

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет
імені Петра Могили
Факультет комп'ютерних наук
Кафедра інтелектуальних інформаційних систем

ДОПУЩЕНО ДО ЗАХИСТУ

Завідувач кафедри інтелектуальних
інформаційних систем, д.т.н., проф.,

_____ Ю.П.Кондратенко

« ____ » _____ 2022 року

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

СИСТЕМА УПРАВЛІННЯ ЛОГІСТИЧНОЮ
ДІЯЛЬНІСТЮ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN

Спеціальність 124 «Системний аналіз»

124 – МКР – 607.21830802

Студент _____ Т. Ю. Д'яченко

« ____ » лютого 2022 р.

Консультант _____ Н. М. Болубаш

канд. пед. наук, доцент

« ____ » лютого 2022 р.

Миколаїв – 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет ім. Петра Могили
Факультет комп'ютерних наук
Кафедра інтелектуальних інформаційних систем

Освітньо-кваліфікаційний рівень магістр

Галузь знань 12 «Інформаційні технології»
(шифр і назва)

Спеціальність 124 «Системний аналіз»
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри інтелектуальних
інформаційних систем, д-р техн. наук, проф.

_____ Ю. П. Кондратенко

«__» _____ 20__ р.

ЗАВДАННЯ

на магістерську кваліфікаційну роботу

Д'яченко Тимуру Юрійовичу

1. Тема магістерської кваліфікаційної роботи «Система управління логістичною діяльністю на основі технології Blockchain».

Керівник роботи Болюбаш Надія Миколаївна, к. пед. наук, доцент.

Затв. наказом Ректора ЧНУ ім. Петра Могили від «__» ____ 20__ р. № _____

2. Строк подання студентом роботи ____ _____ 20__ р.

3. Вхідні (початкові) дані до роботи: загальні відомості про логістичну діяльність та управління нею.

Очікуваний результат роботи: система управління логістичною діяльністю, де передбачено використання технології Blockchain, яка забезпечує накрізний надійний та безпечний моніторинг фінансових та інформаційних потоків між усіма учасниками ланцюга поставок.

4. Перелік питань, що підлягають розробці (зміст пояснювальної записки):

КАЛЕНДАРНИЙ ПЛАН
виконання магістерської кваліфікаційної роботи

Тема: «Система управління логістичною діяльністю на основі технології Blockchain»

№	Найменування роботи	Початок	Закінченн я	Примітк и
1.	Отримання завдання на магістерську наукову роботу	18.10.2021	01.11.2021	Виконано
2.	Огляд літератури за темою роботи	01.11.2021	22.11.2021	Виконано
3.	Аналіз існуючих мережевих сервісів у сфері транспортно-логістичних бізнес-процесів	22.11.2021	26.11.2021	Виконано
4.	Аналіз предметної області та основних складових технології Blockchain	01.12.2021	13.12.2021	Виконано
5.	Робота над першим та другим розділом пояснювальної записки	14.12.2021	27.12.2021	Виконано
6.	Створення дизайну, проектування та програмна реалізація системи	28.12.2021	04.01.2022	Виконано
7.	Робота над третім розділом пояснювальної записки	04.01.2022	14.01.2022	Виконано
8.	Тестування системи	18.01.2022	24.01.2022	Виконано
9.	Розробка методичної частини	24.01.2022	25.01.2022	Виконано
10.	Розробка спеціальної частини з охорони праці	25.01.2022	01.02.2022	Виконано
11.	Створення слайдів для захисту та написання доповіді	01.02.2022	15.02.2022	Виконано
12.	Обговорення отриманих результатів з керівником та попередній захист магістерської роботи	28.01.2022	31.01.2022	Виконано
13.	Корегування роботи за результатами попереднього захисту	01.02.2022	15.02.2022	Виконано
14.	Остаточне оформлення пояснювальної записки та слайдів	16.02.2022		Виконано
15.	Захист магістерської роботи	24.02.2022		Виконано

Розробив студент Д'яченко Т.Ю.

(прізвище та ініціали)

(підпис)

Керівник роботи к.пед.н., доц. Болюбаш Н.М.

(наук. ступінь, вчене звання, прізвище та ініціали)

(підпис)

«_____» _____ 202__p.

АНОТАЦІЯ
до магістерської кваліфікаційної роботи роботи

Тема: «Система управління логістичною діяльністю на основі технології
Blockchain»

Студент: Д'яченко Тимур Юрійович

Керівник: к.пед.н доцент Болюбаш Надія Миколаївна

Магістерська кваліфікаційна робота присвячена проектуванню, розробці та здійсненню програмної реалізації інформаційної системи управління логістичною діяльністю на основі технології Blockchain.

Об'єкт дослідження – транспортно-логістичні бізнес-процеси.

Предмет дослідження – програмні засоби управління логістичною діяльністю з використанням технології Blockchain.

Мета дослідження – підвищення ефективності забезпечення прозорості та безпеки товароруху у наскрізному моніторингу фінансових та інформаційних потоків шляхом створення системи управління логістичною діяльністю на основі технології Blockchain.

Дипломна робота складається з фахового розділу, методичної і спеціальної частини з охорони праці. Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, висновків та додатку.

У першому розділі розкрито теоретичні засади управління транспортно-логістичними бізнес-процесами та розглянути іноваційні підходи до автоматизації процесів у сфері логістики. У другому розділі розкрито сутність технології Blockchain та досліджено основні методи захисту даних і алгоритми досягнення консенсусу. У третьому розділі обґрунтовано вибір технологій і засобів розробки, описано проектування та програмну реалізацію системи управління логістичною діяльністю з використанням технології Blockchain.

У спеціальній частині з охорони праці розглядаються питання аналізу заходів щодо умов праці та протипожежної безпеки.

Дипломна робота містить ___ сторінку (без додатків), ___ рисунків, ___ таблиці, ___ джерел, ___ додаток.

ABSTRACT

for master's scientific work

Subject: “Logistics management system based on Blockchain technology”

Student D'yachenko Timur Yuriyovich

Leader: Ph.D., associate professor Bolyubash Nadiya Mikolaivna

Master's thesis is devoted to the design, development and implementation of software implementation of logistics management information system based on Blockchain technology.

Object of research – transportno-lohistychni biznes-protsesy.

Subject of research – logistics management software using Blockchain technology.

The purpose of the study is to increase the efficiency of ensuring transparency and security of goods movement in the end-to-end monitoring of financial and information flows by creating a logistics management system based on Blockchain technology.

Thesis consists of a professional section, methodical and special part on labor protection. The explanatory note of the thesis consists of an introduction, three sections, conclusions and an appendix.

The first section reveals the theoretical foundations of transport and logistics business processes management and considers innovative approaches to automation of processes in the field of logistics. The second section reveals the essence of Blockchain technology and explores the basic methods of data protection and algorithms for reaching consensus. The third section substantiates the choice of technologies and development tools, describes the design and software implementation of logistics management system using Blockchain technology. The special part of analysis of measures on working conditions and fire safety.

Thesis contains ___ page (without appendices), ___ figures, ___ tables, ___ sources, ___

Пояснювальна записка

до магістерської кваліфікаційної роботи

на тему:

«СИСТЕМА УПРАВЛІННЯ ЛОГІСТИЧНОЮ ДІЯЛЬНІСТЮ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN»

Спеціальність 124 «Системний аналіз»

124 – МКР – 607.21830802

Студент _____ Д'яченко Т.Ю.
«__» _____ 20__ р.

Консультант _____ Болюбаш Н.М.
к.пед.наук, доцент
«__» _____ 20__ р.

Кафедра інтелектуальних інформаційних систем
Система управління логістичною діяльністю на основі технології Blockchain

м. Миколаїв – 2022

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ	3
ВСТУП	4
РОЗДІЛ 1. ТЕОРЕТИЧНІ УПРАВЛІННЯ ТРАНСПОРТНО-ЛОГІСТИЧНИМИ БІЗНЕС-ПРОЦЕСАМИ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ BLOCKCHAIN	7
1.1. Основи управління транспортно-логістичними бізнес-процесами	7
1.2. Сучасні підходи до автоматизації управління логістичною діяльністю	12
1.3. Стан та перспективи розвитку логістичної галузі в Україні	22
1.4. Постановка задачі дослідження	25
Висновок до розділу 1	26
РОЗДІЛ 2. ТЕХНОЛОГІЯ BLOCKCHAIN: СУТНІСТЬ ТА ОСНОВНІ МЕТОДИ ЗАХИСТУ ДАНИХ І АЛГОРИТМИ ДОСЯГНЕННЯ КОНСЕНСУСУ	28
2.1. Основні складові технології Blockchain	28
2.2. Алгоритми консенсусу	35
Висновок до розділу 2	38
РОЗДІЛ 3. РОЗРОБКА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ЛОГІСТИЧНОЮ ДІЯЛЬНІСТЮ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN	40
3.1. Hyperledger Composer: середовище розробки та набір інструментів для оптимізації розгортання системи блокчейн Hyperledger Composer	40
3.2. Опис програмної реалізації	46
3.3. Інтерфейс застосунку	50
Висновок до розділу 3	54
РОЗДІЛ 4. МЕТОДИЧНА ЧАСТИНА	57
РОЗДІЛ 5. СПЕЦІАЛЬНА ЧАСТИНА З ОХОРОНИ ПРАЦІ	76
ВИСНОВКИ	87
СПИСОК ПОСИЛАНЬ	91

ДОДАТОК А Лістинг програмного коду 95

ПЕРЕЛІК СКОРОЧЕНЬ

БП – бізнес-процес

PoW – алгоритм консенсусу Proof-of-Work

PoS – алгоритм консенсусу Proof-of-Stake

PoA – алгоритм консенсусу Proof-of-Authority

ІТС – інтелектуальна транспортна система

ТЗ – транспортний засіб

DLT – технологія розподіленого реєстру (distributed ledger technology)

ІоТ – інтернет речей (Internet of Things)

ПЗ – програмне забезпечення

ВСТУП

Актуальність. В умовах глобалізації сучасного суспільства ланцюги поставок продукції, пов'язані з її виробництвом та доставкою до кінцевого споживача, містять велику кількість об'єктів, які можуть бути розміщені у різних країнах світу. Відстеження та контролювання поставки продукції потребує прозорого моніторингу великої кількості різних операцій усієї мережі роздрібних торговців, дистриб'юторів, транспортників, складських приміщень та інших постачальників. Застосування технології блокчейн у логістиці дозволяє підвищити ефективність товароруку між усіма учасниками ланцюга поставок.

Оптимізація та підвищення ефективності управління логістичними каналами є актуальною задачею, яка розв'язується з використанням сучасних інформаційних технологій. Однак технологія блокчейн у науковій літературі представлена недостатньо широко. Серед програмних рішень, що реалізують технологію блокчейн, існує два ключових напрямки застосування блокчейн – фінансові технології й Інтернет речей. На ринку існує значне число блокчейн-платформ, які розрізняються застосовуваними протоколами шифрування, алгоритмами консенсусу, функціональними можливостями [2]. Серед блокчейн-платформ, які використовують у сфері логістики, було виявлено Ethereum, Ripple, Hyperledger Sawtooth, Hyperledger Fabric, IBM Blockchain Platform, Microsoft Azure Blockchain Platform, Quorum.

Незважаючи на великий потенціал, кількість компаній, які впровадили й адаптували блокчейн під свої потреби в сфері логістики, є невеликою. Тому є потреба у створенні системи управління логістичною діяльністю, яка підвищує ефективність забезпечення прозорості та безпеки товароруку у наскрізному моніторингу фінансових та інформаційних потоків між учасниками ланцюга поставок.

Мета дослідження – підвищення ефективності забезпечення прозорості та безпеки товароруку у наскрізному моніторингу фінансових та інформаційних потоків шляхом створення системи управління логістичною діяльністю на основі технології Blockchain.

Досягнення поставленої мети обумовлює необхідність вирішення наступних **завдань**:

1. Здійснити аналіз теоретичних засад управління транспортно-логістичними бізнес-процесами та розглянути інноваційні підходи до автоматизації процесів у сфері логістики.
2. Розкрити сутність технології Blockchain та дослідити основні методи захисту даних і алгоритми досягнення консенсусу.
3. Обґрунтувати вибір інструментальних засобів розробки та здійснити проектування і програмну реалізацію системи управління логістичною діяльністю на основі технології Blockchain.

Об'єктом дослідження є транспортно-логістичні бізнес-процеси.

Предметом дослідження є програмні засоби управління логістичною діяльністю з використанням технології Blockchain.

Методологічною основою дослідження є загальнонаукові аналітичні методи та методи шифрування і консенсусу Blockchain-технології, які дозволили вивчити предмет та об'єкт дослідження, дослідити розвиток теоретичних та практичних засад, напрямів та шляхів підвищення ефективності роботи транспортно-логістичні бізнес-процеси, яка підвищує ефективності забезпечення прозорості та безпеки товароруку у наскрізному моніторингу фінансових та інформаційних логістичних потоків.

Результати дослідження обговорювалися Всеукраїнській науково-практичній конференції молодих вчених, аспірантів і студентів «Інтелектуальні інформаційні системи» та отримали схвалення.

Наукова новизна одержаних результатів дослідження полягає у тому, що автором: запропоновано та обґрунтовано напрями вдосконалення використання технології Blockchain у сфері логістики; одержали подальший розвиток підходи до вибору алгоритму консенсусу для забезпечення логістичної діяльності; узагальнено теоретичні засади створення інформаційних систем управління логістичною діяльністю.

Практичне значення отриманих результатів полягає в тому, що сформульовані теоретичні положення та практичні рекомендації щодо підвищення ефективності транспортно-логістичних бізнес-процесів можна застосувати для управління логістичною діяльністю шляхом впровадження розробленої системи.

Структура магістерської роботи. Відповідно до мети, завдань і предмета дослідження, магістерська робота містить основну, методичну та спеціальну частини. Основна частина магістерської роботи складається із вступу, трьох розділів, висновку, списку використаних джерел та __ додатків. Загальний обсяг магістерської роботи – __ сторінок, із них основного тексту основної частини – __ сторінок, методичної частини – __ сторінок, спеціальної – __ сторінок. Кількість використаних джерел – __.

РОЗДІЛ 1. ТЕОРЕТИЧНІ УПРАВЛІННЯ ТРАНСПОРТНО-ЛОГІСТИЧНИМИ БІЗНЕС-ПРОЦЕСАМИ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ BLOCKCHAIN

1.1. Основи управління транспортно-логістичними бізнес-процесами

Бізнес-середовище постійно зазнає змін під впливом тих чи інших економічних факторів, а потреби бізнесу змінюються, стають більш складними та багатосторонніми. Для того, щоб ефективно працювати та розвиватися компаніям необхідно використовувати сучасні інструменти ведення бізнесу. Одними із них є саме логістичні методи та інструменти, розумне застосування технологій логістики, виконання її функцій, реалізація основних завдань. IBM, General Motors, Ford Motors, Johnson & Johnson, Proctor & Gamble – перші компанії світового масштабу, які почали застосовувати логістичний підхід ведення бізнесу [1]. Оптимізація логістичної системи підприємства дозволяє правильно організувати роботу в цілому, зменшити суму загальних витрат, підвищити прибуток та конкурентоздатність.

В основі діяльності компанії лежать її бізнес-процеси (БП), які в свою чергу залежать від цілей і завдань. Завдяки ним відбувається реалізація всіх видів діяльності компанії, які пов'язані з виробництвом товарів чи послуг. Кожна робота має своє місце в послідовності виконання, часові рамки та інші вимоги. Бізнес-процеси є складовими однієї робочої системи, чітке їх виконання, аналіз та контроль забезпечують ефективне функціонування підприємства. Бізнес-процес (англ. Business Process) – будь-яка діяльність, що має вхідний продукт, додає вартість до нього, та забезпечує вихідний продукт для внутрішнього або зовнішнього споживача [2]. Основні логістичні бізнес-процеси транспортного підприємства зображено на рисунку 1.1 [3].

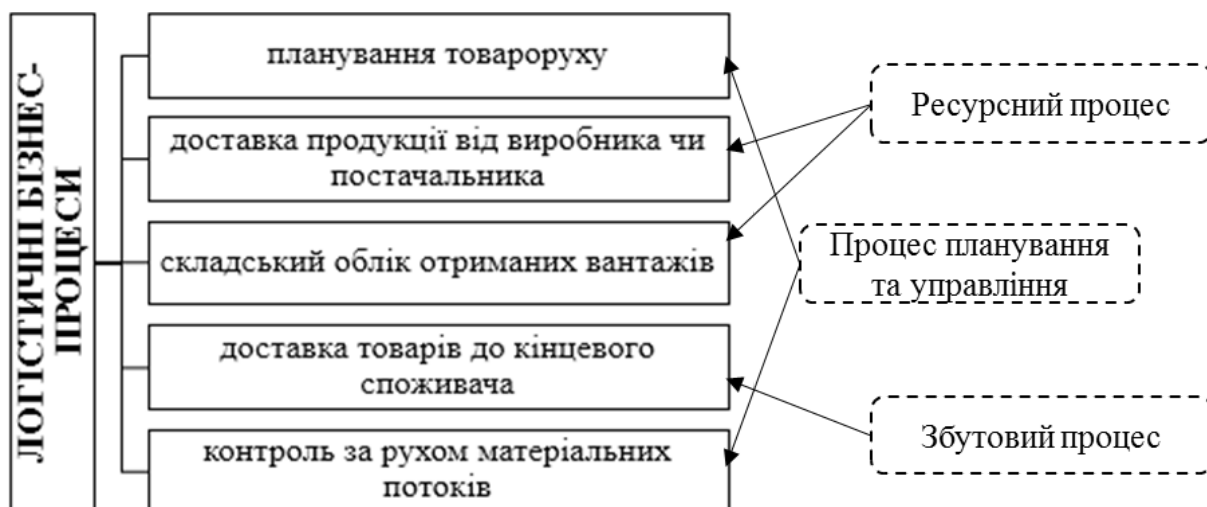


Рис. 1.1. Перелік логістичних бізнес-процесів підприємства

Бізнес-процеси відносяться до категорії керованих, як потенційні об'єкти адміністрування вони піддаються проектуванню на основі вжиття обмежувальної, керівної і описової інформації - за загальними правилами. На реальній практиці проектування БП дезагрегуються на операції і дії, при цьому кожний елемент структури в міру відповідності інформаційним регламентам при включенні його в бізнес-процес для досягнення кінцевого цільового результату знаходить характеристики, існування для організації та оцінки ефективності бізнесу: споживані запаси (витрати), використаний час, продуктивність, якість виконання, ризику [4]. Транспортно-логістичні БП мають діяти у добре побудованій системі. Складові елементи транспортно-логістичної системи (ТЛС) мають: мету, суб'єкт, об'єкт та процес управління, функції, устаткування та інструменти, логістичні операції. Схематично ТЛС зображена на рис. 2 [5]. На вході в ТЛС стоять праця, предмети та засоби праці, необхідні для роботи системи, на виході маємо соціально-економічний результат.

Логістичний бізнес-процес – це взаємопов'язаний комплекс операцій і функцій, які переводять запаси підприємства (при управлінні товарними і

супутніми потоками) у результат, що задається логістичною стратегією фірми, це процеси, які зосереджені на плануванні руху матеріалів, закупівлі, виробництві і поставці товарів споживачам.

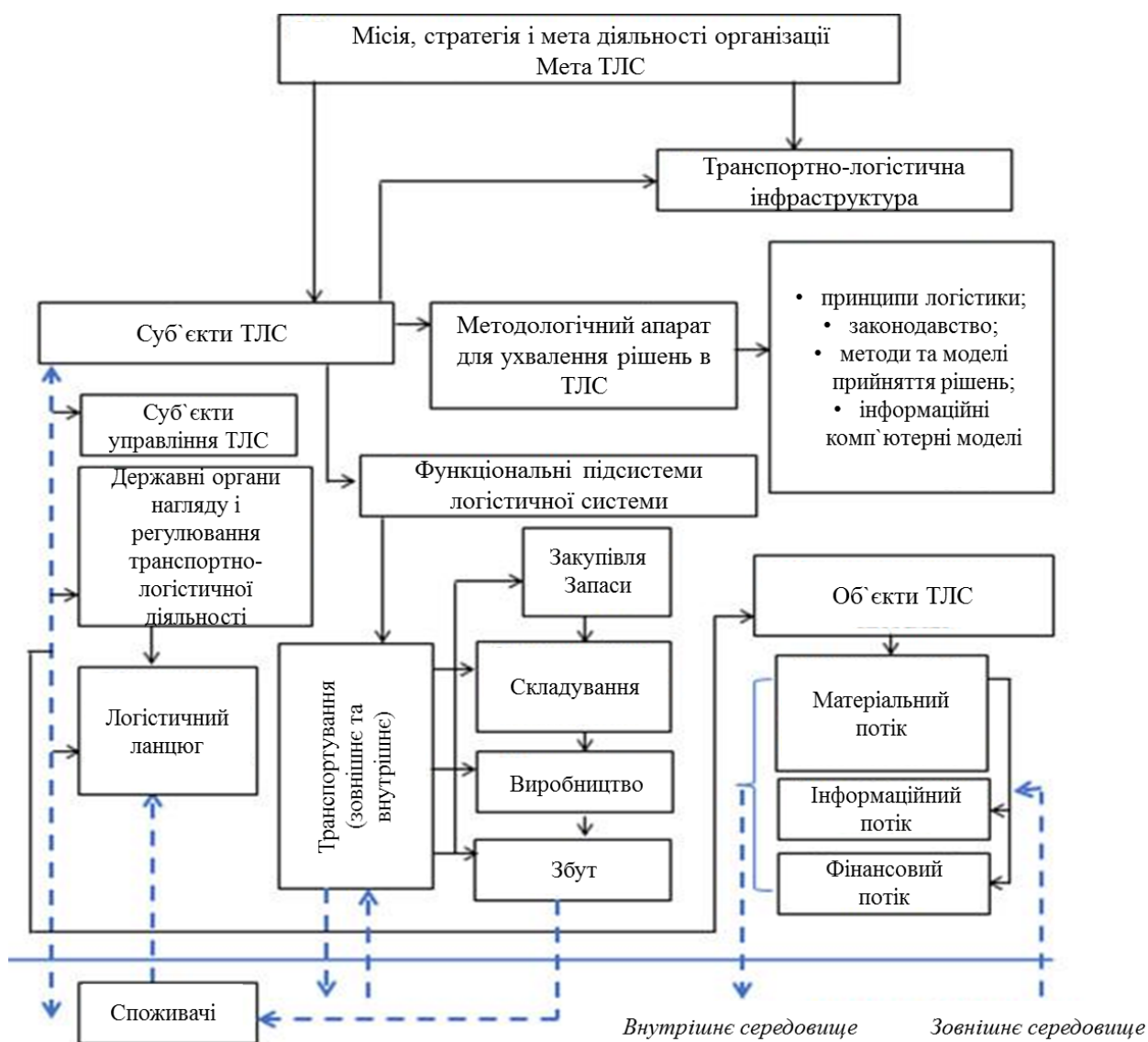


Рис. 1.2. Побудова транспортно-логістичної системи

Не зважаючи на те, що об'єктом логістичного управління є потоки, то потокові процеси, будь-які процеси, що пов'язані з переміщенням будь-чого, керівництво логістичними бізнес-процесами підприємства можливо визначити як інтегроване врядування бізнес-процесами з просування продукції і супутніх потоків від місця їх зародження до кінцевого споживача з метою максимальної

ефективності діяльності підприємства [6]. Всі бізнес процеси можемо розділити на дві групи – основні та допоміжні, до яких належать обслуговуючі, управлінські та БП розвитку (рис. 3) [4].

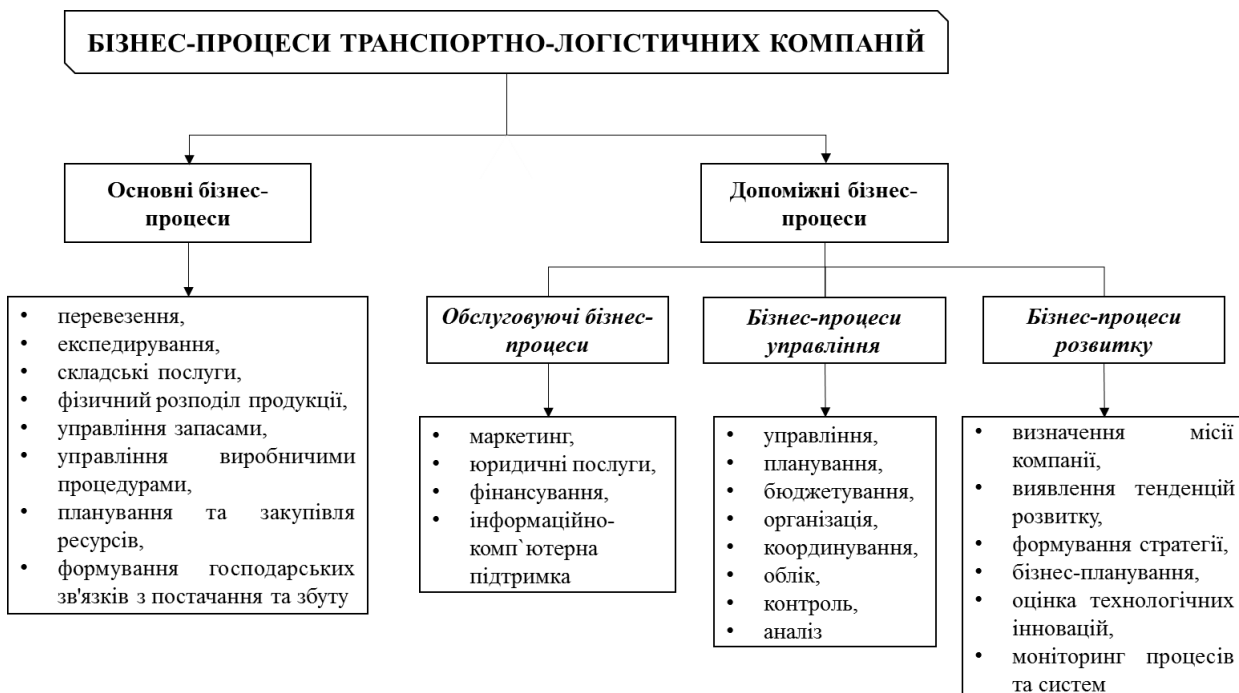


Рис. 1.3. Розподіл бізнес-процесів транспортно-логістичних компаній

Покрокове вивчення бізнес-процесів транспортно-логістичного підприємства із визначенням завдань кожного процесу відображено на рис. Вся майбутня БП впливає із попереднього, бере з нього вихідні дані, оперує ними та передає на другий етап. Якраз важливо чітко побудувати логістичну систему, ефективно нею керувати, удосконалювати. Напрямами поліпшення та розвитку логістичних бізнес- процесів і систем можуть бути такі [4]:

- ✓ удосконалення управління взаємозв'язків зі споживачами завдяки більш швидкому та точному встановленню їхніх потреб;
- ✓ розвиток управління обслуговування споживачів шляхом уточнення специфікації показників функціонування;

- ✓ удосконалення управління попитом через зміну методів планування, зокрема із використанням інформаційних технологій (ІТ);

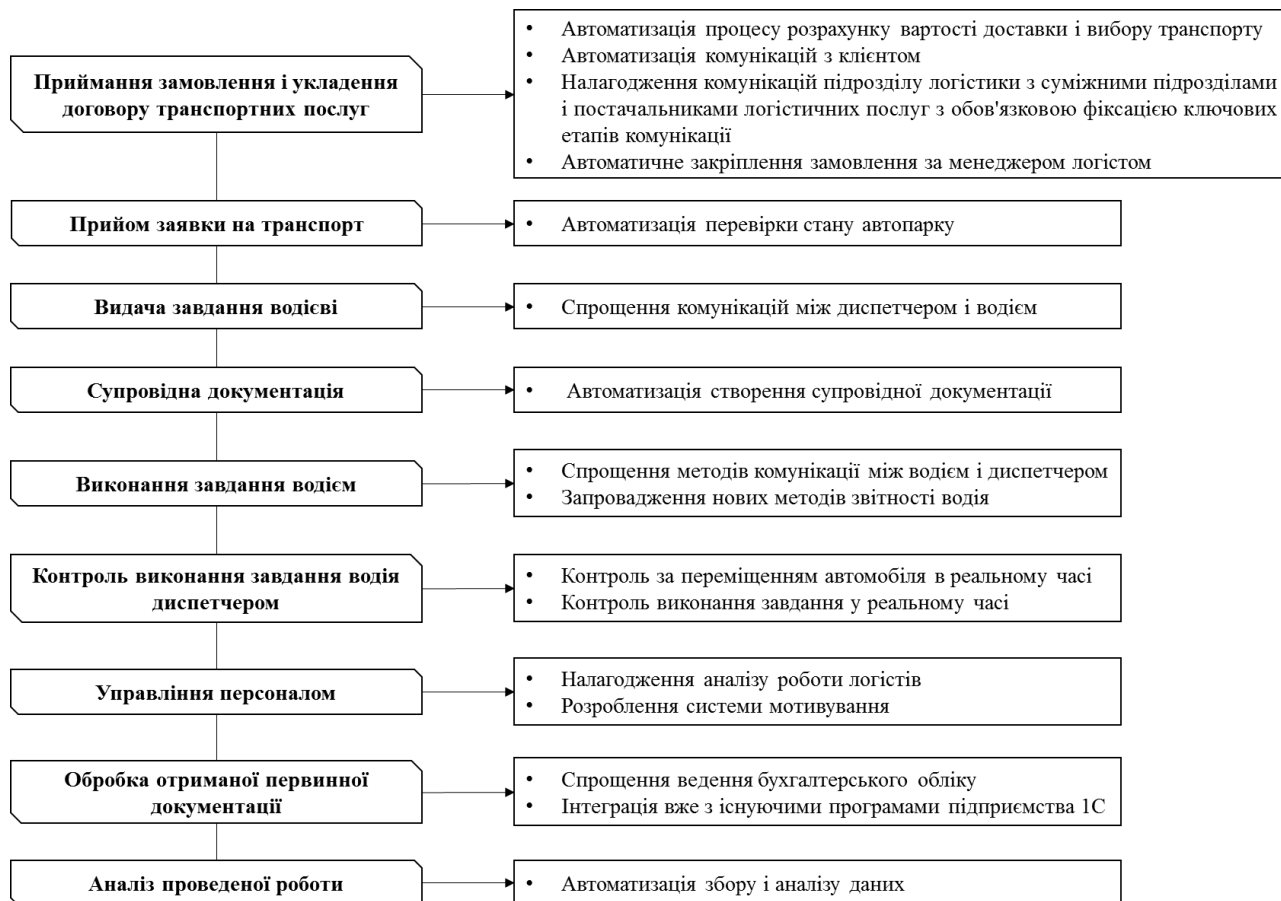


Рис. 1.4. Поетапний аналіз логістичних бізнес-процесів підприємства із визначенням завдань [7]

- ✓ істотне поліпшення виконання замовлень завдяки більш ефективному управлінню дистрибуцією;
- ✓ розвиток управління виробничим потоком через визначення сучасних критеріїв для встановлення пріоритетів;
- ✓ удосконалення системи матеріально-технічного забезпечення (МТЗ) завдяки ІТ-регулюванню вхідного потоку;

- ✓ розроблення і доведення продукції до комерційного використання через вимог до переміщення продукції.

Реалізація нових методів управління в діяльності транспортно-логістичної компанії, заснованих на залученні і використанні сучасних інформаційних систем і технологій має дозволити:

- ✓ визначити оптимальну послідовність виконуваних функцій, яка спричинить скорочення тривалості циклу транспортування вантажу і його експедиційного супроводу, що, сприяє підвищенню оборотності капіталу та зростання всіх фінансово-економічних показників господарської діяльності транспортно-логістичної компанії;
- ✓ оптимізувати використання всіх видів ресурсів у різних бізнес-процесах, що дозволяє знизити витрати і забезпечити оптимальне поєднання різних видів робіт;
- ✓ побудувати адаптивні бізнес-процеси, націлені на швидке реагування на зміну потреб реальних і потенційних клієнтів та партнерів, логістичних та інформаційних технологій, поведінки конкурентів і поліпшення якості обслуговування споживачів в умовах підвищеної динамічності зовнішнього середовища;
- ✓ здійснити синхронізацію, координацію та інтеграцію одночасно виконуваних бізнес-процесів.

Таким чином, можемо сказати, що ефективна діяльність транспортно-логістичної компанії заснована на економічному виконанні всіх бізнес-процесів та логістичних функцій. Через постійні динамічні зміни потрібно здійснювати постійний контроль цих процесів, їх покращення та адаптацію до вимог зовнішнього середовища, яке безпосередньо впливає на роботу транспортно-логістичної системи.

1.2. Сучасні підходи до автоматизації управління логістичною діяльністю

Дуже важливим етапом здійснення транспортно-логістичних бізнес-процесів є без ускладнень ухвалене управлінське рішення. Проте на затвердження рішень впливають різноманітні чинники зовнішнього та внутрішнього середовища, неодноразово вони ставлять певні бар'єри, які дійдеться усунути через ефективності прийнятих рішень (рис.1.5). У свою чергу до основних викликів транспортно-логістичного сектору дозволено віднести створення єдиної транспортної зони із сучасною транспортною інфраструктурою, перехід на транспорт з низьким рівнем викиду вуглецю та пониження економічних зривів, залежних від політичних факторів [8].

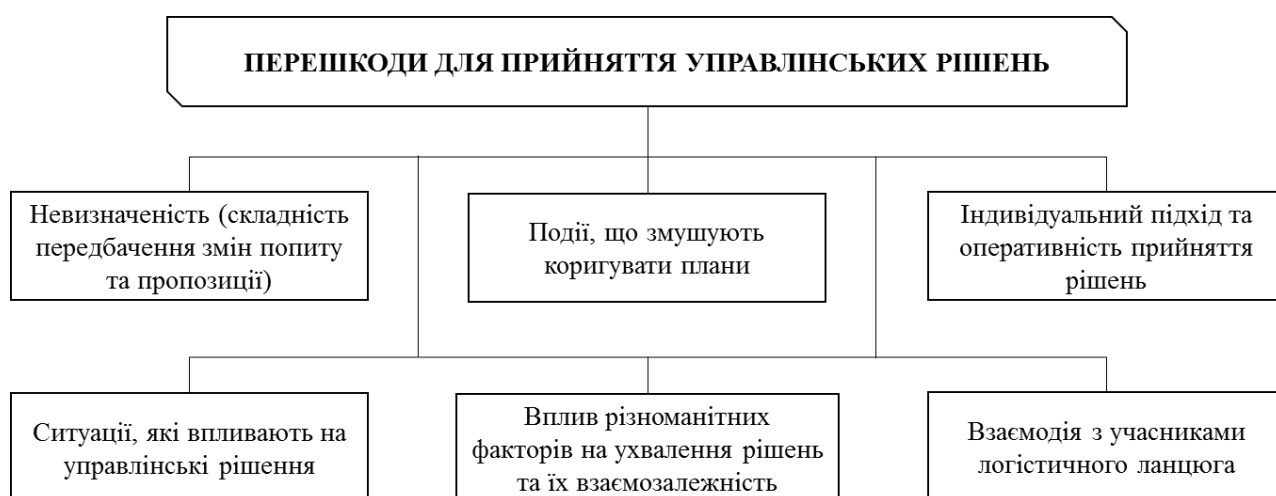


Рис. 1.5. Проблеми на шляху прийняття управлінських рішень

На здійснення бізнес-процесів та застосування різноманітних систем ці та інші фактори мають прямий вплив. Дуже велика кількість ще не оброблених даних, які підпадають під обробку, виконання різноманітних функцій (управління вантажно - розвантажувальними роботами, транспортуванням, складуванням),

просування матеріального потоку в логістичному ланцюгу вимагають застосування різних підходів та інноваційних рішень (рис. 1.6) [9]:

- ✓ Геоінформаційні системи і технології найбільш ефективні під виконання завдань пошуку маршрутів, визначенні найкоротшого шляху, планування перспективних рішень розширення автотранспортної мережі; крім того їх широко використовують для відображення і аналізу формулювання місць найбільш раціонального розташування об'єктів транспортно-логістичної інфраструктури;
- ✓ Автоматична ідентифікація об'єктів транспортних систем сильно допомагає розширити можливості контролю та управління транспортними і логістичними процесами, а також дає можливість обліку вантажів на різних стадіях руху в режимі реального часу, що дозволяє краще планувати та контролювати потоки транспорту з максимальною ефективністю;



Рис. 1.6. Сучасні інноваційні рішення автоматизації управління транспортно-логістичними БП

- ✓ технології організації бездротових мереж зв'язку. Ця технологія є єдиним способом організації безперестанного зв'язку із рухомими транспортними об'єктами для здійснення контролю процесів транспортування та управління ними;
- ✓ технології організації сховищ даних та комплексного багатовимірного аналізу. Ефективність функціонування транспортно-логістичних компаній неможлива без використання технологій зберігання великих інформаційних масивів, їх обробки і виконання на їх основі різноманітних видів аналізу, причому зі швидкістю, близькою до режиму реального часу;
- ✓ «хмарні технології», телеметрія і телемеханіка на транспорті. Телеметрія (технології віддаленого контролю стану автотранспортних засобів) є дієвим засобом покращення функціонування транспортних систем. Дані про поточне місцезнаходження мобільних об'єктів дозволяють передбачати і оперативно усувати різні непередбачувані ситуації. Інформація про стан автомобіля і водія застосовується для розробки оптимального маршруту руху, попередження про втрату водієм робочої спроможності, аналізу техніко-експлуатаційних якостей автомобіля і внесення змін до його конструкції;
- ✓ технології захисту інформації. Від рівня захисту інформації від навмисного або випадкового спотворення на будь-якій стадії зберігання, обробки і передачі даних залежить ефективність функціонування процесів управління транспортними потоками. Це особливо чітко проявляється при здійсненні автоматичного або напівавтоматичного управління і регулювання;
- ✓ технології інформаційного забезпечення процесів аналізу транспортних систем. Інформаційні потоки між елементами транспортних систем утворюються масивами даних, які використовуються для характеристики системи загалом, її частин або окремих транспортних об'єктів. Стислий опис будь-якого транспортного об'єкта, що відрізняється надмірністю мінімальної

інформації, значною мірою сприяє високій ефективності технологій, що використовуються на всіх етапах подальшої передачі і обробки даних;

- ✓ технології транспортного планування. Програмні засоби транспортного планування та моделювання дозволяють сформувати уявлення не тільки про достатній рівень мобільності вантажів, а й отримати відомості про високий рівень доступності транспортних послуг.

У сучасних умовах економічного розвитку світової торгівлі, у якій транспортна логістика відіграє першочергову роль, обсяги даних про стан об'єктів управління постійно зростають. Це потребує комп'ютерної обробки великих масивів вихідних даних (замовлень, параметрів вантажу, автопарку і т.д.). Отримані дані надходять до центру управління в «закритому» вигляді з супутників і ручна обробка такого потоку інформації стає трудомісткою, що призводить до втрати ефективності прийнятих рішень із збільшенням кількості помилок. Можливим вирішенням цієї проблеми в транспортно-логістичних системах може стати впровадження технології блокчейн. Блокчейн (Blockchain або ланцюжок блоків) – це безперервний послідовний ланцюжок блоків, який містить інформацію відповідно до визначених правил. Найчастіше копії ланцюжків блоків зберігаються незалежно один від одного та обробляються на різних комп'ютерах [13]. Технологія блокчейн може вирішувати проблему безпеки в логістиці, а саме запобігти можливості зміни даних і фальсифікації хакерами. Це пояснюється тим, що всі блоки в цій технології взаємопов'язані і здебільшого не підлягають зміні.

Комп'ютерні алгоритми, записані в ланцюжку блоків, які ще називають розумними контрактами, дозволяють автоматизувати багато логістичних бізнес-процесів, що в сукупності зменшує витрати і помилки – так званий вплив людського фактору. Крім того, реалізація технологій блокчейн в транспортно-логістичних системах вигідна для зростання ефективності документообігу, зберіганні даних, управлінні поставками товарів, платіжних системах, електронної

комерції, знижує ризики і значно підвищує стабільність. Впровадження технології блокчейн для розвитку транспортно-логістичних систем надає їм значні переваги (рис. 1.7). Так, інтеграція транспортної логістики через блокчейн-систему дозволить підприємству систематизувати основні інформаційні потоки на підприємстві, знизити трудовитрати на облік товарних потоків і підвищити безпеку цінної інформації [11].

Однією із інноваційних управлінських технологій є Blockchain (ланцюжок блоків) – це багатofункціональна та багаторівнева децентралізована база даних, яка містить інформацію про проведення транзакційних операцій, перевірених та схвалених усіма учасниками захищеної комп'ютерної системи та, яка складається з алгоритмів, що об'єднують упорядковану інформацію блоків даних в одну систему, функціонування якої забезпечується шляхом взаємодії через Інтернет однорангової мережі, або будь-яким іншим способом, що гарантує належний криптографічний захист усіх записів, транзакцій, проведених з використанням відповідної технології [10].

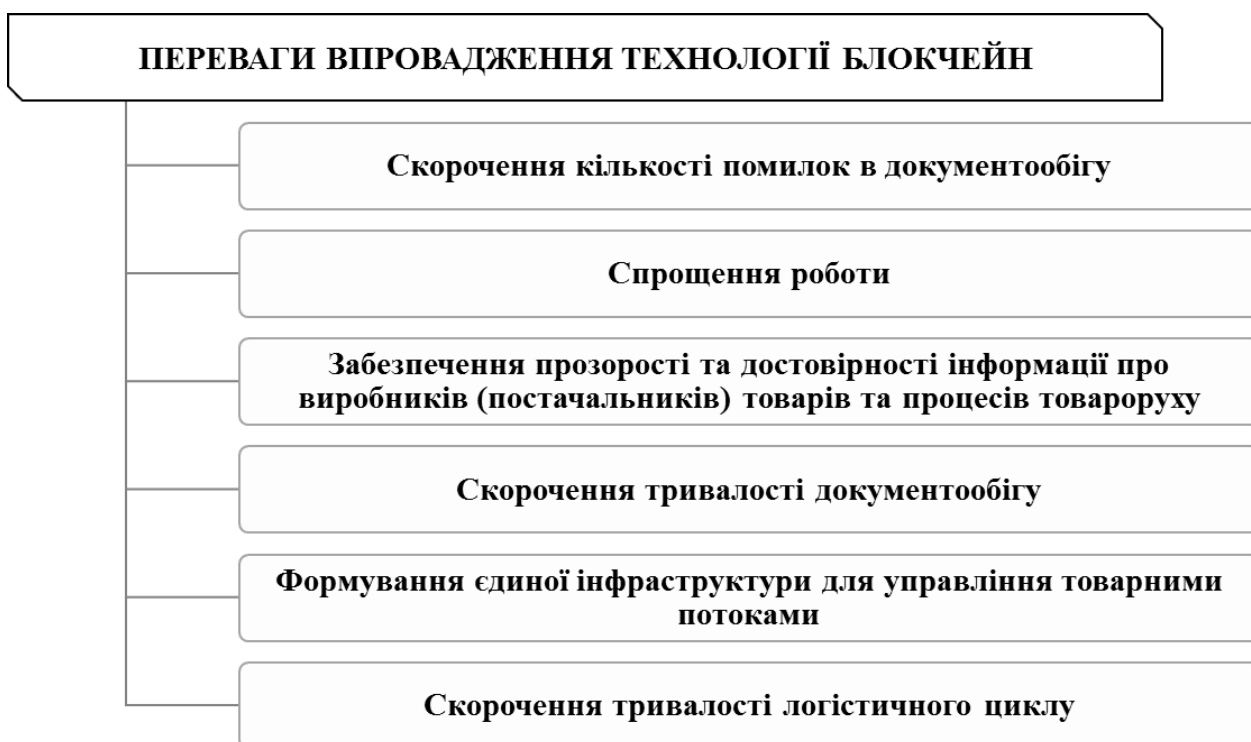


Рис. 1.7. Переваги впровадження технології блокчейн у логістиці

Тобто, технологію блокчейну можна представити своєю обліковою книгою, у якій записано що кому належить, яка є у кожного учасника логістичного ланцюга, яка постійно оновлюється і отримати доступ до якої без спеціального особистого ключа неможливо. У неї можна вписати будь-які операції, що здійснюються в межах логістичних процесів у вигляді спеціальних блоків інформації, де кожен наступний запис посилається на попередній. При використанні цієї технології загубити, спотворити, підмінити або знищити логістичну інформацію фактично неможливо.

Більше того, блокчейн допоможе досягти прозорості та захищеності інформації як для постачальників продукції та послуг, так і для клієнтів, дозволить відстежити весь ланцюг постачання товару від виробника до споживача. Кожна угода або транзакція у такому випадку записується і додається в ланцюжок розподіленої бази даних як новий фрагмент, якому вручну присвоюється унікальний багатозначний числовий шифр. Він зберігає дані про час, дату, учасників, суму угоди – усі важливі та необхідні дані для реалізації визначеної операції та її успішного завершення.

Також за допомогою блокчейну можна організувати фінансові транзакції між банками по всьому світу без єдиного центру, розробити систему постачання різних типів, створити швидку і надійну систему укладання контрактів між покупцем і продавцем або отримувачем та постачальником, організувати систему поштових відправлень, управляти ланцюгами постачання й т.д. Блокчейн може бути надзвичайно корисним для організацій, які обмінюються інформацією, цінними даними, але не дуже довіряють один одному або налагоджують нові партнерські зв'язки. У цьому випадку технологія дозволяє спростити і покращити

процеси обміну та зберігання інформації, що має відношення до взаємодії цих організацій [11].

Технологія блокчейн істотно здешевлює фінансові операції, оформлення та перевірку достовірності документів, ідентифікацію користувачів, охорону інтелектуальної власності, зберігання інформації, ведення різних реєстрів, управління підприємствами, ланцюжки поставок, укладання та виконання контрактів. Сьогодні ринок інноваційних рішень на основі технології блокчейн зростає стрімкими темпами, динаміка якого представлена на рис. 1.8.

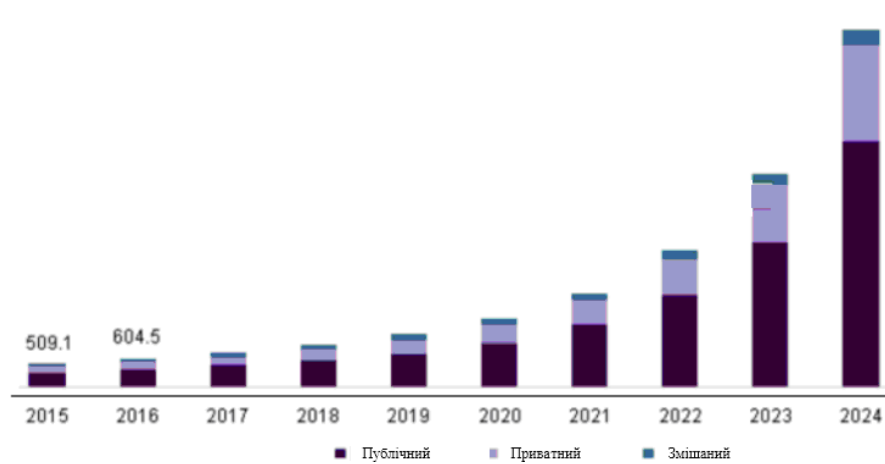


Рис. 1.8. Прогноз динаміки ринку блокчейн-розробок за роками [15]

В останньому звіті TrendInsight від Gartner про вплив блокчейну на трансформацію світу, відзначається, що більшість керівників зосереджено на цій технології для поліпшення поточних бізнес-процесів і управління. Аналітична фірма прогнозує: до 2026 року обсяг економіки блокчейну зросте до 360 млрд. дол., а потім у 2030 році складе більше 3,1 трлн дол. [14]. Наочно прогноз представлений на рис. 1.9.

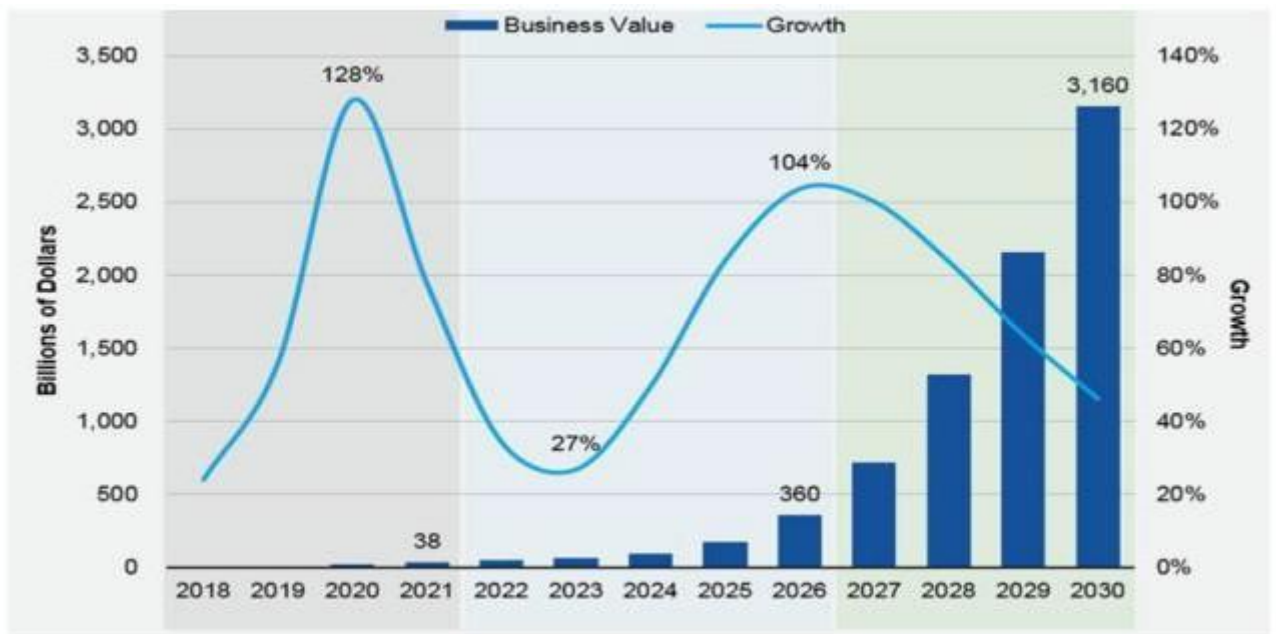


Рис. 1.9. Динаміка зростання блокчейн-бізнесу в 2018-2030 рр.

Області застосування технології блокчейн у сучасній економічній системі постійно розширюються, що у довгостроковій перспективі дозволить вирішити проблему доступу до інформації про логістику для всіх рівнів бізнесу. Тому сьогодні найбільші транснаціональні корпорації надають перевагу цифровим технологіям і роблять капітальні вкладення у відповідні розробки, включаючи створення системи блокчейн і її впровадження в побудову ланцюжка поставок. До таких компаній можна віднести виробника і постачальника апаратного та програмного забезпечення «IBM», торгову мережу «Walmart», лідера інтернет-торгівлі «Amazon», транснаціональні компанії – виробники «Unilever» і «Nestlé», транспортно-експедиційну компанію «UPS».

Серед характеристик та особливостей блокчейну виділяють (рис. 1.10) [10]:

- ✓ доступність: можливість користуватися системою у будь-якому місці з доступом до мережі інтернет та у будь-який час;
- ✓ захищеність: неможливість редагування чи заміни вже зробленого запису у системі блоків;

- ✓ стійкість до неполадок – при втраті частини даних система сама продовжить працювати завдяки розподіленому реєстру;
- ✓ велика кількість користувачів може одночасно зберігати та передавати інформацію;
- ✓ кожен елемент у системі має унікальний номер, що виключає можливість повторення даних;
- ✓ інформація має посилання на час, при поєднанні блоки розташовуються в хронологічному порядку;
- ✓ неможливість фальсифікації згода 51% всіх учасників дозволяє змінити дані.



Рис. 1.10. Характеристики та особливості блокчейну

Таким чином системи, засновані на блокчейні, можуть підвищити ефективність процесів закупівель, логістики і платежів, скоротити ручну обробку імпортно-експортної документації, забезпечити відповідність та доставку товарів і запобігти втратам, що в цілому знижує витрати, покращує безпеку та зводить до мінімуму шахрайство.

Можна виділити наступні етапи впровадження технології блокчейн для управління логістичною діяльністю: 1) оцінка можливості впровадження блокчейн-технології, 2) розробка нової або використання вже готової платформи технології блокчейн, 3) впровадження технології блокчейн, 4) моніторинг

реалізації блокчейн технології, 5) узагальнення результатів впровадження (рис. 1.11).

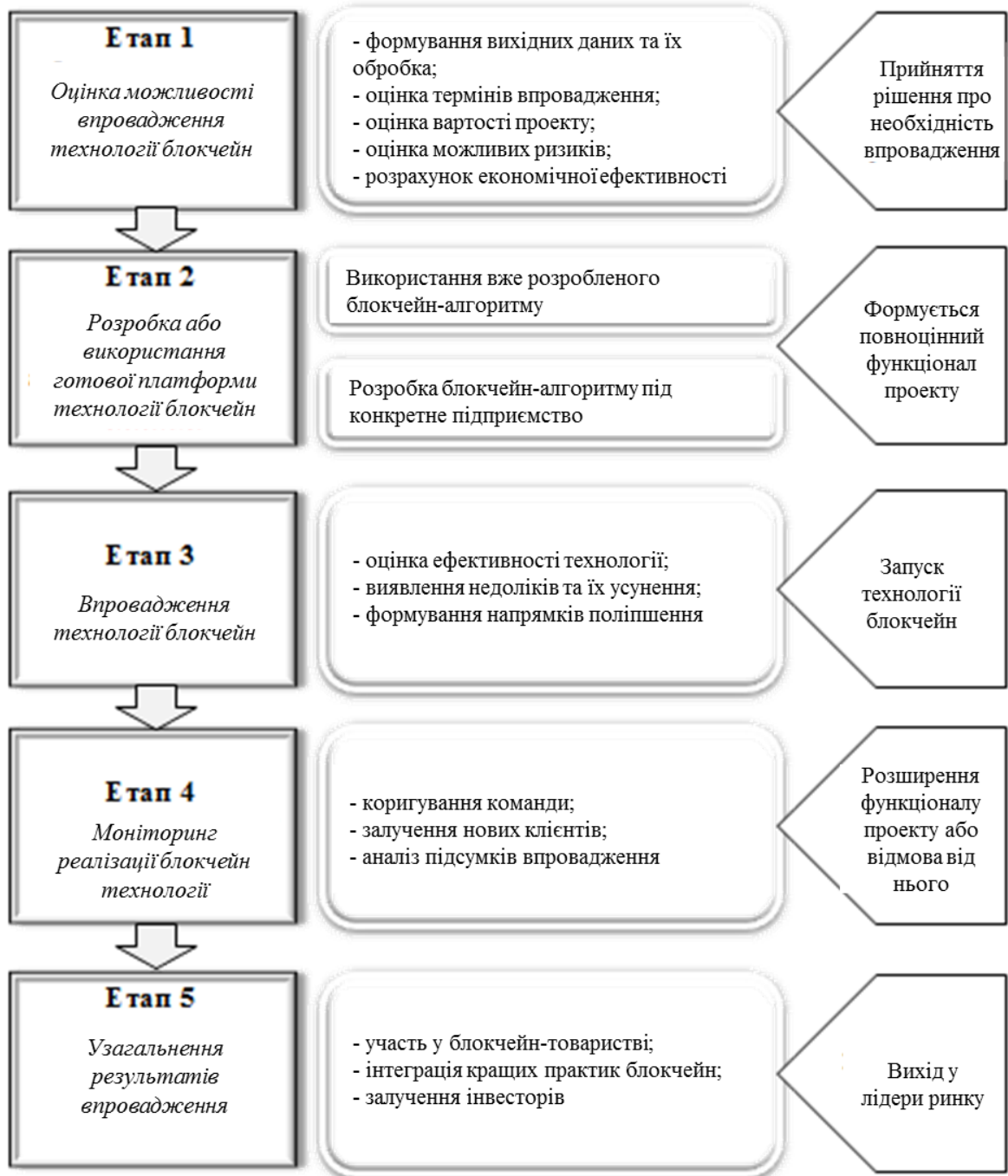


Рис. 1.11. Етапи впровадження технології блокчейн

Отже, діджиталізація та цифрові технології – це спосіб підвищити ефективність галузі та зменшити витрати. Це підтверджують дослідження PwC, які показали, що 54% представників глобальних транспортних компаній в

результаті діджиталізації очікують зростання доходів, 16% очікує від цього прибутку і 11% - підвищення задоволеності клієнтів. Діджиталізація може допомогти створити конкурентну перевагу, досягнення нових та утримання існуючих клієнтів у галузі. Цифрові технології також сприяють створенню мультимодальної транспортної системи та стимулюють впровадження інновацій. У той же час вони створюють ринковий потенціал для кооперативного, інтегрованого та автоматизованого транспортування, що призводить до створення багатьох нових робочих місць. У свою чергу, зв'язок між транспортними засобами, інфраструктурою та іншими учасниками дорожнього руху також має важливе значення для підвищення безпеки майбутніх автоматизованих транспортних засобів та їх повної інтеграції в транспортну систему. Розвиток інтегрованої транспортної мережі усуває бар'єри на ринку та полегшує взаємодію між різними електронними системами та технологічними стандартами [8].

1.3. Стан та перспективи розвитку логістичної галузі в Україні

Україна має високий транспортний потенціал, оскільки є транзитною державою, має вихід до водного простору, її територією проходять міжнародні транспортні коридори (МТК). Це сполучає її з європейськими країнами та дозволяє здійснювати ефективну транспортну політику. Сьогодні глобалізація, науково-технічна революція та світові інтеграційні процеси обумовлюють організацію функціонування і розвиток МТК та залучення їх до міжнародної транспортної мережі, що на сьогодні є одним із головних напрямків реалізації транспортної політики в Україні. А забезпечення сталого економічного росту, підвищення рівня якості життя населення є ключовими та базовими завданнями будь-якої сучасної держави. Однією з найважливіших галузей, так званою «кровоносною системою» національної економіки, без якої розвиток неможливий,

є транспорт, який сприяє поглибленню міжгалузевих інтеграційних процесів. Рівень розвитку транспортної системи держави – одна з найважливіших ознак його технологічного та технічного прогресу, а також фундаментальна умова для інноваційного економічного зростання, структурних і системних економічних перетворень.

У транспортному комплексі світу нині зайнято понад 100 млн. осіб. Частка транспорту у світовому ВВП становить 8-9%. Щороку у світі всіма видами транспорту перевозять понад 100 млрд. т. вантажів і більш ніж 1 трлн. пасажирів. Структура вантажообігу за видами транспорту у світовому масштабі наведена на рис. 1.12. У пасажирообігу на першому місці перебуває автомобільний транспорт (79,3%), на другому – залізничний (10,2%), на третьому – повітряний (10,0%) [12].

За результатами досліджень англійського інституту «Рендел», щодо коефіцієнта транзитивності Україна займає перше місце в Європі. Але ступінь використання транспортної інфраструктури України сьогодні ще досить низький. Транспортна система України не готова повною мірою до належних обсягів забезпечення міжнародних транзитних перевезень.

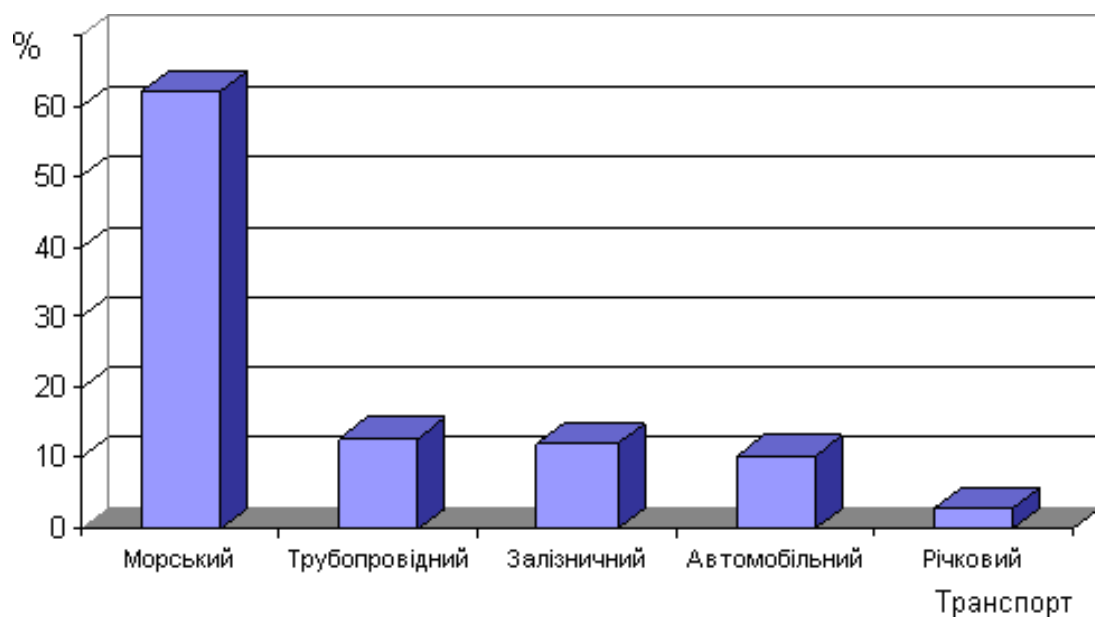


Рис. 1.12. Структура вантажообігу за видами транспорту у світовому

масштабів

Системний підхід до вирішення завдань управління транспортно-логістичними системами чи надто завантажених ділянок доріг забезпечується розробкою і використанням ІТС – системної інтеграції сучасних інформаційних і комунікаційних технологій та засобів автоматизації з транспортною інфраструктурою, транспортними засобами і користувачами, орієнтованої на підвищення безпеки і ефективності транспортного процесу [13].

Ще одним способом розв'язання задач управління міжнародними транспортними потоками (МТП) на сьогодні і у перспективі є впровадження Національної транспортної стратегії України на період до 2030 року, основною метою якої є створення інтегрованого до світової транспортної мережі безпечно функціонуючого та ефективного транспортного комплексу України, задоволення потреб населення у перевезеннях та покращення умов ведення бізнесу для забезпечення конкурентоспроможності та ефективності національної економіки [14].

Крім того, дана стратегія дозволить покращити якість надання транспортних послуг, повинна наблизити рівень їх надання до європейських стандартів та розвитку інфраструктури, підвищити рівень безпеки та зменшити негативний вплив на навколишнє природне середовище, а також забезпечити інноваційний розвиток транспортної галузі та реалізацію глобальних інвестиційних проєктів.

Не дивлячись на оптимістичні стратегії та плани розбудови транспортного ринку, він все ж таки нині має ряд певних проблем (рис. 1.13), які призводять до зниження пропускнуєї спроможності світової транспортної інфраструктури та сповільнюють розвиток світового ринку. Вони призводять до більш значних проблем у цифровій економіці – глобальній мережі економічних та соціальних заходів, реалізованих через платформи Інтернету, мобільні та сенсорні мережі.



Рис. 1.13. Основні проблеми транспортного ринку України

1.4. Постановка задачі дослідження

Дослідивши теоретичні аспекти управління транспортно-логістичними бізнес-процесами зроблено висновок про необхідність розробки системи управління логістичною діяльністю на основі Blockchain-технології.

Об'єктом дослідження є транспортно-логістичні бізнес-процеси.

Предметом дослідження є програмні засоби управління логістичною діяльністю з використанням технології Blockchain.

Метою дослідження є підвищення ефективності забезпечення прозорості та безпеки товароруху у наскрізному моніторингу фінансових та інформаційних потоків шляхом створення системи управління логістичною діяльністю на основі технології Blockchain.

Досягнення поставленої мети обумовлює необхідність вирішення наступних **завдань**:

1. Здійснити аналіз теоретичних засад управління транспортно-логістичними бізнес-процесами та розглянути іноваційні підходи до автоматизації процесів у сфері логістики.
2. Розкрити сутність технології Blockchain та дослідити основні методи захисту даних і алгоритми досягнення консенсусу.
3. Обґрунтувати вибір інструментальних засобів розробки та здійснити проектування і програмну реалізацію системи управління логістичною діяльністю на основі технології Blockchain.

Висновок до розділу 1

Досліджено теоретичні аспекти управління транспортно-логістичними бізнес-процесами. Було розглянуто визначення логістичного БП, проведено поетапний їх аналіз із визначенням завдань кожного на підприємстві, виявлено напрямки вдосконалення та розвитку, описано сучасні інноваційні рішення автоматизації управління транспортно-логістичними бізнес-процесами та визначено, що наша держава має досить високий коефіцієнт транзитивності, сприятливий клімат для розвитку транспортно-логістичної галузі та можливості використовувати сучасні цифрові технології задля автоматизації бізнес-процесів.

Логістичний бізнес-процес – це взаємопов’язана сукупність операцій і функцій, які переводять ресурси підприємства у результат, що задається логістичною стратегією фірми, іншими словами, це процеси, зосереджені на плануванні руху матеріалів, закупівлі, виробництві і поставці товарів споживачам. Вони відбуваються у добре структурованій та побудованій на логістичних принципах транспортно-логістичній системі а ефективна діяльність транспортно-логістичної компанії заснована на економічному виконанні всіх бізнес-процесів та логістичних функцій. Через постійні динамічні зміни потрібно

здійснювати постійний контроль цих процесів, їх покращення та адаптацію до вимог зовнішнього середовища, яке безпосередньо впливає на роботу всієї транспортно-логістичної системи.

Важливим етапом здійснення транспортно-логістичних бізнес-процесів є правильно ухвалене управлінське рішення. Однак на прийняття рішень впливають різноманітні чинники зовнішнього та внутрішнього середовища, часто вони ставлять певні бар'єри та виклики, які необхідно усунути задля ефективності прийнятих рішень. Велика кількість даних, що підпадають під обробку, виконання низки різноманітних функцій, просування матеріального потоку в логістичному ланцюгу вимагають застосування різних підходів та інноваційних рішень, серед яких геоінформаційні системи і технології; технології електронної ідентифікації транспортних засобів; технології організації бездротових мереж зв'язку; технології організації сховищ даних та комплексного багатовимірного аналізу; «хмарні технології», телеметрія і телемеханіка на транспорті; технології захисту інформації; технології інформаційного забезпечення процесів аналізу транспортних систем; технології транспортного планування; блокчейн.

Системи, засновані на блокчейні, можуть підвищити ефективність процесів закупівель, логістики і платежів, скоротити ручну обробку імпортно-експортної документації, забезпечити відповідність та доставку товарів і запобігти втратам, що в цілому знижує витрати, покращує безпеку та зводить до мінімуму шахрайство. Транспортно-логістична галузь має ряд проблем (порушення строків доставки, взаємодія великої кількості посередників, значні ресурсні втрати, ризики крадіжок, неефективний ІТ-сервіс) та задач управління МТП, способами розв'язання яких є використання систем управління транспортною інфраструктурою – інтелектуальних транспортних систем та впровадження Національної транспортної стратегії України.

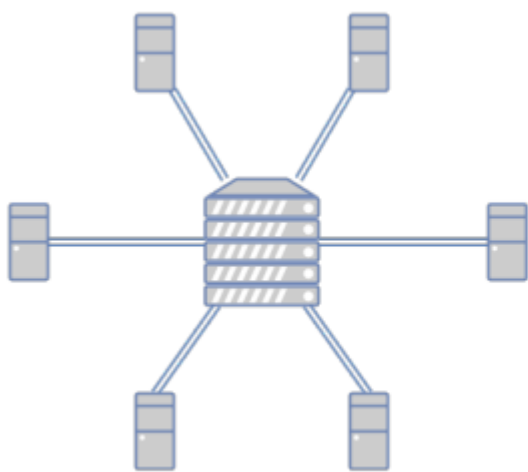
РОЗДІЛ 2. ТЕХНОЛОГІЯ BLOCKCHAIN: СУТНІСТЬ ТА ОСНОВНІ МЕТОДИ ЗАХИСТУ ДАНИХ І АЛГОРИТМИ ДОСЯГНЕННЯ КОНСЕНСУСУ

2.1. Основні складові технології Blockchain

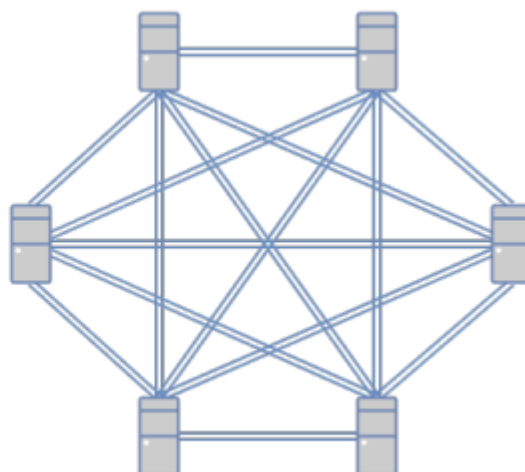
Блокчейн (від англ. "Blockchain" – ланцюжок блоків) – це вибудований за певними правилами неперервний послідовний ланцюжок блоків, що зберігають деякі дані, який репліцирується на кожен із комп'ютерів, об'єднаних в однорангову (пірингову) мережу.

Члени даної однорангової мережі – анонімні особи, які називають вузлами. Всі комунікації усередині мережі використовують асиметричну систему шифрування й хешування, щоб надійно ідентифікувати відправника й одержувача. Коли одині з вузлів хоче додати дані в блокчейн, у мережі формується новий блок і за допомогою алгоритму консенсусу додається в ланцюг.

На сучасному ринку ІТ-систем існує два типи архітектур комп'ютерних мереж: клієнт-серверна мережа (рис. 2.1, а) і однорангова (пірингова) мережа (рис. 2.1, б).



а) клієнт-серверна



б) однорангова (пірингова)

Рис. 2.1. Архітектури комп'ютерних мереж

Мережа із клієнт-серверною архітектурою підтримує централізований контроль даних і доступу. Вся системна логіка й інформація сховані всередині сервера, що дозволяє знизити вимоги до продуктивності клієнтських пристроїв і забезпечити високу швидкість обробки даних, але така мережа має низьку відмовостійкість.

В основі технології блокчейн лежать однорангові або децентралізовані мережі. Така мережа не має головного пристрою, і всі учасники мають рівні права. У такій моделі кожен користувач є не тільки споживачем, але й постачальником сервісу. Перевагою такої системи є доступність даних: немає єдиної точки відмови, як у випадку з базою даних, розташованою на одному сервері й висока відмовостійкість: при припиненні функціонування одного або декількох вузлів працездатність мережі не порушується.

Технологія блокчейн припускає використання розподіленої бази даних, що складається з ланцюжка блоків, який представляє собою зв'язний список, у якому кожен блок містить ідентифікатор попереднього. Для ідентифікації кожного блоку використовується хеш, створений за допомогою криптографічної функції.

Хешування – це перетворення масиву вхідних даних довільної довжини в (вихідний) бітовий рядок установленої довжини, виконуване певним алгоритмом. Криптографічна функція, що втілює алгоритм і виконує перетворення, називається хеш-функцією. Як параметр хеш-функції може бути переданий рядок будь-якої довжини, а результатом її роботи завжди буде бітовий рядок строго фіксованої довжини.

Всі хеш-функції повинні відповідати наступним вимогам:

1. Весь доступний діапазон хешей використовується по максимуму. Тобто, якщо на хеш відведено 32 байта, то різні дані дають максимально різноманітний хеш, що може бути зовсім будь-якою комбінацією бітів.

2. Будь-яка, навіть сама незначна, зміна вхідних даних повинна давати інший хеш.

На практиці можливі випадки, коли хеш-функція перетворює кілька різних повідомлень в однакові – це називається колізією. Імовірність виникнення колізій використовується для оцінки якості хеш-функцій і повинна прямувати до мінімуму.

Кожен блок складається із заголовка й списку транзакцій представлених, коренем хеш-дерева Меркла. Заголовок блоку містить у собі свій хеш, хеш попереднього блоку й додаткову службову інформацію (рис. 2.3).



Рис. 2.3. Зв'язний список блоків

Дерево Меркла (Merkle tree) або бінарне дерево хешів – це двійкове дерево, кінцеві вузли якого - це хеші транзакцій, а внутрішні вершини – результати додавання значень пов'язаних вершин (рис. 2.4).

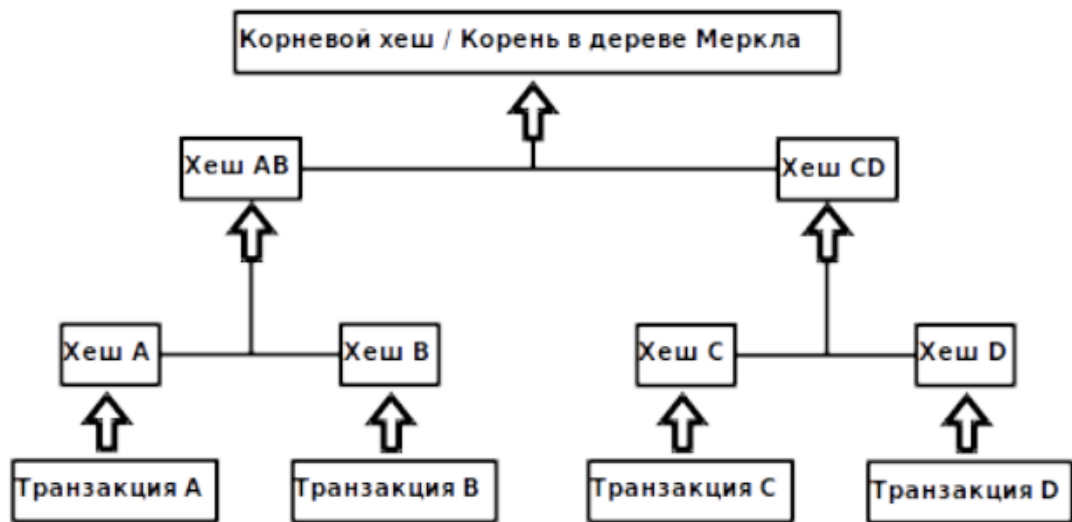


Рис. 2.4. Хеш-дерево Меркла

Оскільки дерево бінарне, то на кожному кроці повинно бути парне число елементів. Тому якщо, на якомусь етапі кількість хешів непарна, то останній хеш дублюється для одержання пари. Переваги такого алгоритму хешування перед хешуванням усіх транзакцій разом, об'єднаних в один великий блок даних, полягає в тому, що він забезпечує не тільки доказ дійсності кожної окремої транзакції, але й унеможливорює внесення зміни в порядок транзакцій. Тому що при переміщенні транзакції з її законного місця зміниться вся галузь хешів і корінь у дереві Мерклу.

Список транзакцій для внесення в новий блок, формується учасниками мережі із черги неопрацьованих транзакцій, ще не записаних у попередні блоки.

Ідентифікатором транзакції є її хеш (ТХІ), що будується на основі складу транзакції. Кожна транзакція містить у собі таблицю входів, таблицю виходів, цифровий підпис відправника, публічний ключ одержувача й кількість засобів для перекладу (рис. 2.5).

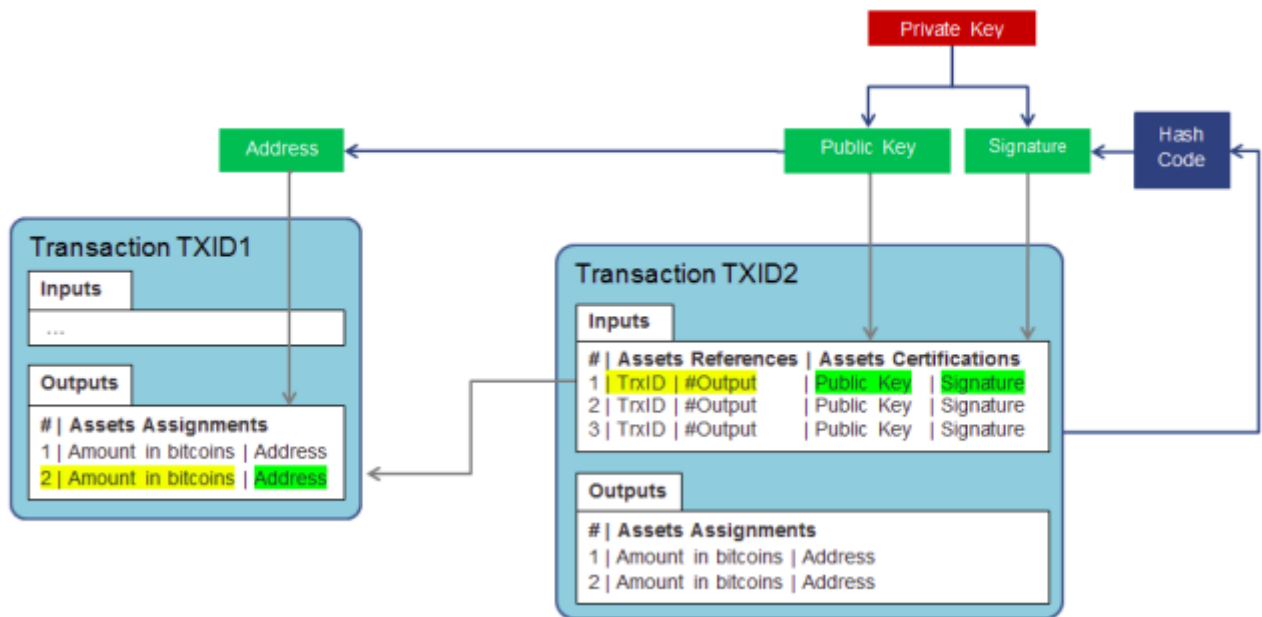


Рис. 2.5. Структура транзакції

Цифрові підписи в блокчейні формуються на основі асиметричної системи шифрування, у якій для кожного користувача по певному алгоритмі генеруються так пари ключів, що складаються з відкритого (публічного) і закритого (особистого) ключів. Це такий набір захисту даних в криптографії, коли відкритий ключ призначений для поширення публічно. Він служить як адреса для прийому повідомлень від інших користувачів. Закритий ключ зберігають у секреті. Він використовується як цифровий підпис для повідомлень, відправлених іншим користувачам.

При відправленні повідомлення відправник шифрує інформацію за допомогою відкритого ключа адресата. Розшифрувати це секретне повідомлення одержувач може тільки, використовуючи закритий ключ із пари з відкритим, котрим воно було зашифровано. У той же час повідомлення зашифроване закритим ключем відправника, може бути розшифроване тільки за допомогою відповідного відкритого ключа з пари із закритим (рис. 2.6).

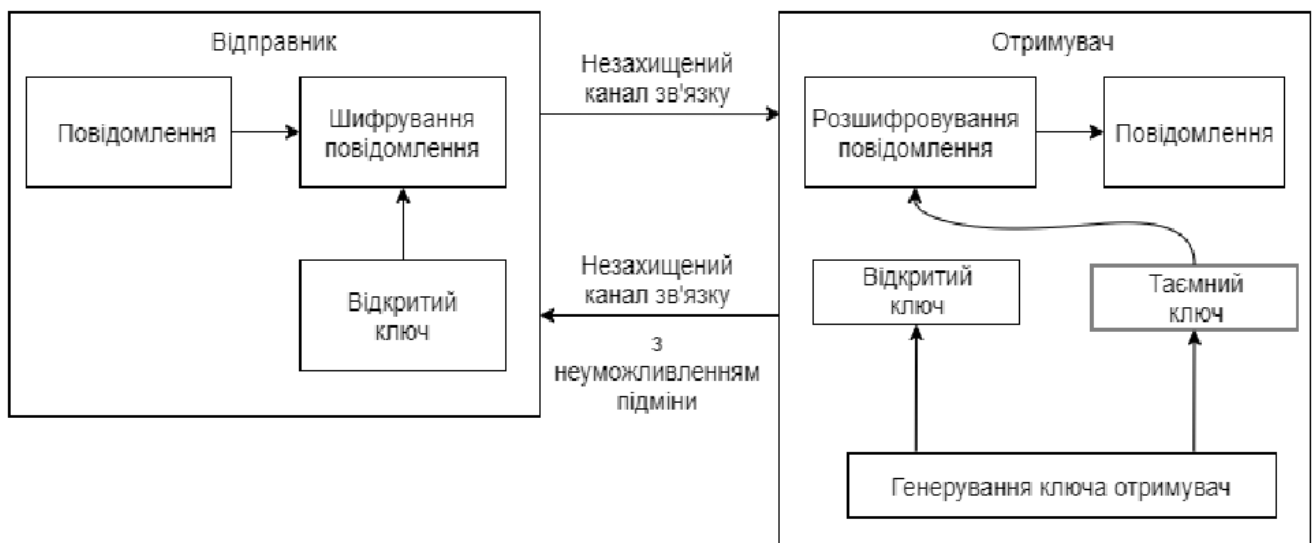


Рис. 2.6. Схема передачі даних у асиметричних криптосистемах

Відкритий і закритий ключі зв'язані один з одним за допомогою деяких математичних виразів. Відкритий ключ реально обчислити на основі закритого ключа, а от зворотне перетворення вимагає неможливого на практиці обсягу обчислень. Таким чином, асиметричне шифрування використовується в блокчейні для аутентифікації відправників і забезпечення цілісності транзакцій.

Стандарти хешування можуть мати різну швидкість, розмір хешу та механізм кодування. До найбільш швидкісних та популярних хеш-функцій відносять стандарти CRC, MD4, MD5 та SHA.

MD5 – алгоритм, який використовується для створення 128-бітного криптографічного рядка будь-якої довжини, який є унікальним для будь-яких даних, призначений для використання цифрових підписів, які вимагають, щоб великі об'єми даних були стиснуті безпечним шляхом перед своїм шифруванням за допомогою ключа в криптосистемі.

SHA-256 – алгоритм криптографічної хеш-функції, вхідний хеш якого складає 256 біт. Цей алгоритм робить злом і розшифрування дуже складним процесом, оскільки чисельність варіантів є дуже великою. Цей алгоритм працює з

розподіленими на 512-бітні блоки даних. Після криптографічного «змішування» на виході отримуємо 256-бітний хеш-код.

Хеш-таблиця – масив даних для зберігання пар значення-ключ, де положення елементів залежать від значення цього самого елемента. В таких таблицях реалізовано 3 типи операцій. Додавання нової пари по типу ключ-значення; операція пошуку по ключу; операція видалення по ключу.

Транзакція вважається виконаною, як тільки вона буде занесена в блокчейн. Для цього вона повинна пройти верифікацію при додаванні в черговий блок, а блок повинен бути доданий у ланцюжок. Виходи виконаної транзакції можуть бути використані як входи нових транзакцій, тим самим створюючи ланцюжок передачі прав власності, у міру того, як інформація переміщується від адреси до адреси. Такі, поки ще невитрачені виходи, мають спеціальну назву - UTXO (unspent transaction output).

При створенні транзакції користувачем, перед додаванням у блок, вона переміщується у список неопрацьованих транзакцій. Блок буде сформований, коли в нього буде додано достатній обсяг транзакцій. Обсяг транзакцій для блоку регламентується не кількістю транзакцій, а їхнім обсягом, що залежить від кількості входів і виходів у транзакції.

Головним учасником процесу майнінгу є майнер – вузол мережі, який збирає транзакції для подальшого додання їх у блок. Після того, як відбулась певна операція майнери отримують транзакції для подальшої їх перевірки. Після чого вони додають їх у певний "пул" пам'яті й починають збирати декілька транзакцій в один блок. Перед запуском процесу, майнер додає транзакцію, у якій прописана нагорода за його роботу. Після хешування всіх функцій вони об'єднуються в хеш-дерево, де сполучаються в пари до тих пір, доки не буде досягнута "вершина дерева". Ідентифікатор кожного блоку утворюється в результаті додання почного хешу з хешем попереднього блоку й певним випадковим числом – за

певним протоколом. Іноді два вузли додають підтверджені блоки й користувачі починають майнити блоки вже на основі цих даних, що є неправильним. У результаті чого конкуренція буде продовжуватись доти, поки не буде створений один блок на основі один із двох попередніх блоків (рис. 2.7).

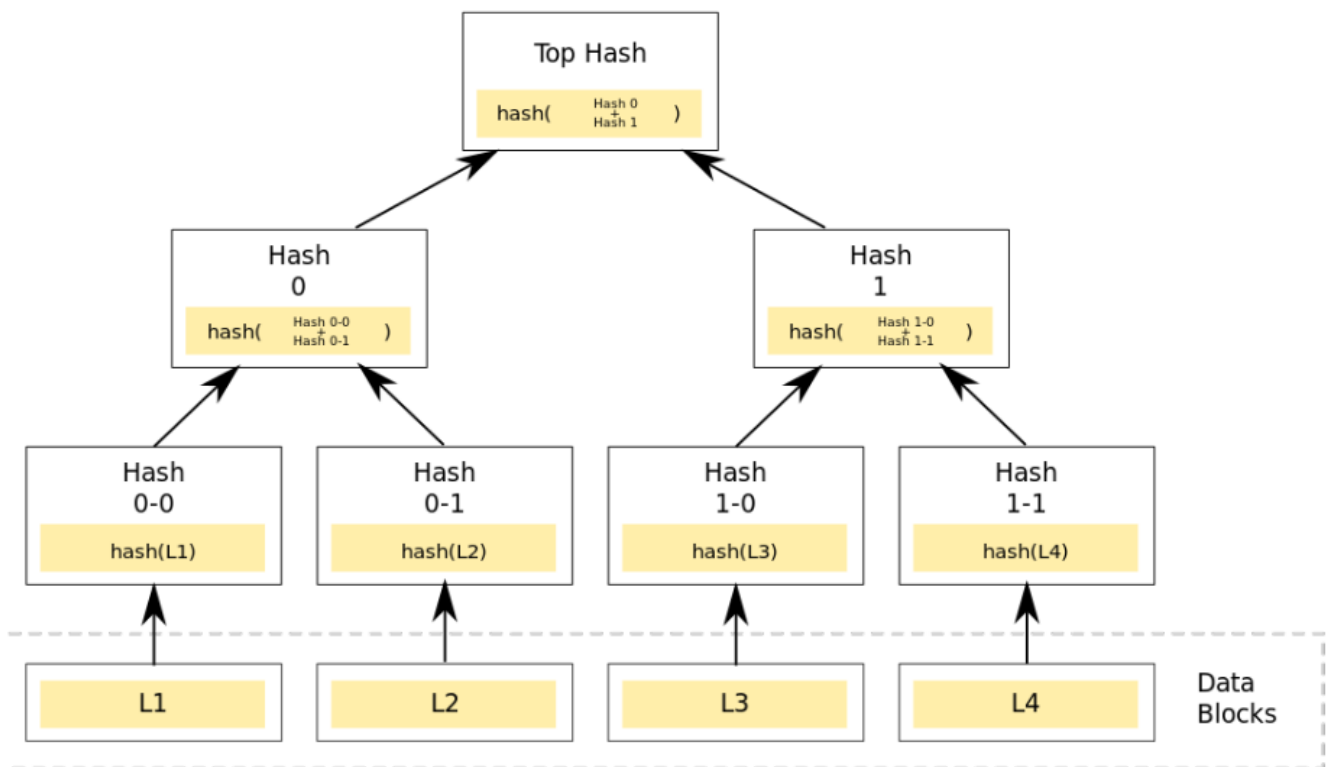


Рис. 2.7. Приклад хеш-дерева (дерева Меркла)

2.2. Алгоритми консенсусу

Перевірку операцій та підтвердження правильності їх запису здійснює вбудований механізм – алгоритм консенсусу. Алгоритм консенсусу гарантує дотримання правил протоколу й вірогідність усіх транзакцій. Найбільш затребувані алгоритми консенсусу серед кращих блокчейн-проектів: Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Proof-of-Authority (рис. 2.8).

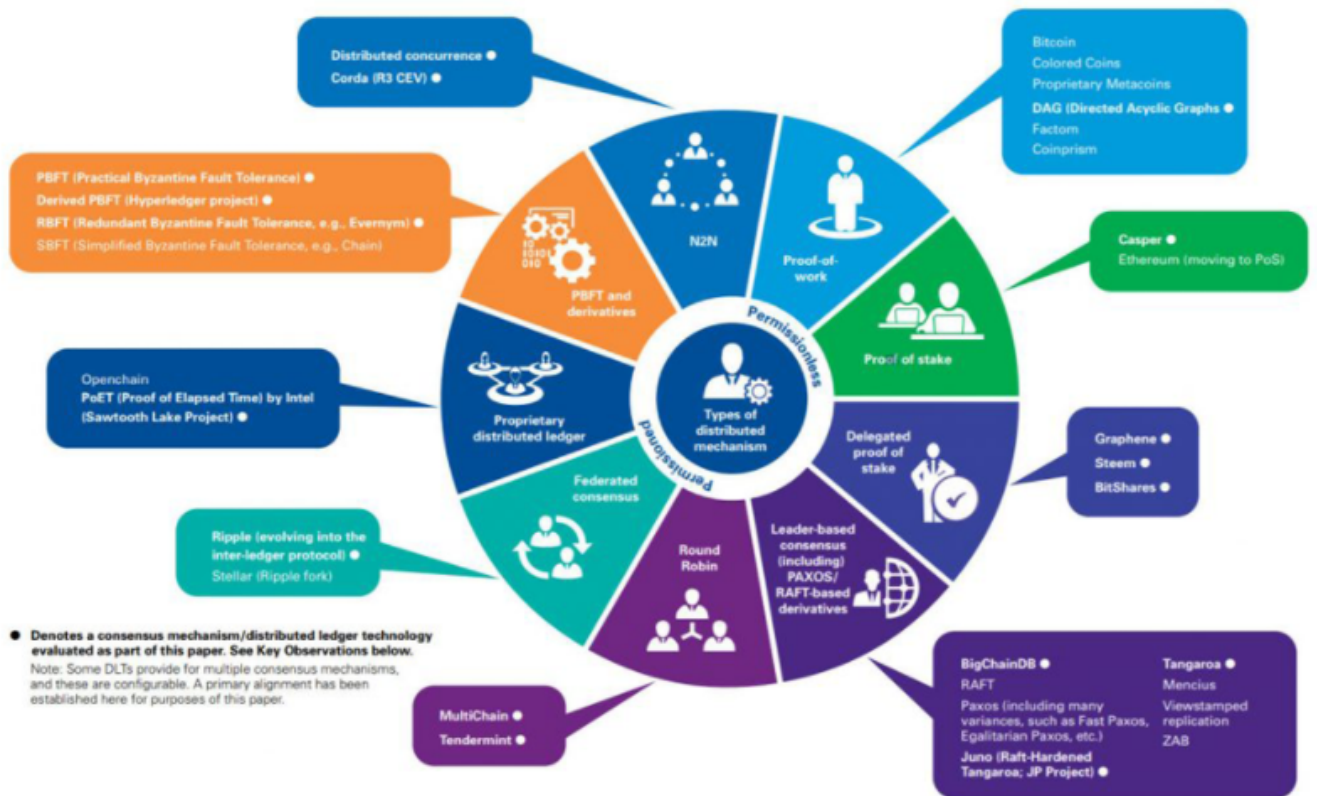


Рис. 2.8. Основні алгоритми консенсусу

Proof of Work (PoW) – це перший алгоритм консенсусу, який використовується в Bitcoin та в інших криптовалютах. Цей алгоритм представляє певну кількість спроб хешування, ця кількість прямо пропорційно залежить від обчислювальної потужності. PoW гарантує, що майнери можуть підтверджувати новий блок транзакцій та додавати його в блокчейн, якщо розподілені вузли досягають консенсусу щодо валідності (правильності) представленого блоку. Блокчейн Ethereum заснований на цьому алгоритмі. Алгоритм Proof-of-Work (PoW) вимагає для підтвердження транзакцій виконання досить складної обчислювальної роботи, наступний блок створює той вузол, який першим закінчив розрахунки. Алгоритм є дуже енергозатратним, має низьку швидкість та погану масштабованість і не підходить для масового повсякденного використання.

Proof of Stake (PoS) – алгоритм, який появився на заміну PoW. Головна його відмінність полягає в тому, що блоки перевіряються відповідно до часток учасників. Proof-of-Stake (PoS) – популярний алгоритм консенсусу, у якому творцем наступного блоку в ланцюжку вибирається вузол, що має більший баланс – кількість ресурсів. Цей алгоритм частково виправляє недоліки алгоритму PoW – низьку швидкість та погану масштабованість, однак потребує витрат та технічних знань.

Proof-of-Capacity (PoC) – алгоритм, який іноді ще називаний Proof-of-Space (PoSpace). PoC працює по наступному принципі:

- Кожен майнер обчислює досить великий обсяг даних, що записується на дискову підсистему (жорсткий диск, хмарні системи зберігання) вузла. Такий первісний набір даних в PoC називається "ділянка".

- Для кожного нового блоку в блокчейні, майнер читає невеликий набір даних (1/4096, що приблизно становить 0.024%) від свого загального збереженого обсягу й повертає результат (дедлайн), як минулий час у секундах з моменту створення останнього блоку, після якого майнер зможе створити новий блок.

- Майнер, що одержав мінімальний час дедлайна, підписує блок й одержує винагороду за транзакції.

У такий спосіб обчислювальні ресурси необхідні майнеру для цієї роботи обмежені часом, який необхідно для читання файлів з дискової підсистеми. Саме цей фактор дозволяє робити майнінг із досить високою енергоефективністю. Майнери змагаються між собою за розміри даних, які зберігаються, на відміну від швидкості роботи встаткування, що є визначальною в майнінгу побудованому на PoW.

Автори алгоритму Proof-of-Activity (PoA) спробували об'єднати два найбільш популярні алгоритми, такі як Proof-of-Work й Proof-of-Stake, з метою

збільшення рівня захисту від потенційно можливих атак (51% attack, Denial-of-Service attacks (DoS). Принцип роботи алгоритму описаний нижче:

- Кожен майнер блокчейн мережі пробує згенерувати заголовок порожнього блоку, що містить у собі хеш попереднього блоку, публічну адресу майнера, індекс поточного блоку в блокчейні й nonce.

- Після генерації заголовку порожнього блоку який відповідає поточним вимогам складності, вузол розсилає цей заголовок у блокчейн мережі.

- Усі вузли мережі розглядають заголовок такого блоку, як дані отримані від псевдовипадкових власників. Використовуючи хеш розісланого заголовка блоку й хеш попереднього блоку + N пресетів із використанням алгоритму follow-the-satoshi вибираються стейкхолдери.

- Кожен стейкхолдер, що перебуває в онлайні, перевіряє отриманий, порожній заголовок блоку на його коректність. Під час перевірки кожен заголовок, що одержав, перевіряє чи є він одним з перших N-1 стейкхолдерів "щасливчиків" цього блоку й у цьому випадку підписує заголовок порожнього блоку своїм секретним ключем і відправляє його в блокчейн мережу.

- Коли N-й стейкхолдер бачить, що він повинен стати підписантом цього блоку, він, на додаток до заголовка порожнього блоку, додає блок із включеними транзакціями (кількість транзакцій, що включають, він вибирає сам), всі підписи N-1 від інших стейкхолдерів і підписує блок.

- Стейкхолдер N розсилає новий, підготовлений блок. Вузли одержують цей блок, переконуються в його законності й додають цей блок у блокчейн.

- Премія за транзакції, що одержав N-стейкхолдер, розподіляється між майнером і N стейкхолдерами "щасливчиками".

Алгоритм Proof-of-Authority (PoA) для своєї роботи не потребує взагалі якого-небудь майнінга, як у випадку з PoW або PoS. У блокчейн мережі, що базується на Proof-of-Authority, всі транзакції й блоки перевіряються за допомогою

схвалених аккаунтсв (валідаторсв). Проведення транзакцій і створення блоків, проходить в автоматичному режимі за допомогою обчислювальних потужностей валідатора. Проведений аналіз дозволив виявити, що при плануванні ланцюгів поставок високу ефективність у логістиці показав алгоритм Proof-of-Authority (PoA), основою якого є система репутації, коли кожен користувач блокчейну має ідентифікатор, який відображає його репутацію. За роботу мережі відповідає фіксоване число валідаторів – ті, хто підтвердив свою особистість.

На ринку існує значне число блокчейн-платформ, які розрізняються застосовуваними протоколами шифрування, алгоритмами консенсусу, функціональними можливостями [2]. Серед блокчейн-платформ, які використовують у сфері логістики, було виявлено Ethereum, Ripple, Hyperledger Sawtooth, Hyperledger Fabric, IBM Blockchain Platform, Microsoft Azure Blockchain Platform, Quorum. Для розробки програмного застосунку підтримки логістичної діяльності доцільно обрати платформи Microsoft Azure Blockchain Platform та Quorum, оскільки вони підтримують алгоритм консенсусу PoA.

Алгоритм консенсусу Practical Byzantine Fault Tolerance (PBFT) було запропоновано у 1999 році як механізм, який забезпечує цілісність роботи розподіленої мережі. Даний алгоритм консенсусу є консенсусним алгоритмом практичної взаїтійської терпимості до помилок, який відповідає за ефективну роботу у асинхронних мережах. Реалізовано механізм, який розв'язує багато проблем, пов'язаних з візантійськими рішеннями по відмовостійкості. Основою для алгоритму став уже існуючий механізм BFT, що дозволяє досягти консенсусу, навіть якщо деякі вузли в мережі не відповідають або подають невірну інформацію (візантійська помилка – один із генералів захворів та саботує колег).

Під час воєї роботи PBFT досить інтенсивно використовує мережу для обміну повідомленнями між вузлами мережі для забезпечення цілісності роботи в мережі, тому він краще підходить для роботи у довірених мережах –

внутрішньокорпоративних або міжорганізаційних блокчейнах. Цей алгоритм використовується у середовищі Hyperledger Fabric, яке було використане у даному дослідженні для розробки застосунку управління логістичною діяльністю.

Висновок до розділу 2

Установлено, що ключовими в технології блокчейн є наступні операції: взаємодія учасників, формування блоків, формування ключів, шифровка записів. У логістиці дані, що утворюють ланцюг блоків, можуть містити таку інформацію: відомості про угоди, людей, об'єкти, транзакції, серійні номери, видані кредити та інші дані, які стосуються товароруку між учасниками поставок продукції. Ланцюжки блоків дозволяють відправляти дані в будь-яку точку світу, де буде доступний файл блокчейна за умови наявності закритого ключа, створеного за криптографічним алгоритмом, щоб дозволити доступ тільки до тих блоків, якими володіє конкретна особа. Надаючи закритий ключ, можна передати сторонній особі певну інформацію, яка зберігається у відповідному розділі ланцюжка блоків.

Використання складної системи шифрування забезпечує наявність у кожного блока свого унікального ключа, даючи можливість кожному користувачеві змінювати тільки ті блоки ланцюга, до яких у них є доступ. Ця особливість технології блокчейн дозволяє реалізувати довірчі відносини між користувачами й унеможлиблює підробку інформації у розподіленій базі даних. Перевірку операцій та підтвердження правильності їх запису здійснює вбудований механізм – алгоритм консенсусу. Алгоритм консенсусу гарантує дотримання правил протоколу й вірогідність усіх транзакцій. Найбільш затребувані алгоритми консенсусу серед кращих блокчейн-проектів: Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Proof-of-Authority. Проведений аналіз дозволив виявити, що при плануванні ланцюгів поставок високу ефективність у логістиці показав

алгоритм Proof-of-Authority (PoA), основою якого є система репутації, коли кожен користувач блокчейну має ідентифікатор, який відображає його репутацію. За роботу мережі відповідає фіксоване число валідаторів – ті, хто підтвердив свою особистість.

Виявлено, що на ринку існує значне число блокчейн-платформ, які розрізняються застосовуваними протоколами шифрування, алгоритмами консенсусу, функціональними можливостями [2]. Серед блокчейн-платформ, які використовують у сфері логістики, було виявлено Ethereum, Ripple, Hyperledger Sawtooth, Hyperledger Fabric, IBM Blockchain Platform, Microsoft Azure Blockchain Platform, Quorum.

У даному дослідженні було обрано алгоритм консенсусу Practical Byzantine Fault Tolerance (PBFT), який дозволяє досягти консенсусу, навіть якщо деякі вузли в мережі не відповідають або подають невірну інформацію.

РОЗДІЛ 3. РОЗРОБКА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ЛОГІСТИЧНОЮ ДІЯЛЬНІСТЮ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN

3.1. Hyperledger Composer: середовище розробки та набір інструментів для оптимізації розгортання системи блокчейн Hyperledger Composer

Для швидкого розгортання корпоративної блокчейн-платформи для управління логістичною діяльністю було вирішено використати проєкт Hyperledger Composer. Це один із проєктів з відкритим вихідним кодом у рамках корпоративної блокчейн-компанії Hyperledger, який є інструментом для реалізації фреймворків блокчейн.

Використовуючи Hyperledger Composer, без технічних знань можна легко співпрацювати з розробником для створення конкретних функцій. Вони включають визначення бізнес-правил, на основі яких оброблятимуться транзакції блокчейну, визначення активів, якими обмінюються у випадках використання на основі блокчейну, а також визначення засобів контролю для учасників, їхніх ідентичностей, ролей та рівнів доступу для виконання різних видів транзакцій.

Аналогічно, розробник, який використовує Hyperledger Composer, може легко створювати та налаштовувати основні компоненти блокчейну, які включають цифрові активи мережі, логіку транзакцій, учасників та засоби контролю доступу. Composer підтримує спільне використання, можливість повторного використання та масштабованість компонентів у різних організаціях. За допомогою Hyperledger Composer можна легко створити необхідні сценарії та API, необхідні для бізнес-реалізації. Він також підтримує варіанти використання та тестування в режимі реального часу, яке

навіть можна виконувати через веб-майданчик Composer без необхідності локального встановлення.

Використовуючи Hyperledger Composer, можна створювати та запускати зразок блокчейну і надавати обмежений дозвіл різним учасникам. Наприклад, можна легко побудувати «Мережу швидкопсувних товарів», яка полегшує торгівлю такими товарами, як фрукти та овочі, включає учасників, таких як фермери, вантажовідправники та імпортери, визначає індивідуальні ролі для кожного учасника, визначає та виконує умови угоди між учасниками, відстежує відправлення, підтвердження, моніторинг та звітність про стан товарів на різних етапах ланцюга поставок, а також управління платежами.

До ключових концепцій Hyperledger Composer відносять наступне. Hyperledger Composer - це єдина у своєму роді програма моделювання, що поставляється з мовами моделювання й API-інтерфейсами для визначення бізнес-мереж. За допомогою смарт-контракта Hyperledger Composer легко пропонує учасникам функції обміну активами. В основному активи являють собою цифрову форму будь-яких нематеріальних або матеріальних товарів, властивостей або послуг у мережі. І все це зберігається в реєстрах. Необхідно переконатися, що всі активи мають унікальні ідентифікатори, які допоможуть їх відслідковувати. Більше того, їх можна визначати за своїм розсудом.

Активи необхідні для функціонування бізнес-мережі, а учасники є членами цієї системи й можуть воодіти активами та брати участь у відправці транзакцій. Учасників моделюють у відповідності з потребами логістичних процесів. Транзакції абсолютно необхідні для смарт-контракта Hyperledger Composer. Це засіб взаємодії з активом на платформі. Що ж, щоб підтримувати бізнес-процеси в мережі, потрібні особливі правила контролю доступу. Це допомагає визначити, хто й до чого має доступ та допомагає

контролювати доступ до певних активів й умов, у яких однорангові вузли можуть їх використовувати. Всі транзакції системи будуть зберігатися в реєстрі блокчейна. Поточний стан учасників й активів зберігається в базі даних станів блокчейна.

В архітектурі Hyperledger Composer усього вісім високорівневих компонентів:

1. Середовище виконання - пропонує підключення різних середовищ виконання:
 - a. Hyperledger Fabric – стан зберігається у розподіленому реєстрі;
 - b. вбудоване середовище, яке виконується безпосередньо всередині процесу Node.js і використовується для модульного тестування бізнес-логіки, зберігається у пам'яті у вигляді KV;
 - c. Web – виконується безпосередньо в Web для демонстрації Playground, стан зберігається у локальному сховищі браузера.
2. REST сервер – генерує Open API або Swagger REST API для бізнес-мережі. Весь процес його створення відбувається автоматично. Сервер REST (на основі технології LoopBack) перетворить модель Composer у визначення Open API й реалізує підтримку CURD.
3. Інтерфейс командного рядка допомагає розробникам та адміністраторам управляти мережею.
4. JavaScript SDK – набір різних API-інтерфейсов Node.js, які допомагають розробникам створювати нові додатки, що можуть взаємодіяти й управляти створеною бізнес-мережею. Ці API розділені на два модуля:
 - a. composer-client: відправити запит на транзакцію в бізнес-мережу й виконати операції CURD з активами й учасниками;
 - b. composer-admin: використовується для керування бізнесом-мережею, установки, запуску, відновлення.

5. Плагін редактора VSCode й Atom - розширення редактора VSCode й Atom. VSCode - це надпотужне розширення, що може перевіряти файли ACL або моделі Composer. Він також може пропонувати підсвічування синтаксису, підтримку фрагментів і виявлення помилок.
6. Генератор коду Йомена - це фреймворк із відкритим вихідним кодом, що генерує кістяк будь-якого проєкту: js застосунку, Angular веб- застосунку, скелетної бізнес-мережі.
7. Користувальницький веб-інтерфейс Playground Web UP - це веб-інтерфейс користувача для тестування й визначення бізнесів-мереж. Більше того, це гарантує, що аналітик створить прототип або зразок бізнес-логіки, що працює в середовищі виконання Fabric або в Інтернеті.
8. Коннектор LoopBack – сервер REST використовує коннектор LoopBack. Однак багато інструментів інтеграції можуть використати його автономно, тому що підтримують LoopBack. Крім того, інструменти LoopBack також можуть використати його для більше просунутого рівня налаштування REST API.

Основним механізмом забезпечення консенсусу в Hyperledger Composer є алгоритм Practical Byzantine Fault Tolerance (PBFT) (рис. 3.1). Використання саме цього механізму позбавляє систему від випадків невизначеності, пов'язаних із відмовостікістю у асинхронних мережах. Протокол має високу продуктивність, просту та швидку реалізацію для приватних мереж з відомим учасниками та великою кількістю транзакцій. Попередньо відібрані довірені учасники підтримують консенсус, навіть якщо 1/3 з них зазнають невдачі або є зловмисними.

Коли валідатор одержує повідомлення, він повинен прийняти рішення - вірити йому чи ні. Для цього він виконує свої перевірки й після опитує всі інші ноди по черзі, чи дійсна транзакція на їхню думку. Якщо 2/3 учасників

за цю транзакцію, нода її приймає й передає своє рішення в мережу для інших валідаторів. Таким чином, консенсус досягається на основі підтвердження, що буде представлено всіма валідаторами.

PBFT може забезпечити механізм узгодження через спілкування між декількома репліками одного файлу, навіть у випадку ушкодження однієї з них. Позначимо набір реплік як R , $R = \{0 \dots |R| - 1\}$. Для простоти припускаємо, що $R = 3f - 1$, де f - кількість поганих вузлів.

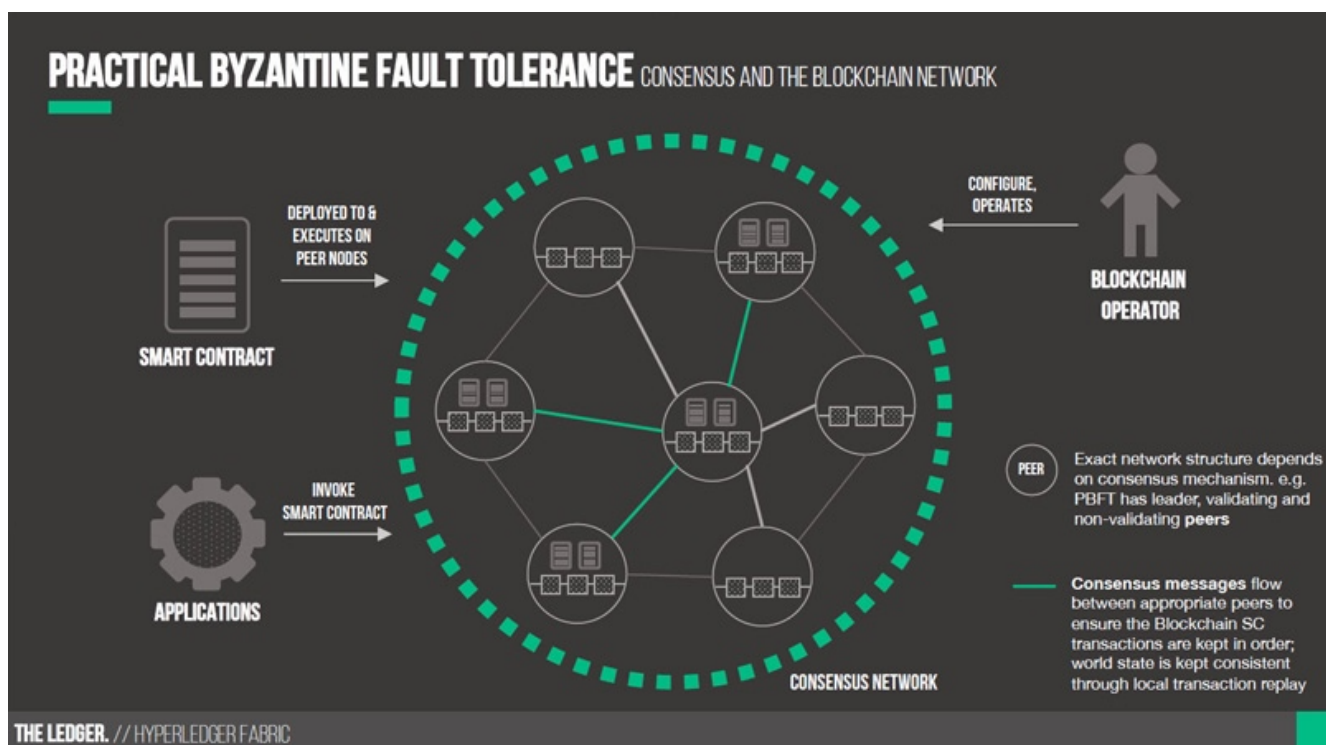


Рис. 3.1. Схема PBFT

Репліки рухаються через послідовність конфігурацій, що називаються представленнями (англ. view). У представленні одна репліка є основною (англ. primary), а інша - резервною. Репліки нумеруються послідовно. Основною частиною репліки є репліка p така, що $p = v \bmod |R|$, де v – номер view (представлення). Функція зміни репліки ChangeView виконується коли основна репліка невдала. Етапи алгоритму:

1. Клієнт відправляє запит, на виклик сервісної операції, до основної репліки.
2. Основна репліка відправляє запити до всіх резервних копій.
3. Репліки виконують запит і надсилають відповідь клієнту.
4. Клієнт чекає відповідей $f + 1$ з різних реплік з однаковим результатом, це результат операції.

Для операції фіксації блоку та досягнення консенсусу вузли в мережі PBFT проходять три фази: попередня підготовка (англ. pre-preparing), підготовка (англ. preparing), фіксація (англ. committing). На рисунку 3.1 зображено дані три фази для 4 вузлів, де вузол під номером 3 є ненадійним.

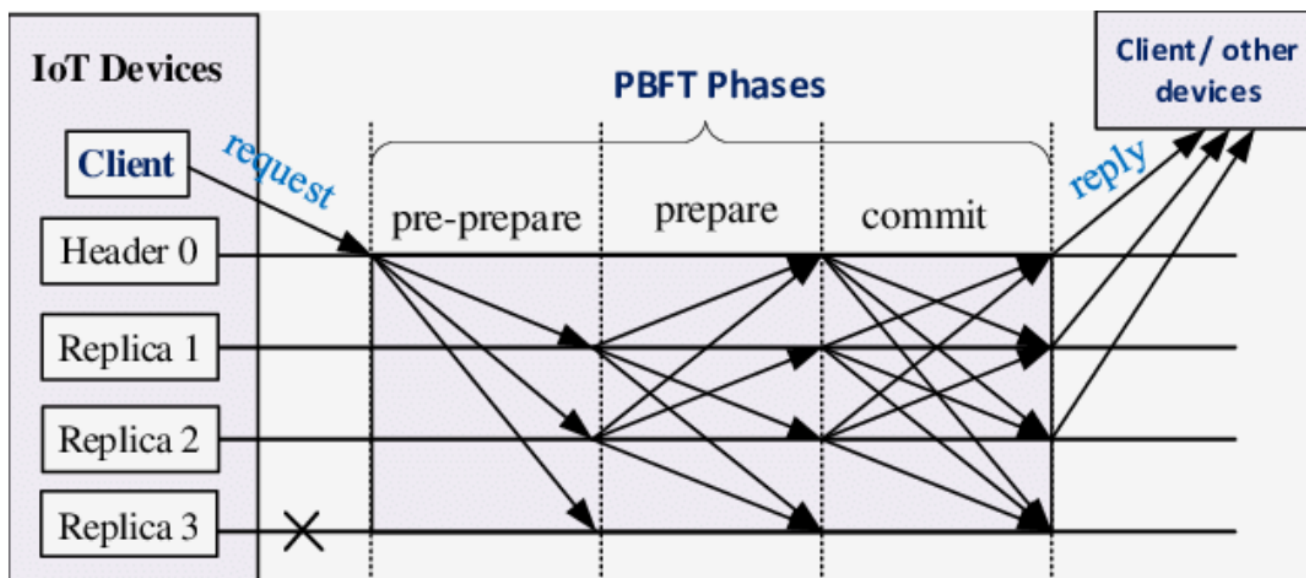


Рис. 3.2. Операції PBFT

Підготовка. Як тільки вузол отримав блок і попередньо підготовлене повідомлення для блоку, і блок, і повідомлення були додані до журналу вузла, вузол перейде до фази підготовки. На етапі підготовки вузол буде транслювати повідомлення про підготовку до решти мережі (включаючи себе). Підготовка повідомлень, як і попередньо підготовлені повідомлення, містить ідентифікатор та

номер блоку, для якого вони є, а також номер i номер перегляду вузла.

Щоб перейти до наступної фази, вузол повинен почекати, поки він не отримає $2f + 1$ підготовлених повідомлень, які мають однаковий ідентифікатор блоку, номер блоку та номер стану з різних вузлів. Дочекавшись $2f + 1$ відповідних підготовлених повідомлень, вузол може бути впевнений, що на цьому етапі всі належним чином функціонуючі вузли (ті, які не є несправними та не шкідливими) узгоджуються. Після того, як вузол прийняв потрібні $2f + 1$ відповідні підготовлені повідомлення та додав їх до свого журналу, він готовий перейти до фази фіксації.

Фіксація. Коли вузол переходить у фазу фіксації, він передає повідомлення про фіксацію всій мережі (включаючи себе). Як і інші типи повідомлень, повідомлення фіксації містять ідентифікатор та номер блоку, для якого вони створені, разом із номером перегляду вузла та ідентифікатором. Як і у фазі підготовки, вузол не може завершити фазу фіксації, поки не отримає $2f + 1$ відповідних повідомлення фіксації з різних вузлів. Знову ж таки, це гарантує, що всі несправні вузли в мережі погодилися зафіксувати цей блок, а це означає, що вузол може безпечно зафіксувати блок, знаючи, що його не потрібно буде повертати. Приймавши необхідні повідомлення $2f + 1$ для фіксації у своєму журналі, вузол може спокійно фіксувати блок.

Після того, як первинний вузол закінчить фазу фіксації та здійснив блок, він запустить весь процес заново, створивши блок, опублікувавши його та транслуючи попередньо підготовлене повідомлення до нього.

Hyperledger Composer Hyperledger Composer побудований на JavaScript, незалежній від платформи мові програмування, яка також підтримує використання вбудованих бібліотек і використовує доступні функції та сценарії, щоб зробити утиліти більш масштабованими та придатними для повторного використання. Визначити структуру моделювання для розгортання логістичної бізнес-мережі можна, використовуючи мову програмування JavaScript.

JavaScript — це текстова мова програмування, яка використовується як на стороні клієнта, так і на стороні сервера, що дозволяє зробити веб-сторінки інтерактивними. Якщо HTML і CSS є мовами, які надають структуру і стиль веб-сторінкам, JavaScript надає веб-сторінкам інтерактивні елементи, які залучають користувача. Включення JavaScript покращує роботу веб-сторінки, перетворюючи її зі статичної сторінки в інтерактивну.

Використовується JavaScript в основному для веб-застосунків і веб-браузерів. Але JavaScript також використовується за межами Інтернету в програмному забезпеченні, серверах та вбудованих апаратних елементах керування. JavaScript дозволяє користувачам взаємодіяти з веб-сторінками. У даному проєкті JavaScript використовується для додавання інтерактивної поведінки на веб-сторінки.

Принципову схема роботи системи наведено на рисунку 3.1.

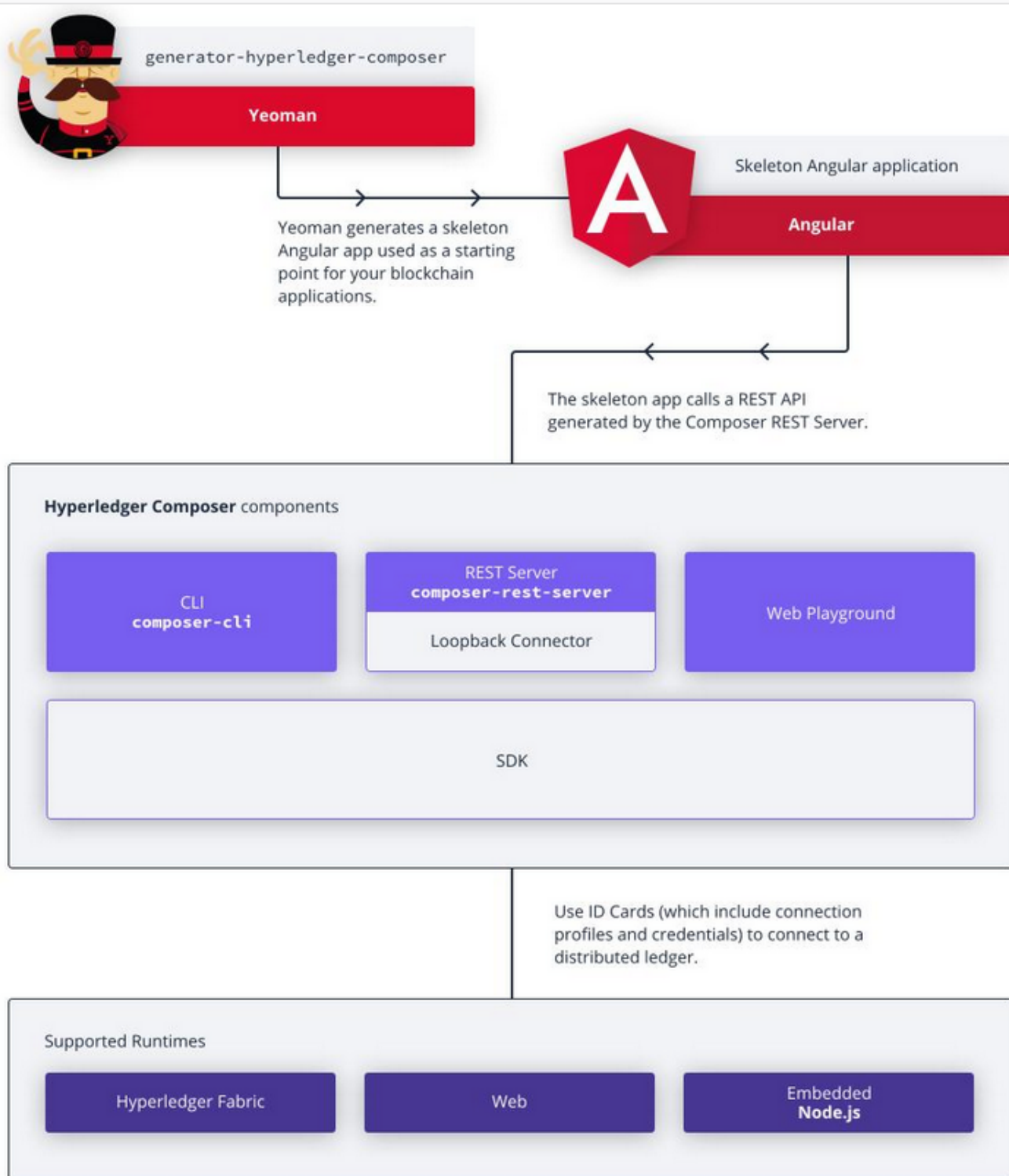


Рис. 3.1. Архітектура системи Hyperledger Composer

Відмінною особливістю Hyperledger Composer є спрощена схема дизайну: усі коди можна написати на JavaScript, створення готових

застосунків можливе прямо із браузера, для інтеграції в систему використовується LoopBack, що дозволяє підключитися до блокченс-истеми миттєво. Структуру взаємодії користувача з Hyperledger Fabric відображено на рисунку 3.2, процес запису в Hyperledger Fabric – на рисунку 3.3.

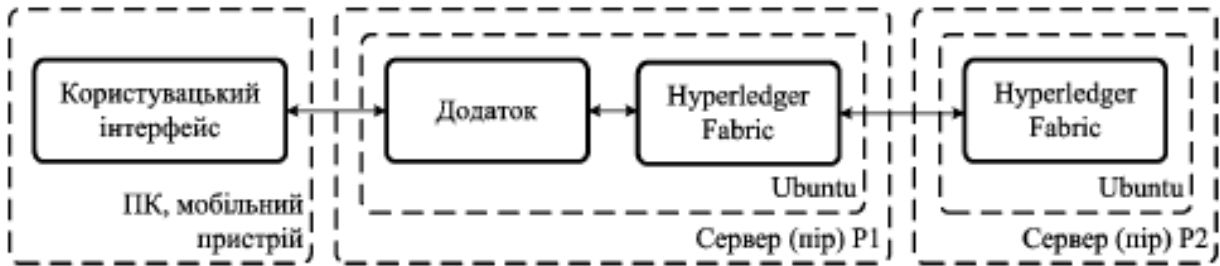


Рис. 3.2. Структура взаємодії користувача з Hyperledger Fabric

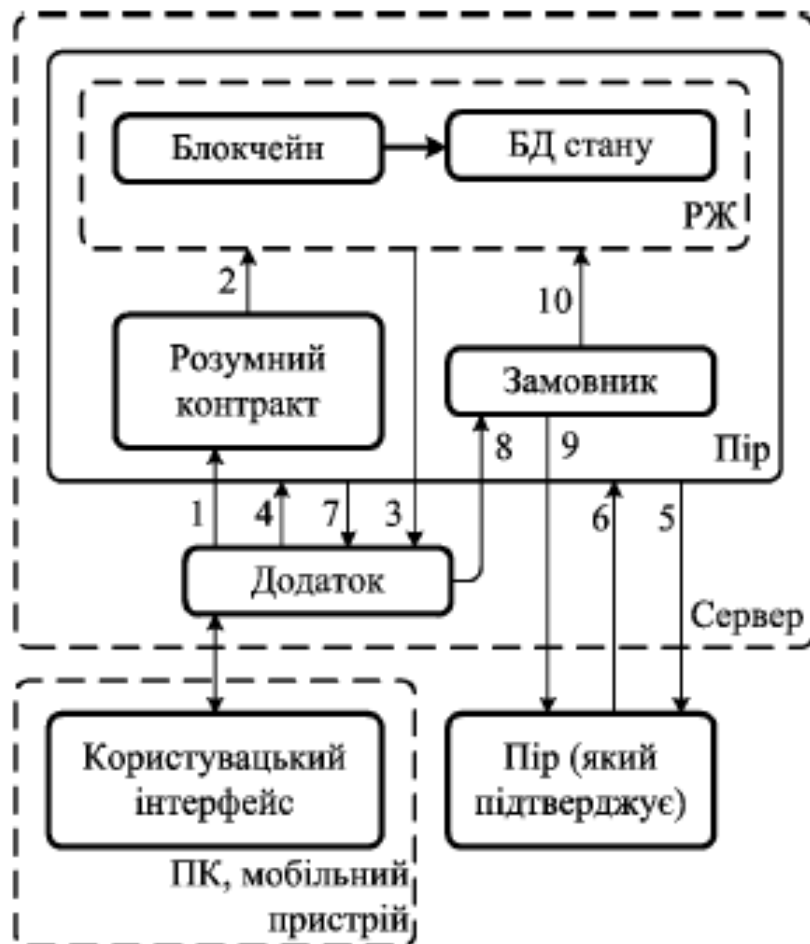


Рис. 3.3. Процес запису в Hyperledger Fabric

Серед інших переваг, які спрощують та прискорюють розроблення блокчейн рішення, є автоматичне створення: REST APIs (Representational State Transfer Application Programming Interface), які надають доступ до блокчейн логіки веб чи мобільним додаткам; скелету веб додатку. Логіку структури взаємодії Hyperledger Composer та Hyperledger Fabric подано на рис. 3.4.

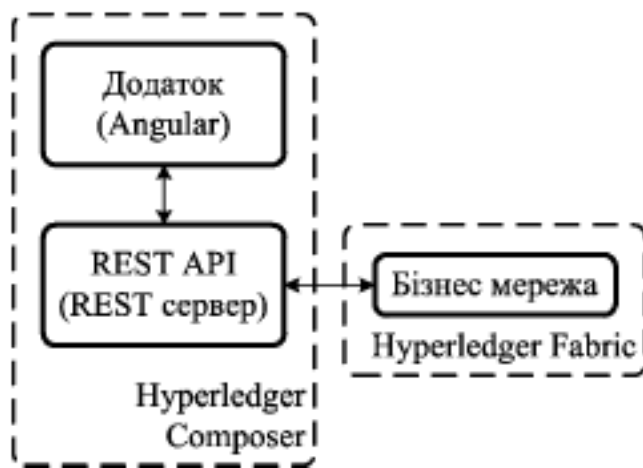


Рис. 3.4. Структура взаємодії Hyperledger Composer та Hyperledger Fabric

3.2. Опис програмної реалізації

Для початку розробки системи управління логістичною діяльністю було використано середовище Visual Studio Code. Для створення проекту в VS Code було створено файл серверної частини config.json (рис. 3.5).

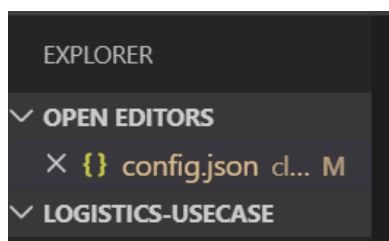


Рис. 3.5. Створення файла проекту config.json

У файлі потрібно вказати сервер який буде використовуватися в подальшому, здійснити необхідні налаштування і зберегти файл. Цей файл конфігурації має бути у форматі JSON. Він містить два розділи: `serverUrl` і `timeRaster`. Фізично проект складається із декількох папок в яких є файли програмного застосунку з вихідним кодом (рис. 3.6). У папці із проектом буде створена структура файлів. Розглянемо їх докладніше.

App.js – програмний файл із підключенням всіх компонентів та стилів, з використанням якої виробляються різні дії над самим проектом.

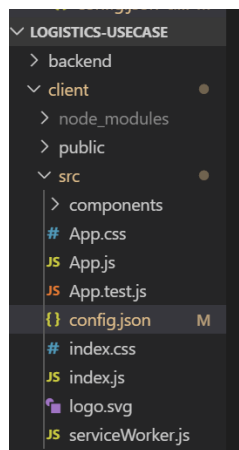


Рис. 3.6. Структура проекту BlockChain

Внутрішня папка *src* – в якій містяться всі некомпільовані файли, що містить компоненти, які відносяться до проекту і задають його конфігурацію (ключові налаштування). У даній папці лежать компоненти в папці *components*, а саме:

Seller – всі налаштування проекту для вкладки *Seller*.

Sidebar – розмітка бокової вкладки де перемикаються екрани в проекті. Завжди компонент відображається з лівого боку сторінки.

Header - модуль з верхньою частиною сайту. Завжди відображається в самому верху застосунку.

По замовчуванню установлений *Composer playground*, який легко налаштовується у проекті, оскільки не потребує окремих бібліотек для її підтримки. Необхідна для установки команда:

```
npm install -g composer-playground@0.20
```

Після установки потрібно запустити Composer playground, для цього використовується команда:

```
composer-playground.
```

Hyperledger Composer - це набір інструментів і сценаріїв на основі Javascript, які можуть спростити створення мережі на основі Blockchain. Використовуючи ці інструменти, ми можемо створити для нашої мережі всю необхідну структуру.

Веб-інтерфейс Composer Playground, який ми використовуємо для моделювання та тестування нашої мережі. Він підходить для простого моделювання, тому що використовує локальне сховище браузера для симуляції ланцюга блоків. Однак, якщо ми запустимо локальне середовище виконання Fabric і розгортанням для неї, ми також зможемо отримати доступ за допомогою Playground. У цьому випадку Playground не моделює сет, він напряму зв'язується з версією Fabric.

Використовуючи Composer REST Server інструмент, який дозволяє нам генерувати REST API-сервери на основі визначення мережі. Додаток може використовувати цей API і дозволить нам інтегруватися в набір додатків, які не є блокчейнами. Запуск застосунка, використовуючи використовуючи Composer REST Server (рис. 3.7).

```
ubuntu@ip-172-31-12-181:~/fabric-dev-servers$ composer-rest-server
? Enter the name of the business network card to use: admin@logistics-network
? Specify if you want namespaces in the generated REST API: never use namespaces
? Specify if you want to use an API key to secure the REST API: No
? Specify if you want to enable authentication for the REST API using Passport: No
? Specify if you want to enable the explorer test interface: Yes
? Specify a key if you want to enable dynamic logging: logistics
? Specify if you want to enable event publication over WebSockets: No
? Specify if you want to enable TLS security for the REST API: No

To restart the REST server using the same options, issue the following command:
  composer-rest-server -c admin@logistics-network -n never -u true -d logistics

Discovering types from business network definition ...
Discovering the Returning Transactions..
Discovered types from business network definition
Generating schemas for all types in business network definition ...
Registering named query: getAllShipmentByStatus
Registering named query: getShipmentsForLogistics
Registering named query: getShipmentsForBuyer
Generated schemas for all types in business network definition
Adding schemas for all types to Loopback ...
Swagger: skipping unknown type "Shipment".
Swagger: skipping unknown type "Shipment".
Swagger: skipping unknown type "Shipment".
Swagger: skipping unknown type "Shipment".
Added schemas for all types to Loopback
Web server listening at: http://localhost:3000
Browse your REST API at http://localhost:3000/explorer
Rest Server dynamic logging is enabled
```

Рис. 3.7. Запуск застосунка

Ця локальна мережа повинна часто запускатися, зупинятися і знищуватися для розробки. Для середовища виконання з більш постійним станом необхідно розвернути мережу за межами середовища розробки. Ми можемо зробити це, запустивши установку в Kubernetes або на хостинговій платформі, як IBM Blockchain. Структура роботи Composer зображена на рис 3.8.

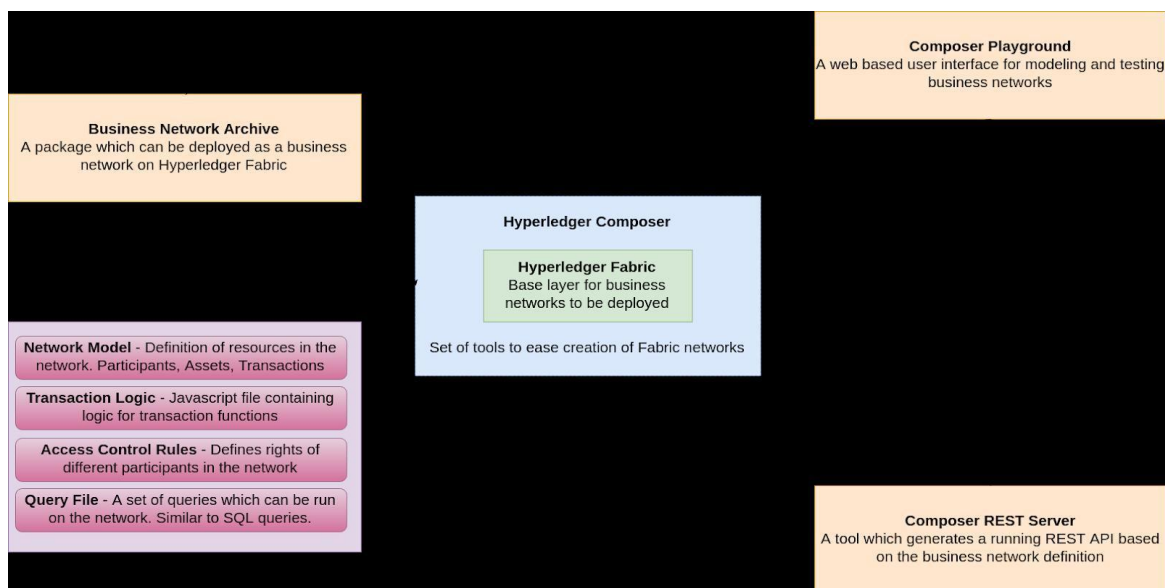


Рис. 3.8. Структура роботи Composer

Yo представляє нам екосистему генератора, де генератор являє собою плагін, який можна запустити за допомогою команди `yo`. Це використовується для налаштування прикладів додатків для різних проектів `generator-hyperledger-composer`. Це генератор `Yo`, який ми будемо використовувати, оскільки він містить специфікації для створення шаблонів мережі.

Hyperledger Composer підтримує присутню інфраструктуру блокчейна Hyperledger Fabric і середу виконання, яка підтримує протоколи консенсуса блокчейна, щоб гарантувати, що транзакції перевіряються в с політикою назначеними учасниками бізнес-мережі.

Застосунок може використовувати дані з бізнес-мережі, передаючи кінцевим користувачам прості і контролюємі точки доступа. Ми використовуємо Hyperledger Composer для бистрого моделювання нашої поточної мережі, яка має дані і транзакції, зв'язані з ними. В рамках моделі нашої мережі ми вибираємо транзакції, які можуть взаємодіяти с активами. Мережі також включають

учасників, котрі взаємодіють з ними, кожен з яких може бути зв'язаний з унікальним ідентифікатором в декількох мережах.

3.3. Інтерфейс застосунку

Опишемо інтерфейс створеного програмного застосунку.

Розроблена система управління логістичною діяльністю складається з одного вікна та трьох вкладок, які міняють стани завдяки перемиканню по вкладкам. Спочатку користувач потрапляє на стрінку реєстрації, де необхідно додати користувачів, та ввести інформацію про нього: нік, пароль та тип користувача для входу у систему (рис. 3.9). Після реєстрації користувачеві пропонують ввести свій обліковий запис (рис. 3.10).

3. CREDENTIALS FOR NETWORK ADMINISTRATOR

You must provide credentials in one of the following formats before you deploy this business network

The credentials will be used to access the business network once it is deployed

Certificates
Required here are certificate and private key files.

ID and Secret
These can be created when accessing a business network.

An Enrollment ID and Secret must be created by someone who already has access to the Business Network you are connecting to.

Enrollment ID: admin

Enrollment Secret: Enter adminpw in enrollment secret

Рис. 3.9. Сторінка реєстрації користувача

Ввійшовши в свій обліковий запис авторизацію користувач потрапляє на головну сторінку застосунку (рис. 3.11).

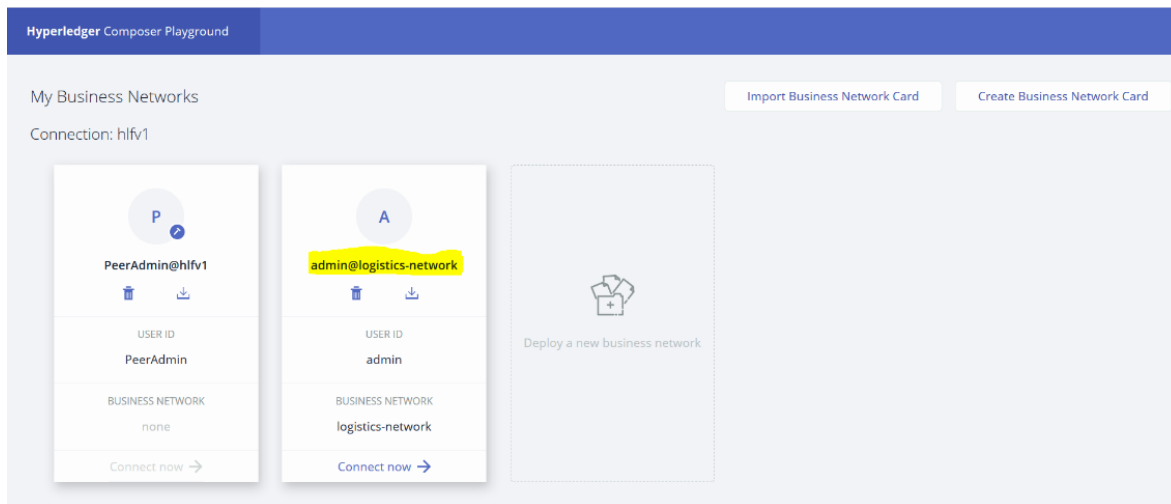


Рис. 3.10. Сторінка вибору облікового запису

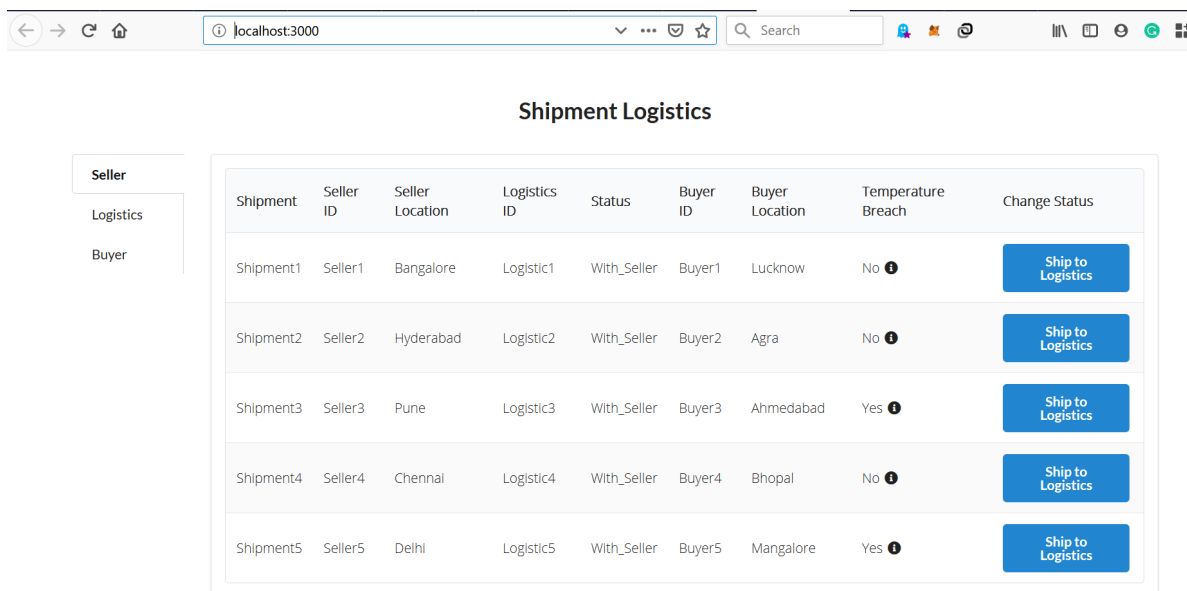


Рис. 3.11. Головна сторінка програмного застосунку

На вкладці зліва обравши пункт *Seller* - продавець, користувач має можливість для перегляду всіх наявних замовлень по доставці, бачити всю інформацію про кожне замовлення (рис. 3.12). При перемиканні на вкладці зліва пункт *Logistics*, користувач переходить до сторінки списку компаній (рис. 3.13). Сторінка містить дані, які відображаються про кожну компанію, а саме: назву, id, статус, локацію.

Shipment Logistics

Seller

Logistics

Buyer

Shipment	Seller ID	Seller Location	Logistics ID	Status	Buyer ID	Buyer Location	Temperature Breach	Change Status
Shipment1	Seller1	Bangalore	Logistic1	In_transit	Buyer1	Lucknow	No ⓘ	Ship to Logistics
Shipment2	Seller2	Hyderabad	Logistic2	With_Seller	Buyer2	Agra	No ⓘ	Ship to Logistics
Shipment3	Seller3	Pune	Logistic3	With_Seller	Buyer3	Ahmedabad	Yes ⓘ	Ship to Logistics
Shipment4	Seller4	Chennai	Logistic4	With_Seller	Buyer4	Bhopal	No ⓘ	Ship to Logistics
Shipment5	Seller5	Delhi	Logistic5	With_Seller	Buyer5	Mangalore	Yes ⓘ	Ship to Logistics

Рис. 3.12. Сторінка доступних замовлень

Shipment Logistics

Seller

Logistics

Buyer

Shipment	Seller Location	Logistics ID	Status	Buyer ID	Buyer Location	Temperature Breach	Change Status
Shipment1	Bangalore	Logistic1	In_transit	Buyer1	Lucknow	No ⓘ	Ship to Buyer

Рис. 3.13. Сторінка списку компаній

На третій вкладці *Buyer* є можливість для адміністратора є можливість змінити статус замовлення (рис. 3.14), та побачити всю інформацію про замовлення.

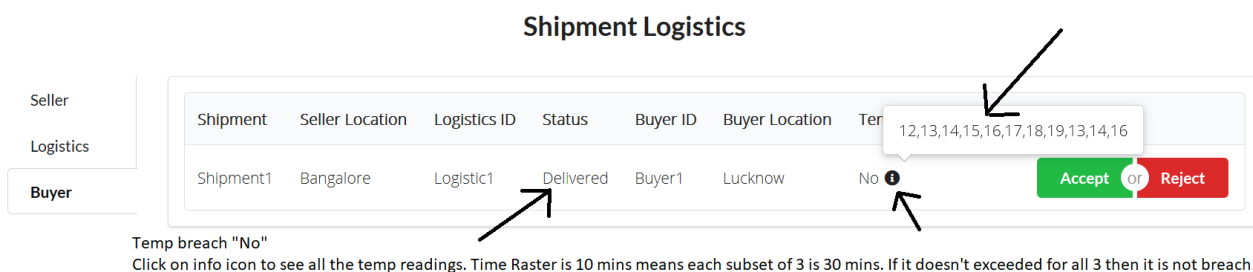


Рис. 3.14. Зміна статусу замовлення

Після перевірки всього замовлення адміністратор натискає кнопку *Accept*, після чого статус зміниться на *Accepted by buyer* – прийнято покупцем (рис. 3.15, 3.16).

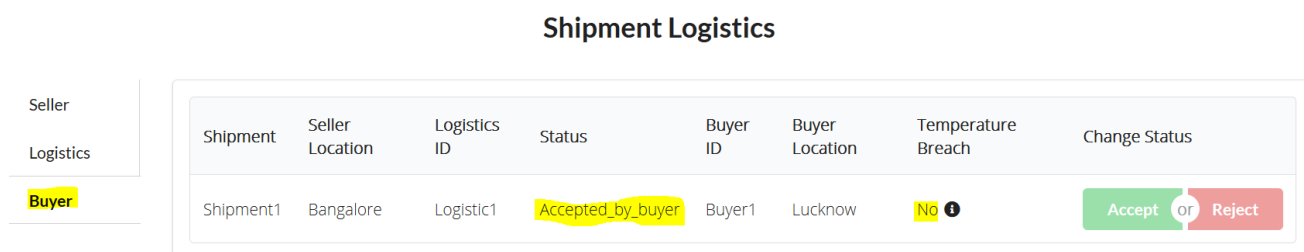


Рис. 3.15. Зміна статусу

Обравши знову пункт *Seller* - продавець, користувач можна побачити зміну інформації про наявні замовлення (рис. 3.16).

Shipment Logistics

Shipment	Seller ID	Seller Location	Logistics ID	Status	Buyer ID	Buyer Location	Temperature Breach	Change Status
Shipment1	Seller1	Bangalore	Logistic1	Accepted_by_buyer	Buyer1	Lucknow	No ⓘ	Ship to Logistics
Shipment2	Seller2	Hyderabad	Logistic2	In_transit	Buyer2	Agra	No ⓘ	Ship to Logistics
Shipment3	Seller3	Pune	Logistic3	Rejected_by_buyer	Buyer3	Ahmedabad	Yes ⓘ	Ship to Logistics
Shipment4	Seller4	Chennai	Logistic4	With_Seller	Buyer4	Bhopal	No ⓘ	Ship to Logistics
Shipment5	Seller5	Delhi	Logistic5	With_Seller	Buyer5	Mangalore	Yes ⓘ	Ship to Logistics

Рис. 3.16. Сторінка перегляду статусу замовлень

Висновок до розділу 3

Для швидкого розгортання корпоративної блокчейн-платформи для управління логістичною діяльністю було вирішено використати проєкт Hyperledger Composer. Hyperledger Composer містить вісім компонентів, які є засобами розробки: 1) Середовище виконання (Hyperledger Fabric, вбудоване середовище, яке виконується безпосередньо всередині процесу Node.js, Web – виконується безпосередньо в Web для демонстрації Playground); 2) REST сервер – генерує Open API або Swagger REST API для бізнес-мережі; 3) Інтерфейс командного рядка допомагає розробникам та адміністраторам управляти мережею; 4) JavaScript SDK – набір різних API-інтерфейсов Node.js, які допомагають розробникам створювати нові додатки, що можуть взаємодіяти й

управляти створеною бізнес-мережею; 5) Плагін редактора VSCode й Atom - розширення редактора VSCode й Atom; 6) Генератор коду Йомена - це фреймворк із відкритим вихідним кодом, що генерує кістяк будь-якого проєкту: js застосунку, Angular веб- застосунку, скелетної бізнес-мережі; 7) Користувальницький веб-інтерфейс Playground Web UP - це веб-інтерфейс користувача для тестування й визначення бізнесів-мереж; 8) Коннектор LoopBack – сервер REST використовує коннектор LoopBack. Відмінною особливістю Hyperledger Composer є спрощена схема дизайну: усі коди можна написати на JavaScript, створення готових застосунків можливе прямо із браузера, для інтеграції в систему використовується LoopBack, що дозволяє підключитися до блокченс-истеми миттєво.

Здійснено розробку, програмну реалізацію та тестування системи управління логістичною діяльністю на основі технології Blockchain яка дозволяє вдосконалити та підвищити ефективність забезпечення прозорості та безпеки товароруху у наскрізному моніторингу фінансових та інформаційних потоків між усіма учасниками ланцюга поставок шляхом використання складної системи шифрування та реалізації довірчих відносин між користувачами з унеможливленням підробки інформації у розподіленій базі даних.

Розроблена система підвищує ефективність процесів закупівель, логістики і платежів, скорочує ручну обробку документації, забезпечує відповідність та доставку товарів і запобігти втратам, що в цілому знижує витрати, покращує безпеку та зводить до мінімуму шахрайство. Додаток на основі блокчейну має потенціал для поліпшення ланцюжків поставок, на яких нині будується торгівля і виробництво, надаючи інфраструктуру для реєстрації, сертифікації і відстеження товарів, що передаються.