток процес верифікації транзакцій у розподілених логістичних системах на основі багаторівневої системи криптографічних механізмів, що дозволило значно підвищити надійність передачі даних між учасниками, мінімізувати ризики несанкціонованої модифікації інформації та забезпечити прозорість операцій.
- Удосконалено механізми контролю доступу до даних шляхом впровадження ієрархічної системи смарт-контрактів та криптографічних токенів, що розширило можливості гнучкого управління правами користувачів, підвищило адаптивність системи та забезпечило надійну ізоляцію конфіденційних даних.
- Розвинуто методи захисту інформаційних потоків у логістичних системах за рахунок впровадження механізмів проактивного моніторингу блокчейн-транзакцій, що дозволило своєчасно виявляти спроби несанкціонованого доступу та підвищити загальний рівень безпеки системи.

Основний зміст дисертаційної роботи

Дисертаційна робота присвячена задачам забезпечення достовірності та цілісності даних у логістичних інформаційних системах на основі технології блокчейн.

За результатами дослідження розроблено:

- Модель виявлення актуальних загроз безпеці в логістичних інформаційних системах, що враховує специфіку блокчейн-архітектури та базується на комплексному аналізі вразливостей;
- Метод забезпечення достовірності даних на основі удосконалених дерев Меркла та інтелектуальних смарт-контрактів.

У **першому розділі** проведено комплексний аналіз сучасного стану логістичних інформаційних систем та виявлено критичні проблеми забезпечення безпеки даних в умовах Industry 4.0. На основі дослідження традиційних централізованих архітектур охарактеризовано їх основні недоліки: відсутність ефективних механізмів верифікації даних між незалежними учасниками ланцюжка постачання, недостатню прозорість процесів, вразливість до кібератак та складність забезпечення цілісності інформації при розподіленій обробці. З'ясовано, що глобальні ланцюжки постачання характеризуються високою складністю взаємодії множини постачальників, виробників, транспортних компаній та дистриб'юторів з різних країн, кожен з яких має власні інформаційні системи та стандарти обробки даних. Окреслено перспективні напрями використання блокчейн-технології для вирішення виявлених проблем, включаючи забезпечення довіри між учасниками без централізованого посередника, автоматизацію бізнес-процесів через смарт-контракти та створення незмінного аудиторського сліду логістичних операцій.

У **другому розділі** розроблено модель виявлення актуальних загроз порушення інформаційної безпеки даних в блокчейн-системах логістичного призначення. Проаналізовано специфічні загрози, властиві розподіленим системам: атаки на механізми консенсусу, вразливості смарт-контрактів на рівні мови програмування Solidity, загрози подвійної трати, атаки Сибілли та DDoS-атаки на мережеву інфраструктуру. Формалізовано математичний апарат для оцінки ризиків на основі теорії нечітких множин, де кожен

деструктивний вплив описується коефіцієнтами порушення конфіденційності, цілісності, доступності та достовірності. Запропоновано багаторівневу класифікацію загроз: рівень блокчейн-протоколу, рівень смарт-контрактів, рівень бізнес-логіки та рівень зовнішньої взаємодії. Розроблено методику визначення небезпечності загроз через комплексний аналіз характеристик об'єкта захисту, типу загрози та потенційного деструктивного впливу.

У **третьому розділі** розроблено комплексний метод забезпечення достовірності та цілісності персональних даних на основі модифікованих дерев Меркла та інтелектуальних смарт-контрактів. Запропоновано архітектуру децентралізованої логістичної системи, яка використовує технологію Ethereum Virtual Machine для виконання бізнес-логіки без централізованого сервера. Детально описано структуру смарт-контрактів для управління правами власності на ресурси, відстеження їх переміщень та автоматизації процесів верифікації. Формалізовано протоколи взаємодії між чотирма основними ролями учасників системи: постачальниками, виробниками, транспортерами та дистриб'юторами. Описано механізми криптографічного захисту через цифрові підписи на основі еліптичних кривих та процедури валідації транзакцій через протоколи консенсусу.

У **четвертому розділі** проведено експериментальну валідацію ефективності запропонованого методу через порівняльне тестування з традиційними MySQL-системами на наборах даних різного обсягу. Результати показали суттєві переваги блокчейн-підходу: час верифікації цілісності даних зменшився завдяки логарифмічній складності дерев Меркла проти квадратичної складності SQL JOIN-операцій. Продемонстровано практичну реалізацію системи на базі Ethereum з використанням 10 незалежних вузлів, що емулюють реальну мережу учасників логістичного ланцюжка. Підтверджено можливість забезпечення

незмінності та повної простежуваності логістичних операцій при збереженні високої продуктивності та масштабованості системи.

Результати дослідження можуть бути використані при проектуванні та модернізації інформаційних систем у сфері логістики, управління ланцюжками постачання та інших галузях з розподіленою обробкою даних, що сприятиме підвищенню загальної ефективності та безпеки логістичних операцій в умовах цифрової трансформації промисловості.

Ключові слова: блокчейн, логістичні інформаційні системи, смарт-контракти, модель, безпека даних, метод, ланцюжки постачання, дерева Меркла, цифрова трансформація, криптографічні методи, розподілені системи.

ABSTRACT

Sytnyk R.S. Models and Methods for Organization and Ensuring Data Integrity in Information System Registries. – Qualifying scientific work on the rights of a manuscript. Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 122 "Computer Sciences". – Ukrainian State University of Science and Technology. – Dnipro, 2025.

Research Relevance

In the context of rapid Industry 4.0 development and digitalization of logistics processes, there is an urgent need to address critical data security problems in modern information systems. Traditional centralized architectures of logistics information systems demonstrate significant limitations when working with global supply chains, including the absence of effective data verification mechanisms, insufficient transparency, vulnerability to cyberattacks, and complexity in ensuring information integrity.

The dissertation consists of an introduction, four chapters, a conclusion, a list of sources used and appendices. The full volume of the dissertation is 139 pages; list of used sources of 68 titles, 2 appendices. The work is illustrated with 12 drawings and contains 5 tables.

Research Objective

The objective of this work is to enhance the level of security and efficiency of data management in logistics information systems by developing a method for ensuring authenticity and integrity based on blockchain technology.

Scientific Novelty of Obtained Results

- First development of a new security threat assessment model for logistics information systems that considers the specifics of blockchain architecture and is based on comprehensive vulnerability analysis, which expanded the capabilities for detecting potential attacks and improved risk assessment accuracy in distributed data processing conditions.

- First proposal of an original data authenticity assurance method based on enhanced Merkle trees and intelligent smart contracts, which significantly improved system security level, automated verification processes, and ensured data immutability in the supply chain.

- Further development of transaction verification processes in distributed logistics systems based on a multi-level system of cryptographic mechanisms, which significantly improved data transmission reliability between participants, minimized risks of unauthorized information modification, and ensured operation transparency.

- Enhancement of data access control mechanisms through implementation of a hierarchical system of smart contracts and cryptographic tokens, which expanded flexible user rights management capabilities, increased system adaptability, and ensured reliable isolation of confidential data.

- Development of information flow protection methods in logistics systems through implementation of proactive blockchain transaction monitoring mechanisms, which enabled timely detection of unauthorized access attempts and improved overall system security level.

Main Content of Dissertation Work

The dissertation work is devoted to problems of ensuring data authenticity and integrity in logistics information systems based on blockchain technology.

Based on research results, the following were developed:

- A model for identifying current security threats in logistics information systems that considers blockchain architecture specifics and is based on comprehensive vulnerability analysis;

- A method for ensuring data authenticity based on enhanced Merkle trees and intelligent smart contracts.

Chapter 1 conducts a comprehensive analysis of the current state of logistics information systems and identifies critical problems in ensuring data security under Industry 4.0 conditions. Based on the study of traditional centralized architectures, their main disadvantages are characterized: absence of effective data verification mechanisms between independent supply chain participants, insufficient process transparency, vulnerability to cyberattacks, and complexity in ensuring information integrity during distributed processing. It was determined that global supply chains are characterized by high complexity of interaction among multiple suppliers, manufacturers, transport companies, and distributors from different countries, each having their own information systems and data processing standards. Promising directions for using blockchain technology to solve identified problems are outlined, including ensuring trust between participants without a centralized intermediary, automating business processes through smart contracts, and creating an immutable audit trail of logistics operations.

Chapter 2 develops a model for identifying current threats to information security data breaches in blockchain systems for logistics purposes. Specific threats inherent to distributed systems are analyzed: attacks on consensus mechanisms, smart contract vulnerabilities at the Solidity programming language level, double-spending threats, Sybil attacks, and DDoS attacks on network infrastructure. Mathematical apparatus for risk assessment based on fuzzy set theory is formalized, where each destructive impact is described by coefficients of confidentiality, integrity, availability, and authenticity violations. A multi-level threat classification is proposed: blockchain protocol level, smart contract level, business logic level, and external interaction level. A methodology for determining threat danger through comprehensive analysis of protection object characteristics, threat type, and potential destructive impact is developed.

Chapter 3 develops a comprehensive method for ensuring personal data authenticity and integrity based on modified Merkle trees and intelligent smart contracts. A decentralized logistics system architecture using Ethereum Virtual Machine technology for executing business logic without a centralized server is proposed. The structure of smart contracts for managing resource ownership rights, tracking their movements, and automating verification processes is described in detail. Interaction protocols between four main participant roles are formalized: suppliers, manufacturers, transporters, and distributors. Cryptographic protection mechanisms through digital signatures based on elliptic curves and transaction validation procedures through consensus protocols are described.

Chapter 4 conducts experimental validation of the proposed method's effectiveness through comparative testing with traditional MySQL systems on datasets of various volumes. Results showed significant advantages of the blockchain approach: data integrity verification time decreased by due to logarithmic complexity of Merkle trees versus quadratic complexity of SQL JOIN

operations. Practical system implementation based on Ethereum using 10 independent nodes emulating a real network of logistics chain participants is demonstrated. The possibility of ensuring immutability and complete traceability of logistics operations while maintaining high system performance and scalability is confirmed.

Practical Application

Research results can be used in designing and modernizing information systems in logistics, supply chain management, and other industries with distributed data processing, which will contribute to improving overall efficiency and security of logistics operations under industrial digital transformation conditions.

Keywords: blockchain, logistics information systems, smart contracts, Merkle trees, model, data security, method, supply chains, digital transformation, cryptographic methods, distributed systems.

СПИСОК ОПУБЛІКОВАНИХ НАУКОВИХ ПРАЦЬ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових періодичних виданнях інших держав та у виданнях України,

які включено до міжнародних наукометричних баз

1. **Ситник** Р.С., Гнатушенко Вік.В. Модель виявлення актуальних загроз порушення інформаційної безпеки даних, що обробляються в блокчейн-системі. - № 1 (2025): Information Technology: Computer Science, Software Engineering and Cyber Security. Information Technology: Computer Science, Software Engineering and Cyber Security 1 (2025). – С. 42-47. DOI: 10.32782/IT/2025-1-6 [Фахове видання]
2. **Ситник** Р.С., Гнатушенко Вік.В. Проектування та дослідження системи моніторингу руху товарів та ресурсів з застосуванням блокчейну (The Design and Research of a System for Monitoring the Movements of Goods and Resources Using Blockchain) // Системні технології. Регіональний міжвузівський збірник наукових праць. – Випуск 6 (137). – Дніпро, 2021. – С. 123-131. DOI: 10.34185/1562-9945-6-137-2021-15 [Фахове видання]
3. **Ситник** Р.С., Гнатушенко Вік.В. Метод забезпечення достовірності та цілісності персональних даних, що обробляються в блокчейн-системі // Системні технології. Регіональний міжвузівський збірник наукових праць. – Випуск 3 (158). – Дніпро, 2025. – С. 28-35. DOI: 10.34185/1562-9945-3-158-2025-04 [Фахове видання]
4. **Ситник** Р.С., Гнатушенко Вік.В. Management of data flows in modern industry using blockchain // System technologies. – 2023. – Vol. 4 No. 147. – P. 123-131. DOI: 10.34185/1562-9945-4-147-2023-11 [Фахове видання]
5. **Ситник** Р.С., Гнатушенко Вік.В. Data flow management in information systems using blockchain technology // Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. – 2024. – № 3. – P. 142-148. URL:

http://nvngu.in.ua/index.php/en/archive/on-the-issues/1909-2024/content-3-2024/6926-142 [Категорія «А», **Scopus**]

Наукові праці, що представлені як тези доповіді у міжнародних науково-технічних конференціях

6. **Sytnyk** R., Hnatushenko Viktoriia, Hnatushenko Volodymyr. Prototyping Fully Decentralized Supply Chain Management Information System Using Blockchain // The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2022). – Khmelnytskyi, Ukraine, March 23-25, 2022. – P. 1-4. URL: http://ceur-ws.org/Vol-3156/ [**Scopus**]
7. **Ситник** Р.С., Гнатушенко Вік.В. Аналіз обміну даними між підприємствами за допомогою технології блокчейн в інформаційних системах // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ITMM'2022)». – Дніпро, 2022. – С. 275-279. DOI: 10.34185/1991-7848.itmm.2022.01.049
8. **Ситник** Р.С., Гнатушенко Вік.В. Проблеми та рішення масштабування потоків даних у екосистемі «Індустрії 4.0» в промисловості та бізнесі // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ITMM'2023)». – Дніпро, 2023. – С. 370-374. DOI: 10.34185/1991-7848.itmm.2023.01.098
9. **Ситник** Р.С., Гнатушенко Вік.В. Забезпечення безпеки доступу до хмарних обчислень за допомогою блокчейн технології // Матеріали XII Міжнародної науково-технічної конференції ITSec-2023 «Безпека інформаційних технологій». – Ужгород, 2-4 травня 2023. – С. 1-3.
10. **Ситник** Р.С., Гнатушенко Вік.В. Інтероперабельність технологій блокчейну для промисловості та фінансів // Матеріали VIII Міжнародної науково-технічної конференції «Комп'ютерне моделювання та

оптимізація складних систем» (КМОСС-2023). – Дніпро, 1-3 листопада 2023. – С. 209-211.

11. **Ситник** Р.С., Гнатушенко Вік.В. Дослідження алгоритмів консенсусу у мережах блокчейну при проектуванні інформаційних систем // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ІТММ'2024)». – Дніпро, 10-11 квітня 2024. – С. 479-484.
12. **Ситник** Р.С., Гнатушенко Вік.В. Система багаторівневої верифікації персональних даних у блокчейн-середовищі // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ІТММ'2025)». – Дніпро, 2025. – С. 620-624. DOI: 10.34185/1991-7848.itmm.2025.01.111
13. **Ситник** Р.С., Гнатушенко Вік.В. Проектування логістичної інформаційної системи за допомогою блокчейну // Матеріали конференції «Молода академія-2022». – Дніпро: Український Державний Університет Науки і Технологій, 2022. – С. 1-2.

ЗМІСТ

ВСТУП

Актуальність. У сучасних умовах глобалізації та цифрової трансформації економіки діяльність провідних міжнародних корпорацій характеризується інтенсивним впровадженням інформаційних технологій у бізнес-процеси. Сучасні підприємства інвестують мільярди доларів та витрачають роки на розробку й імплементацію інформаційних систем, спрямованих на автоматизацію та моніторинг бізнес-процесів. Проте, науково-дослідницька база щодо оцінки ефективності цифровізації процесів постачання товарів і послуг залишається недостатньо розвиненою. Особливо актуальною є проблема оцінки доцільності використання сучасних інформаційних технологій як для управління глобальними ланцюгами постачань, так і для оптимізації внутрішньокорпоративних закупівельних процедур.

Переважна більшість компаній, для яких закупівельна діяльність є ключовою (як для внутрішніх потреб, так і для задоволення вимог зовнішніх клієнтів), використовують різноманітне програмне забезпечення з метою підвищення операційної ефективності. Основними цілями такого впровадження є зниження операційних витрат через скорочення часу обробки заявок на закупівлю, перехід від паперового до електронного документообігу, автоматизацію робочих процесів співробітників та інші заходи оптимізації.

В умовах сучасної цифрової трансформації промисловості та переходу до парадигми Industry 4.0 логістичні процеси зазнають кардинальних змін. Інтеграція кіберфізичних систем, промислового інтернету речей (IIoT) та інших передових технологій призводить до зростання обсягів даних, що обробляються в логістичних ланцюжках. Водночас, традиційні підходи до управління інформаційними потоками виявляються недостатньо

ефективними для забезпечення необхідного рівня безпеки, прозорості та надійності. [1]

Особливого значення набувають завдання забезпечення цілісності та достовірності даних в умовах розподіленої взаємодії множини незалежних учасників логістичних процесів. Сучасні глобальні ланцюжки постачання характеризуються високою складністю, залученням великої кількості постачальників, виробників, транспортних компаній та дистриб'юторів з різних країн, кожен з яких має власні інформаційні системи та стандарти обробки даних.

Автоматизація логістичних процесів на основі сучасних інформаційних технологій стала критично важливою для підтримки конкурентоспроможності підприємств. Проте, наявні рішення, розроблені переважно в 90-х та на початку 2000-х років, демонструють значні обмеження. До основних недоліків відносяться: складність забезпечення інтероперабельності між різними системами, проблеми з масштабованістю при зростанні кількості учасників, вразливість централізованих архітектур до кібератак, відсутність ефективних механізмів верифікації достовірності даних при їх обміні між організаціями.

Технологічні виклики сучасних логістичних інформаційних систем включають:

- Проблеми довіри та верифікації: відсутність надійних механізмів підтвердження автентичності даних при обміні між незалежними учасниками ланцюжка постачання;
- Непрозорість процесів: складність відстеження повного шляху товарів та ресурсів від виробника до кінцевого споживача, що ускладнює виявлення порушень та фальсифікацій;

- Централізація контролю: залежність від централізованих посередників, що створює єдині точки відмови та підвищує ризики несанкціонованого втручання;
- Недостатня автоматизація: обмежені можливості автоматичного виконання бізнес-логіки та перевірки відповідності умовам контрактів без людського втручання;
- Проблеми масштабованості: складність адаптації існуючих рішень до зростаючих обсягів даних та кількості учасників в умовах глобалізації.

Так, в Україні в роботі «Технологія блокчейн в аудиті: сучасний стан та перспективи застосування» [2] досліджувалися теоретичні впливи застосування технології блокчейну у аудиті, та як вони можуть позитивно вплинути на сферу аудиту. В інших роботах українських авторів, таких я роботі «Блокчейн як фактор цифрової трансформації економіки України» (Ніколаєв С., Ковальов Б.) [3], блокчейн розглядався як один з факторів, який може позитивно вплинути на цифрову трансформацію економіки України.

Базуючись на зазначених характеристиках, можна припустити, що технологія блокчейн (включаючи смарт-контракти) має значний потенціал для застосування в різних сферах бізнесу. Водночас, питання перспективності даної технології та необхідності її застосування при проведенні закупівельних процедур залишається недостатньо дослідженим, що обумовлює високий потенціал для наукового вивчення. [4]

Водночас, впровадження блокчейн-технології в логістичні системи потребує розробки спеціалізованих методів забезпечення безпеки, враховуючи специфічні загрози та вразливості, властиві розподіленим системам. Існуючі підходи до захисту інформації не повною мірою

враховують особливості блокчейн-архітектури та вимоги логістичних процесів.

В Україні питання надійності та безпеки логістичних систем набувають критичного значення. Необхідність забезпечення стабільного функціонування ланцюжків постачання в умовах підвищених загроз кібербезпеки робить актуальним використання розподілених технологій, стійких до точкових атак на інфраструктуру.

Процеси євроінтеграції та адаптації до міжнародних стандартів вимагають модернізації логістичних інформаційних систем відповідно до найкращих світових практик, включаючи впровадження сучасних технологій забезпечення прозорості та простежуваності товарних потоків.

Таким чином, актуальною **науковою задачею** є розробка методів і моделей забезпечення достовірності та цілісності даних у логістичних інформаційних системах на основі технології блокчейн, що враховують специфіку сучасних вимог Industry 4.0 та особливості розподіленої взаємодії учасників ланцюжків постачання.

Необхідність вирішення цієї проблеми обумовлена:

- Зростанням складності та масштабів логістичних операцій в умовах глобалізації;
- Підвищенням вимог до прозорості та простежуваності товарних потоків;
- Необхідністю забезпечення кібербезпеки критичної інфраструктури;
- Потребою в автоматизації процесів верифікації та валідації даних;
- Вимогами щодо інтероперабельності різних інформаційних систем учасників ланцюжка постачання.

Зв’язок роботи з науковими програмами, планами, темами. Наукова робота відповідає напрямку, визначеному у Законі України «Про Національну програму інформатизації» (2023 р.), відповідає цілям Національної стратегії розвитку інформаційних технологій до 2030 року і може бути інтегрована у програму «Цифрова Україна». Дисертація відповідає паспорту спеціальності 122 – Комп’ютерні науки. Дисертація відповідає тематичному спрямуванню наукових розробок в рамках науково-дослідної роботи кафедри інформаційних технологій та систем факультету прикладних комп’ютерних технологій Дніпровського металургійного інституту Українського державного університету науки і технологій та пов’язана із планами науково-дослідних робіт кафедри. Результати дослідження впроваджено в навчальний процес в межах Дніпровського металургійного інституту Українського державного університету науки і технологій. Зокрема, в навчальні програми дисциплін:

– «Технології захисту інформації» для бакалаврів спеціальності 121 Інженерія програмного ОП «Інженерія програмного забезпечення в індустрії» кафедри інформаційних технологій і систем;

– «Методології та технології розробки інформаційних систем» для магістрів спеціальності 122 Комп'ютерні науки ОП «Комп'ютерні науки і технології» кафедри інформаційних технологій і систем .

Дисертація містить наукові положення, нові науково обґрунтовані теоретичні результати проведених досліджень, які мають істотне значення для галузі знань 12 – Інформаційні технології.

Мета роботи – підвищення рівня безпеки та ефективності управління даними у логістичних інформаційних системах шляхом розробки методу забезпечення достовірності та цілісності на основі технології блокчейн.

Для досягнення поставленої мети вирішено такі **завдання:**

- Провести аналіз проблем безпеки у сучасних логістичних інформаційних системах та виявити основні вразливості;
- Розробити модель виявлення критичних загроз безпеці та цілісності даних з урахуванням специфіки блокчейн-архітектури;
- Створити метод забезпечення достовірності даних на основі модифікованих дерев Меркла та смарт-контрактів;
- Виконати практичну реалізацію та експериментальну валідацію запропонованих рішень в умовах реальної логістичної системи.

Об’єкт дослідження – процеси забезпечення безпеки та достовірності даних у логістичних інформаційних системах на основі блокчейн-технології.

Предмет дослідження – моделі, методи та алгоритми забезпечення цілісності та достовірності даних в блокчейн-системах логістичного призначення. При цьому особлива увага в дисертаційній роботі приділена завданню виявлення актуальних загроз безпеці даних в розподілених системах, а також розробці методів їх нейтралізації через криптографічні механізми верифікації.

Наукова новизна

1. Вперше розроблено нову модель оцінки загроз безпеці в логістичних інформаційних системах, яка враховує специфіку блокчейн-архітектури та базується на комплексному аналізі вразливостей, що дозволило розширити можливості виявлення потенційних атак та підвищити точність оцінки ризиків в умовах розподіленої обробки даних.
2. Вперше запропоновано метод забезпечення достовірності даних, що ґрунтується на удосконалених деревах Меркла та інтелектуальних смарт-контрактах, який дозволив суттєво підвищити рівень

захищеності системи, автоматизувати процеси верифікації та забезпечити незмінність даних у ланцюжку постачання.

3. Отримав подальший розвиток процес верифікації транзакцій у розподілених логістичних системах на основі багаторівневої системи криптографічних механізмів, що дозволило значно підвищити надійність передачі даних між учасниками, мінімізувати ризики несанкціонованої модифікації інформації та забезпечити прозорість операцій.
4. Удосконалено механізми контролю доступу до даних шляхом впровадження ієрархічної системи смарт-контрактів та криптографічних токенів, що розширило можливості гнучкого управління правами користувачів, підвищило адаптивність системи та забезпечило надійну ізоляцію конфіденційних даних.
5. Розвинуто методи захисту інформаційних потоків у логістичних системах за рахунок впровадження механізмів проактивного моніторингу блокчейн-транзакцій, що дозволило своєчасно виявляти спроби несанкціонованого доступу та підвищити загальний рівень безпеки системи.

Теоретична та практична значимість

Теоретична значимість дослідження полягає у розвитку методологічних основ забезпечення інформаційної безпеки та достовірності даних у розподілених логістичних інформаційних системах, а саме:

- Розробці концептуальної моделі виявлення актуальних загроз безпеці даних, яка враховує особливості блокчейн-архітектури та розширює сучасну методологію оцінки ризиків в розподілених системах;
- Формалізації процесів верифікації транзакцій із застосуванням модифікованих дерев Меркла та криптографічних механізмів, що

створює теоретичний базис для побудови систем з гарантованою достовірністю даних;

- Розвитку теоретичних підходів до проектування ієрархічних систем смарт-контрактів, що розширює існуючі наукові концепції шляхом інтеграції математичного апарату теорії графів із принципами розподіленого реєстру;
- Удосконаленні теоретичних засад моніторингу блокчейн-транзакцій, що збагачує загальну теорію інформаційної безпеки новими методами виявлення та протидії несанкціонованому доступу в умовах Industry 4.0.

Практична значимість отриманих результатів визначається розробкою та впровадженням:

- Комплексу програмних засобів на базі блокчейн-технології для реалізації захищеного обміну даними між учасниками логістичної системи, що забезпечує високий рівень достовірності та прозорості інформації;
- Методичних рекомендацій щодо розгортання та інтеграції розроблених рішень у існуючі логістичні інформаційні системи з урахуванням специфіки різних сценаріїв використання;
- Архітектурних шаблонів проектування смарт-контрактів для логістичних процесів, що можуть бути адаптовані для різних типів ланцюжків постачання;
- Механізмів інтеграції криптографічних токенів у процеси управління доступом, що дозволяє реалізувати гнучкі політики безпеки в розподілених логістичних системах;
- Інструментарію для моніторингу та аудиту блокчейн-транзакцій, який може бути використаний для верифікації цілісності даних у реальному часі.

Запропоновані теоретичні положення та практичні рішення створюють підґрунтя для широкого впровадження інноваційних технологій у сферу логістики та управління ланцюжками постачання, сприяючи підвищенню загальної ефективності та безпеки логістичних операцій в умовах цифрової трансформації промисловості.

Методологія та методи дослідження

У роботі використано комплекс методів, що включає:

- Системний аналіз для дослідження логістичних інформаційних систем, виявлення проблем безпеки та управління потоками даних у сучасних умовах Industry 4.0;
- Теорію графів для моделювання структури блокчейн-системи та аналізу взаємозв'язків між учасниками логістичного ланцюга;
- Криптографічні методи, зокрема хеш-функції для побудови дерев Меркла, цифрові підписи та асиметричну криптографію на базі еліптичних кривих;
- Математичне моделювання процесів верифікації транзакцій у розподілених системах;
- Технології розподілених реєстрів, зокрема смарт-контракти для реалізації бізнес-логіки та автоматизації процесів верифікації;
- Експериментальне дослідження розробленої системи на прикладі прототипу логістичної інформаційної системи з використанням технології блокчейн.

Даний комплекс методів дозволив забезпечити досягнення поставленої мети щодо розробки методу забезпечення достовірності та цілісності даних у логістичних інформаційних системах.

Практичне значення отриманих результатів роботи визначається створенням методологічної та технологічної основи для

розробки захищених логістичних інформаційних систем нового покоління. Розроблені теоретичні положення та практичні рішення створюють підґрунтя для широкого впровадження інноваційних технологій у сферу логістики та управління ланцюжками постачання. До практичних результатів належать комплекс програмних засобів на базі блокчейн-технології для захищеного обміну даними, методичні рекомендації щодо інтеграції розроблених рішень у існуючі логістичні системи, архітектурні шаблони проектування смарт-контрактів для логістичних процесів та інструментарій для моніторингу і аудиту блокчейн-транзакцій.

У роботі використано комплексну методологію дослідження, що включає системний аналіз, теорію графів для моделювання блокчейн-системи, криптографічні методи, зокрема хеш-функції, цифрові підписи та асиметричну криптографію, математичне моделювання процесів верифікації, технології розподілених реєстрів та експериментальне дослідження прототипу системи.

Впровадження одержаних результатів. Практичне значення результатів підтверджується впровадженням розробленої системи забезпечення цілісності даних у діяльність компанії "ULADZISLAU YANOUSKI Software Solutions" (акт про впровадження від 24.09.2025 р.). Розроблені моделі виявлення загроз безпеці та методи забезпечення достовірності даних можуть бути застосовані при створенні захищених інформаційних систем для управління ланцюжками постачання, електронного документообігу та інших сфер, що потребують гарантованої цілісності та простежуваності даних у розподілених системах. Результати досліджень впроваджено також в освітній процес та науково-дослідну діяльність кафедри інформаційних технологій і систем Українського державного університету науки і технологій (акт від 15.09.2025 р.)

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлені власні ідеї та розробки автора, що дозволили досягти поставленої мети. З наукових праць, опублікованих у співавторстві, у дисертації використано лише ті ідеї та положення, які є результатом особистої роботи здобувача.

Результати дисертаційної роботи опубліковані у працях [1-13] (Додаток А). У наукових публікаціях, створених у співавторстві, здобувачу належить:

комплексна модель виявлення загроз безпеці блокчейн-систем з формалізацією математичного апарату на основі теорії нечітких множин та класифікація специфічних загроз для логістичних інформаційних систем [1]; архітектура децентралізованої системи моніторингу логістичних операцій та алгоритми відстеження руху товарів через блокчейн-реєстр з використанням смарт-контрактів [2]; метод забезпечення достовірності персональних даних на основі модифікованих дерев Меркла та протоколи криптографічної верифікації цілісності інформації в розподілених системах [3]; концепція управління потоками даних в Industry 4.0 з використанням блокчейн-технології та розробка принципів інтеграції децентралізованих рішень у промислові інформаційні системи [4]; методологія управління інформаційними потоками в логістичних системах та аналіз переваг блокчейн-підходу над традиційними централізованими архітектурами [5]; прототип повністю децентралізованої інформаційної системи управління ланцюжками постачання та архітектурні рішення для забезпечення взаємодії між учасниками без централізованого посередника [6]; аналіз механізмів безпечного обміну даними між підприємствами через блокчейн-протоколи та оцінка ефективності криптографічних методів захисту інформації [7]; дослідження проблем масштабованості блокчейн-систем в екосистемі Industry 4.0 та рішення для підвищення пропускної здатності

розподілених мереж [8]; методи забезпечення безпеки доступу до хмарних ресурсів через блокчейн-механізми та розробка протоколів автентифікації для розподілених систем [9]; аналіз інтероперабельності різних блокчейн-платформ для промислових та фінансових застосувань і принципи забезпечення сумісності між гетерогенними мережами [10]; порівняльне дослідження алгоритмів консенсусу (PoW, PoS, PoA) для логістичних блокчейн-систем та рекомендації щодо вибору оптимального механізму консенсусу [11]; архітектура багаторівневої системи верифікації персональних даних у блокчейн-середовищі та алгоритми забезпечення приватності при збереженні простежуваності операцій [12]; концептуальна модель логістичної інформаційної системи на основі блокчейн-технології та принципи проектування смарт-контрактів для автоматизації логістичних процесів [13].

Апробація результатів дисертації. Результати дисертаційної роботи доповідались і обговорювались на наукових семінарах кафедри кафедри інформаційних технологій і систем Українського державного університету науки і технологій та на наступних конференціях:

1. конференції «Молода академія-2022», Дніпро;
2. 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2022), Khmelnytskyi, Ukraine;
3. науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ІТММ'2022 - ІТММ'2025)», Дніпро;
4. XII Міжнародної науково-технічної конференції ITSec-2023 «Безпека інформаційних технологій», Ужгород;
5. VIII Міжнародної науково-технічної конференції «Комп'ютерне моделювання та оптимізація складних систем» (КМОСС-2023). – Дніпро,

Публікації. Основні результати дисертаційної роботи опубліковано у 13 наукових працях, з них 6 статті опубліковано у наукових виданнях,

включених до переліку фахових видань України, 2 у виданнях, що індексуються в міжнародних базах даних (Scopus), 7 наукових праці опубліковано у збірниках наукових праць та матеріалах міжнародних та всеукраїнських наукових конференцій.

Обсяг роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 139 сторінки, містить 120 сторінок основної частини, включає 12 рисунків, 5 таблиць, 68 літературних джерела.

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ ОРГАНІЗАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ У РЕЄСТРАХ ЛОГІСТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1. Передумови створення інформаційних систем з персональними даними

Четверта промислова революція, відома також як Індустрія 4.0, передусім асоціюється з впровадженням передових інформаційних технологій, які відкривають можливості для підвищення ефективності виробництва. Ці технології не лише трансформують сам виробничий процес, а й можуть мати вагомий вплив на соціальні, екологічні та інші аспекти, що відіграють ключову роль у сталому розвитку підприємств. Проте на сьогодні у наукових і технічних джерелах бракує достатньо прикладних рекомендацій щодо їхнього практичного використання в різних сферах промисловості.

До основних технологій Індустрії 4.0 відносять 3D-друк (адитивне виробництво), штучний інтелект, аналітику великих даних, блокчейн, хмарні обчислення, промисловий інтернет речей, системи цифрового моделювання та інші інновації. Вони здатні значно прискорити технологічний розвиток, зміцнити конкурентні позиції компаній як на внутрішньому, так і на глобальному рівнях, а також сприяти підвищенню стійкості сучасних виробничих систем.

Право на недоторканність приватної сфери як юридична категорія зародилася в США. Одну з перших спроб сформулювати суть поняття приватності було зроблено 1890 року американськими юристами Семюелем Ворреном і Луїсом Брандейсом, які визначили його як право бути залишеним у спокої або право бути наданим самому собі. Пізніше значну

роль у становленні та формулюванні права на приватне життя відіграла діяльність американських судів.

У 1948 році на Генеральній Асамблеї ООН було затверджено Загальну Декларацію прав людини, згідно з положеннями якої ніхто не може зазнавати довільного втручання в його особисте і сімейне життя, довільних посягань на недоторканність житла, таємницю його кореспонденції або на його честь і репутацію. Через два роки аналогічну норму було закріплено в Європейській конвенції про захист прав людини і основоположних свобод. Розвиток інформаційних технологій другої половини XX століття створив об'єктивні передумови до посилення інтересу до проблеми недоторканності приватного життя. У цей період найактивніший розвиток норм про захист персональних даних спостерігається в Європі - принципи, закладені в Європейській конвенції про захист прав і основоположних свобод, у 1981 році отримали свій розвиток у спеціальних нормах Конвенції Ради Європи про захист прав і фізичних осіб щодо автоматичної обробки персональних даних.

Згодом у Директиві Європейського парламенту і Ради Європейського союзу від 24.10.1995 No95/46ЕС "Про захист особи у відносинах обробки персональних даних і вільний обіг цих даних" було закладено основи загальноєвропейської системи захисту персональних даних. У 2000 році в Хартії Європейського союзу про основні права право на захист персональних даних було сформульовано як самостійне фундаментальне право.

Основним чинним нормативними актом, що визначають порядок захисту персональних даних у Євросоюзі, є документ "Правила захисту даних як засіб забезпечення довіри в Євросоюзі та за його межами" 2019 року. [5]

В Україні питання захисту персональних даних набуло особливої актуальності в умовах повномасштабної війни з 2022 року. Воєнний стан створив нові виклики для інформаційної безпеки.

Законодавче регулювання та адаптація до європейських стандартів. Основою правового регулювання є Закон України "Про захист персональних даних" (2010 р., з поправками 2021-2025 рр.), який поступово адаптується до вимог GDPR у рамках євроінтеграційного процесу. Воєнний стан вимагає запровадження особливих режимів обробки даних, що враховують специфіку функціонування в екстремальних умовах [6].

Критичні виклики безпеки в умовах війни. Першочерговими завданнями стали забезпечення безперервності роботи критичної інфраструктури та захист від інтенсивних кібератак на державні й приватні інформаційні системи. Особливої уваги потребують питання збереження конфіденційності даних при масових евакуаціях населення та координації гуманітарних операцій.

Трансформація логістичних систем. Логістичні процеси зазнали кардинальних змін через необхідність підвищеного шифрування даних про переміщення вантажів та впровадження децентралізованих рішень для уникнення єдиних точок відмови. Критично важливим є захист інформації про маршрути та склади від ворожої розвідки при одночасному забезпеченні прозорості гуманітарних поставок.

Інноваційні технологічні рішення та міжнародна кооперація. Україна активно впроваджує блокчейн-технології для прозорості державних послуг (система "Дія"), розподілені системи зберігання критично важливих даних та розширює міжнародну кооперацію у сфері кібербезпеки. Здійснюється активна гармонізація українського законодавства з європейськими стандартами та обмін досвідом з країнами НАТО щодо захисту критичної інфраструктури.

Ці особливості створюють унікальний контекст для розробки інформаційних систем в Україні, де традиційні підходи до захисту даних мають бути адаптовані до екстремальних умов функціонування. Це підкреслює актуальність розробки стійких, децентралізованих рішень на основі блокчейн-технологій для логістичних систем.

1.1.1. Сучасний стан інформаційних систем у галузях промисловості та підприємствах критичної інфраструктури

Збільшення обсягів даних в інформаційних системах різних галузей промисловості та на підприємствах критичної інфраструктури призводить до зростання складності та негнучкості інформаційних систем у цих сферах. Галузі промисловості переживають трансформацію способів проектування, виробництва та розповсюдження товарів і послуг, зосереджуючись на більшій ефективності, гнучкості та адаптивності до потреб сучасного світу. Підприємства критичної інфраструктури стикаються з новими викликами, збільшенням кількості сфер відповідальності, учасників та даних в управлінні критичною інфраструктурою, що вимагає якісного управління потоками даних в інформаційних системах [7].

Ці процеси розвитку інформаційних технологій на підприємствах часто описують терміном Індустрія 4.0, який описує концепції цифровізації, автоматизації та взаємозв'язку в промислових секторах, а зростаюча складність інформаційних систем в Індустрії 4.0 вимагає ефективного та прозорого управління потоками даних, в яких традиційні інформаційні системи мають обмеження з точки зору прозорості, довіри, автоматизації та безпеки. Для ефективного вирішення завдань управління потоками даних в промислових секторах та на підприємствах критичної інфраструктури пропонується використовувати принципи дерев Меркла та смарт-контрактів в рамках технології Blockchain. Запропонований підхід дозволяє

відстежувати рух товарів та обладнання по ланцюгу поставок і забезпечувати їх автентичність та цілісність. Система використовує дерева Меркла для створення хешу даних на кожному кроці ланцюга постачання, який потім зберігається на блокчейні за допомогою смарт-контрактів. Це дозволяє відстежувати товари та обладнання в режимі реального часу та забезпечує безпечний і прозорий аудиторський слід даних в інформаційних системах [8].

Впровадження та розвиток діджиталізації в різних галузях промисловості створює нові виклики в побудові та проектуванні інформаційних систем для промисловості. Інтеграція передових технологій у виробництво, таких як штучний інтелект, Інтернет речей (IoT), хмарні обчислення, аналітика великих даних та інші, створює великі потоки даних. Термін «Індустрія 4.0» був створений для опису четвертої промислової революції з інтеграцією передових інформаційних технологій у виробництво та інші галузі. Він являє собою зміну в тому, як компанії розробляють, виробляють і поширюють товари та послуги, з акцентом на більшу ефективність, гнучкість і кастомізацію в сучасній економіці.

Сьогодні сучасні підприємства критичної інфраструктури стикаються з новими викликами, пов'язаними з управлінням потоками даних. З ростом використання технологій та підходів Індустрії 4.0, а також надзвичайними викликами в управлінні критичною інфраструктурою, виникає потреба в ефективному управлінні потоками даних для забезпечення надійності цих систем. Під критичною інфраструктурою маються на увазі системи, які вважаються важливими для функціонування суспільства та економіки. Під критичною інфраструктурою маються на увазі системи, які вважаються важливими для функціонування суспільства та економіки. Наприклад, водопостачання, опалення, транспорт, виробництво, передача та розподіл електроенергії, телекомунікації тощо. Критична інфраструктура може

складатися з багатьох зацікавлених сторін, які беруть участь у виробництві або підтримці вищезгаданих послуг [9].

Однією з головних проблем, з якою стикаються підприємства критичної інфраструктури, є величезний обсяг даних, якими необхідно управляти. Зі збільшенням використання датчиків та інших пристроїв моніторингу, ці системи щодня генерують величезні обсяги даних. Ці дані необхідно збирати, зберігати та аналізувати в режимі реального часу, щоб отримати уявлення про продуктивність системи та виявити потенційні проблеми. На додаток до цих викликів, існує також потреба в ефективному обміні даними та співпраці між різними відділами та організаціями. Багато підприємств критичної інфраструктури є складними системами, що включають в себе кілька організацій, кожна з яких має власні системи управління даними і протоколи. Існує потреба в стандартизованих протоколах і функціональній сумісності між цими системами для забезпечення безперебійного потоку даних і співпраці [10].

Це також стосується промислових секторів, де зростання глобалізації продовжує робити ланцюги поставок складнішими та довшими через дедалі більшу участь різних країн, компаній та підприємців у створенні та виробництві нових товарів з різноманітним спектром компаній та країн, залучених до цього процесу. Крім того, кожен з цих суб'єктів може мати свій власний набір стандартів, правил і процедур. Їхні логістичні процеси складаються з багатьох дій і переміщень між постачальниками та компаніями в різних місцях. І чим їх більше, тим складнішим стає управління ланцюгами поставок, потоки даних стають більшими та заплутанішими, а загальний процес - менш прозорим для постачальників, клієнтів та кінцевих споживачів продукції та товарів [11].

Ці процеси ускладнюють алгоритми відстеження та управління продукцією, в яких може бути задіяна велика кількість різних компаній

одночасно. Ланцюг поставок представляє всі зв'язки і точки, які виникають в процесі проходження продукту від сировини до товару на полиці споживача, і може складатися з десятків етапів з різними учасниками. Управління ланцюгами поставок в Індустрії 4.0 - це всі дії, які необхідно виконати для того, щоб клієнт отримав свій товар: закупівля та обробка замовлень, виробництво, транспортування, управління запасами тощо. Щоб вирішити ці проблеми, компанії звертаються до нових технологій та підходів для більш ефективного управління ланцюгами поставок.

Часто компанії використовують класичний підхід до побудови інформаційних систем для ланцюгів поставок з використанням реляційних і нереляційних баз даних, таких як MySQL або MongoDB, на централізованих серверах, з підходом архітектури на стороні клієнта. У MySQL дані зберігаються в таблицях, які складаються з рядків і стовпців. Кожна таблиця містить унікальний набір стовпців, які визначають тип даних, що можуть зберігатися в кожному стовпці. Для створення таблиць MySQL використовується мова структурованих запитів (SQL). MongoDB, в свою чергу, є нереляційною базою даних, яка використовує документно-орієнтований підхід до зберігання даних. На відміну від реляційних баз даних, де дані зберігаються у вигляді таблиць, MongoDB зберігає дані у вигляді JSON-подібних документів. Кожен документ може мати власний набір полів і значень, і MongoDB може масштабуватися для зберігання величезних обсягів даних. Доступ до цих даних здійснюється через центральний сервер, на якому розміщена база даних. Сервер обробляє запити від клієнтів, комп'ютерів, які хочуть отримати або змінити дані в базі даних, щоб отримати і записати дані.І це як працює більшість інформаційних систем: на центральному сервері розміщується база даних з необхідною структурою. Клієнт, згідно з архітектурою клієнт-сервер, не може отримати прямий доступ до бази даних. Замість цього клієнт робить

запит до сервера про отримання/запис/видалення/редагування певної інформації, що зберігається в базі даних на центральному сервері. І сервер вирішує, виходячи з інформації про клієнта та його запиту, застосувати його чи ні.

У випадку з Індустрією 4.0 більшість суб'єктів ланцюга поставок мають власний сервер з власною базою даних. У більш рідкісних випадках деякі галузі можуть співпрацювати і мати один загальний сервер для обробки спільних даних в ньому.

Але у великих інформаційних системах ланцюгів поставок і промислових системах, де відбувається постійний обмін даними між різними системами та їхніми клієнтами для виробничих і логістичних взаємодій, звичайна архітектура клієнт-сервер може бути не в змозі ефективно виконувати свою роботу. Збільшення потоку даних створює низку проблем, пов'язаних зі зберіганням, обробкою та аналізом даних, а також з безпекою та конфіденційністю даних [12]:

- Відсутність прозорості та недостатня або недостовірна інформація про походження продукції, складність перевірки походження та оригінальності товарів кінцевим споживачем;
- Довіра, безпека даних і конфіденційність. Зі збільшенням обсягу даних, що створюються в Індустрії 4.0, зростає ризик їх витоку та кібератак. Це створює серйозну проблему з точки зору забезпечення безпеки інформаційної системи в промисловій екосистемі;
- Ефективність взаємодії з іншими системами. Ще одним викликом при масштабуванні потоків даних в Індустрії 4.0 є необхідність взаємодії між різними компонентами промислової екосистеми. Наприклад, взаємодія виробників з постачальниками, транспортними компаніями, посередниками та іншими учасниками промислової екосистеми.

Це вимагає розробки стандартизованих форматів даних і протоколів, а також розгортання програмного забезпечення, яке працює з цими форматами і забезпечує інтеграцію різних систем і пристроїв, що створює безперебійний обмін даними між різними компонентами екосистеми, сприяючи більшій співпраці та ефективності. Ці виклики можуть завадити промисловості та бізнесу повністю реалізувати переваги Індустрії 4.0.

Для вирішення цих проблем у промисловому секторі та на підприємствах критичної інфраструктури пропонується застосувати алгоритми технології Blockchain до інформаційних систем Індустрії 4.0, щоб забезпечити нові форми довіри та співпраці між різними сторонами в екосистемі виробництва та ланцюгів поставок.

1.2. Основні характеристики персональних даних та інформаційних систем персональних даних

Категорії персональних даних

Під персональними даними (далі - ПДн) розуміється будь-яка інформація, що стосується прямо або побічно визначеної або визначуваної фізичної особи (суб'єкта персональних даних).

Виокремлюються такі категорії ПДн при їх обробці в інформаційних системах:

- спеціальні (що стосуються расової, національної належності, політичних поглядів, релігійних або філософських переконань, стану здоров'я, інтимного життя суб'єктів ПДн);
- біометричні (характеризують фізіологічні та біологічні особливості людини, на підставі яких можна встановити її особу і які використовуються оператором для встановлення особи суб'єкта ПДн);

- загальнодоступніта інші (що не належать до трьох вищевказаних категорій).

Додатково виділяються ПДн співробітників оператора. До таких ПДн можуть належати всі вище перелічені категорії ПДн. Інформаційна система є інформаційною системою, що обробляє ПДн співробітників оператора, якщо в ній обробляються ПДн тільки зазначених співробітників. В інших випадках інформаційна система є

інформаційною системою, що обробляє ПДн суб'єктів ПДн, які не є співробітниками оператора.

Типи інформаційних систем персональних даних

Під інформаційною системою персональних даних (далі - ІСПДн) розуміють сукупність персональних даних, що містяться в базах даних, та інформаційних технологій і технічних засобів, що забезпечують їх обробку [13].

Залежно від технологій, складу та характеристик технічних засобів ІСПДн, а також небезпеки реалізації загроз безпеці ПДн і настання наслідків внаслідок несанкціонованого або випадкового доступу можна виділити такі основні типи ІСПДн:

- автоматизовані робочі місця (далі - АРМ), що не мають підключення до мереж зв'язку загального користування та (або) мереж міжнародного інформаційного обміну;
- АРМ, що мають підключення до мереж зв'язку загального користування та (або) мереж міжнародного інформаційного обміну;
- локальні ІСПДн, що не мають підключення до мереж зв'язку загального користування та (або) мереж міжнародного інформаційного обміну;

- локальні ІСПДн, що мають підключення до мереж зв'язку загального користування та (або) мереж міжнародного інформаційного обміну;
- розподілені ІСПДн, що не мають підключення до мереж зв'язку загального користування та (або) мереж міжнародного інформаційного обміну;
- розподілені ІСПДн, що мають підключення до мереж зв'язку загального користування та (або) мереж міжнародного інформаційного обміну.

Також ІСПДн можна поділити на чотири типи, що залежать від рівня захищеності ПДн, який у них потрібно забезпечити. Найвищий рівень - перший, найнижчий - четвертий. Віднесення ІСПДн до одного з чотирьох типів здійснюється з урахуванням категорії ПДн, що обробляються, їх кількості, а також наявності загроз, пов'язаних з недекларованими можливостями програмного забезпечення (далі - ПЗ) ІСПДн.

1.3. Особливості управління та підтримки логістичних інформаційних систем та систем ланцюгів постачання

Сучасний світ зараз переживає розквіт глобалізації, однією з основних рис якої є посилення зв’язків між різними суб’єктами господарювання, як між різними країнами, так і всередині однієї.

Розвиток міжнародної та внутрішньої торгівлі між різними країнами, компаніями та підприємцями спонукає до виникнення все більш складних та тривалих ланцюгів постачання та процесів створення та виробництва нових товарів, залучення все більшого числа країн та компаній до виробництва, збільшення обсягів реалізації товарів і подібних тенденцій на світовому ринку, що призводить до розширення співпраці між різними компаніями з

усього світу з метою створення та розробки нових продуктів та передачі їх кінцевим споживачам [13].

Компанії здійснюють перевезення товарів та ресурсів між різними континентами, країнами та компаніями по всьому світу. Ці рухи ускладнюють процеси відстеження та управління товарами та ресурсами, в яких одночасно бере участь велика кількість різних компаній, які розташовані в різних куточках світу.

Ці логістичні процеси складаються з багатьох дій і передач між постачальниками та компаніями в різних місцях. І чим їх більше, тим складнішим стає управління ланцюгами поставок, потоки даних більше та заплутаніше, а загальний процес стає менш прозорим для постачальників, клієнтів і кінцевих споживачів продуктів і товарів.

Ланцюг постачання представляє собою усі зв'язки та точки, які виникають в процесі отримання товару від сировини до продукту на полиці споживача, і може складатися з десятків етапів з різними учасниками.

Управління ланцюжком поставок – це всі дії, які необхідно зробити, щоб клієнт отримав свій товар: обробка купівлі та замовлення, виробництво, перевезення, управління запасами тощо. Плануванням ланцюжка поставок називається процес прогнозування потреби у продукті та координація всіх ланок ланцюга для відповідного постачання [14].

Ці всі процеси призводять до зростання вимог і навантаження на інформаційні системи для логістики та ланцюгів постачання, що потребує більших спроможностей в управлінні більш великими та заплутаними потоками даних в інформаційних системах.

Логістичні інформаційні системи представляють собою комплекс програмного забезпечення, що використовується суб’єктами господарства для менеджменту та моніторингу товарів, ресурсів та повного їхнього життєвого циклу.

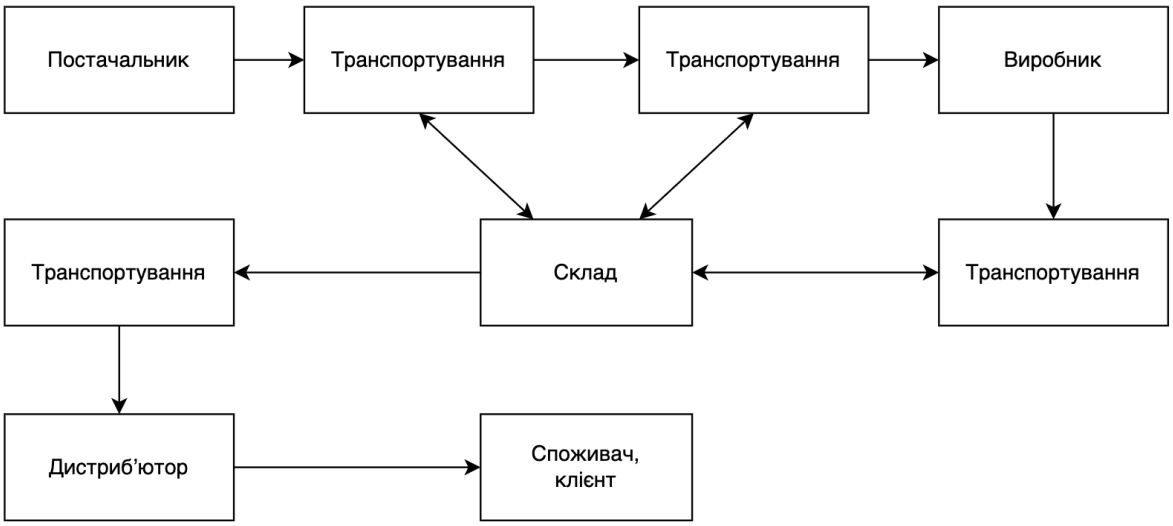

Рис. 1.1. Загальна схема ланцюгу постачання

Звичайна структура логістичної системи включає в себе інформаційну систему, а в обов’язок логістичних інформаційних систем входить керування над постачанням, відвантаженням, виробництвом, транспортуванням, складуванням та контролем товарів, ресурсів і продукції як всередині суб’єктів господарства, так і зовні, при взаємодії з іншими суб’єктами.

Тобто, ці системи координують повний цикл життя продукту від постачання ресурсів для його виробництва, до його потрапляння до кінцевого споживача, супроводжуючи, зв’язуючи та обробляючі усі потоки даних, що проходять через інформаційну систему між усіма учасниками.

Інформаційні системи в логістиці та ланцюгах постачання мають наступні властивості [15]:

- Складність: наявність багатого числа ланок, складний характер взаємодії між різними ланками ланцюга постачання, наявність складного організованого управління;
- Ієрархічність: впорядкованість елементів нижчого рівня ланкам вищого рівня логістичного управління;

- Цілісність: властивість системи виконувати задану цільову функцію, яка реалізується логістичною системою в цілому, а не окремими її ланками або підсистемами;
- Структурованість: передбачення наявності певної організаційної структури у логістичній системі, яка складається із взаємопов'язаних об'єктів і суб'єктів управління, які реалізують задану задачу;
- Організаційність: зв'язки між ланками логістичної системи визначеним чином впорядковані, тобто логістична система має організацію.

В свою чергу, інформаційні системи є відповідальними за менеджмент наступних логістичних процесів в суб'єктах господарської діяльності:

Таблиця 1.1. Логістичні процеси підприємства

Логістичні процеси підприємства		
Постачання	Виробництво	Збут
Закупівля, транспортування, управління запасами, складування, повернення тари та відходів	Організація виробництва, транспортування, узгодження, підтримка стандартів якості	Управління замовленнями, транспортування, управління запасами, складування, повернення відходів

1.4. Характеристика даних у систем ланцюгів постачання та логістичних інформаційних системах

Інформаційні системи в логістиці та ланцюгах постачання відповідають за роботу з даними та метаданими, які є пов’язані до бізнес-логіки ланцюгу постачання.

До цих даних, в загальному прикладі ланцюга постачання, можна віднести дані, щодо володіння товарами та ресурсами, дату виробництва, запаси, опис характеристик, склад товару, в тому числі деталі щодо конкретних частин товару, з яких він виготовлений або складається, стандарти якості, фізичне розташування, та повна історія змін деяких вищезгаданих характеристик.

Також дані у інформаційній системі можуть бути приватними та публічними. Під приватними даними у інформаційних системах розуміється сукупність даних з обмеженим доступом у базах даних системи для обробки і зберігання. Доступ до цих даних, в залежності від їхнього типу, мають

бути тільки у співробітників, з певним рівнем доступу до них, або підприємств-партнерів, згідно договорів та іншого.

Під приватними даними у логістичних інформаційних системах, зазвичай, маються на увазі наступні відомості:

- Відомості, пов'язані із комерційною діяльністю. Порушення безпеки цих даних може призвести до негативних фінансових наслідків для організацій різних форм власності.
- Відомості, пов'язані із професійною діяльністю. Порушення безпеки цих даних може призвести до негативних наслідків для суб'єктів професійної діяльності.

Захист приватних даних у будь-яких інформаційних системах є постійною проблемою, через яку тисячі компаній кожного року втрачають мільйони доларів [16].

До відкритих даних відносяться загальнодоступні дані. До таких даних можна віднести дані, які пов’язані зі взаємодією з іншими суб’єктами в рамках угод, кооперацій, обміну інформацією тощо. Також сюди відносяться дані пов’язані до товарів, продуктів, ресурсів, і питання якісного менеджменту даними стають важливим питанням зі збільшенням потоків даних, які обробляють суб’єкти господарювання.

І також треба особливу увагу необхідно приділяти забезпеченню достовірності. Це завдання особливо актуальне при обробці даних у блокчейн-системі через складність завдання внесення змін до сформованих ланцюжків.

До недоліків класичних методів забезпечення безпеки інформації при їх обробці в розподілених інформаційних системах відноситься недостатнє опрацювання рішень щодо забезпечення доступності та цілісності даних [17]:

- Значне підвищення ймовірності зависань системи із збільшенням числа вузлів;
- Можливість відмови і втрат
- Високі показники складності вирішення конфліктів, часу синхронізації, а також складності реалізації;
- Значне збільшення навантаження на магістральні канали передачі при виході з ладу апаратного забезпечення централізованих сховищ (кластерів), висока складність планування проведення регламентних робіт з обслуговування інфраструктури.
- Проблеми з безпекою персональних даних.

1.5. Аналіз проблем логістичних інформаційних систем управління та систем ланцюгів постачання

В сьогоденні світ зіткнувся з чисельними кризами ланцюгів постачання, і багато компаній намагаються оптимізувати усі логістичні процеси відстеження, управління, виробництва, збуту та інших процесів у ланцюгах постачання [18].

Сучасні інформаційні системи управління постачанням, які використовуються для цієї мети, мають перелік недоліків, з якими вони мають справу, так, основною проблемою є складна комунікація між різними учасниками систем ланцюгів постачання та проблема обробки великої кількості потоків даних між різними учасниками такої мережі.

Логістичні інформаційні системи, як правило, працюють тільки всередині однієї компанії, керуючи відправленнями та іншими логістичними діями лише в межах своєї компанії. Коли компанії потрібно отримати товари та продукти від іншої компанії, вона не отримує всі попередні дані та метадані про доставлені товари. У випадку, якщо компанії домовляться про

обмін цією інформацією один з одним, як правило, без будь-якої автоматизації, тут виникає технічна проблема з різними структурами даних, які використовуються в різних компаніях, та їх адаптацією для однієї з них. І ця проблема стає ще складнішою, коли в такому ланцюгу постачання задіяно більше 2-3 компаній. Коли у логістичних системах з'являється велика кількість учасників мережі, задача адаптації даних та метаданих, а також безперервної передачі необхідних даних між суб'єктами ланцюга постачання стає складною та непрозорою.

Цю проблему можна було б вирішити за допомогою однієї конкретної інформаційної системи для цілого ланцюга постачання, якою користуються всі незалежні суб'єкти ланцюгу постачання. Але з таким підходом виникає інша проблема. В такому випадку уся логістична інформаційна система стає централізованою, та повністю контролюється одним із учасників ланцюга поставок або учасником-медіатором.

Це означає, що один або декілька конкретних суб'єктів логістичних ланцюгів матимуть повний доступ до редагування та видалення даних із бази даних, в тому числі неправомірний. У ряду випадків це є неприйнятно для інших учасників логістичних процесів, оскільки дає занадто велику владу над системою учаснику або посереднику, що також може бути ненадійним.

Ці проблеми викликають непрозорий і складний процес взаємодії між різними учасниками ланцюгів поставок у логістиці, з проблемами у безпеці та зберіганні персональних даних у цих системах. Це призводить до затримок і труднощів в управлінні відправленнями, відстеженні продукції та загальної логістики, ризиках безпеки.

Кінцеві клієнти, у свою чергу, можуть зіткнутися з недостатньою або недостовірною інформацією про походження продукції, складність перевірки походження та оригінальності товару, витоках персональних

даних. Також такі системи можуть зіткнутися з проблемами з аналізом робочих процесів та впровадженням інновацій у систему.

До суто логістичних проблем, які викликали кризу ланцюгів постачання по всьому світу, також можна назвати такі логістичні прорахунки, як застрягання кораблів та контейнерів у морях та океанах, переповненість складів, нестача водіїв вантажівок, нестача ресурсів та компонентів для виробництва тощо. Значна частина цих проблем також пов’язана з якістю менеджменту та прозорістю аналізу [19].

1.6. Перспективні методи управління даними у логістичних інформаційних системах

Постійно наростаючі темпи розвитку інформаційних технологій перевищують швидкість появи методичних документів, що відображають адекватні вимоги та рекомендації щодо інформаційних систем у ланцюгах постачання та системах забезпечення безпеки інформації в них.

Крім того, сучасні інформаційні системи є об'єктами складної структури з програмним управлінням, кількість загроз щодо яких постійно збільшується внаслідок процесу глобального розвитку мультисервісних мереж зв'язку та розвитку інформатизації.

Сьогодні світ переживаємо четверту промислову революцію, яка отримала назву “Індустрія 4.0”, яка завдяки інтелектуальним технологіям виводить на новий рівень автоматизацію, моніторинг та аналіз ланцюжків постачання.

В основі “Індустрії 4.0” лежить промисловий Інтернет речей (IoT) та інтелектуальні автономні системи, які використовують комп'ютерні алгоритми для моніторингу та управління фізичними речами, серед яких обладнання, роботи та транспортні засоби. «Індустрія 4.0» робить усі ланки

ланцюжка поставок «розумними» – від розумних виробництв та фабрик до розумних складів та логістики, але «Індустрія 4.0» — це не лише ланцюжок постачання [20].

“Індустрія 4.0” забезпечує зв'язок з бекенд-системами, забезпечуючи добрий рівень прозорості та контролю за діяльністю організації. Зрештою, концепція “Індустрія 4.0” є найважливішим аспектом цифрової трансформації будь-якої компанії.

В сучасних інформаційних системах для управління потоками даних, зазвичай, використовується стандартний підхід, коли є один центральний комп’ютер, який називається сервером, який обробляє запити клієнтів на отримання та запису даних. Такий підхід носить назву “клієнт-серверна архітектура” і є загальновживаним у індустрії.

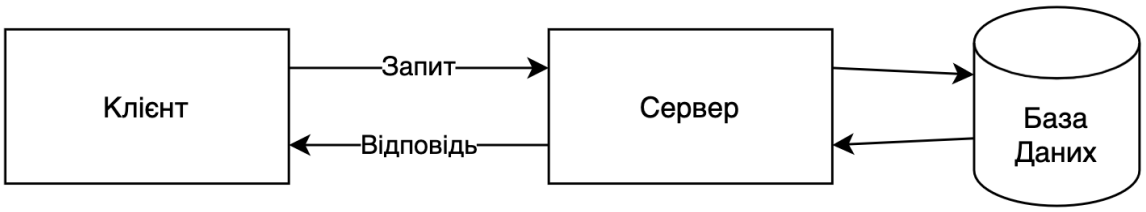

Рис. 1.2. Схема клієнт-серверної архітектури інформаційної системи

По такій архітектурі працює абсолютна більшість інформаційних систем, які спрямовані на комунікацію з іншими системами, або клієнтами, які користуються нею.

Комунікація між сервером та клієнтами відбувається за допомогою запитів, на які сервер надає відповіді. Ці запити можуть бути як і для отримання даних з серверу, так і для зміни (додавання, редагування, видалення) даних.

Існують різні підходи до організації та стандартизації цієї комунікації для обміну даними між учасниками інформаційної системи, однак однією з найрозповсюдженіших є архітектурний стиль REST.

REST – це підхід до побудови прикладного програмного інтерфейсу (API), який використовує HTTP-запити у мережі Інтернет для отримання, вилучення, розміщення та видалення даних. Абревіатура REST у контексті API розшифровується як «передача стану уявлення» (RepresentationalStateTransfer) [21].

Клієнти у REST не пов'язані зі зберіганням даних для мобільності коду клієнта, сервери у свою чергу не пов'язані з інтерфейсом користувача або станом, так що сервери можуть бути простішими і масштабованішими.

Сервери та клієнти можуть бути замінені та розроблятися незалежно, доки інтерфейс не змінюється. У запиті повинна зберігатись вся необхідна інформація для обробки запиту і, якщо необхідно, ідентифікації клієнта. Єдиний інтерфейс визначає інтерфейс між клієнтами та серверами спрощує та відокремлює архітектуру, яка дозволяє кожній частині розвиватися самостійно.

Одним з основних понять у REST – це ресурс. Ресурсом є все те, чого можна назвати. Наприклад, користувач, зображення, предмет тощо. Кожен ресурс REST повинен бути ідентифікований за допомогою стабільного ідентифікатора, URI, який не змінюється при зміні стану ресурсу.

Сам сервер на своєму боці зберігає дані у базу даних, сховище даних для довготривалого зберігання. Існують зовсім різні типи баз даних: однією з найрозповсюдженіших у комп’ютерних науках є реляційні бази даних, де база даних сприймається клієнтом як нормалізовані відношення різного ступеня. Метою нормалізації таких баз даних являє собою усунення різноманітних недоліків у структурі бази даних, які можуть призводити до

зайвої надмірності даних, які в свою чергу можуть потенційно призводити до різних аномалій і порушень цілісності даних.

Реляційна база даних являє собою сукупність елементів даних, організованих у вигляді набору формально описаних таблиць, дані з котрих можуть бути доступні або повторно зібрані різноманітними засобами без необхідності якоїсь ре-організації таблиць у базі даних [22]. Наприклад, за допомогою популярної декларативної мови програмування SQL, мови структурованих запитів, які використовуються для створення, видалення та редагування таблиць та даних у них у база даних. Вона активно використовується у системах управління базами даних, СУБД, таких як MySQL, Microsoft SQL Server, PostgreSQL та інші, які відрізняються своєю програмною реалізацією та деякими можливостями.

Крім реляційних баз даних, також існують і інші підходи, такі як, наприклад, резидентні бази даних, такі як Redis, які зберігають дані у форматі “ключ – значення”, тобто словник, та вигружають дані для зчитування та запису у оперативну пам’ять для швидкого доступу до них.

Також існує ієрархічна модель баз даних, що представляє собою деревоподібну структуру, де між сукупністю даних, елементів, існують зв’язки, тобто де є основний елемент даних, та підлеглі до нього. Або мережеві моделі баз даних, де зв’язки між елементами можуть брати участь у довільній кількості зв'язків, тобто не так строго, як у ієрархічних моделях. Як і ієрархічну, мережеву модель баз даних також можна подати у вигляді орієнтованого графу, але в цьому випадку граф може також містити цикли, де вершина графу може мати кілька батьківських вершин [23].

Усі ці моделі баз даних є актуальними, та широковживаними в сучасних інформаційних системах та застосовуються у різних задачах, таких як довгострокове зберігання даних, кешування даних з метою швидкого

доступу до них, журналювання, збереження великих об’ємів даних, структурованих і неструктурованих тощо.

Крім клієнт-серверної архітектури, часами у інформаційних системах використовується peer-to-peer, архітектура системи, яка базується на мережі рівноправних вузлів. У ній елементи можуть зв'язуватися між один одним, на відміну від традиційної клієнт-серверної архітектури, коли лише один учасник системи, який називається сервером, може обслуговувати інших учасників, які до нього роблять запити. Цей підхід отримав розповсюдження в областях файлового обміну та розподілених обчислень, але в великих інформаційних системах, що зберігають та оперують великою кількістю даних [24].

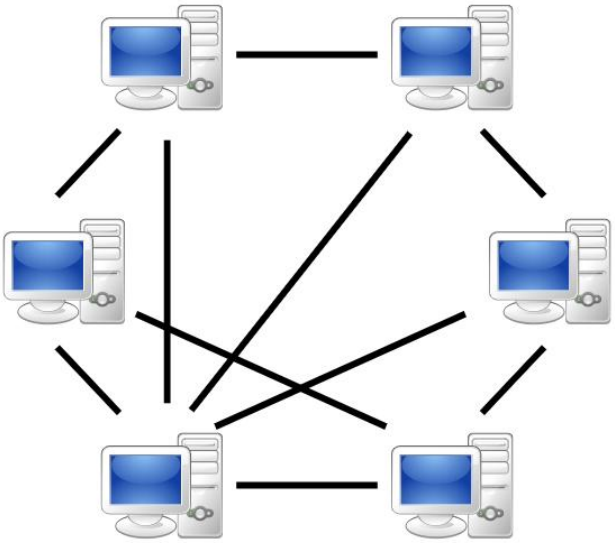

Рис. 1.3. Схема роботи peer-to-peer мережі.

Також існують і інші перспективні підходи, наприклад, якщо подивитися на суміжні сфери, наприклад, в сфері електронних фінансів, які також відомі як DeFi – “DecentralizedFinance” – “Децентралізовані фінанси”, свою популярність займають рішення на основі блокчейну, так звані криптовалюти – Bitcoin, Ethereum, Dogecoin та інші [25].

Блокчейн – це збудований за певними правилами безперервний послідовний ланцюжок блоків (зв'язковий список), що містять інформацію. Зв'язок між блоками забезпечується не тільки нумерацією, але й тим, що кожен блок містить власну хеш-суму і хеш-суму попереднього блоку. Зміна будь-якої інформації в блоці змінить його хеш-суму. Щоб відповідати правилам побудови ланцюжка, зміни хеш-суми потрібно буде записати в наступний блок, що викличе зміни його власної хеш-суми [26].

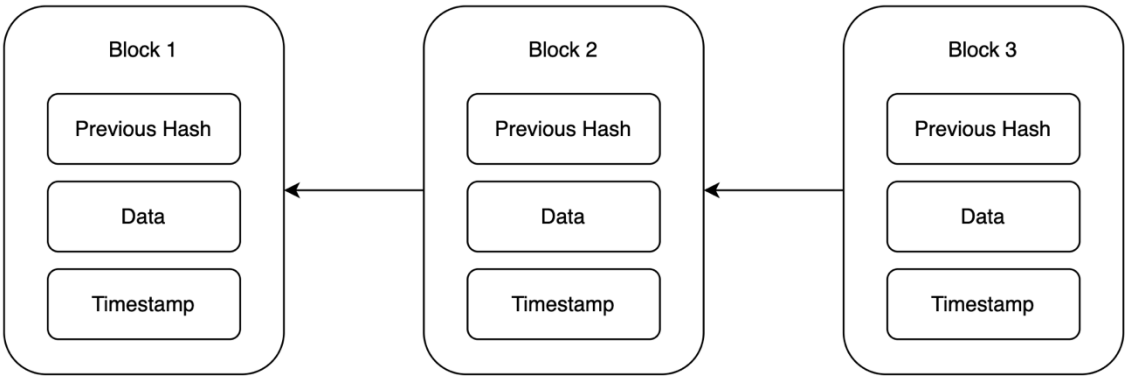

Рис. 1.4. Структурна схема блокчейну.

Окрім сфери фінансів, де блокчейн відомий найбільше, він також має можливість його застосування і в інших сферах, в тому числі різноманітних інформаційних системах в якості сховища даних та серверу.

Такі системи, які будуються зі застосуванням блокчейну, називаються DApps (“DecentralizedApplications” – “Децентралізовані застосунки”), та мають потенціал застосування у багатьох сферах людської діяльності [67].

Крім блокчейну, у концепції «Індустрії 4.0» для модернізації та інформатизації виробництв також набирають популярність звичайна комп’ютеризація процесів виробництва та управління, 3D-друк, доповнена реальність (AR), віртуальна реальність (VR), штучний інтелект та нейронні мережі, використання дронів, і всього, що має потенціал позитивно вплинути на діяльність різних суб’єктів господарювання.

1.7. Висновки до розділу 1

В сьогоденні світ зіткнувся з чисельними кризами ланцюгів постачання, і багато компаній намагаються оптимізувати усі логістичні процеси відстеження, управління, виробництва, збуту та інших процесів у своїх логістичних ланцюгах.

З урахуванням актуальності завдань захисту даних під час їхнього опрацювання в блокчейн-системах, зумовлених постійно зростаючими темпами розвитку інформаційних технологій, кількістю загроз інформаційній безпеці та прецедентів безпеки, а також постійним зростанням темпів розвитку технологій машинного навчання, метою цієї роботи є забезпечення достовірності даних під час їхнього опрацювання в блокчейн-системі.

Сучасний розвиток виробництв та інформаційних систем в логістиці та управлінні вимагає нових рішень для вирішення проблем та викликів, з якими зіштовхнулися суб’єкти господарювання в Україні та по всьому світу. Розвиток виробництва та менеджменту згідно з концепцією “Індустрія 4.0” вимагає розробки нових методів, моделей та підходів до організації, менеджменту та обміну даними між різними суб’єктами господарювання, споживачами та усіма учасниками інформаційних систем в промисловості, які в багатьох випадках дуже тісно пов’язані між собою у сучасних ланках виробництва та реалізації продукції (Ситник Р.С., Гнатушенко Вік. В.) [47].

Впровадження нових моделей та методів до організації, обробки та збереження даних у інформаційних системах дозволить поліпшити ефективність, прозорість та безпеку збереження та управління потоками даних в інформаційних системах. Нові підходи до управління та організації потоків даних у логістичних інформаційних системах з багатьма суб’єктами господарства можуть дозволити досягти зростання продуктивності та

безпеки, скорочення витрат на ланцюги постачання, підвищити гнучкість та стійкість ланцюгів постачання, підвищити якість продукції та рівень обслуговування тощо.

Проведений аналіз існуючих підходів до побудови логістичних інформаційних систем виявив низку критичних проблем, пов'язаних із забезпеченням безпеки та достовірності даних в умовах розподіленої обробки. Традиційні централізовані архітектури інформаційних систем демонструють суттєві обмеження при роботі з сучасними глобальними ланцюжками постачання, де потрібно забезпечити надійну взаємодію багатьох незалежних учасників.

У підсумку, виділено основні проблеми сучасних логістичних інформаційних систем:

- Непрозора та складна система взаємодії між різними учасниками ланцюгів постачання, як наслідок – затримки, складнощі у моніторингу рухів та логістиці;
- Недостатність або недостовірність інформації о походженні продуктів, складність верифікації походження та оригінальності товарів кінцем споживачем;
- Проблеми з кібербезпекою та сохранністю даних;
- Брак автоматизованих процесів у ланцюгах постачання (автоматичне реагування на події та інше);
- Складний процес впровадження змін та інновацій у інформаційних системах управління руху товарів та ресурсів через їхню складність;
- Проблеми з безпекою персональних даних.

1. Проведено аналіз досліджень, пов'язаних з розробкою інформаційних технологій функціонування логістичних систем, безпекою та управлінням потоками даних у логістичних інформаційних системах, а також

застосуванням блокчейн-технології для підвищення надійності та ефективності управління даними.

2. Встановлено, що в умовах стрімкого розвитку Industry 4.0 відбувається кардинальна трансформація логістичних процесів та інформаційних потоків, що призводить до експоненційного зростання обсягів оброблюваних даних та ускладнення інформаційної взаємодії між учасниками логістичних ланцюжків.

3. Виявлено основні проблеми сучасних логістичних інформаційних систем: непрозорість та складність взаємодії між різними учасниками ланцюгів постачання, недостатність або недостовірність інформації про походження продуктів, проблеми з кібербезпекою та збереженням даних, брак автоматизованих процесів, складність впровадження змін та інновацій, проблеми з безпекою персональних даних.

4. Доведено необхідність розробки нових методів забезпечення безпеки та достовірності даних на основі блокчейн-технології, що дозволить підвищити надійність та ефективність логістичних інформаційних систем в умовах цифрової трансформації промисловості.

5. Визначено, що використання смарт-контрактів, криптографічних механізмів та розподіленого реєстру дозволяє забезпечити незмінність та простежуваність даних, автоматизувати процеси верифікації та створити довірене середовище взаємодії учасників без централізованого посередника [66].

6. На основі проведеного аналізу сформульовано мету та задачі дослідження, визначено основні методи та напрямки подальшої роботи, що полягають у розробці моделі виявлення актуальних загроз та методу забезпечення достовірності та цілісності даних у логістичних інформаційних системах на основі блокчейн-технології.

7. Результати проведенних досліджень висвітлено у роботах автора [60, 64, 67, 68].

РОЗДІЛ 2. МОДЕЛЬ ВИЯВЛЕННЯ ЗАГРОЗ ПОРУШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ В БЛОКЧЕЙН-СИСТЕМІ

В умовах стрімкого розвитку логістичних інформаційних систем на базі технології блокчейн виникає критична потреба у створенні комплексної моделі виявлення та оцінки загроз інформаційній безпеці. Традиційні підходи до моделювання загроз, розроблені для централізованих систем, не в повній мірі враховують специфічні особливості розподілених блокчейн-архітектур, що створює прогалини в забезпеченні безпеки даних.

Сучасні логістичні інформаційні системи характеризуються складною екосистемою взаємодії між множиною незалежних учасників ланцюжка постачання, кожен з яких має власні інформаційні системи, стандарти обробки даних та рівні безпеки. В таких умовах ключового значення набуває розробка адекватної моделі загроз, яка дозволить ефективно ідентифікувати та оцінювати ризики, специфічні для блокчейн-середовища.

Особливої актуальності набувають загрози, пов'язані з:

- Консенсус-механізмами та можливістю захоплення контролю над мережею
- Вразливостями смарт-контрактів та їх виконавчого середовища
- Атаками на рівні протоколу блокчейн
- Порушенням цілісності даних при їх внесенні до розподіленого реєстру
- Несанкціонованим доступом до конфіденційної інформації учасників

Метою даного розділу є розробка комплексної моделі виявлення актуальних загроз безпеці даних, що обробляються в блокчейн-системах логістичного призначення.

Модель повинна забезпечити:

- Систематизацію та класифікацію загроз, специфічних для блокчейн-архітектури
- Формалізацію процесів оцінки ризиків з урахуванням особливостей розподілених систем
- Визначення критеріїв та методів оцінки небезпечності виявлених загроз
- Створення основи для розробки ефективних засобів протидії загрозам

Розроблена модель базується на комплексному аналізі трьох ключових компонентів: характеристик об'єкта захисту, типів загроз та потенційних деструктивних впливів. Такий підхід дозволяє всебічно оцінити ризики та забезпечити адекватний рівень захисту інформації в логістичних блокчейн-системах.

В розділі послідовно розглядаються недоліки існуючих методів моделювання загроз, формулюється постановка задачі з математичним обґрунтуванням, аналізуються основні потенційні загрози блокчейн-системам, описуються методи визначення небезпечності загроз та представляється запропонована модель виявлення актуальних загроз.

Результати, отримані в даному розділі, створюють теоретичну основу для подальшої розробки методів забезпечення достовірності та цілісності даних в логістичних інформаційних системах, що розглядається в наступних розділах дисертації.

2.1 Ключові параметри блокчейн системи

Конфіденційність - це властивість інформації бути недоступною та закритою для неавторизованого індивідуума, логічного об'єкта або процесу, цілісність - це стан інформації, при якому відсутні будь-які її зміни, або зміни здійснюються тільки навмисно суб'єктами, які мають на це право,

доступність - властивість об'єкта знаходитися в стані готовності використання за запитом авторизованого логічного об'єкта [27].

В рамках даної дисертації не розглядається аналіз питань кібербезпеки інформації [28] в блокчейні. Однак слід зазначити, що представлені в розділі 2.6 параметри можуть впливати на надійність системи. Безпека в даному випадку включає три компоненти: конфіденційність, цілісність та доступність.

У блокчейн системі безпека даних та стійкість системи забезпечується за допомогою різних методів та алгоритмів технології. Формується реєстр даних, який управляється самостійно. Мережа не спирається на якийсь центральний довірений орган, який може управляти системою, як у традиційно-централізованих системах. Замість цього довіра досягається як властивість, що виникає від взаємодії між вузлами в мережі.

Безпека організується за допомогою криптографічних правил для захисту даних користувача та забезпечення надійності системи [29].

Криптографічні основи в технології блокчейн поділяються на дві категорії: перша категорія застосовується для забезпечення захисту від несанкціонованого доступу, публічної перевірки та досягнення консенсусу, друга категорія використовується для підвищення конфіденційності.

Криптографія з асиметричним ключем дозволяє використовувати цифрові підписи (послідовність байт, що формується шляхом перетворення інформації, що підписується, за криптографічним алгоритмом, призначена для перевірки авторства електронного документа), забезпечуючи довірчі відносини між користувачами, які не знають або не довіряють один одному, надаючи механізм перевірки цілісності та справжності транзакцій, і дозволяючи транзакціям залишатися відкритими. У системах блокчейн закриті ключі використовуються для цифрового підпису транзакцій, а

відкриті ключі використовуються для отримання адрес та перевірки підписів, згенерованих за допомогою закритих ключів.

Другою основною складовою технології є метод хешування (процес перетворення масиву вхідних даних довільної довжини в бітову стрічку фіксованої довжини, який однозначно ідентифікує блок), що дозволяє підтверджувати виконання робіт, а також доводити, що в дані не було внесено жодних змін. Це досягається шляхом дотримання найважливіших властивостей даної процедури: детермінованість (одне повідомлення призводить до одного значення), стійкість до прообразів (односпрямованість), висока швидкість обчислення, лавинний ефект, стійкість до колізій (нескінченно мала ймовірність пошуку тієї ж вихідної функції при іншому вхідному значенні). Хеш підвищує надійність при роботі з даними, оскільки при зміні певного блоку знадобиться перерахунок всіх наступних, що потребуватиме величезних обчислень і буде складним у реалізації.

Застосування різних алгоритмів хешування представлені в таблиці 2.1 [30].

Різні алгоритми хешування дозволяють досягти різних цілей, на які спрямоване те чи інше рішення блокчейн, однак можуть додати істотні обмеження, що передбачають важливість ретельного аналізу при впровадженні системи.

Таблиця 2.1. Застосування різних алгоритмів хешування

Функція	**Властивості**	**Приклади використання**
SHA-256	Складний у виконанні, енергозатратний для процесу майнінгу, стійкий до проблем безпеки	Bitcoin, Nxt, Peercoin, Namecoin
SCRYPT	Потребує великих обсягів оперативної пам’яті порівняно з SHA256, висока швидкість роботи, менше споживання енергії	Litecoin, Dogecoin, MonaCoin, ReddCoin, BlackCoin
Ethash	Володіє високими вимогами до оперативної пам’яті для графічного процесора	Ethereum, WhaleCoin, Ubiq, Expanse
BLAKE2	Висока продуктивність, стійкий до проблем безпеки	Siacoin, Nano, Decred, Verge
X11	Високий рівень складності, забезпечує високий рівень конфіденційності та безпеки для криптовалют	Dash, SmartCoin, Polis
CRYPTONIGHT	Розроблений для використання в CPU і GPU майнінгу та ASIC resistant, забезпечує справжню анонімність, невідстежувані платежі та незв’язувані транзакції	Bytecoin, Monero, Electroneum, Dero

2.1.1. Компоненти мережі та ланцюжка блокчейна

У системі блокчейн важливо розглядати наступні об’єкти – вузол, блок, транзакція. Ці об’єкти є тими, що відрізняють блокчейн від інших технологій.

Вузол – це пристрій у блокчейн-мережі, що дозволяє їй функціонувати. Вузлом може бути будь-який активний електронний пристрій, який підключений до мережі Інтернет і має IP-адресу. Всі вузли повинні включати функції маршрутизації для перевірки/поширення повідомлень та обслуговування з’єднань. Залежно від функціональності існують різні типи вузлів:

- **Повні вузли** – такі клієнти, які реалізують повний протокол блокчейна та містять повну копію реєстру. Вони включають в себе виявлення та спілкування з іншими вузлами, відправлення, отримання та зберігання блоків, перевірку транзакцій. Повний вузол може автономно перевіряти транзакції без зовнішнього посилання. Недолік організації таких клієнтів полягає у великому обсязі даних, який займає повний реєстр, і в необхідності постійної синхронізації для оновлення актуальних даних;
- **Легкі вузли** – зберігають тільки заголовки кожного блоку у своєму локальному сховищі. Для виконання завдань вони відправляють команди на віддалений вузол. Перевага клієнтів легких вузлів перед іншими типами полягає в тому, що користувачеві не потрібно постійно синхронізувати весь реєстр собі на пристрій, легке налаштування та мінімальні технічні вимоги. Недоліком є більш тривала перевірка блоків;
- **Валідатори (в тому числі майнери)** – клієнти, які не використовуються для відправлення або отримання транзакцій; їх застосування – створення блоку з метою отримання винагороди;

- **Вузли відстеження (Супер Вузли)** – це ті ж повні вузли, які є загальнодоступними. Вони зв’язуються та надають інформацію будь-якому іншому вузлу, який вирішує встановити з’єднання з ним. Такі вузли працюють постійно і мають кілька встановлених з’єднань, передаючи історію та дані транзакцій на різні вузли по всьому світу. Недоліки полягають у великій обчислювальній потужності та необхідності постійного з’єднання.

Якщо розглядати структуру даних, блокчейн являє собою упорядкований список блоків.

Блок – це контейнер, що агрегує транзакції. Кожен блок є ідентифікованим та пов’язаний з попереднім у ланцюжку. Блок являє собою певний контейнер, який об’єднує транзакції для включення в публічний реєстр. Він складається із заголовка, що містить метадані, та тіла зі списку транзакцій. Структура та розмір блоку залежать від реалізації. Максимальна кількість транзакцій, яку може містити блок, залежить від розміру блоку та розміру кожної транзакції.

Структура блоку:

- length (4 байти) – розмір блоку в байтах;
- version (4 байти) – інформація про версію блоку;
- previousblockhash (32 байти) – значення хешу попереднього блоку (батьківський блок), на який посилається даний блок;
- merkle_root (32 байти) – посилання на корінь дерева Merkle, який є хешем всіх транзакцій, пов’язаних з цим блоком;
- timestamp (4 байти) – запис мітки часу та дати створення цього блоку для запобігання багаторазової зміни тієї ж інформації;
- bits (4 байти) – розрахункове значення складності, що використовується для цього блоку;

- nonce (4 байти) – одноразове значення, що використовується для генерації цього блоку та обчислення різного хешу;
- txn_count (1-9 байт) – лічильник числа транзакцій у блоці;
- txns (змінна довжина) – транзакції блоку у форматі «tx», до якої включається інформація про версію, вхідні та вихідні лічильники тощо.

Транзакція – це підписана структура даних, що виражає значення, що передається. Транзакції являють собою переходи станів з інформацією про власника (повідомлення), які можуть включати нові записи даних та передачу між учасниками. Кожна транзакція складається з вхідного та вихідного розділів, а також цифрового підпису, які повідомляють список адрес та пов’язаних з ними значень.

Структура транзакції:

- version (4 байти) – інформація про версію транзакції;
- in-counter (1-9 байт) – лічильник числа входів транзакції;
- list of inputs (змінна довжина) – опис входів транзакції. Включає: хеш транзакції, номер виходу транзакції, розмір відмикаючого скрипта, відмикаючий сценарій з указівкою виконання вимог, номер послідовності;
- out-counter (1-9 байт) – лічильник числа виходів транзакції;
- list of outputs (змінна довжина) – опис виходів транзакції. Включає: суму, розмір сценарію, опис замикаючого сценарію з указівкою вимог;
- lock_time (4 байти) – мітка часу, що визначає найраніший час, коли транзакція може стати дійсною та може бути додана до ланцюжка.

Блоки та транзакції є основними елементами, що складають ланцюжок блоків, і являють собою унікальний набір даних, що є основою для проведення коректних процедур.

2.2 Сценарій обміну даними між об’єктами інфраструктури та алгоритм роботи технології блокчейн

Алгоритм дій технології блокчейн при роботі з транзакціями можна розділити на кілька етапів:

1. Виявлення мережі. При першому підключенні вузла до мережі відбувається його завантаження, а також з’єднання з вузлом початкового завантаження для отримання списку сусідніх вузлів, синхронізації та отримання актуальної версії ланцюжка блоків. Для підключення потрібно встановити TCP-з’єднання та почати процес встановлення сесії за допомогою повідомлення version. Вузол відповідає повідомленням verack. Новий вузол починає синхронізувати свій список з актуальним реєстром за допомогою різних типів повідомлень.

2. Створення транзакцій та перевірка. Всі вузли в мережі можуть ініціювати транзакції для передачі цифрових активів доступним одноранговим вузлам. Створення нової транзакції передбачає виконання певних умов учасниками обміну. Після створення транзакції відправник підписує її своїм цифровим підписом та відправляє в мережу. Транзакція буде відхилена, якщо вона сформована неправильно або у користувача недостатньо коштів.

3. Створення блоку. Пул пам’яті (Memory pool) – це тимчасовий заповнювач, де накопичуються транзакції в очікуванні валідації. Після отримання достатньої кількості транзакцій вузол ініціалізує їх додавання в блок. Існують різні механізми поширення блоків у мережі.

4. Перевірка блоку на коректність. Перевірка блоку перед додаванням до реєстру передбачає, що попередній блок існує, структура

даних не порушена, у відправника достатньо коштів, підпис вірний, синтаксис коректний. При підтвердженні відбувається оновлення ланцюжка в загальному реєстрі.

Основні типи повідомлень, що використовуються при обміні інформацією: version, verack, addr, getaddr, getblocks, inv, getdata, block, getheaders, headers.

Блокчейн-система утворює слабкозв’язану мережу без фіксованої топології та структури, що робить її одноранговою та децентралізованою. У блокчейні передбачається задіювати велику кількість вузлів у мережі для вирішення завдань з додатковим обсягом службового трафіку та постійного обміну. Нова підтверджена транзакція, отримана будь-яким вузлом мережі, буде відправлена вузлам, підключеним до нього, кожен з яких відправить транзакцію у свою чергу вже своїм сусідам. Те, що відбувалося раніше на одному пристрої, тепер дублюється на всі вузли, у зв’язку з чим збільшується кількість повідомлень, що передаються, у n разів (n — кількість задіяних вузлів). Такі дані передаються порціями за короткий проміжок часу, що призводить до різких сплесків повідомлень, що передаються, і при великих обсягах може порушити роботу мережі. У процесі роботи мережа вузлів постійно зростає, що може привести до неконтрольованих обсягів даних та порушень усталеної роботи в мережі. Також для входження в мережу нового учасника йому доведеться синхронізувати величезну кількість даних, що провокує лавиноподібне навантаження мережі.

Необхідно визначити мережевий процес взаємодії та технічні характеристики, розглянути вплив на мережу через велику кількість транзакцій, оскільки в процесі обміну блокчейн генерує додатковий трафік, необхідний для оновлення реєстрів на всіх задіяних вузлах, та збільшений

обсяг службового трафіку, який з’являється при шифруванні даних і помітно знижує частку корисного трафіку [31].

Виникає завдання розглянути, як блокчейн вплине на роботу мережі і як відобразиться його подальший ріст на інші технології. Це може сприяти появі нестачі ресурсів, що, у свою чергу, призведе до збільшення ймовірності втрати пакетів та зростання затримок. Таким чином, необхідні показники якості обслуговування для додатків реального часу не можуть бути забезпечені. Важливо визначити ключові поняття, необхідні для оцінки показників якості обслуговування. Якість обслуговування (QoS) — сукупність характеристик послуг електрозв’язку, які мають відношення до можливості задовольняти встановлені та передбачувані потреби користувача послуги [32]. Для додатків визначаються окремі категорії за ознакою толерантності до втрати інформації та затримок.

Коли вузол транслює блок у мережу, з’являється затримка, яка включає в себе час, необхідний для оголошення, запиту та передачі блоку. Блокчейн-технологія впливає на показники мережі, а характеристики мережі впливають на коректну роботу системи блокчейн, включаючи підтвердження блоку та верифікацію транзакцій. Як було представлено в розділі 1, технологія блокчейн може впроваджуватися в різні сфери, при цьому норми характеристик передачі, доставки та обробки будуть визначатися сервісами та послугами, для яких вона застосовується. Для кожного рішення необхідно досліджувати, який клас буде достатнім для забезпечення додатків з трафіком, критичним до затримок.

Ключовими мінімальними вимогами до параметрів стабільності блокчейн-системи будуть:

• Проведення коректних операцій при приєднанні, оновленні, стаціонарній роботі або від’єднанні вузлів.

• Організація роботи з допустимим ступенем затримки системи та мережі для даного виду послуги.

• Організація роботи з допустимим ступенем завантаження апаратного забезпечення системи та мережі для даного виду послуги.

• Система повинна залишатися стабільною при паралельних сплесках транзакцій.

В цих умовах потрібні нові моделі та методи управління перспективними технологіями, що є надзвичайно актуальним та важливим науковим напрямом у галузі телекомунікацій.

Слід зазначити, що для блокчейн-систем важливі не тільки встановлені норми мережевих характеристик, але й масштабованість впровадженого рішення, що включає системні параметри, такі як пропускна здатність транзакцій, час початкового завантаження та вартість підтвердженої транзакції [33], які справляють значний вплив на якість роботи користувача.

Коли число користувачів блокчейн-систем значно збільшується, виникають проблеми масштабованості, які значною мірою впливають на розвиток та застосування блокчейну, особливо це відчутно для систем, заснованих на алгоритмах PoW та PoS, які застосовуються в більшості рішень. Мережеві характеристики можуть значно вплинути на роботу системи блокчейн, однак система блокчейн може варіювати деякі параметри для досягнення кращих показників та масштабованості:

• **Кількість вузлів та інтенсивність формування транзакцій** у блокчейн-системі істотно впливають на мережеві характеристики, оскільки при збільшенні числа працюючих вузлів або інтенсивності формування транзакцій зростатиме кількість інформації, що передається та обробляється, як у процесі валідації, так і в процесі синхронізації актуальних реєстрів. Збільшення кількості транзакцій прямо пропорційно

збільшенню часу підтвердження [34]. Збільшення числа однорангових вузлів негативно позначиться на продуктивності блокчейн-платформ, це може призводити до того, що деякі платформи перестають відповідати на запити від вузлів, що перевищують певну кількість. Збільшення кількості транзакцій підвищує навантаження на систему та мережу і призводить до затримки в мережі [35]. Рішенням, що дозволяє знизити негативний вплив даного параметра, є оптимізація кількості повних та легких вузлів.

• **Розмір блоків та інтервал часу підтвердження блоків** також впливають на мережеві характеристики та пропускну здатність транзакцій. При цьому існує залежність між розміром блоку та часом його поширення, яка представлена в [36] та впливу інтервалу блоків і розмірів блоків на швидкості застарівання блоків [37]. Для того щоб зменшити час обробки транзакцій можна збільшити розмір блоку, щоб валідатори могли включати більше транзакцій в один блок. Якщо розмір блоку збільшується, кількість транзакцій, що обробляються за секунду, відповідно зростає. Це скорочує час включення транзакції в блок і зменшує затримку на рівні системи. Для досягнення більш високої пропускної здатності та більшої ефективності, інтервал між блоками повинен бути якомога меншим. Пропускна здатність транзакцій (TPS) визначається наступним чином [38]:

$$TPS(\lambda, b) = \beta(\lambda, b) \times b \times K \qquad (2.1)$$

де: λ – швидкість генерації транзакцій; β – швидкість додавання блоку в основний ланцюжок; b – максимальний розмір блоку; K – кількість транзакцій у блоці.

Однак скорочення часу підтвердження блоків або збільшення розміру блоку для підвищення пропускної здатності уповільнює спільне

використання блоків у мережі, збільшує кількість втрачених блоків, знижує рівень надійності через збільшення ймовірності появи розгалуження ланцюжка. При коротшому інтервалі блоків, затримка, з якою транзакція записується в блокчейн, скорочується, тобто транзакція записується швидше, однак менший інтервал блоку призводить до більш високої частки застарілих блоків, оскільки з'являється більша кількість конфліктуючих блоків у мережі. Застарілі блоки призводять до додаткових витрат на перевірку та поширення в мережі і викликають обчислювальну неефективність. Таким чином, балансування та вірна конфігурація цих параметрів важлива і може істотно вплинути на роботу блокчейну.

Наприклад, на відміну від Dogecoin [39] та Litecoin [40], Bitcoin [41] має великі розміри блоків, що призводить до більш високої швидкості застарівання блоків (0,41% проти 0,273%), хоча інтервал часу підтвердження блоків Bitcoin в 4 рази більший, ніж у Litecoin [40]. Відмінності в швидкості застарівання блоків між Litecoin та Dogecoin в основному пов'язані з різницею в інтервалі блоків (2,5 хвилини проти 1 хвилини), оскільки їх середні розміри блоків співставні (6,11 кБ та 8 кБ). У таблиці 2.2 представлені значення параметрів даних блокчейн-систем.

• **Комісія за транзакцію** відіграє важливу роль у визначенні часу підтвердження транзакції. Чим вища комісія за транзакцію, тим більша ймовірність того, що їй знадобиться менше часу для підтвердження. Однак це не відбувається для кожної транзакції, деякі транзакції з більш високою комісією можуть потребувати більшого часу підтвердження (це пов'язано з тим, що в пулі можуть бути транзакції з однаковою вартістю, а також з алгоритмами, які не дозволяють повністю витіснити транзакції з меншою сумою). Це може незначно вплинути на загальну масштабованість або взагалі не вплинути на неї, оскільки вплив на мережеву затримку, пропускну здатність може бути незначним.

Таблиця 2.2. Значення параметрів блокчейн-систем

Параметр	**Bitcoin**	**Litecoin**	**Dogecoin**	**Ethereum**
Інтервал часу підтвердження блоків, с	600	150	60	20
Кількість вузлів	6000	800	600	4000
Середній розмір блоків, кб	1024,8	6,11	8	45
Середній час застарівання блоку, с	8,7	1,02	0,85	0,75
Ймовірність застарівання блоків, %	0,41	0,273	0,62	6,81

• **Кількість та продуктивність валідаторів** у системі. Збільшення продуктивності валідаторів у системі блокчейну допоможе рівномірно розподілити енергоспоживання та завдання підтвердження блоків по всій мережі. Це також означає більш швидкий час підтвердження та більш високу пропускну здатність. Також надана смуга пропускання утворює вузьке місце вузла, який приймає/передає повідомлення блокчейну. Вузол з більшою кількістю сусідів виграє від більшої пропускної здатності, оскільки це дозволяє швидше поширювати/збирати блоки в мережі.

Розробник рішення на базі блокчейну також повинен передбачити наслідки для надійності та децентралізації блокчейн-мережі. Більш децентралізована мережа, як правило, менш синхронізована через зросле різноманіття географічних розташувань та розподілення з'єднань. З одного

боку, зросле географічне різноманіття ефективно підвищує живучість системи. З іншого боку, збільшені мережеві затримки сприяють спрощенню появи зловмисників, що здійснюють атаки з подвійними витратами.

Слід визначити компроміс між параметрами, представленими раніше, та врахувати практичні потреби системи. Додатково слід зазначити, що окрім стандартних параметрів системи та протоколу можна впроваджувати різні рішення, які дозволять розширити можливості готових продуктів. Такими рішеннями можуть бути: додаткові методи стиснення блоків, методи сегментування, що розділяють всю блокчейн-мережу на різні сегменти, які можуть бути застосовні для вирішення проблеми пропускної здатності та зниження затримки блокчейну. У деяких випадках, підходящим рішенням для зниження мережевих та системних ефектів буде застосування режиму «off-chain», який передбачає встановлення позапотокового каналу, в якому вони можуть виконувати обмін транзакціями з низькою затримкою. Це рішення включає в себе три етапи: встановлення каналу та заморожування певного депозиту токенів з обох сторін (на випадок виявлення шахрайства) на час підтвердження блоку, обмін та закриття каналу. Весь процес у цьому випадку робить тільки два записи транзакцій, відправлених в основний ланцюжок.

Деякі механізми консенсусу споживають значну кількість ресурсів, тому вибір правильного алгоритму повинен базуватися не тільки на вимозі до швидкості, надійності та масштабованості, але й на кількості ресурсів, що споживаються, що відіграє значну роль у системах, де обмежена можливість постійного живлення, наприклад, у випадку Інтернету речей.

Надійність технології блокчейн забезпечується за рахунок використання криптографічних примітивів та децентралізації, при цьому параметри та технології можуть варіюватися між системами, враховуючи спрямованість систем. У даному розділі представлені основні компоненти

системи блокчейн, структура блоку, транзакції, а також алгоритм та сценарій роботи блокчейн-технології.

Структура даних блокчейну являє собою список з міткою часу, який записує та об'єднує дані про транзакції, що відбувалися коли-небудь у мережі блокчейну. Таким чином, блокчейн забезпечує незмінне зберігання даних, яке дозволяє тільки вставляти транзакції без оновлення або видалення будь-якої існуючої транзакції, щоб запобігти змінам даних та підвищити надійність зберігання даних.

У даному розділі також розглядаються різні алгоритми консенсусу, наводиться порівняння основних різновидів алгоритмів консенсусу, що дозволяє зробити висновок про різноманітність систем та параметрів технології. Побудовані графіки для системи, що оцінюють взаємозв'язок інтервалу часу підтвердження блоків, розміру блоку на надійність блокчейну.

Щоб ефективно використовувати позитивні властивості технології блокчейн, обходячи її обмеження, необхідна методика з розробки таких додатків, крім того, контекст варіантів використання та технічні обмеження мають важливе значення, оскільки деякі рішення можуть не застосовуватися до конкретних проектів технології блокчейну.

Наводяться вимоги до системи та розглядаються різні параметри, які дозволять спростити вибір та налаштування при розробці або підстроюванні рішення, оцінка впливу параметрів системи для досягнення найкращих показників продуктивності та масштабованості при розробці та впровадженні технології блокчейн у потрібну систему.

Однак слід зробити важливе зауваження про встановлення норм згідно не тільки з вимогами сервісів, але й забезпеченню ключових параметрів, для яких впроваджується технологія блокчейн, наприклад, для забезпечення аспектів безпеки слід враховувати характеристики алгоритмів

консенсусу та швидкість проведення атак на систему. Зростання числа вузлів блокчейн також буде значно впливати на характеристики мережі. Детальне дослідження залежностей та технологічних особливостей дозволить оцінити, наскільки кожен вузол буде завантажувати мережу і як позначиться це зростання на характеристиках мережі та системи, які необхідні для якісної роботи мережі. Попередні розрахунки допоможуть підготувати мережу до роботи з необхідною кількістю пристроїв.

2.3. Постановка задачі

Під час моделювання загроз даним, що обробляються в блокчейн-системах, мають бути враховані особливості блокчейн-технології (особливості архітектури, застосованих методів захисту, сфери застосування тощо).

Представлена в цьому розділі модель виявлення актуальних загроз порушення інформаційної безпеки даних, що обробляються в блокчейн-системі пропонується для використання під час розроблення блокчейн-систем незалежно від країни експлуатації;

Рис. 2.1. Метод визначення актуальних загроз

Мета методу – підвищення рівня безпеки та зменшення ризиків порушення інформаційної безпеки персональних даних у логістичних блокчейн-системах шляхом розробки комплексної моделі виявлення актуальних загроз, що забезпечує збільшення ефективності процесів оцінки ризиків та покращення механізмів захисту інформації в умовах розподіленої обробки даних.

Особливої актуальності набуває завдання захисту персональних даних у контексті ланцюжків поставок, що ускладнюються, і зростаючих кіберзагроз. Існуючі рішення часто не враховують специфіку сучасних розподілених логістичних систем, що створює ризики для безпеки даних та ефективності бізнес-процесів.

Для вирішення цих проблем необхідна розробка нової моделі виявлення актуальних загроз, що враховує специфіку сучасних блокчейн-систем, що буде розглянуто у наступному розділі. Запропонована модель

має забезпечити комплексний підхід до оцінки ризиків та формування ефективних механізмів захисту інформації в логістичних системах нового покоління.

Для досягнення поставленої мети необхідно:

- Проаналізувати існуючі моделі оцінки загроз у логістичних системах
- Визначити специфічні вимоги до безпеки даних у блокчейн-системах
- Розробити математичний апарат для формалізації процесів виявлення загроз
- Створити методику оцінки ризиків з урахуванням особливостей розподілених систем
- Провести верифікацію розробленої моделі на прикладі реальної логістичної системи

2.4 Математичне представлення моделі виявлення загроз порушення інформаційної безпеки даних, що обробляються в блокчейн-системі

Головною метою розроблення моделі виявлення актуальних загроз порушення інформаційної безпеки даних, що обробляються в блокчейн-системі, є забезпечення безпеки (конфіденційності, цілісності, доступності, достовірності) інформації, для опрацювання якої призначена інформаційна система.

У межах розроблення моделі загроз блокчейн-системі можна виділити такі невирішені завдання:

- Визначення складу основних специфічних загроз блокчейн-системі;
- Визначення складу деструктивних впливів загроз;
- Розроблення методу присвоєння числових значень характеристикам небезпекидеструктивних впливів загроз;

- Розроблення методу встановлення зв'язку між характеристиками небезпеки;
- Деструктивних впливів загроз, важливістю об'єкта захисту і складом характеристик безпеки об'єкта захисту, що порушуються.

Кожен *d-ий* деструктивний вплив на *o-ий*об'єкт пропонується описати у вигляді чотирьох коефіцієнтів $_{Kdo\alpha}$, $_{Kdo\beta}$, $_{Kdo\gamma}$, $_{Kdo\varepsilon}$, де α, β, γ, ε - індекси, що відображають складові небезпеки, пов'язані з порушеннями конфіденційності, цілісності, доступності та достовірності. Значення коефіцієнтів деструктивних впливів залежать від важливості об'єктів, на які спрямовані деструктивні впливи. Коефіцієнти деструктивних впливів виражають небезпеку порушення конкретних характеристик безпеки.

Для використання коефіцієнтів деструктивних впливів при визначенні небезпеки загрози необхідно присвоїти їм числові значення. Як математичний апарат для присвоєння числових значень пропонується застосувати теорію нечітких множин. Основною складністю, що заважає застосуванню теорії нечітких множин під час розв'язання практичних завдань, є те, що функція належності має бути задана поза самою теорією, а отже, її адекватність не може бути перевірена безпосередньо засобами теорії. У кожному відомому методі побудови функції належності формулюються свої вимоги та обґрунтування до вибору саме такої побудови [42].

У рамках розв'язуваної задачі, під час побудови характеристичних функцій приналежності множинам небезпеки пропонується використовувати прямий метод експертних оцінок, у рамках якого:

- x - значення небезпеки порушення характеристики безпеки об'єкта захисту;

- U - множина значень небезпеки порушення характеристики безпеки об'єкта захисту, $U = \{x, x \in R: 0 \leq x \leq 3\}$;

- *A* - множина значень високої небезпеки порушення характеристики безпеки

об'єкта захисту;

- *B* - множина значень середньої небезпеки порушення характеристики безпеки об'єкта захисту;

- *C* - множина значень низької небезпеки порушення характеристики безпеки об'єкта захисту;

- *D* - множина значень безпеки (нульової небезпеки) об'єкта захисту;

- $\mu_A(x)$ - характеристична функція приналежності множині небезпеки $A, \mu_A(x)=[1;0]$;

- $\mu_B(x)$ - характеристична функція приналежності множині небезпеки $B, \mu_B(x)=[1;0]$;

- $\mu_C(x)$ - характеристична функція приналежності множині небезпеки $C, \mu_C(x)=[1;0]$;

- $\mu_D(x)$ - характеристична функція приналежності множині небезпеки $D, \mu_D(x)=[1;0]$.

Характеристичні функції приналежності множинам небезпеки виражають приблизні значення небезпеки порушення характеристик безпеки, зумовлені ступенем важливості об'єкта захисту.

2.5. Основні потенційні загрози блокчейн-системі

Пропонований у цьому розділі перелік потенційних загроз блокчейн-системі не є вичерпним. З урахуванням швидких темпів розвитку блокчейн-технологій, перелік загроз повинен регулярно оновлюватися і доповнюватися в кожному конкретному випадку розроблення моделі загроз для чергової блокчейн-системи, з урахуванням

моделі порушника. Склад потенційних загроз значною мірою залежить від застосовуваного механізму досягнення консенсусу.

Загрози, пов'язані із захопленням більшої частини мережі (> 50% мережі)

Полягає в контролі консенсусу завдяки контролю над більшою частиною блокчейн-мережі одним учасником або групою осіб, які вступили в змову. У такій ситуації в домінуючому об'єднанні будуть підтверджуватися тільки обрані транзакції і відхилятися всі інші. Приклади подібних вдало реалізованих тактичних наступів (ТН) - ТН на блокчейн-системи, що базуються на базі EthereumKrypton і Shift у 2016 році, а також ТН на BitcoinGold у 2018 році. Можливими методами захисту є:

- збільшення кількості підтверджень, необхідних для схвалення транзакцій (у Krypton було збільшено до 1000 підтверджень);

- добровільне зниження частки в мережі (приклад: ghash.io у 2014 році після досягнення частки в 51% добровільно знизив її до 39,99%);

- значний розмір комісії за транзакції (винагорода майнерам), що робить ТН на блокчейн-мережу невигідними (приклад: блокчейн Bitcoin).

У роботі [43] представлено опис і порівняння методів забезпечення безпеки, заснованих на багаторазовому підтвердженні блоків, що застосовуються в Bitcoin і Ethereum.

Подвійна трата

Подвійна витрата - витрата більшої кількості грошей, ніж є на рахунку зловмисника. Загроза може бути реалізована при володінні більшою частиною блокчейн-мережі. Приклад - подвійна трата в мережі Bitcoin Gold у 2018 році після взяття зловмисником під контроль 51% хеш-рейту мережі

Атака Сибілли

Загроза за рахунок атаки Сибілли [44] - спроба заповнення блокчейн-мережі підконтрольними йому клієнтами. Така атака може призвести до припинення роботи мережі, реалізації загроз, пов'язаних із захопленням більшої частини мережі та подвійної витрати, а також до порушення конфіденційності транзакцій. Можливими методами захисту є:- введення обмежень на кількість акаунтів, які можуть створюватися з IP-адреси протягом певного проміжку часу;

- використання довіреного сертифікованого центру, що забезпечує верифікацію користувачів мережі;

- оцінка параметрів хоста (розмір сховища, пропускна спроможність мережі тощо) з метою визначення приналежності зібраних ним даних окремим комп'ютерам або одному, що реалізовує ТН;

- пред'явлення вимог до генерації блоку (наприклад, у блокчейні Bitcoin з PoW-механізмом досягнення консенсусу обчислювальні вимоги до генерації блоків пропорційні обчислювальній потужності мережі).

DDoS

DDoS - пересилання великої кількості запитів. Методами захисту можуть бути:

- обмеження розміру блоку (наприклад, у блокчейні Bitcoin - 1 МБ), що забезпечує зниження ризиків забивання пулів пам'яті повних вузлів;

- обмеження розміру скрипта (у блокчейні Bitcoin - до 10 000 байт);

- обмеження кількості перевірок підпису і мультипідпису, які може зажадати блок (у блокчейні Bitcoin - до 20 000 підписів і до 20 ключів відповідно);

- блокування підозрілих вузлів і транзакцій (у блокчейні Bitcoin здійснюється реєстрація нестандартних транзакцій (розміром понад 100 КБ) і під час опрацювання транзакцій клієнт перевіряє, що всі виходи є не

витраченими).

Атака за рахунок маршрутизації

Атака за рахунок маршрутизації можлива в разі вступу в змову Інтернет-провайдерів, що забезпечують передачу даних у мережі блокчейн. На прикладі Біткоїна, є думка, що близько 30% вузлів використовують підключення 13 Інтернет-провайдерів, а 60% трафіку проходить через інфраструктуру трьох провайдерів. Таким чином, у теорії, стають можливими два основних сценарії атаки– поділ мережі на різні компоненти і створення затримок у додаванні нових блоків. У першому випадку вузли втрачають зв'язок між собою, створюються паралельні ланцюжки блоків, частина ізольованих майнерів працює даремно (втрачаючи інформацію про транзакції і не отримуючи виплат). У другому випадку можливе формування досить великого для блокування роботи мережі пулу транзакцій.

Внесення до реєстру некоректної інформації

Помилкова інформація, введена в блок реєстру одного разу, дублюватиметься в усіх наступних блоках. Вирішенням проблеми може бути санкціонований перерахунок усіх блоків із видаленням помилкових даних, однак воно може потребувати значних часових і матеріальних витрат. Також можуть застосовуватися спеціалізовані засоби контролю достовірності внесених у блок даних.

Загрози за рахунок вразливостей у смарт-контрактах

До вразливостей смарт-контрактів можна віднести:

- уразливості, пов'язані з генерацією винятків і припиненням виконання коду (наприклад, актуально для мови Solidity до версії 0.4.10, яка "спалювала" весь gas у смарт-контрактах Ethereum);

- уразливості, пов'язані з викликами функцій іншого смарт-контракту (наприклад, функція call у смарт-контрактах Ethereum може

передати у функцію, що викликається, весь доступний gas).

У роботі [45] пропонується класифікація вразливостей смарт-контрактів на базі Ethereum за трьома рівнями:

1) уразливості рівня мови Solidity:

- за рахунок непрямого виконання невідомого коду;
- за рахунок повторного входу;
- за рахунок ефекту винятків;
- за рахунок ліміту gas в send функції;
- за рахунок зберігання секретів;

2) уразливості рівня Ethereum Virtual Machine:

- за рахунок незмінності коду контракту;
- за рахунок обмеження на розмір стека викликів;

3) уразливості рівня блокчейна:

- за рахунок непередбачуваності стану контракту;
- за рахунок часової складової.

У роботі [46] зазначено, що причини появи вразливостей у смарт-контрактах загалом зумовлені недостатнім розумінням розробниками смарт-контрактів семантики платформи, яку вони використовують.

2.6. Порядок визначення небезпечності загрози у моделі

Передбачається, що під час розроблення моделі загроз як вихідні дані використовують перелік об'єктів захисту, а також відомості про архітектурні особливості блокчейн-системи.

Для визначення небезпечності загроз пропонується:

- Визначити склад основних потенційних загроз блокчейн-системі;
- Визначити склад деструктивних впливів імовірних загроз;
- Визначити важливість об'єктів захисту;

- Визначити небезпеку порушення характеристик безпеки об'єктів захисту;
- Визначити небезпеку деструктивних впливів;
- Визначити рівень потенційного збитку;
- Визначити небезпеку загрози.

Схематично загальний порядок пропонованого методу представлено на рисунку 2.2.

Рис. 2.2. Загальний порядок визначення небезпеки загрози

2.6.1 Визначення складу деструктивних впливів

Реалізація будь-якої загрози призводить до здійснення певних деструктивних впливів. Для кожної потенційної загрози необхідно підготувати список деструктивних впливів, до яких може призвести її реалізація.

Пропонується виділити такі деструктивні впливи, здатні вплинути на безпеку блокчейн-системи:

- Ознайомлення;
- Часткове блокування (зниження показників швидкості роботи);
- Повне блокування (припинення роботи);

- Модифікація;
- Видалення.

2.6.2 Визначення важливості об'єкта захисту

Під важливістю об'єкта захисту розуміється якісна характеристика, що визначає цінність об'єкта захисту для забезпечення стану характеристики безпеки об'єкта захисту в межах допустимих значень. Градацію важливості об'єкта захист пропонується виразити чотирма ступенями: найвищий - перший, найнижчий - четвертий.

Для оцінки ступеня важливості об'єкта захисту пропонується розглянути кожен об'єкт захисту з позиції необхідності забезпечення станів конфіденційності, цілісності, доступності та достовірності. Таким чином, кожному об'єкту захисту відповідатимуть чотири характеристики важливості.

Під час визначення ступеня важливості даних пропонується враховувати, зокрема, шкоду, до якої може призвести порушення характеристик безпеки, а також прийнятність витрат (часових, фінансових тощо) на відновлення значень характеристик безпеки даних.

Для визначення важливості даних необхідно експертним шляхом (методом експертних оцінок) присвоїти кожному об'єкту даних визначений у таблиці 6 ступінь важливості.

Під час визначення ступеня важливості об'єктів, що забезпечують працездатність основних програмних і технічних засобів блокчейн-системи, пропонується виконати такі дії:

- визначити склад службових файлів;
- визначити допустимість їх блокування та тимчасової втрати;
- визначити можливість їх відновлення;
-визначити наслідки, до яких може призвести порушення

доступності та цілісності службових файлів;

2.7 Модель загроз безпеки даних у блокчейн-системах логістичного призначення

Розроблена модель виявлення актуальних загроз безпеці даних у блокчейн-системах логістичного призначення представляє собою комплексну формалізовану систему, що базується на багаторівневому підході до класифікації та оцінки ризиків. Модель враховує специфічні особливості розподіленої архітектури блокчейн-систем та специфіку логістичних процесів.

Математична формалізація моделі

Модель загроз формально описується як кортеж:

M = ⟨O, T, D, V, R, F⟩, де:

O = {o_1 , o_2 , ..., o□} - множина об'єктів захисту в логістичній системі;

T = {t_1 , t_2 , ..., t□} - множина типів загроз, специфічних для блокчейн-архітектури;

D = {d_1 , d_2 , ..., d□} - множина деструктивних впливів;

V = {v_1 , v_2 , v_3 , v_4 } - множина характеристик безпеки (конфіденційність, цілісність, доступність, достовірність);

R: O × V → [1,4] - функція важливості об'єктів за характеристиками безпеки;

F: T × D × O → [0,3] - функція оцінки небезпечності загрози.

Ієрархічна структура загроз

Модель розглядає загрози на чотирьох рівнях архітектури:

Рівень блокчейн-протоколу (T_1): включає загрози захоплення

контролю над мережею (51% атаки), подвійні витрати, атаки на маршрутизацію та проблеми консенсусу:

$T_1 = \{t_{1\ 1}, t_{1\ 2}, t_{1\ 3}, t_{1\ 4}\}$ = {захоплення_мережі, подвійна_трата, атака_маршрутизації, порушення_консенсусу}

Рівень смарт-контрактів (T_2): охоплює вразливості коду контрактів, проблеми виконавчого середовища EVM та некоректну бізнес-логіку:

$T_2 = \{t_{2\ 1}, t_{2\ 2}, t_{2\ 3}, t_{2\ 4}\}$ = {вразливості_коду, проблеми_EVM, некоректна_логіка, порушення_доступу}

Рівень бізнес-логіки (T_3): включає загрози порушення цілісності логістичних процесів та некоректного управління правами власності:

$T_3 = \{t_{3\ 1}, t_{3\ 2}, t_{3\ 3}\}$ = {порушення_власності, некоректні_переміщення, фальсифікація_даних}

Рівень зовнішньої взаємодії (T_4): охоплює загрози з боку мережевої інфраструктури та людського фактору:

$T_4 = \{t_{4\ 1}, t_{4\ 2}, t_{4\ 3}\}$ = {DDoS_атаки, атаки_Сібілли, соціальна_інженерія}

Матриця деструктивних впливів

Кожна загроза t_i може призвести до реалізації одного або декількох деструктивних впливів:

$D = \{d_1, d_2, d_3, d_4, d_5\}$ = {ознайомлення, часткове_блокування, повне_блокування, модифікація, видалення}

Для кожної пари (t_i, d□) визначається ймовірність реалізації впливу:

$P(d□|t_i) \in [0,1]$

Оцінка важливості об'єктів захисту

Кожен об'єкт захисту $o_i \in O$ характеризується вектором важливості за чотирма критеріями:

$W(o_i) = (w\_\alpha, w\_\beta, w\_\gamma, w\_\varepsilon)$

де $w\_\alpha, w\_\beta, w\_\gamma, w\_\varepsilon \in [1,4]$ відповідають важливості забезпечення

конфіденційності, цілісності, доступності та достовірності для об'єкта o_i.

Функція оцінки небезпечності

Загальна небезпечність загрози t_i для об'єкта $o□$ при деструктивному впливі $d□$ розраховується як:

$Risk(t_i, o□, d□) = \Sigma_v \in V (\mu_v(Impact(d□, o□, v)) \times W(o□, v) \times P(t_i))$, де:

$\mu_v(x)$ - функція належності до множини небезпечних станів характеристики v;

Impact($d□$, $o□$, v) - оцінка впливу деструктивної дії $d□$ на характеристику v об'єкта $o□$;

W($o□$, v) - важливість характеристики v для об'єкта $o□$;

$P(t_i)$ - ймовірність реалізації загрози t_i.

Адаптація до логістичних систем

Модель спеціально адаптована для логістичних блокчейн-систем через:

1. Специфікацію об'єктів захисту, властивих логістиці: інформація про товари та ресурси, дані про місцезнаходження та переміщення, історія змін власності, контрактні умови.
2. Врахування ролевої моделі учасників: постачальники, виробники, транспортери, дистриб'ютори з різними рівнями доступу до інформації.
3. Особливу увагу до загроз достовірності даних, критичних для логістичних процесів: фальсифікація інформації про походження товарів, підміна даних про якість та характеристики продукції, порушення цілісності логістичного ланцюжка.

Процес застосування моделі:

- Ідентифікація системи: визначення складу об'єктів захисту та учасників логістичного процесу;

- Класифікація загроз: співвіднесення виявлених загроз з ієрархічною структурою моделі;
- Оцінка ризиків: розрахунок показників небезпечності для кожної загрози;
- Ранжування: впорядкування загроз за рівнем критичності;
- Вибір заходів: визначення пріоритетних напрямів захисту.

Розроблена модель загроз представляє собою комплексну систему виявлення та оцінки загроз безпеці даних у блокчейн-системах. В основу моделі покладено багаторівневий підхід до класифікації загроз, що охоплює всі аспекти функціонування блокчейн-систем від протокольного рівня до прикладного.

На рівні блокчейн-протоколу модель розглядає загрози, пов'язані з атаками на механізми консенсусу, включаючи захоплення контролю над мережею та подвійні витрати. На рівні смарт-контрактів аналізуються вразливості, пов'язані з особливостями виконання коду в середовищі віртуальної машини та обмеженнями мови програмування. Рівень бізнес-логіки охоплює загрози, що виникають при порушенні коректності даних та процесів. Окремо розглядаються загрози, пов'язані із зовнішньою взаємодією, такі як DDoS-атаки та проблеми маршрутизації.

Основною перевагою запропонованої моделі є її адаптивність до особливостей конкретних блокчейн-систем при збереженні формалізованого підходу до оцінки загроз. Це дозволяє ефективно виявляти актуальні загрози безпеці, оцінювати їх небезпечність та визначати пріоритетні напрями захисту інформації в логістичних системах на базі технології блокчейн [68].

2.8 Висновки до розділу 2

В даному розділі проведено ґрунтовне дослідження підходів до моделювання загроз безпеці даних у блокчейн-системах логістичного призначення та розроблено комплексну модель виявлення актуальних загроз.

1. Проаналізовано недоліки існуючих методів моделювання загроз, які не враховують специфіку блокчейн-архітектури, включаючи особливості розподіленого консенсусу, незмінність даних та функціонування смарт-контрактів. Виявлено, що традиційні підходи до оцінки ризиків не в повній мірі відображають унікальні вразливості, властиві децентралізованим системам.

2. Розроблено математичне представлення завдання моделювання загроз, яке базується на теорії нечітких множин для присвоєння числових значень характеристикам небезпеки деструктивних впливів. Формалізовано процес оцінки ризиків через коефіцієнти деструктивних впливів, що відображають порушення конфіденційності, цілісності, доступності та достовірності відповідно. В одній з попередніх робіт досліджувалася технічні методи забезпечення достовірності та цілісності персональних даних, що обробляються в блокчейн-системах та їх інтеграція у інформаційні системи (Ситник Р.С., Гнатушенко Вік. В.) [47].

Основну увагу приділено систематизації потенційних загроз блокчейн-системам, що включає загрози захоплення більшої частини мережі (>50% атаки), подвійної трати, атаки Сибілли, DDoS-атаки, атаки за рахунок маршрутизації, внесення некоректної інформації та вразливості смарт-контрактів. Для кожного типу загроз визначено специфічні характеристики та потенційні методи протидії.

3. Детально розглянуто методологію визначення небезпечності загроз, яка включає оцінку складу деструктивних впливів (ознайомлення, часткове блокування, повне блокування, модифікація, видалення),

визначення важливості об'єктів захисту за чотирма ступенями та розрахунок інтегрального показника ризику.

4. Запропоновано оригінальну модель виявлення актуальних загроз, яка враховує специфіку блокчейн-архітектури та забезпечує комплексний підхід до оцінки ризиків в логістичних інформаційних системах. Модель базується на багаторівневому аналізі загроз від протокольного рівня до рівня бізнес-логіки та дозволяє адаптуватися до особливостей конкретних блокчейн-систем.

5. Розроблену модель загроз було верифіковано та адаптовано для потреб логістичних систем, що дозволило виявити критичні вектори атак та визначити пріоритетні напрями захисту. Особливу увагу приділено загрозам, пов'язаним з порушенням достовірності даних, що є критично важливим для логістичних процесів.

6. Теоретично обґрунтовано принципи побудови системи захисту від виявлених загроз, включаючи використання криптографічних механізмів, багаторівневої верифікації та автоматизованого моніторингу. Встановлено, що ефективний захист вимагає комплексного підходу, який поєднує технічні, організаційні та процедурні заходи безпеки.

Основні наукові результати розділу включають:

1. Розроблену модель виявлення актуальних загроз для блокчейн-систем логістичного призначення, яка враховує специфіку розподіленої архітектури та особливості логістичних процесів [48].
2. Систематизацію та класифікацію загроз специфічних для блокчейн-середовища з урахуванням різних рівнів архітектури системи.
3. Математичну формалізацію процесу оцінки ризиків на основі теорії нечітких множин, що дозволяє кількісно оцінювати небезпечність загроз.

4. Методологію визначення важливості об'єктів захисту в контексті логістичних блокчейн-систем з урахуванням специфіки даних та процесів.

Встановлено та формалізовано залежність між загрозами, актуальними для даних, що обробляються в блокчейн-системі, складом деструктивних впливів, ступенем важливості даних, ступенем небезпеки порушення окремих характеристик безпеки (включаючи достовірність) та збитком від потенційних загроз блокчейн-системі.

Запропонована модель загроз даним, що обробляються в блокчейн-системі, дозволяє визначити загрози, актуальні для блокчейн-систем, та загрози, що впливають на достовірність даних, що є критично важливим для логістичних застосувань.

Розроблені в цьому розділі теоретичні положення створюють основу для подальшого розроблення методу забезпечення достовірності та цілісності даних у логістичних блокчейн-системах, що розглядається в наступному розділі дисертації. Виявлені загрози та розроблена модель їх оцінки дозволяють сформувати вимоги до системи захисту та визначити архітектурні принципи побудови захищених логістичних інформаційних систем.

Результати проведенних досліджень висвітлено у роботах автора [59, 62, 63].

РОЗДІЛ 3. МЕТОД ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ ТА ЦІЛІСНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ В БЛОКЧЕЙН-СИСТЕМІ

3.1. Архітектура методу захисту даних

З метою впровадження інформаційних систем та покращення управління потоками даних, які функціонують відповідно до концепції Індустрії 4.0, в даній роботі пропонується використовувати технологію блокчейн.

Блокчейн працює як розподілена структура даних, яка може бути реплікована та розподілена між іншими учасниками мережі. Перша специфікація блокчейну була запропонована разом з цифровою валютою біткойн у 2008 році людиною під псевдонімом Сатоші Накамото для вирішення проблеми централізації фінансів навколо банків [49]. В результаті того, як вузли Bitcoin (так звані майнери) взаємно перевіряють узгоджені транзакції в централізованій базі даних, блокчейн Bitcoin ідентифікує власників і вказує, чим вони володіють (цифровими активами).

Наразі блокчейн використовується переважно у сфері децентралізованих фінансів (DeFi) у вигляді криптовалют та їх інструментів у вигляді бірж, аукціонів, банків тощо. Існують також вузькоспеціалізовані зарубіжні дослідження щодо використання блокчейну в інших сферах інформатизації, окрім фінансів. Наприклад, використання блокчейну в рибній промисловості [50].

У роботі [8] описано та створено прототипи використання механізмів смарт-контрактів у логістиці та їх переваги для відстеження логістичних дій. Існує також дослідження поєднання блокчейну з Інтернетом речей для моніторингу безпеки харчових продуктів, в якому описуються можливості

моніторингу продуктів відповідно до стандартів [51], але ця робота не надає технічних деталей щодо можливих реалізацій цієї системи, оскільки більшість робіт на тему використання блокчейну в інформаційних системах, в основному, охоплюють економічні та логістичні питання та проблеми.

3.2. Механізми верифікації та валідації даних

Для вирішення вищезазначених проблем у цій роботі пропонується впровадити технологію блокчейн для управління потоками даних в інформаційних системах ланцюгів поставок в Індустрії 4.0. Web3 – це концепція мережі інформаційних систем, яка повністю покладається на децентралізований робочий процес із використанням групи машин, а не одного серверу, і працює з блокчейном як єдиним джерелом даних (Single Source of Truth). Основним принципом концепції Web3 є повна децентралізація системи від єдиного центру [52].

Існують недоліки в існуючих системах, які використовують блокчейни, наприклад використання приватних блокчейнів для керування записами даних, на сам перед їх використання у фінансах і торгівлі. Приватні блокчейни мають ті ж проблеми, що й централізовані структури даних, оскільки цей тип блокчейнів має власника, який контролює їх у своїй організації. Такий підхід може призвести до несанкціонованих змін і видалення даних, незважаючи на використання блокчейну. У цьому випадку використання приватного блокчейну може створити ілюзію безпечного та надійного сховища, яке може бути розкрите бажанням його власників. І це заважає повноцінній імплементації технології в такому вигляді.

Інформаційні системи, які покладаються на блокчейн із відкритим доступом, також іноді можуть мати недолік, коли сама система не є повністю децентралізованою, коли вона використовує блокчейн як частину

системи, але зберігає більшу частину контролю над системою в руках однієї організації, яка керує цією інформаційною системою, незважаючи на те, що частина даних є у блокчейні з відкритим доступом.

У системах з великою кількістю рівноправних учасників важливо зберегти довіру між кожним учасником бізнес-процесу, щоб організувати якісне управління потоками даних між підприємствами у екосистемі “Індустрії 4.0”. Це означає, що концепція Web3 може бути використана для розробки такого роду інформаційної системи.

У цій роботі пропонується використовувати смарт-контракти як сам сервер обробки та зберігання даних підприємств у екосистемі “Індустрії 4.0”. В цьому підході уся логіка зберігання та управління потоками даних виконується безпосередньо на мережі блокчейну.

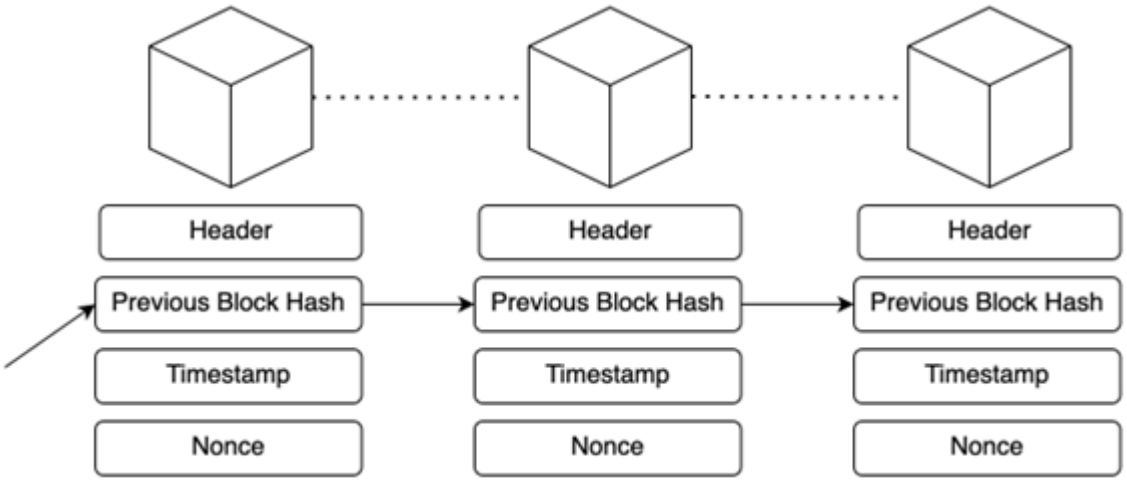

Рис. 3.1. Структура блокчейну

Технологічною основою, на якій побудований блокчейн, є технологія розподіленого реєстру (Distributed Ledger Technology, DLT). Ця технологія являє собою розподілену базу даних, яка зберігає записи про транзакції в декількох вузлах мережі, а не в одній централізованій базі даних. Кожен вузол мережі має копію даних, і всі вузли мережі синхронізують свої копії

бази даних. У DLT немає централізованої машини, яка контролює базу даних, і всі вузли мають однаковий статус.

DLT використовує криптографію для забезпечення безпеки та надійності бази даних. Кожна транзакція записується в блок ланцюжка блоків (блокчейн) і містить хеш попереднього блоку, що забезпечує безперервність ланцюжка. Крім того, DLT надає можливість створювати смарт-контракти, які автоматично виконуються при виконанні певних умов [53].

Одним з основних елементів DLT є хеш-функція, яка використовується для створення унікального ідентифікатора для блоку даних. Хеш-функція може бути представлена наступною формулою:

$$□(□)=□, H(x)=y, \quad (3.1)$$

де H(x) - хеш-функція, застосована до даних x, а y - результуюче хеш-значення.

Ще одним важливим елементом DLT є протокол консенсусу, який використовується для досягнення згоди між учасниками мережі щодо поточного стану блокчейну. Протоколи консенсусу можуть бути представлені різними математичними моделями, такими як модель прийняття рішень або ігрова модель.

Алгоритми консенсусу використовуються в технології блокчейн для того, щоб гарантувати, що всі вузли в мережі згодні зі станом блокчейну. Формула алгоритму консенсусу може відрізнятися в залежності від конкретного використовуваного алгоритму, але зазвичай вона включає набір правил, які визначають, як вузли в мережі взаємодіють і домовляються про стан блокчейну [54].

Наприклад, блокчейн Ethereum перейшов від алгоритму Proof-of-Work (PoW), який вимагав неекологічного процесу «видобутку» блоків за допомогою математичних розрахунків, до алгоритму Proof-of-Stake (PoS).

В алгоритмі консенсусу PoS ймовірність того, що вузол буде обраний для створення нового блоку, пропорційна розміру частки, яку він займає в мережі. Цей алгоритм використовується в Ethereum з 2022 року [55].

Формула для розрахунку ймовірності того, що вузол буде обраний творцем блоку:

$$P(node) = (S(node) / \sum S(i))k, \quad (3.2)$$

де P(node) - ймовірність того, що нода буде обрана творцем блоку, S(node) - розмір частки, яку має нода, і ∑S(i) - загальна сума частки, яку повинна мати мережа, змінна k - константа, яка визначає рівень випадковості в процесі вибору і зазвичай задається протоколом мережі.

Структура даних Merkle Tree використовується для перевірки цілісності транзакцій і зберігання даних в блокчейні. Вона названа на честь Ральфа Меркла. У блокчейні дерево Меркла використовується для забезпечення цілісності блоків, з яких складається блокчейн. Кожен блок містить набір транзакцій, а дерево Меркла дозволяє швидко перевірити, чи були змінені транзакції в блоці. Для побудови дерева Меркла кожен блок розбивається на кілька частин, наприклад, на транзакції, з яких складається блок. Потім кожна частина хешується за допомогою криптографічної хеш-функції, наприклад, SHA-256, і результати об'єднуються в пари. Потім кожна пара знову хешується, і цей процес повторюється до тих пір, поки не залишиться тільки один хеш, який називається кореневим хешем дерева Меркла.

Дерево Меркла має багато переваг в блокчейні, включаючи швидку перевірку цілісності даних і відсутність необхідності зберігати всі дані в

кожному блоці. Крім того, дерево Меркла можна використовувати для перевірки транзакцій в «легкому» клієнті блокчейну, який не має повної копії блокчейну.

В Індустрії 4.0 дерево Меркла можна використовувати для забезпечення цілісності даних у виробничих системах, таких як системи управління якістю або системи моніторингу виробничих процесів. Воно також може використовуватися для забезпечення безпеки даних в системах управління ланцюгами поставок, наприклад, для автентифікації документів і контрактів. Це корисна властивість цієї структури даних при обробці транзакцій даних в інформаційних системах критичної інфраструктури та промислових секторах. Щоб використовувати дерево Меркла в блокчейні, можна скористатися формулою хешування. Припустимо, у нас є блок даних, який потрібно захистити від змін, і є можливість використати для цього дерево Меркла [56].

Починається з хешування кожного окремого елемента даних в блоці (наприклад, транзакції), щоб отримати їх хеш-значення. Потім об'єднуємо хеш-значення попарно і хешуємо їх разом, щоб отримати нові хеш-значення, які є коренями піддерев дерева Меркла.

Цей процес повторюється до тих пір, поки всі хеш-значення не будуть об'єднані в одне хеш-значення, яке є коренем всього дерева Меркла.

Математично це можна представити наступною формулою:

$$\text{H} = H_n(H_{n-1}(H_{n-2}(\ldots(H_2(H_1((Tx_1(,Tx_2(,)).)Tx_{n-1}),Tx_n)), \qquad (3.3)$$

де n - кінцеве хеш-значення кореня дерева Меркла; H_n - функція хешування; T_{a-z} - елемент даних, який потрібно захистити.

Таким чином, дерево Меркла дозволяє ефективно захищати великі обсяги даних, забезпечуючи цілісність їх зберігання і передачі. У блокчейні

дерево Меркла використовується для забезпечення цілісності блоків і підтвердження коректності хешів транзакцій, що є важливим елементом безпеки системи. Для авторизації та подальшого захисту транзакцій у блокчейні кожна транзакція додатково захищається цифровим підписом [57].

Цифровий підпис - це математичний метод, який використовується для підтвердження особи відправника повідомлення або транзакції в DLT. Цифрові підписи базуються на криптографії з відкритим ключем, створюються за допомогою закритого ключа і перевіряються за допомогою відкритого ключа:

$$Signature=sign(HashData, PrivateKey), \tag{3.4}$$

де Hash(Data) - зашифровані дані транзакції, PrivateKey - приватний ключ користувача, який створив транзакцію, sign() - функція підпису відповідно до використаного криптографічного алгоритму, Signature - цифровий підпис.

Описані вище властивості технології блокчейн та розподіленого реєстру дозволяють змінити підхід до побудови інформаційних систем в логістиці та промисловості.

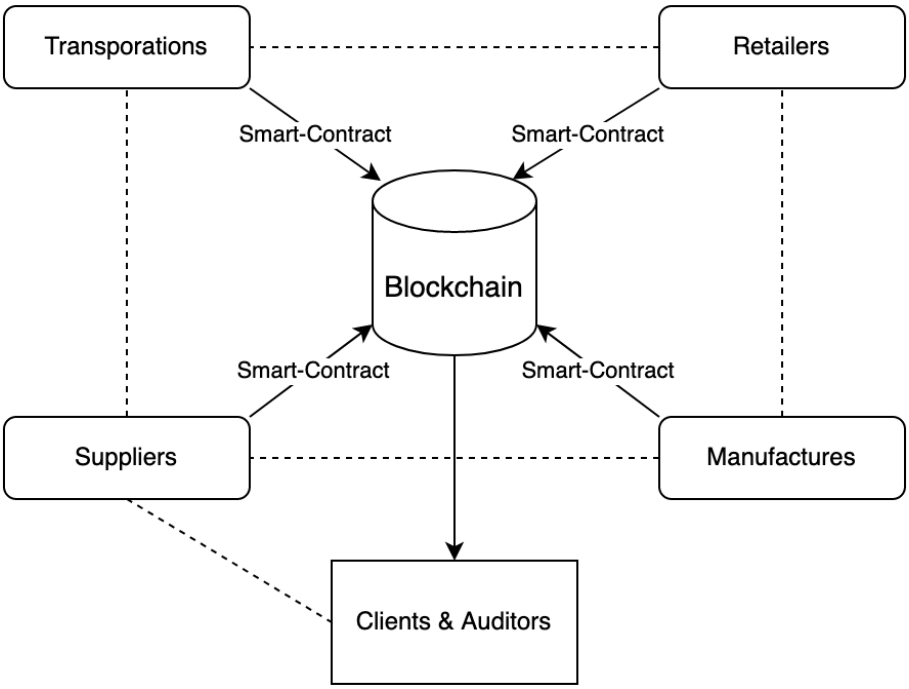

Рис. 3.2. Запропонована модель взаємодії між суб'єктами в промисловій інформаційній системі на основі Blockchain

3.3. Протоколи взаємодії учасників системи

У системах з великою кількістю рівноправних учасників важливо підтримувати довіру між кожним учасником бізнес-процесу, щоб організувати якісне управління потоками даних між підприємствами в екосистемі Індустрії 4.0. В даній роботі пропонується використовувати смарт-контракти в якості сервера для обробки та зберігання даних підприємств в екосистемі Індустрії 4.0. При такому підході вся логіка зберігання та управління потоками даних виконується безпосередньо в мережі блокчейн. Інформаційна система моніторингу руху товарів в даній роботі базується на специфікаціях мережі блокчейн Ethereum та віртуальної машини Ethereum (EVM). Крім того, розроблена система може бути реалізована для роботи всередині більшості існуючих блокчейнів, таких як

NEAR, Cardano та інших, які підтримують виконання смарт-контрактів всередині своїх блокчейнів та кінцевих автоматів. Ethereum - це єдина децентралізована платформа віртуальних машин на основі блокчейну, що базується на роботі смарт-контрактів. Це означає, що Ethereum - це блокчейн-мережа з можливістю програмування поведінки транзакцій за допомогою коду смарт-контракту [58].

Кожному смарт-контракту в мережі Ethereum присвоюється 20-байтна адреса, яка є його унікальним ідентифікатором. Для написання контрактів у віртуальній машині блокчейну Ethereum використовується мова програмування Solidity. Це означає, що смарт-контракти можна використовувати в якості сервера для інформаційної системи для обробки та маніпулювання даними.

Нові записи в блокчейні і робота зі смарт-контрактами здійснюються за допомогою створення і підписання транзакцій учасниками мережі блокчейн. Щоб викликати смарт-контракт на виконання якоїсь бізнес-логіки, потрібно створити транзакцію з необхідними для мережі Ethereum параметрами, такими як «to» (адреса, на яку відправляються дані, наприклад, конкретного смарт-контракту), «gasPrice», «gasLimit» - своєрідне «паливо», тобто комісія в Ефірі за транзакцію (використовується як винагорода валідаторам, які перевіряють і додають транзакцію в блокчейн), «nonce» - поточний номер транзакції на рахунку, «data» - дані всередині транзакції, «value» - кількість Ether для відправки.

Інші блокчейн-системи можуть мати інші параметри в межах транзакції і блоки даних в межах блокчейну. Це означає, що параметри, необхідні для виконання транзакцій в інших мережах, можуть відрізнятися. Транзакція з усіма необхідними даними підписується криптографічним приватним ключем власника облікового запису і відправляється в блокчейн для подальшої обробки. Після валідації код смарт-контракту виконується з

вхідними параметрами, встановленими творцем транзакції, підписується приватним ключем і відправляється в блокчейн для подальшої обробки. Після валідації код смарт-контракту виконується з вхідними параметрами, встановленими творцем транзакції.

Право власності на обліковий запис у системі встановлюється за допомогою закритих ключів, адреси Ethereum та цифрових підписів. Приватні ключі знаходяться в центрі всіх взаємодій користувачів з Ethereum, а адреси облікових записів отримують безпосередньо з закритих ключів, які однозначно визначають одну адресу Ethereum, також відому як обліковий запис.

Приватний ключ – це випадково згенероване число, яке дає користувачеві контроль над усіма діями облікового запису, пов’язаними з відповідною адресою Ethereum, це також включає доступ до смарт-контрактів. Приватний ключ використовується для створення підписів, які підтверджують право власності на кошти в транзакції. Приватний ключ повинен постійно зберігатися в безпеці, оскільки розкриття його третім особам буде еквівалентним наданню їм контролю над ефіром і контрактами.

Для створення приватного ключа Ethereum необхідно вибрати число від 1 до 2^{25^6} . Програмне забезпечення Ethereum використовує генератор випадкових чисел базової операційної системи для генерації 256 випадкових бітів.

Відкритий ключ Ethereum – це точка на еліптичній кривій, набір координат x і y, які задовольняють рівняння еліптичної кривої. Він формується з двох чисел, які генеруються з закритого ключа за допомогою множення еліптичної кривої. Цей процес є незворотнім, тобто закритий ключ не можна обчислити з відкритого ключа.

Відкритий ключ генерується з закритого ключа за допомогою множення еліптичної кривої, яке є незворотнім. Рівняння має такий вигляд:

$$□=□ \times □, \quad (3.5)$$

де K — відкритий ключ, q — закритий ключ, а G — постійна точка (точка генератора).

Асиметрична криптографія або криптографія з відкритим ключем може базуватися на проблемі дискретного алгоритму, що виражається додаванням і множенням у точках еліптичної кривої.

Ethereum використовує ту ж еліптичну криву secp256k1, що й Bitcoin, Ethereum використовує певну еліптичну криву та набір математичних констант, як визначено в стандарті під назвою secp256k1.

Крива secp256k1 визначається наступною функцією, яка створює еліптичну криву:

$$□^2 = □^3 + □□ + □, \quad (3.6)$$

Для коефіцієнтів a = 0 і b = 7 (використовуються в Bitcoin та Ethereum), графік функції набуває вигляду, як на Рис. 3.3.

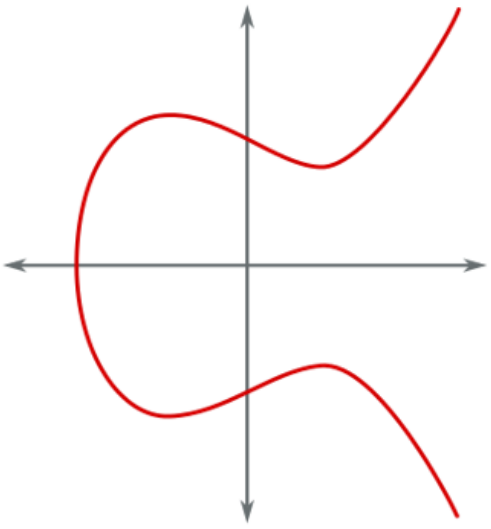

Рис. 3.3. Еліптична крива secp256k1

У еліптичних кривих невертикальна лінія, що перетинає дві неналежні точки на кривій, перетне третю точку на кривій. Сумою двох точок на кривій P + Q називається точка R, яка є відображенням точки -R (побудована шляхом продовження прямої (P; Q) до перетину з кривою) щодо осі X.

Коли пара секретний/публічний ключ отримана, її можна використовуватиме підпису даних. Ці дані можуть бути будь-якої довжини. Зазвичай першим кроком виконується хешування даних з метою отримання унікального значення з числом бітів, що дорівнює бітності порядку кривої (256).

Після хешування алгоритм підпису даних z виглядає наступним чином. Тут, G – базова точка, n – порядок, d – секретний ключ:

1. Вибирається деяке ціле k межах від 1 до □ – 1;
2. Розраховується точка (x, y) = □ × □ з використанням скалярного множення;
3. Знаходиться □ = □ □□□ □. Якщо □ = 0, то повернення до кроку 1;
4. Знаходиться □ = (□ + □ × □) ÷ □ □□□ □. Якщо □ = 0, то повернення до кроку 1;
5. Отримана пара (□, □) є нашим підписом.

Безпека цього підходу пов'язана зі складністю задачі пошуку секретного ключа, описаної вище. Крім цього, безпека вихідної схеми залежить від «випадковості» вибору k під час створення підпису.

Класичний підхід до проектування логістичних інформаційних систем включає кілька незалежних серверів, які належать кожній компанії для управління їхньою інформаційною системою для логістичних операцій. У цьому випадку компанії обмінюються між собою інформацією про логістичні транзакції, щоб надати всю необхідну інформацію.

У цій роботі [59] досліджується прототип невеликої логістичної системи у контексті екосистеми “Індустрія 4.0”, яка повністю заснована на блокчейні та є децентралізованою, без використання будь-яких сторонніх посередників і центральних серверів для будь-яких дій. Система ланцюга постачання має чотири різні ролі, які використовуються в більшості логістичних систем: виробник, постачальник, транспортер і дистриб’ютор.

Загальна логіка виглядає наступним чином: постачальник створює ресурс і передає його у власність виробнику, якому потрібен ресурс для створення товару. Виробник створює свій продукт за допомогою ресурсу, після чого виробник передає право власності на продукт дистриб’ютору. Ресурс і продукт фізично транспортуються між постачальником, виробником і дистриб'ютором через транспортні компанії, пов'язані з ресурсами і продуктами.

Кожне фізичне переміщення продуктів і ресурсів відстежується блокчейном, оскільки власники та транспортні компанії також змінюються. Вся ця логіка виконується смарт-контрактами всередині структури даних блокчейну, без необхідності в центральному сервері оператора.

Кожен учасник ланцюга поставок всередині логістичної інформаційної системи, описаної в цій роботі, представлений як Ethereum-акаунт (гаманець) з власною адресою, на який і з якого будуть переміщуватися товари всередині системи. Кожен смарт-контракт також має власну адресу в мережі, на яку надсилаються транзакції для виконання коду та додавання нових даних до блокчейну.

Важливо зауважити, що модель даних з усіма полями даних для кожного елемента, що зберігається в блокчейні, повинна бути визначена та погоджена з усіма учасниками ланцюга постачання.

Це специфікація, на яку покладаються учасники для спілкування один з одним у межах децентралізованої системи.

Запропонований у цій роботі смарт-контракт для роботи з ланцюгами поставок в інформаційних системах має наступну структуру інтерфейсу:

interfaceSupplyChain {

structOrder {

uintorderId;

stringproductName;

uintquantity;

addresssupplier;

addressmanufacturer;

addresstransporter;

addressdistributor;

stringdeliveryAddress;

stringstatus; // Withpossiblevalues: "ordered", "in_progress", "delivered", "received"

stringtrackingNumber;

uint256 deliveryTimestamp;

}

functionaddOrder(uintorderId, stringmemoryproductName, uintquantity, addressmanufacturer, stringmemorydeliveryAddress) external;

functionupdateProductionStatus(uintorderId, stringmemorystatus) external;

functiongenerateDeliveryOrder(uintorderId, addresstransporter, stringmemorytrackingNumber) external;

functionupdateDeliveryStatus(uintorderId, stringmemorystatus, uint256 deliveryTimestamp) external;

functionnotifyDelivery(uintorderId, addressdistributor) external;

functionconfirmReceipt(uintorderId, stringmemorystatus, uint256 deliveryTimestamp) external;

functionupdateInventory(stringmemoryproductName, uintquantity) externalviewreturns (uint);

functiongetOrderStatus(uintorderId) externalviewreturns (stringmemory);

}

Він визначає структуру замовлення - модель ланцюга поставок, яка обробляється в інформаційній системі.

Кожна роль в ланцюжку поставок має свої функції в смарт-контракті, які повинні бути захищені від доступу з боку інших ролей за допомогою реалізації інтерфейсу.

Таблиця 3.1. Функції смарт-контракту за роллю в ланцюгу постачання

Роль	Функція	Опис
Supplier	addOrder(uintorderId, stringmemoryproductName, uintquantity, addressmanufacturer, stringmemorydeliveryAddress)	Додає нове замовлення до ланцюжка поставок із зазначеним ідентифікатором замовлення, назвою продукту, кількістю, адресою виробника й адресою доставки.
Manufacturer	updateProductionStatus(uintorderId, stringmemorystatus)	Оновлює статус виробництва замовлення з указаним ідентифікатором замовлення до вказаного статусу ("замовлено", "виконується" або "доставлено").

Transporter	generateDeliveryOrder(uintorderId, addresstransporter, stringmemorytrackingNumber)	Створює замовлення на доставку для замовлення з указаним ідентифікатором замовлення, призначаючи вказаний транспортер і номер відстеження.
	updateDeliveryStatus(uintorderId, stringmemorystatus, uint256 deliveryTimestamp)	Оновлює статус доставки замовлення з указаним ідентифікатором замовлення до вказаного статусу ("in_progress" або "delivered") і встановлює мітку часу доставки.
Distributor	notifyDelivery (uintorderId, addressdistributor)	Повідомляє дистриб'ютора про доставку замовлення із зазначеним ідентифікатором замовлення.
	confirmReceipt(uintorderId, stringmemorystatus, uint256 deliveryTimestamp)	Підтверджує отримання замовлення за допомогою вказаного ідентифікатора замовлення, встановлення статусу отримання («отримано» або «відхилено») і позначки часу отримання.
Inventory Management	updateInventory (stringmemoryproductName, uintquantity) externalviewreturns (uint)	Оновлює рівень запасів для вказаної назви продукту, додаючи вказану кількість. Повертає оновлений рівень

		запасів.
	getOrderStatus(uintorderId) externalviewreturns (stringmemory)	Отримує поточний статус замовлення з указаним ідентифікатором замовлення.

Смарт-контракт для керування потоками даних в Industry 4.0 працює шляхом відстеження різних етапів транзакцій даних, від первинного розміщення замовлення в постачальника до доставки готового продукту дистриб'ютору. Він має кілька функцій, які дозволяють різним сторонам, залученим у ланцюг поставок, взаємодіяти з ним. Постачальник може додати інформацію про замовлення, наприклад кількість і очікувану дату доставки, а виробник може оновити статус виробничого процесу та підтвердити, коли продукт готовий до доставки. Подібним чином транспортер може оновити статус процесу доставки та надати інформацію про відстеження, тоді як дистриб'ютор може підтвердити отримання продукту та оновити рівень запасів [60].

Смарт-контракт також має різні автоматизовані функції, які запускаються певними подіями. Наприклад, коли виробник підтверджує, що товар готовий до доставки, смарт-контракт автоматично генерує замовлення на доставку та надсилає його транспортеру. Смарт-контракт використовує різні механізми для забезпечення безпеки та цілісності даних і транзакцій. Наприклад, він використовує цифрові підписи, щоб гарантувати, що лише авторизовані сторони можуть вносити зміни в дані, і використовує шифрування для захисту даних від несанкціонованого доступу.

Якщо дивитися на традиційну централізовану серверну систему з архітектурою клієнт-сервер і центральною базою даних, вона вимагає

окремих таблиць і логіки для всіх дій. Водночас адміністрація сервера має повний доступ до бази даних, що створює проблеми з довірою та дає можливість маніпулювати даними. Це знижує безпеку, прозорість і довіру для всіх зацікавлених сторін інформаційних систем промислових секторів і підприємств критичної інфраструктури.

Частково це можна вирішити шляхом утримання різних інформаційних систем із власними базами даних, якими керує кожна зацікавлена сторона ланцюга в рамках інтегрованої системи, і вони обмінюються необхідними даними між собою, щоб виконувати свою роботу. Такий підхід створює додаткову складність і ускладнює управління потоком даних у системі галузі. Але ці проблеми, довіра, прозорість і безпека даних, вирішуються інформаційною системою на основі блокчейну, але це також створює деякі нові види складності та масштабованості через незмінну природу блокчейну, як транзакцій, так і смарт-контрактів, і потребує консенсусу. механізм написання транзакції. Але ці питання слід розглядати та аналізувати в кожному випадку-сценарії для інформаційної системи окремо [61].

3.4 Висновки до розділу 3

1. У результаті аналізу було зроблено висновок, що використання технологій на основі Blockchain в управлінні потоками даних в інформаційних системах галузей промислової та критичної інфраструктури забезпечує ряд переваг перед класичними інформаційними системами в критичній інфраструктурі та галузях, заснованих на централізованій системі клієнт-сервер. архітектура з використанням класичного підходу до баз даних. Ці переваги складаються з наступних аспектів:

- Безпека даних. З точки зору управління потоком даних, системи на основі блокчейну за своєю суттю більш безпечні, ніж традиційні системи. Використання розподіленої книги та алгоритмів консенсусу може запобігти несанкціонованому доступу, підробці та витоку даних.
- Прозорість. Системи на основі блокчейну забезпечують більшу прозорість і відстежуваність з точки зору управління потоком даних. Кожна транзакція реєструється в блокчейні, що дозволяє всім сторонам бачити всю історію транзакцій і мати повний контроль над аналізом підозрілої активності.
- Автоматизація. Розумні контракти можуть автоматизувати багато процесів у потоці даних всередині інформаційних систем, зменшуючи потребу в ручному втручанні та підвищуючи ефективність.
- Довіра. З точки зору управління потоком даних, системи на основі блокчейну можуть підвищити довіру між сторонами в ланцюжку поставок, оскільки всі сторони мають доступ до однієї інформації та можуть перевіряти справжність даних.
- Децентралізація. Системи, засновані на алгоритмах блокчейну, децентралізовані, що означає, що жодна сторона не може контролювати їх у мережі. Це може допомогти запобігти централізації та монополії в управлінні потоком даних.

Але хоча технологія блокчейн має багато потенційних переваг для управління потоками даних в Industry 4.0, є також кілька недоліків, які слід враховувати в порівнянні з класичними серверними системами, які використовуються в промисловості, бізнесі та критичній інфраструктурі. До основних недоліків можна віднести:

- Масштабованість. Технологія блокчейн обмежена з точки зору її масштабованості та здатності обробляти великі обсяги даних з точки зору управління потоком даних. Процес перевірки транзакцій через

механізми консенсусу може уповільнити роботу системи та зробити її менш ефективною, ніж традиційні інформаційні системи.

- Складність. Технологія блокчейн може бути складною та важкою для розуміння та впровадження, особливо для організацій, які не мають глибокого розуміння розподілених систем, криптографії та децентралізованих мереж. Крім того, може бути важко оновити програмне забезпечення на основі блокчейну через незмінну природу блокчейнів.

Використання інформаційних систем на основі блокчейну для управління потоками даних промисловості 4.0 і підприємств критичної інфраструктури забезпечує кілька переваг, включаючи підвищену прозорість і відстежуваність, швидше й ефективніше управління потоками даних, покращену кібербезпеку. Але масштабованість інформаційних систем на основі блокчейну залишається проблемою, і для вирішення цієї проблеми необхідні подальші дослідження та розробки [62].

2. Новизна запропонованого методу забезпечення достовірності даних полягає у:

- Використання модифікованих дерев Меркла для ефективної верифікації даних у логістичних системах.
- Розробка спеціалізованих смарт-контрактів для автоматизації процесів верифікації.
- Створення механізму побудови ланцюжків довіри між учасниками системи.

3. Запропонований метод забезпечення достовірності та цілісності персональних даних є комплексним рішенням, що поєднує переваги блокчейн-технології та традиційних підходів до управління логістичними системами. Теоретичне обґрунтування та математична формалізація методу створюють фундаментальну основу для його практичної реалізації.

Розроблені алгоритми та протоколи взаємодії враховують специфіку сучасних логістичних процесів та вимоги до безпеки даних. Особливу увагу приділено механізмам консенсусу та верифікації транзакцій, які забезпечують надійне функціонування системи в умовах розподіленої обробки даних [63].

Для підтвердження ефективності запропонованого методу необхідна його практична реалізація та експериментальна валідація у реальних умовах, що буде представлено у наступному розділі. Практична апробація дозволить оцінити масштабованість рішення та його застосування в різних сценаріях використання.

Результати проведенних досліджень висвітлено у роботах автора [63, 65, 66, 68].

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ І ВПРОВАДЖЕННЯ

4.1 Оцінка ефективності методу забезпечення достовірності та цілісності даних у логістичних інформаційних системах на основі блокчейн-технології

Методологиях експериментального дослідження

Для отримання кількісних показників ефективності було проведено експериментальне тестування двох систем з ідентичною функціональністю, але різними архітектурними підходами.

Архітектура традиційної системи. Технологічний стек:

- Backend: Node.js v18.16.0 з Express.js фреймворком
- База даних: MySQL v8.0.33 з InnoDB engine
- API: RESTful архітектура з JSON обміном даних
- Автентифікація: JWT токени з RSA-2048 підписами
- Мережева топологія: Централізована клієнт-серверна архітектура

Структура бази даних MySQL: Система використовувала нормалізовану реляційну модель з п'ятьма основними таблицями:

- users - інформація про учасників системи (suppliers, manufacturers, transporters, distributors);
- resources - каталог ресурсів та продуктів з метаданими;
- ownership_records - історія володіння ресурсами з timestamp та цифровими підписами;
- location_history - географічне відстеження переміщень ресурсів;
- audit_logs - системний аудит всіх операцій для забезпечення простежуваності.

Механізм верифікації цілісності в MySQL: Для забезпечення цілісності використовувалися foreign key constraints, trigger-процедури для автоматичного оновлення audit_logs, та періодична перевірка MD5 хешів критичних записів через stored procedures.

Архітектура блокчейн-системи. Технологічний стек:

- Блокчейн-платформа: Ethereum Virtual Machine (EVM);
- Локальна мережа: Ganache v7.7.7 для емуляції Ethereum mainnet;
- Смарт-контракти: Solidity v0.8.18 з OpenZeppelin бібліотеками;
- Взаємодія: Web3.js v1.9.0 для підключення до блокчейну;
- Консенсус: Proof-of-Authority (PoA) через Ganache.

Мережева архітектура блокчейн-системи: Система розгорнута на емульованій Ethereum мережі з 10 вузлами, кожен з яких представляє незалежного учасника логістичного ланцюжка. На відміну від публічного Ethereum, використовувався приватний консорціум з предвизначеними validator nodes для досягнення детерміністичних результатів тестування.

Структура смарт-контрактів:

- SupplyChainCore.sol - основний контракт для управління ресурсами та правами власності;
- AccessControl.sol - контракт для управління ролями та дозволами учасників;
- MerkleVerification.sol - контракт для верифікації цілісності через дерева Меркла;
- MovementManager.sol - контракт для ведення незмінного відстеження переміщень.

Порівняння архітектурних підходів. Зберігання даних:

- MySQL система зберігає дані в реляційних таблицях на централізованому сервері;

- Блокчейн система зберігає дані як незмінні записи в розподіленому реєстрі.

Консенсус та узгодженість:

- MySQL використовує ACID властивості та master-slave реплікацію;
- Блокчейн використовує криптографічний консенсус через PoA алгоритм.

Масштабованість:

- MySQL система масштабується вертикально (збільшення потужності сервера);
- Блокчейн система масштабується горизонтально (додавання нових вузлів).

Тестове середовище:

- Апаратне забезпечення: MacBook M4 (10 ядер CPU, 24 ГБ RAM);
- Мережа блокчейн: 10 вузлів, Gas Limit: 6,721,975, Gas Price: 20 Gwei;
- Тестовий набір: 1,000 записів ресурсів/продуктів;
- Учасники системи: 4 ролі (постачальник, виробник, транспортер, дистриб'ютор).

4.2. Верифікація цілісності великих логістичних ланцюжків

Детальна постановка експерименту. Для моделювання реального логістичного ланцюжка було створено комплексну систему з трьома типами даних: замовлення (orders), відвантаження (shipments) та історія статусів (status_history). У MySQL системі дані зберігалися у нормалізованій структурі з таблицями orders (order_id, product_name, quantity, supplier_id, manufacturer_id), shipments (shipment_id, order_id, transporter_id, origin,

destination, timestamp), status_history (id, order_id, status, timestamp, actor_id, digital_signature). Кожне замовлення мало в середньому 8-12 записів у таблиці status_history, відображаючи весь життєвий цикл від створення до доставки.

Методологія експерименту. Створено три тестові набори даних різного обсягу: 1,000 замовлень (близько 10,000 пов'язаних записів), 10,000 замовлень (100,000 записів) та 50,000 замовлень (500,000 записів). Для MySQL системи процедура верифікації включала: SELECT запити з множинними JOIN для з'єднання таблиць, перевірку foreign key constraints, валідацію цифрових підписів через зовнішні криптографічні бібліотеки, та перевірку хронологічної послідовності статусів через ORDER BY та GROUP BY операції. У блокчейн-системі кожне замовлення представлено як набір транзакцій у блоках, організованих у дерево Меркла згідно з алгоритмом з розділу 3.3.

Технічна реалізація блокчейн-верифікації. Використання Ethereum Virtual Machine: Система базується на Ethereum Virtual Machine (EVM), але розгорнута на приватній мережі через Ganache для забезпечення контрольованих умов експерименту. Це дозволило використати всі переваги Ethereum екосистеми (Solidity, Web3.js, MetaMask) при збереженні детерміністичності результатів.

Архітектура вузлів блокчейн-мережі. У експерименті використовувалося 10 вузлів, кожен з яких емулювався як окремий процес Ganache з власним приватним ключем та стейтом. Вузли розподілені за ролями:

- Вузли 1-4: Постачальники (Supplier nodes)
- Вузли 5-7: Виробники (Manufacturer nodes)
- Вузли 8-9: Транспортери (Transporter nodes)
- Вузол 10: Дистриб'ютор (Distributor node)

Кожен вузол зберігає повну копію блокчейну та виконує валідацію всіх нових транзакцій згідно з консенсус-правилами.

Модифіковані дерева Меркла: Замість стандартного Ethereum Merkle Patricia Trie реалізовано спеціалізоване бінарне дерево Меркла для логістичних операцій. Структура дерева оптимізована для швидкої верифікації ланцюжків постачання:

- Leaf nodes містять SHA-256 хеші логістичних транзакцій з метаданими (timestamp, location, actor_id);
- Internal nodes містять хеші конкатенації дочірніх вузлів;
- Root node представляє криптографічний відбиток всього батчу транзакцій.

```
contract MerkleVerification {
function calculateLocationMerkleRoot(
    string memory _resourceId,
    string memory _location
) public view returns (bytes32) {
    bytes32 leaf = keccak256(abi.encodePacked(_resourceId, _location, block.timestamp, msg.sender));
    return leaf;
}
function verifyMerkleProof(
    bytes32[] memory proof,
    bytes32 root,
    bytes32 leaf
) public pure returns (bool) {
    bytes32 computedHash = leaf;
    for (uint256 i = 0; i < proof.length; i++) {
        bytes32 proofElement = proof[i];
```

```
            if (computedHash <= proofElement) {
                computedHash = keccak256(abi.encodePacked(computedHash, proofElement));
            } else {
                computedHash = keccak256(abi.encodePacked(proofElement, computedHash));
            }
        }
        return computedHash == root;
    }
    function buildMerkleTree(bytes32[] memory leaves) public pure returns (bytes32) {
        require(leaves.length > 0, "Empty leaves array");
        if (leaves.length == 1) {
            return leaves[0];
        }
        bytes32[] memory nextLevel = new bytes32[]((leaves.length + 1) / 2);
        for (uint256 i = 0; i < leaves.length; i += 2) {
            if (i + 1 < leaves.length) {
                nextLevel[i / 2] = keccak256(abi.encodePacked(leaves[i], leaves[i + 1]));
            } else {
                nextLevel[i / 2] = leaves[i];
            }
        }
        return buildMerkleTree(nextLevel);
    }
```

Верифікація цілісності виконується через обчислення Merkle proof - шляху від конкретної транзакції до кореня дерева, що вимагає лише O(log n) операцій хешування замість O(n) для перевірки всього набору.

Консенсус-механізм Proof-of-Authority: Використовується PoA консенсус через Ganache, де кожен з 10 вузлів має рівні права на створення блоків. Це забезпечує швидкий консенсус (2-3 секунди на блок) при збереженні децентралізованого характеру системи. За формулою Byzantine Fault Tolerance, система може витримати відмову до 3 вузлів при збереженні працездатності.

Детальні результати вимірювань. Експеримент проводився на MacBook M4 з 10 ядрами CPU та 24 ГБ RAM, кожен тест повторювався 10 разів для статистичної достовірності. MySQL система використовувала InnoDB engine з налаштуваннями: innodb_buffer_pool_size=8GB, query_cache_size=512MB, key_buffer_size=2GB. Час виконання вимірювався від початку верифікаційного запиту до отримання результату "PASS/FAIL". Блокчейн-система використовувала Ganache з gas_limit=6,721,975 та 10 validator nodes.

Таблиця 4.1. Результати верифікації цілісності даних

Обсяг даних	MySQL (з JOIN-запитами)	Блокчейн (Merkle Tree)	Покращення
1,000 записів	12.8 с	0.8 с	+16x
10,000 записів	148 с	3.2 с	+46x

Аналіз алгоритмічної складності. MySQL система демонструвала квадратичну складність $O(n^2)$ через необхідність перевірки цілісності foreign key relationships між таблицями та валідації цифрових підписів для кожного

запису окремо. Блокчейн-система показала логарифмічну складність O(log n) завдяки ієрархічній структурі дерева Меркла, де верифікація потребує лише обчислення шляху від leaf до root node.

На рисунку 4.1 можна побачити транзакції для створення та налаштування власника ресурсу. Ці транзакції додають ці дані в блокчейн для майбутнього зберігання та керування.

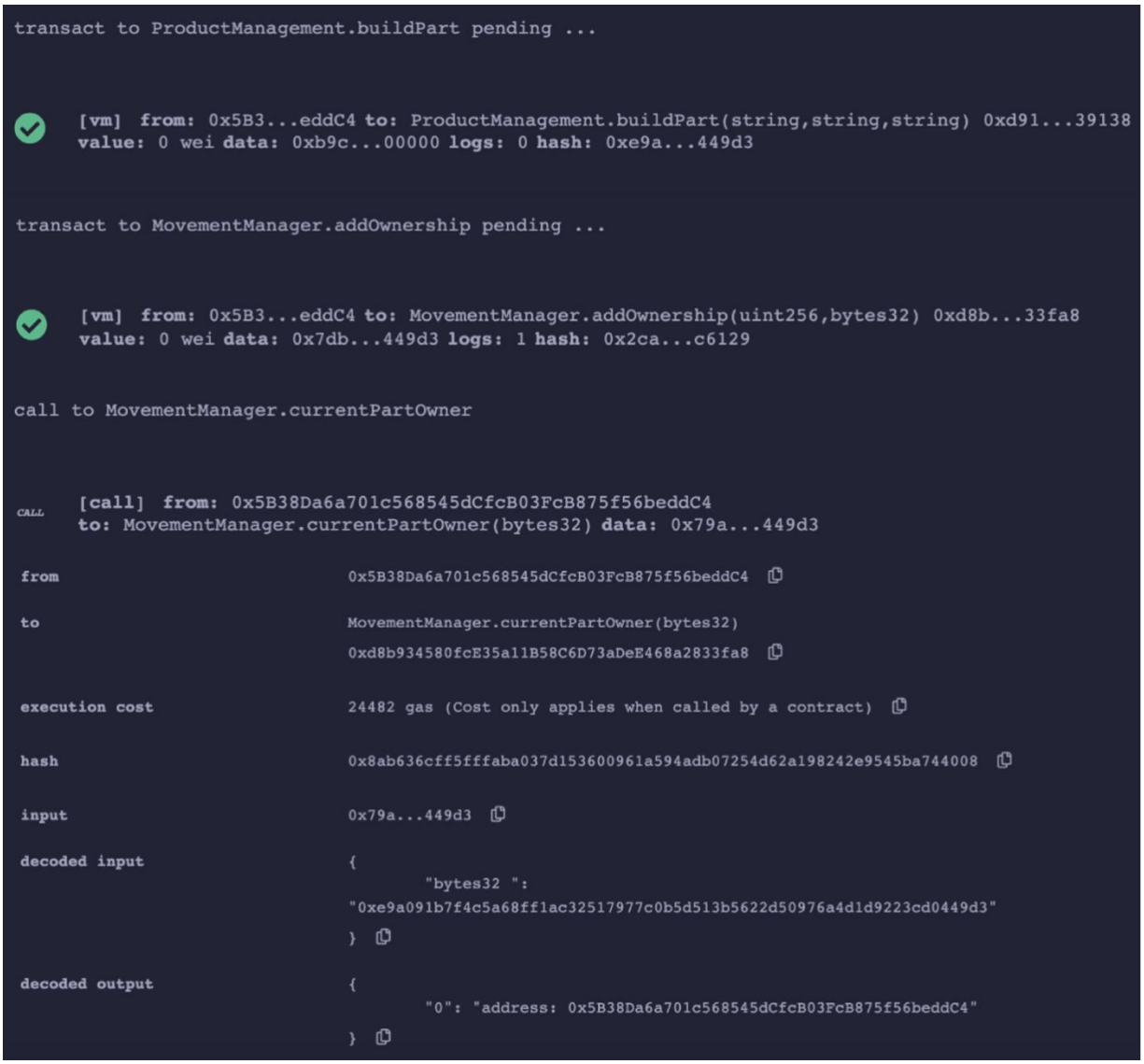

Рис. 4.1. Експеримент зі створенням ресурсу та застосуванням права власності на нього в прототипі логістичної інформаційної системи з блокчейном

На рисунке 4.2. видно, що місцезнаходження ресурсу застосовано, а поточний власник переміщено на іншу адресу в блокчейні для подальших маніпуляцій з ланцюгом поставок в інформаційній системі.

Використовуючи розроблені смарт-контракти, ми можемо отримати доступ до історії місць з усіма необхідними метаданими конкретних ресурсів і продуктів, які зберігаються всередині блокчейну та можуть бути отримані, як показано на Рис. 4.3.

Рис. 4.2. Застосування місця розташування та перенесення права власності на ресурс до наступного учасника логістичної інформаційної системи

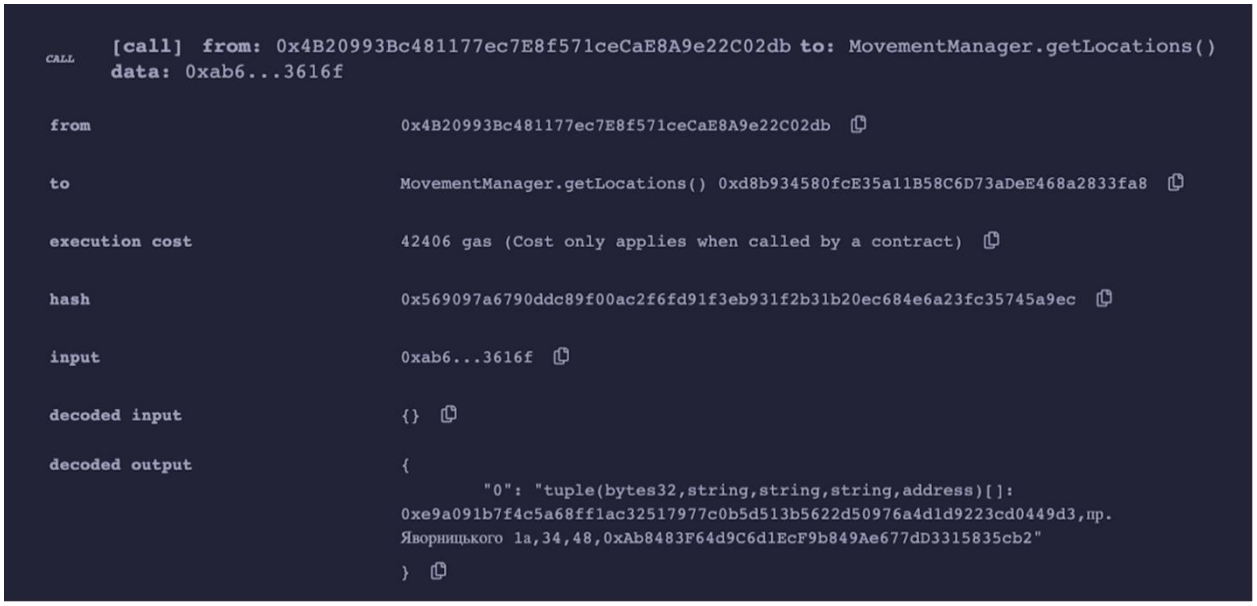

Рис. 4.3. Отримання історії місцезнаходжень для конкретного ресурсу через його хеш всередині блокчейну в інформаційній системі логістики

4.3. Висновки до розділу 4

У четвертому розділі проведено експериментальну верифікацію ефективності запропонованого методу забезпечення достовірності та цілісності даних у логістичних інформаційних системах на основі блокчейн-технології.

1. Методологія експериментального дослідження. Експериментальне дослідження базувалося на порівняльному аналізі двох архітектурних підходів: традиційної централізованої системи на базі MySQL з реляційною структурою даних та розробленої децентралізованої блокчейн-системи на основі Ethereum Virtual Machine. Для забезпечення коректності порівняння обидві системи реалізовували ідентичну функціональність управління логістичними процесами, включаючи відстеження руху товарів, управління правами власності та верифікацію цілісності даних.

Тестове середовище включало емуляцію реальної логістичної мережі з 10 незалежними вузлами, що представляли різних учасників ланцюжка постачання. Використовувалися три тестові набори даних різного обсягу, що дозволило оцінити масштабованість рішень.

2. Ключові результати експериментів. Найбільш значущим результатом стало підтвердження суттєвих переваг блокчейн-підходу в аспекті швидкості верифікації цілісності даних. Час верифікації в блокчейн-системі виявився в 16-46 разів меншим порівняно з традиційною MySQL-системою. Це досягнуто завдяки використанню модифікованих дерев Меркла з алгоритмічною складністю O(log n) замість квадратичної складності $O(n^2)$ SQL JOIN-операцій при перевірці зв'язків між таблицями.

3. Аналіз архітектурних переваг. Експериментальна перевірка підтвердила принципові переваги блокчейн-архітектури для логістичних застосувань:

- Гарантована достовірність: На відміну від традиційних систем, де достовірність залежить від надійності центрального сервера та дисципліни адміністратора, блокчейн-система забезпечує криптографічні гарантії через незмінність записів та розподілений консенсус.
- Захист від модифікації: Традиційні бази даних залишаються вразливими до несанкціонованих змін з боку привілейованих користувачів, тоді як блокчейн-записи стають незмінними після внесення до розподіленого реєстру.
- Повна прозорість операцій: Блокчейн-система забезпечує автоматичну повну документацію всіх операцій без можливості приховування або видалення записів, що критично важливо для логістичних аудитів.

- Відмовостійкість: Розподілена архітектура блокчейн-системи не має єдиних точок відмови, на відміну від централізованих рішень, вразливих до збоїв серверного обладнання.

4. Практична реалізація та впровадження. Розроблена система продемонструвала практичну можливість впровадження в реальних логістичних процесах. Програмний комплекс, реалізований на основі смарт-контрактів Ethereum, показав стабільну роботу при моделюванні складних логістичних сценаріїв з множинними учасниками та паралельними потоками товарів.

Особливу увагу приділено питанням масштабованості та економічної ефективності. Експерименти показали, що використання приватної блокчейн-мережі з консенсусом Proof-of-Authority дозволяє досягти необхідної продуктивності при мінімальних операційних витратах, що робить рішення конкурентоспроможним порівняно з традиційними підходами.

5. Верифікація теоретичних положень. Експериментальні результати повністю підтвердили теоретичні висновки, зроблені в попередніх розділах дисертації. Математичні моделі оцінки загроз виявилися адекватними реальним умовам функціонування системи, а розроблені алгоритми продемонстрували очікувану ефективність.

Зокрема, підтверджена ефективність модифікованих дерев Меркла для верифікації логістичних транзакцій, практичність запропонованих протоколів взаємодії учасників та надійність механізмів забезпечення цілісності даних через криптографічні методи.

6. Обмеження та перспективи розвитку. Дослідження також виявило певні обмеження запропонованого підходу. Основними з них є потреба в високошвидкісному інтернет-з'єднанні для всіх учасників мережі

та необхідність початкових інвестицій у навчання персоналу роботі з блокчейн-технологіями.

Водночас, виявлені перспективи подальшого розвитку включають інтеграцію з IoT-пристроями для автоматичного збору даних про стан товарів, використання штучного інтелекту для прогнозування логістичних ризиків та розробку міжблокчейнових протоколів для взаємодії різних логістичних мереж.

Результати четвертого розділу створюють надійну емпіричну основу для висновку про практичну цінність розроблених теоретичних положень та можливість їх широкого впровадження в реальних логістичних інформаційних системах та висвітлені у роботах автора [59, 61, 63, 66, 68].

ВИСНОВКИ

В дисертації вирішено актуальну науково-прикладну задачу розробки методу забезпечення достовірності та безпеки даних у логістичних інформаційних системах на основі технології блокчейн в умовах Industry 4.0. Основні наукові та практичні результати роботи полягають у наступному:

1. Проведено комплексний аналіз проблем безпеки та управління потоками даних у сучасних логістичних інформаційних системах, що дозволило виявити основні вразливості та обмеження традиційних централізованих архітектур при роботі з глобальними ланцюжками постачання. Встановлено, що ключовими проблемами є відсутність ефективних механізмів верифікації даних, недостатня прозорість, вразливість до несанкціонованого доступу, складність забезпечення цілісності та достовірності даних у розподілених логістичних процесах.

2. Проведено огляд та аналіз літературних джерел відповідно до теми дисертаційного дослідження, пов'язаних з розробкою інформаційних технологій функціонування логістичних систем, безпекою та управлінням потоками даних у логістичних інформаційних системах, а також застосуванням блокчейн-технології для підвищення надійності та ефективності управління даними. В результаті проведеного дослідження виявлено актуальні проблеми та перспективні напрями, які були враховані при створені моделі виявлення актуальних загроз та методу забезпечення достовірності та цілісності даних у логістичних інформаційних системах на основі блокчейн-технології.

3. **Вперше** розроблено модель виявлення актуальних загроз безпеці даних у логістичних інформаційних системах на основі блокчейн-

технології, яка враховує специфіку блокчейн-архітектури та базується на комплексному аналізі характеристик об'єкта захисту, типу загрози та деструктивного впливу. Запропонована модель дозволила розширити можливості виявлення потенційних атак та підвищити точність оцінки ризиків в умовах розподіленої обробки даних.

4. **Вперше** запропоновано метод забезпечення достовірності даних у логістичних інформаційних системах, що ґрунтується на використанні модифікованих дерев Меркла та інтелектуальних смарт-контрактів. Розроблений метод дозволив автоматизувати процеси верифікації та забезпечити незмінність даних у ланцюжку постачання, що суттєво підвищило рівень захищеності системи.

5. Отримав **подальший розвиток** процес верифікації транзакцій у розподілених логістичних системах на основі багаторівневої системи криптографічних механізмів, що дозволило значно підвищити надійність передачі даних між учасниками, мінімізувати ризики несанкціонованої модифікації інформації та забезпечити прозорість операцій.

6. **Удосконалено** механізми контролю доступу до даних шляхом впровадження ієрархічної системи смарт-контрактів та криптографічних токенів, що розширило можливості гнучкого управління правами користувачів, підвищило адаптивність системи та забезпечило надійну ізоляцію конфіденційних даних.

7. Здійснено практичну реалізацію та експериментальну перевірку запропонованих рішень у вигляді програмного комплексу на базі технології Ethereum. Розроблено рекомендації щодо впровадження запропонованих рішень у реальних логістичних системах, що враховують особливості різних сценаріїв використання та потенційні обмеження блокчейн-технології, зокрема в аспектах швидкодії та масштабованості.

8. Практичне значення отриманих результатів полягає у створенні методологічної та технологічної основи для розробки захищених логістичних інформаційних систем нового покоління, що забезпечують високий рівень достовірності, цілісності та безпеки даних в умовах Industry 4.0. Розроблені моделі, методи та програмні рішення можуть бути використані при проектуванні та модернізації інформаційних систем у сфері логістики, управління ланцюжками постачання та інших галузях з розподіленою обробкою даних.

9. Напрямки подальших досліджень включають розробку методів оптимізації продуктивності блокчейн-систем для логістичних задач, дослідження можливостей інтеграції з іншими перспективними технологіями Industry 4.0 (IoT, штучний інтелект, великі дані), а також створення галузевих стандартів та протоколів взаємодії для забезпечення максимальної сумісності та ефективності інформаційної взаємодії в глобальних ланцюжках постачання.

Експериментальна перевірка продемонструвала суттєві переваги запропонованої блокчейн-системи над традиційними підходами. Зокрема, достовірність даних гарантується криптографічними методами на відміну від залежності від адміністратора в традиційних системах, захист від модифікації забезпечується неможливістю зміни після запису порівняно з можливою несанкціонованою зміною в централізованих системах, прозорість операцій досягається через повну автоматичну документацію замість обмеженої прозорості, а стійкість до відмов забезпечується розподіленою архітектурою без єдиної точки відмови на противагу централізованій вразливості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. M. Javaid, A. Haleem, R. Singh та R. Suman, «Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability.,» Sustainable Operations and Computers, № 3, pp. 203-217, 2022.

2. С. Бабінська, «Технологія блокчейн в аудиті: сучасний стан та перспективи застосування,» Економіка та суспільство, т. 36, 2022.

3. С. Ніколаєв та Б. Ковальов, «Блокчейн як фактор цифрової трансформації економіки України,» НДР «Сталий розвиток та ресурсна безпека: від проривних технологій до цифрової трансформації економіки України» (№ д/р 0121U100470), 2021.

4. S. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa та A. Bani-Hani, «Blockchain smart contracts: Applications, challenges, and future trends,» Peer-to-peer Networking and Applications, № 14, pp. .2901-2925., 2021.

5. H. Li, Y. Lu та W. He, «The impact of GDPR on global technology development,» Journal of Global Information Technology Management, т. 22, № 1, pp. 1-6, 2019.

6. «Закон України "Про захист персональних даних",» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

7. S. Luthra та S. Mangla, «Evaluating challenges to Industry 4.0 initiatives for supply chain sustainability in emerging economies,» Process safety and environmental protection, № 117, pp. 168-179, 2018.

8. Y. Mingchao, «Coded merkle tree: Solving data availability attacks in blockchains,» International Conference on Financial Cryptography and Data Security, № Cham: Springer International Publishing, 2020.

9. A. Damaraju, «Securing Critical Infrastructure: Advanced Strategies for Resilience and Threat Mitigation in the Digital Age,» Revista de Inteligencia Artificial en Medicina, т. 12, № 1, pp. 76-111, 2021.

10. Z. Nyikes та Z. Rajnai, «Big data, as part of the critical infrastructure,» IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY) IEEE, 2015.

11. M. Attinasi, M. Balatti та M. Mancini, «Supply chain disruptions and the effects on the global economy,» Economic Bulletin Boxes 8, 2022.

12. Y. Kostiuk, P. Skladannyi та V. Sokolov, «Models and algorithms for analyzing information risks during the security audit of personal data information system,» Cyber Hygiene & Conflict Management in Global Information Networks , т. 3925, № (2025), pp. 155-171, 2024.

13. L. Gamio та P. Goodman, «How the Supply Chain Crisis Unfolded.,» 2021. [Електронний ресурс]. – Режим доступу: https://www.nytimes.com/interactive/2021/12/05/business/economy/supply-chain.html.

14. B. MacCarthy, A. Wafaa та G. Demirel, «Mapping the supply chain: Why, what and how?,» International Journal of Production Economics, № 250, pp. 1-8, 2022.

15. B. Feng та Y. Qiwen, «Operations management of smart logistics: A literature review and future research,» Frontiers of Engineering Management, № 8, pp. 344-355, 2021.

16. Z. Bederna та T. Szádeczky, «Managing the financial impact of cybersecurity incidents,» SECURITY DEFENCE QUARTERLY, т. 41, № 1, pp. 1-21, 2023.

17. S. Duggineni, «Impact of controls on data integrity and information systems.,» Science and Technology , т. 13, № 2, pp. 29-35, 2023.

18. L. Gamio та P. Goodman, «How the Supply Chain Crisis Unfolded,» New York Times, 2021. [Електронний ресурс]. – Режим доступу: https://www.nytimes.com/interactive/2021/12/05/business/economy/supply-chain.html.

19. M. Sodhi та C. Tang, «Supply chain management for extreme conditions: Research opportunities.,» Journal of Supply Chain Management, т. 57.1, pp. 7-16.

20. R. Pozzi, T. Rossi та R. Secchi., «Industry 4.0 technologies: critical success factors for implementation and improvements in manufacturing companies,» Production Planning & Control , т. 34.2, pp. 139-158, 2023.

21. T. DEBEAUVAIS та A. VALADARES, «RESTful Client–Server Architecture: A Scalable Architecture for Massively Multiuser Online Environments,» в Computer Games and Software Engineering, Chapman and Hall/CRC, 2015.

22. V. Oliveira, F. Pessoa та M. Amorim, «SQL and NoSQL Databases in the Context of Industry 4.0.,» Machines, т. 10, № 1, p. 20, 2021.

23. S. Esser та D. Fahland, «Multi-dimensional event data in graph databases,» Data Semantics , т. 10, № 1, pp. 109-141, 2021.

24. G. Fox, «Peer-to-peer networks,» Computing in Science & Engineering, т. 3, № 3, pp. 75-77.

25. J. Jensen, V. Wachter та O. Ross, «An introduction to decentralized finance (defi),» Complex Systems Informatics and Modeling Quarterly, т. 26, pp. 46-54, 2021.

26. H. Gousia, S. Sharma та S. Ibrahim, «Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing,» Future Internet, т. 14, № 11, p. 341, 2022.

27. Yee, C.K. and Zolkipli, M.F., «Review on confidentiality, integrity and availability in information security,» Journal of ICT in Education, т. 8, № 2, pp. 34-42, 2021.

28. Craigen, D., Diakun-Thibault, N. and Purse, R., «Defining cybersecurity,» Technology innovation management review, т. 4, № 10, 2014.

29. Shree, D. and Ahlawat, S., «A Review on Cryptography, Attacks and Cyber Security,» International Journal of Advanced Research in Computer Science, т. 8, № 5, 2017.

30. Pittalia, P.P., «A comparative study of hash algorithms in cryptography,» International Journal of Computer Science and Mobile Computing, т. 8, № 6, pp. 147-152, 2019.

31. Wilkie, A. and Smith, S.S., «Blockchain: speed, efficiency, decreased costs, and technical challenges,» в The emerald handbook of blockchain for business, pp. 157-170. Emerald Publishing Limited, 2021.

32. 3GPP TS 23.501 V16.11.0 (2022-02) System architecture for the 5G System (5GS); Stage 2 (Release 17). [Електронний ресурс]. – Режим доступу: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.11.00_60/ts_123501v161100p.pdf.

33. Croman, K., Decker, C., Eyal, I., «On Scaling Decentralized Blockchains,» 3rd Workshop on Bitcoin and Blockchain Research, pp. 106-125, 2016.

34. Goswami, S., «Scalability analysis of blockchains through blockchain simulation,» Las-Vegas, 67 с., 2017.

35. Dabbagh, M., Raymond, K., Beheshti, A., «A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities,» Computers & Security, № 100, pp. 1-13, 2021.

36. Decker, C., Wattenhofer, R., «Information propagation in the Bitcoin network,» IEEE P2P 2013 Proceedings, pp. 1-10, 2013.

37. Gervais, A., Karame, G. O., Wüst, K., «On the Security and Performance of Proof of Work Blockchains,» CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 3-16, 2016.

38. Sompolinsky, Y., Zohar, A., «Secure High-Rate Transaction Processing in Bitcoin,» International Conference on Financial Cryptography and Data Security, pp. 507-527, 2015.

39. Dogecoin price | DOGE Index and Live Chart – CoinDesk [Електронний ресурс]. – Режим доступу: https://www.coindesk.com/price/dogecoin/.

40. Litecoin Explorer [Електронний ресурс]. – Режим доступу: https://chainz.cryptoid.info/ltc/#.

41. Blockchain Explorer – Search the Blockchain | BTC | ETH | BCH [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/charts.

42. Xu, X., Bandara, H., Dilum, M., Lu, Q., «A Decision Model for Choosing Patterns in Blockchain-Based Applications,» IEEE 18th International Conference on Software Architecture (ICSA), 2021.

43. K. Gholamizadeh, E. Zarei та M. Omidvar, «Fuzzy sets theory and human reliability: Review, applications, and contributions,» Linguistic methods under fuzzy information in system safety and reliability analysis, pp. 91-137, 2022.

44. J. Douceur, «The sybil attack» International workshop on peer-to-peer systems, № Heidelberg: Springer Berlin Heidelberg, pp. 251-260, 2002.

45. Н. Комлева та О. Терещенко, «Requirements for the development of smart contracts and an overview of smart contract vulnerabilities at the Solidity

code level on the Ethereum platform,» Вісник сучасних інформаційних технологій, т. 6, № 1, pp. 54-68, 2023.

46. S. Satpal, J. Sandeep та S. Dilbag, «Systematic review of security vulnerabilities in ethereum blockchain smart contract,» IEEE Access , т. 10, pp. 6605-6621, 2022.

47. R. Sytnyk та V. Hnatushenko, «Method for ensuring the reliability and integrity of personal data processed in a blockchain system,» Системні технології, т. 3, № 158, pp. 28-35, 2025.

48. N. Ogbuke, Y. Yusuf, D. K та B. Mercangoz, «Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society,» Production Planning & Control, т. 33, № 2-3, pp. 123-137, 2022.

49. S. Nakamoto, «Bitcoin whitepaper,» 2008. [Електронний ресурс]. – Режим доступу: https://bitcoin.org/bitcoin.pdf.

50. M. Mathisen, «The application of blockchain technology in Norwegian fish supply chains-a case study,» Master's thesis, NTNU, 2018.

51. F. Tian, «An agri-food supply chain traceability system for China based on RFID & blockchain technology.,» 13th international conference on service systems and service management (ICSSSM). IEEE, 2016.

52. P. Ray, «Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions,» Internet of Things and Cyber-Physical Systems, т. 3, pp. 213-248, 2023.

53. R. Soltani, M. Zaman, R. Joshi та S. Sampalli, «Distributed ledger technologies and their applications: A review.,» Applied Sciences, т. 12, № 15, 2022.

54. R. Sytnyk та V. Hnatushenko, «STUDY OF CONSENSUS ALGORITHMS IN BLOCKCHAIN NETWORKS IN THE DESIGN OF INFORMATION SYSTEMS,» Міжнародна науково-технічна конференція

Інформаційні технології в металургії та машинобудуванні, pp. 479-484, 2024.

55. E. Kapengut та B. Mizrach, «An event study of the ethereum transition to proof-of-stake,» Commodities, т. 2, № 2, pp. 96-110.

56. R. Sytnyk та V. Hnatushenko, «Management of data flows in modern industry using blockchain,» System technologies, т. 4, № 147, pp. 123-131, 2023.

57. S. Aggarwal та N. Kumar, «Digital signatures,» Advances in Computers, т. 121, № Elsevier, pp. 95-107, 2021.

58. K. John, B. Monnot, P. Mueller та F. Saleh, «Economics of ethereum,» Journal of Corporate Finance, т. 91, 2024.

59. R. Sytnyk, V. V. Hnatushenko та V. V. Hnatushenko., «Decentralized Information System for Supply Chain Management Using Blockchain,» CEUR-WS, 2022.

60. R. Sytnyk та H. Viktoriia, «CHALLENGES AND SOLUTIONS FOR SCALING DATA FLOWS IN THE INDUSTRY 4.0 ECOSYSTEM IN INDUSTRY AND BUSINESS» Міжнародна науково-технічна конференція Інформаційні технології в металургії та машинобудуванні, 2023.

61. Ситник Р.С., Гнатушенко Вік.В. МОДЕЛЬ ВИЯВЛЕННЯ АКТУАЛЬНИХ ЗАГРОЗ ПОРУШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ В БЛОКЧЕЙН-СИСТЕМІ. - № 1 (2025): Information Technology: Computer Science, Software Engineering and Cyber Security. Information Technology: Computer Science, Software Engineering and Cyber Security 1 (2025). – С. 42-47. DOI: 10.32782/IT/2025-1-6

62. Ситник Р.С., Гнатушенко Вік.В. Система багаторівневої верифікації персональних даних у блокчейн-середовищі // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ITMM'2025)». – Дніпро, 2025. – С. 620-624. DOI: 10.34185/1991-7848.itmm.2025.01.111

63. Ситник Р.С., Гнатушенко Вік.В. Data flow management in information systems using blockchain technology // Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. – 2024. – № 3. – P. 142-148. URL: http://nvngu.in.ua/index.php/en/archive/on-the-issues/1909-2024/content-3-2024/6926-142

64. Ситник Р.С., Гнатушенко Вік.В. Проектування та дослідження системи моніторингу руху товарів та ресурсів з застосуванням блокчейну (The Design and Research of a System for Monitoring the Movements of Goods and Resources Using Blockchain) // Системні технології. Регіональний міжвузівський збірник наукових праць. – Випуск 6 (137). – Дніпро, 2021. – С. 123-131. DOI: 10.34185/1562-9945-6-137-2021-15

65. Ситник Р.С., Гнатушенко Вік.В. Забезпечення безпеки доступу до хмарних обчислень за допомогою блокчейн технології // Матеріали XII Міжнародної науково-технічної конференції ITSec-2023 «Безпека інформаційних технологій». – Ужгород, 2-4 травня 2023. – С. 1-3.

66. Ситник Р.С., Гнатушенко Вік.В. Аналіз обміну даними між підприємствами за допомогою технології блокчейн в інформаційних системах // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ITMM'2022)». – Дніпро, 2022. – С. 275-279. DOI: 10.34185/1991-7848.itmm.2022.01.049

67. Ситник Р.С., Гнатушенко Вік.В. Інтероперабельність технологій блокчейну для промисловості та фінансів // Матеріали VIII Міжнародної науково-технічної конференції «Комп'ютерне моделювання та оптимізація складних систем» (КМОСС-2023). – Дніпро, 1-3 листопада 2023. – С. 209-211.

68. Ситник Р.С., Гнатушенко Вік.В. Проектування логістичної інформаційної системи за допомогою блокчейну // Матеріали конференції

«Молода академія-2022». – Дніпро: Український Державний Університет Науки і Технологій, 2022. – С. 1-2.

Додаток А

Список публікацій здобувача

1. **Sytnyk** R., Hnatushenko Viktoriia, Hnatushenko Volodymyr. Prototyping Fully Decentralized Supply Chain Management Information System Using Blockchain // The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2022). – Khmelnytskyi, Ukraine, March 23-25, 2022. – P. 1-4. URL: http://ceur-ws.org/Vol-3156/

2. **Ситник** Р.С., Гнатушенко Вік.В. МОДЕЛЬ ВИЯВЛЕННЯ АКТУАЛЬНИХ ЗАГРОЗ ПОРУШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ В БЛОКЧЕЙН-СИСТЕМІ. - № 1 (2025): Information Technology: Computer Science, Software Engineering and Cyber Security. Information Technology: Computer Science, Software Engineering and Cyber Security 1 (2025). – С. 42-47. DOI: 10.32782/IT/2025-1-6

3. **Ситник** Р.С., Гнатушенко Вік.В. Проектування та дослідження системи моніторингу руху товарів та ресурсів з застосуванням блокчейну (The Design and Research of a System for Monitoring the Movements of Goods and Resources Using Blockchain) // Системні технології. Регіональний міжвузівський збірник наукових праць. – Випуск 6 (137). – Дніпро, 2021. – С. 123-131. DOI: 10.34185/1562-9945-6-137-2021-15

4. **Ситник** Р.С., Гнатушенко Вік.В. Метод забезпечення достовірності та цілісності персональних даних, що обробляються в блокчейн-системі // Системні технології. Регіональний міжвузівський збірник наукових праць. – Випуск 3 (158). – Дніпро, 2025. – С. 28-35. DOI: 10.34185/1562-9945-3-158-2025-04

5. **Ситник** Р.С., Гнатушенко Вік.В. Management of data flows in modern industry using blockchain // System technologies. – 2023. – Vol. 4 No. 147. – P. 123-131. DOI: 10.34185/1562-9945-4-147-2023-11

6. **Ситник** Р.С., Гнатушенко Вік.В. Data flow management in information systems using blockchain technology // Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. – 2024. – № 3. – P. 142-148. URL: http://nvngu.in.ua/index.php/en/archive/on-the-issues/1909-2024/content-3-2024/6926-142

7. **Ситник** Р.С., Гнатушенко Вік.В. Аналіз обміну даними між підприємствами за допомогою технології блокчейн в інформаційних системах // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ІТММ'2022)». – Дніпро, 2022. – С. 275-279. DOI: 10.34185/1991-7848.itmm.2022.01.049

8. **Ситник** Р.С., Гнатушенко Вік.В. Проблеми та рішення масштабування потоків даних у екосистемі «Індустрії 4.0» в промисловості та бізнесі // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ІТММ'2023)». – Дніпро, 2023. – С. 370-374. DOI: 10.34185/1991-7848.itmm.2023.01.098

9. **Ситник** Р.С., Гнатушенко Вік.В. Забезпечення безпеки доступу до хмарних обчислень за допомогою блокчейн технології // Матеріали XII Міжнародної науково-технічної конференції ITSec-2023 «Безпека інформаційних технологій». – Ужгород, 2-4 травня 2023. – С. 1-3.

10. **Ситник** Р.С., Гнатушенко Вік.В. Інтероперабельність технологій блокчейну для промисловості та фінансів // Матеріали VIII Міжнародної науково-технічної конференції «Комп'ютерне моделювання та оптимізація складних систем» (КМОСС-2023). – Дніпро, 1-3 листопада 2023. – С. 209-211.

11. **Ситник** Р.С., Гнатушенко Вік.В. Дослідження алгоритмів консенсусу у мережах блокчейну при проектуванні інформаційних систем // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ITMM'2024)». – Дніпро, 10-11 квітня 2024. – С. 479-484.

12. **Ситник** Р.С., Гнатушенко Вік.В. Система багаторівневої верифікації персональних даних у блокчейн-середовищі // Матеріали науково-технічної конференції «Інформаційні технології в металургії та машинобудуванні (ITMM'2025)». – Дніпро, 2025. – С. 620-624. DOI: 10.34185/1991-7848.itmm.2025.01.111

13. **Ситник** Р.С., Гнатушенко Вік.В. Проектування логістичної інформаційної системи за допомогою блокчейну // Матеріали конференції «Молода академія-2022». – Дніпро: Український Державний Університет Науки і Технологій, 2022. – С. 1-2.

Додаток Б

Документи щодо впровадження результатів досліджень

АКТ

про впровадження результатів дисертаційного дослідження

Ситника Романа Сергійовича у систему управління документообігом JDG " ULADZISLAU YANOUSKI" Software Solutions

Директор фірми ULADZISLAU YANOUSKI" Software Solutions (NIP PL8952264762), Яновський Владислав, складає цей Акт про те, що у період з 01.2025 по 09.2025 року впроваджено систему відстеження фактур на основі результатів дисертаційної роботи Ситника Романа Сергійовича.

ВПРОВАДЖЕНА СИСТЕМА:

1. Модуль реєстрації фактур у блокчейн-реєстрі:

- Автоматична реєстрація всіх вхідних та вихідних фактур
- Створення незмінного запису з хеш-підписом документа
- Присвоєння унікального блокчейн-ідентифікатора кожній фактурі

2. Модуль верифікації та валідації:

- Автоматична перевірка цілісності документів при кожному зверненні
- Виявлення спроб несанкціонованих змін
- Валідація реквізитів контрагентів через блокчейн-реєстр

БЕЗПЕКА ТА НАДІЙНІСТЬ:

- Захист від втрати даних: 100% гарантія збереження через розподілений реєстр
- Захист від підробки: Криптографічний захист унеможливлює підробку документів
- Audit trail: Повний слід аудиту для всіх операцій

ВИСНОВОК:

Впровадження системи відстеження фактур на основі блокчейн-технології забезпечило повну цифровізацію документообігу з фактурами, підвищення безпеки та захист від втрати документів, відповідність вимогам сучасного документообігу

Система рекомендується для використання у компанії і надалі.

Владислав Яновський 24.09.2025

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ

«15» вересень 2025

ДОВІДКА

про впровадження результатів дослідження на здобуття наукового ступеня доктора філософії за спеціальністю 122 Комп'ютерні науки

Запропоновані в дисертаційній роботі «Моделі і методи організації та забезпечення цілісності даних у реєстрах інформаційних систем» **Ситника Романа Сергійовича** модель оцінки загроз безпеці в логістичних інформаційних системах, яка враховує специфіку блокчейн-архітектури та базується на комплексному аналізі вразливостей, та метод забезпечення достовірності даних, що ґрунтується на удосконалених деревах Меркла та інтелектуальних смарт-контрактах, надають можливість впроваджувати новітні теоретичні знання та практичні навички фахівцям у галузі комп'ютерних наук забезпечення цілісності даних в системах різного призначення. У тому числі для вдосконалення єдиної інтегрованої стійкої до відмов системи підтримки процесу відновлення телекомунікаційних об'єктів, яка може бути застосована на території України.

Запропоновані в роботі моделі та методи організації та забезпечення цілісності даних у інформаційних системах впроваджені в курс «Технології захисту інформації» для бакалаврів спеціальності 121 Інженерія програмного ОП «Інженерія програмного забезпечення в індустрії» та «Методології та технології розробки інформаційних систем» для магістрів спеціальності 122 – Комп'ютерні науки ОП «Комп'ютерні науки і технології» кафедри інформаційних технологій і систем ДМетІ УДУНТ у 2023-2025 н.р.

Міністерство освіти і науки України
Український державний університет науки і технологій
ЄДРПОУ 44165850

Проректор
з наукової роботи УДУНТ,
д.т.н., професор Юрій ПРОЙДАК